CBPL

Commissie voor de bescherming
van de persoonlijke levenssfeer

RICHTSNOEREN MET BETREKKING TOT DE INFORMATIEBEVEILIGING VAN PERSOONSGEGEVENS

December 2014

Versie: 2.0

Opdeling van de normen in:

- deel A – globale beleidsgerelateerde normen en maatregelen
- deel B – specifieke/technische implementatienormen

1 Toepassingsgebied

1.1 Algemeen toepassingsgebied

Het document "Richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens" legt de voor iedere instelling – rechtspersoon, onderneming of administratie – die persoonsgegevens bewaart, gebruikt, verwerkt of meedeelt en waarvoor een voorafgaande machtiging vereist is, na te leven veiligheidsdoeleinden vast. Het streeft de beveiligingscultuur na zoals aanbevolen door de OESO in haar document "Richtlijnen inzake de netwerk- en informatieveiligheid" en is geïnspireerd op de ISO 27002:2013-norm[1], de ISO 27005:2011-norm[2] en de ISO 27018:2014-norm[3]. Het vormt voor de verwerkingen van persoonsgegevens die onderworpen zijn aan een voorafgaande machtiging een verdere uitwerking van de referentiemaatregelen van de Commissie voor de bescherming van de persoonlijke levenssfeer. De "*referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens*" zijn beschikbaar op de website van de Privacycommissie en gelden voor alle verwerkingen van persoonsgegevens.

De implementatie en de verificatie van deze beveiligingsrichtsnoeren bij derden die voor rekening van een instelling persoonsgegevens verwerken, behoren in eerste instantie tot de verantwoordelijkheid van de instelling die aan die derde werkzaamheden toevertrouwt.

De *wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna Privacywet) bepaalt heel nauwkeurig de voorwaarden en de omstandigheden voor een verwerking of een doorgifte van persoonsgegevens. De uitvoering van bepaalde verwerkingen, gelet op het delicate karakter van de gegevens, is echter niet mogelijk zonder een voorafgaande machtiging van het bevoegde sectorale comité van de Commissie voor de bescherming van de persoonlijke levenssfeer. Iedere instelling die een aanvraag tot machtiging indient, moet beschikken over een beveiligingsbeleid dat gestoeld is op

[1] Code of practice for information security controls.
[2] Information security risk management.
[3] Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

deze richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens en moet in voorkomend geval een consulent inzake informatiebeveiliging (hierna veiligheidsconsulent) aanstellen.

1.2 Bijzondere toepassingsgebieden

Voor instellingen van de sociale zekerheid en instellingen die gebruik maken van de federale dienstenintegrator zijn onderhavige richtsnoeren van toepassing op informatiebeveiliging in de ruime betekenis zoals gedefinieerd in het koninklijk besluit van 17 maart 2013 betreffende de veiligheidsadviseurs ingevoerd door de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator: "Strategie, regels, procedures en middelen voor het beschermen van alle soorten informatie zowel in de transmissiesystemen als in de verwerkingssystemen om de vertrouwelijkheid, de beschikbaarheid, de integriteit, de betrouwbaarheid, de authenticiteit en de onweerlegbaarheid ervan te garanderen". Deze definitie betreft m.a.w. niet enkel persoonsgegevens, maar alle gegevens.

Instellingen van de sociale zekerheid zijn bovendien, overeenkomstig artikel 2, eerste lid, 2° van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid, verplicht de minimale normen, zoals bepaald door de Kruispuntbank van de Sociale Zekerheid, na te leven.

2 Enkele definities

Wat is informatiebeveiliging?

Informatiebeveiliging is het geheel aan beheersmaatregelen die er voor zorgen dat de vertrouwelijkheid, de integriteit en de beschikbaarheid van alle vormen van informatie – zowel elektronische, digitale als papieren vorm – behouden blijven, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van informatiebeveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.
Onder de term "beheersmaatregel" dienen alle maatregelen verstaan te worden met betrekking tot het beleid, procedures, richtlijnen, werkwijzen en organisatiestructuren. Deze maatregelen kunnen zowel administratief, technisch, beheersmatig als juridisch van aard zijn.

Veiligheidsconsulent

Binnen de Commissie voor de bescherming van de persoonlijke levenssfeer zijn sectorale comités ingesteld. Ze zijn samengesteld uit leden van de Commissie en uit deskundigen die specifiek vertrouwd zijn met de sector waarvoor het Comité bevoegd is. Op dit ogenblik zijn er vijf sectorale comités. Om bepaalde persoonsgegevens te mogen verwerken is een machtiging vereist van één of meerdere van deze sectorale comités. In het kader van deze machtigingsprocedures dient de aanstelling van een veiligheidsconsulent soms te worden gemeld aan en/of bekrachtigd door het bevoegde sectorale comité.

De veiligheidsconsulent is de initiatiefnemer en de drijvende kracht achter het informatiebeveiligingsbeleid. Hij is het die beveiligingsvoorstellen doet, bepaalt welke doelen er moeten bereikt worden, de verschillende personen aanstuurt die het beveiligingssysteem installeren, …. Hij onderzoekt en bestudeert informatiebeveiligingsincidenten en stelt beheersmaatregelen voor. Hij rapporteert rechtstreeks aan de directie of het hoogste beslissingsorgaan.

Op de website van de Commissie voor de bescherming van de persoonlijke levenssfeer worden nog meer termen toegelicht in het lexicon (zie http://www.privacycommission.be/nl/lexicon).

3 Interpretatie van de richtsnoeren

3.1 Controle op naleving van de richtsnoeren voor de informatiebeveiliging

De Commissie voor de bescherming van de persoonlijke levenssfeer, de Vlaamse Toezichtcommissie, de Brusselse Controlecommissie, la Commission Wallonie-Bruxelles de contrôle des échanges de données en/of elk ter zake bevoegd sectoraal comité kunnen controles uitvoeren of door een externe instantie laten uitvoeren op de naleving van specifieke aspecten van de beveiligingsrichtsnoeren. De richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens moeten worden toegepast in het kader van machtigingen verleend door elk van de sectorale comités ingesteld bij de Commissie voor de bescherming van de persoonlijke levenssfeer.

3.2 Interpretatie en herziening van de beveiligingsrichtsnoeren

De beveiligingsrichtsnoeren normen zijn opgesplitst in een deel A waarin de globale beleidsgerelateerde normen en maatregelen worden opgenomen en een deel B bestaande uit de specifieke/technische implementatienormen.

De instellingen dragen de verantwoordelijkheid om in functie van hun specifieke situatie en al naargelang de belangrijkheid van de te beveiligen werkingsmiddelen, de meest aanwezen beveiligingsmiddelen te implementeren.

Tot slot dient worden opgemerkt dat deze beveiligingsrichtsnoeren voor herziening vatbaar zijn. Ze zullen aldus worden aangepast in functie van de evolutie die zich wettelijk, technisch, inzonderheid inzake veiligheidsrisico's, of op ander vlak, inzonderheid de ISO-normeringen, voordoet.

4 Beoogde doelstellingen

De richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens vormen een leidraad die toelaat om een gedocumenteerd Information Security Management System (hierna ISMS) vast te stellen en te beheren, d.w.z. vaststellen, uitvoeren, controleren, beoordelen, bijhouden en verbeteren binnen het kader van de bedrijfsactiviteiten en –risico's in verband met de verwerking van persoonsgegevens van de instelling. Het ISMS moet gebaseerd zijn op de kwaliteitscirkel van Deming die bestaat uit vier cyclische activiteiten: PLAN (= kijk naar de huidige werking en ontwerp een plan voor de verbetering van de werking, stel hierbij steeds doelstellingen vast), DO (= voer de geplande verbetering uit), CHECK (= meet het resultaat van de verbetering en toets deze aan de vooropgestelde doelstellingen), ACT (= bijstellen aan de hand van de gevonden resultaten in Check). Daarbij moet de directie of het hoogste beslissingsorgaan het bewijs kunnen leveren van haar betrokkenheid met betrekking tot het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van het ISMS. De doeltreffendheid van het ISMS moet continu verbeterd worden door gebruikmaking van het informatiebeveiligingsbeleid, de informatiebeveiligingsdoelstellingen, auditresultaten, analyse van gecontroleerde gebeurtenissen, corrigerende en preventieve maatregelen en de directiebeoordeling of beoordeling van het hoogste beslissingsorgaan.

Deze beveiligingsrichtsnoeren zijn voor de verwerkingen van persoonsgegevens die onderworpen zijn aan een voorafgaande machtiging een precisering van de algemene referentiemaatregelen die de Commissie voor de bescherming van de persoonlijke levenssfeer heeft uitgevaardigd ten opzichte van allen die persoonsgegevens verwerken.

5 Richtsnoeren – structuur

De richtsnoeren met betrekking tot de informatiebeveiliging van de persoonsgegevens schrijven zich in in de doelstellingen en principes van de OESO richtlijnen inzake netwerk- en informatieveiligheid. Ze zijn geïnspireerd op de ISO 27002:2013-norm (zie o.a. http://www.iso27001security.com/html/27002.html), de ISO 27005:2011-norm en de ISO 27018:2014-norm.

Onderhavige richtsnoeren zijn opgedeeld in 15 hoofdstukken. Elk hoofdstuk behandelt een bepaald aspect van informatiebeveiliging waarbij elk punt specifiek gericht is op informatiebeveiliging bij het gebruik en de verwerking van persoonsgegevens.

Er is een onderscheid gemaakt tussen enerzijds de globale normen en anderzijds de technische invulling van deze globale normen. De basisconcepten of de globale beleidsgerelateerde normen en maatregelen zijn opgenomen in deel A, de wijze van technische implementatie van informatiebeveiliging is opgenomen in deel B.

DEEL A – GLOBALE BELEIDSGERELATEERDE NORMEN EN MAATREGELEN

1 RISICO ***(zie ISO 27005 – Risicomanagement voor informatiebeveiliging)***	
1.1 BEOORDELEN VAN BEVEILIGINGSRISICO'S ***(zie ISO 27005 – 8 Beoordelen van beveiligingsrisico's)***	
A-1.1.1	De beveiligingsrisico's en -behoeften rond uw informatie die eigen zijn aan uw organisatie en die het gebruik en de verwerking van persoonsgegevens betreffen moeten, na identificatie en analyse, regelmatig geëvalueerd worden in samenspraak met het hoogste beslissingsorgaan van uw organisatie.
1.2 BEHANDELEN VAN BEVEILIGINGSRISICO'S ***(zie ISO 27005 – 9 Behandelen van beveiligingsrisico's)***	
A-1.2.1	Voor elk relevant risico omtrent het gebruik en de verwerking van persoonsgegevens vastgesteld na de informatierisicobeoordeling moeten de nodige beheersmaatregelen genomen en opgevolgd worden.

2 BELEID ***(zie ISO 27002 – 5 Informatiebeveiligingsbeleid)***	
2.1 INFORMATIEBEVEILIGINGSBELEID ***(zie ISO 27002 – 5.1 Aansturing van de directie inzake informatiebeveiliging)***	
A-2.1.1	Uw organisatie moet over een formeel, geactualiseerd en door het hoogste beslissingsorgaan van uw organisatie goedgekeurd informatiebeveiligingsbeleid ("*information security policy*") beschikken dat op regelmatige basis naar alle relevante partijen gecommuniceerd wordt.
A-2.1.2	Er moet een duidelijke ondersteuning zijn van het hoogste beslissingsorgaan van uw organisatie om de implementatie van informatiebeveiliging in uw organisatie op te starten, te beheersen, te onderhouden en waar nodig bij te sturen. Voorbeelden van documenten m.b.t. informatiebeveiliging zijn: - een jaarverslag inzake informatiebeveiliging;

	- een meerjarenplan inzake informatiebeveiliging.

3 ORGANISATIE ***(zie ISO 27002 – 6 Organisatie van informatiebeveiliging)***	
3.1 INTERNE ORGANISATIE ROND INFORMATIEBEVEILIGING ***(zie ISO 27002 – 6.1 Interne organisatie)***	
A-3.1.1	Uw organisatie moet de nodige werkkredieten en middelen ter beschikking stellen teneinde te kunnen voorzien in de correcte coördinatie en uitvoering van het informatiebeveiligingsbeleid. De uitvoering van het beveiligingsbeleid moet opgevolgd worden door de informatiebeveiligingscel geleid door een veiligheidsconsulent. Deze taken kunnen ook aan een extern erkende gespecialiseerde dienst toevertrouwd worden. De informatiebeveiligingscel heeft een adviserende, stimulerende, documenterende en controlerende opdracht binnen uw organisatie. Daartoe moet de veiligheidsconsulent instaan voor: - het verstrekken van deskundige adviezen aan de persoon belast met het dagelijks bestuur en verantwoordelijk voor de gegevensverwerking; - het uitvoeren van opdrachten die hem door de persoon belast met het dagelijks bestuur en verantwoordelijk voor de gegevensverwerking worden toevertrouwd.
A-3.1.2	De veiligheidsconsulent moet steeds over de nodige competenties en informatie beschikken om zijn taak correct en tijdig uit te voeren.
A-3.1.3	Uw organisatie moet over een actief beslissingsplatform beschikken dat op regelmatige basis samenkomt voor de validatie en de goedkeuring van de beheersmaatregelen voor informatiebeveiliging voorgesteld door de informatiebeveiligingscel.
A-3.1.4	Uw organisatie moet, ongeacht het soort project, informatiebeveiliging steeds integreren in de projectbeheermethode(n) teneinde informatiebeveiligingsrisico's te identificeren en aan te pakken.

3.2 Mobiel werken ***(zie ISO 27002 – 6.2 Mobiele apparatuur en telewerken)***	
A-3.2.1	Uw organisatie moet beschikken over een formeel beleid inzake mobiel gebruik van apparatuur waarbij rekening wordt gehouden met de risico's van het werken in onbeschermde omgevingen. Medewerkers die mobiele apparatuur gebruiken, moeten getraind worden zodat ze zich (1) bewust worden van de extra risico's die deze manier van werken met zich meebrengt en (2) weten welke beheersmaatregelen dienen getroffen te worden.
A-3.2.2	Organisaties die telewerken toestaan, behoren een beleid uit te vaardigen dat de voorwaarden en beperkingen definieert voor het telewerken.

4 PERSONEELSBELEID ***(zie ISO 27002 – 7 Veilig personeelsbeleid)***	
4.1 INFORMATIEBEVEILIGING VOORAFGAAND AAN HET DIENSTVERBAND ***(zie ISO 27002 – 7.1 Voorafgaand aan het dienstverband)***	
A-4.1.1	Uw organisatie dient duidelijk het belang van informatiebeveiliging tijdens het rekruteringsproces aan te duiden aan de potentiële kandidaten.
A-4.1.2	Alle kandidaten dienen hun arbeidsovereenkomst te ondertekenen waarin ook clausules staan omtrent hun verantwoordelijkheden voor de informatiebeveiliging van persoonsgegevens.
4.2 INFORMATIEBEVEILIGING TIJDENS HET DIENSTVERBAND ***(zie ISO 27002 – 7.2 Tijdens het dienstverband)***	
A-4.2.1	Opdat gegarandeerd zou worden dat alle interne medewerkers zich engageren om hun verplichtingen tot de vertrouwelijkheid en de veiligheid van persoonsgegevens te respecteren moet uw organisatie alle interne medewerkers die betrokken zijn bij het gebruik en de verwerking van de persoonsgegevens op de hoogte stellen van de vertrouwelijkheids- en beveiligingsverplichtingen onder de vorm van: - een gedragscode; - en/of vermelding van deze gedragscode in het arbeidsreglement; - en/of een functiebeschrijving met vermelding van de vertrouwelijkheids- en beveiligingsverplichtingen; - en/of contractuele bepalingen; - en daarnaast onder de vorm van geschikte bewustzijnsopleiding en -training en regelmatige bijscholing.

A-4.2.2	Uw organisatie moet alle externe medewerkers (ingehuurd personeel en externe gebruikers) belast met het gebruik en/of de verwerking van de persoonsgegevens op de hoogte stellen van de vertrouwelijkheids- en beveiligingsverplichtingen door een gedragscode en het ondertekenen van een contractueel document met duidelijke contractuele bepalingen.
A-4.2.3	Uw organisatie moet over een formele en gecommuniceerde disciplinaire procedure beschikken om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.
4.3 INFORMATIEBEVEILIGING BIJ BEEINDIGING OF WIJZIGING VAN DIENSTVERBAND ***(zie ISO 27002 – 7.3 Beëindiging en wijziging van dienstverband)***	
A-4.3.1	Uw organisatie moet de verantwoordelijkheden en taken m.b.t. informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband definiëren, communiceren naar de interne of externe medewerker en ten uitvoer brengen.

5 BEDRIJFSMIDDELEN ***(zie ISO 27002 – 8 Beheer van bedrijfsmiddelen)***	
5.1 CLASSIFICATIE VAN INFORMATIE ***(zie ISO 27002 – 8.2 Informatieclassificatie)***	
A-5.1.1	Bij de persoonsgegevensverwerkingen moet uw organisatie een duidelijk onderscheid maken tussen de volgende gegevenstypes: - anonieme gegevens: dit zijn gegevens die niet in verband kunnen gebracht worden met een geïdentificeerde of identificeerbare persoon en zijn dus geen persoonsgegevens; - persoonsgegevens: een persoonsgegeven is iedere informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon. - gevoelige persoonsgegevens: het gaat om gegevens over ras, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuigingen, lidmaatschap van een vakvereniging, gezondheid, seksuele leven, verdenkingen, vervolgingen, strafrechtelijke of bestuurlijke veroordelingen. Het is in principe verboden om dergelijke gegevens te verwerken; - gecodeerde al dan niet gevoelige persoonsgegevens: dit zijn persoonsgegevens die slechts door middel van een code in verband kunnen gebracht worden met een geïdentificeerde of identificeerbare persoon.
A-5.1.2	Alle gebruikers die persoonsgegevens gebruiken/verwerken moeten op de hoogte zijn van dit onderscheid.

5.2 BEHANDELEN VAN MEDIA ***(zie ISO 27002 – 8.3 Behandelen van media)***	
A-5.2.1	Uw organisatie dient procedures te hebben voor het beheer van verwijderbare media waarop persoonsgegevens worden opgeslagen en die de beveiligingsperimeter van uw organisatie kunnen verlaten. Denk hierbij ook aan de verwijderbare media in apparatuur zoals multifunctionele printers en copiers.
A-5.2.2	Uw organisatie moet de nodige maatregelen bepalen om fysieke media (inclusief papieren documenten) die persoonsgegevens bevatten tijdens het transport te beschermen tegen onbevoegde toegang, misbruik of corruptie.

6 TOEGANG TOT PERSOONSGEGEVENS ***(zie ISO 27002 – 9 Toegangsbeveiliging)***	
6.1 EISEN VOOR TOEGANGSBEVEILIGING ***(zie ISO 27002 – 9.1 Bedrijfseisen voor toegangsbeveiliging)***	
A-6.1.1	Uw organisatie moet een goedgekeurd en geactualiseerd toegangsbeveiligingsbeleid hebben met betrekking tot het toekennen, veranderen en verwijderen van toegangsrechten tot toepassingen en systemen die persoonsgegevens gebruiken/verwerken. Dit beleid moet vastgesteld, gedocumenteerd en beoordeeld zijn op basis van de classificatie van de persoonsgegevens.
A-6.1.2	Met betrekking tot netwerken of netwerkdiensten moet uw organisatie de gepaste beveiligingsmaatregelen bepalen opdat iedere persoon slechts toegang zou hebben tot de persoonsgegevens waarvoor hij uitdrukkelijk een autorisatie heeft verkregen.
6.2 VERANTWOORDELIJKE VOOR TOEGANGSRECHTEN VAN GEBRUIKERS ***(zie ISO 27002 – 9.2 Beheer van toegangsrechten van gebruikers)***	
A-6.2.1	Uw organisatie moet een verantwoordelijke aanstellen die belast wordt met het beheer van alle aanvragen m.b.t. de toegang tot persoonsgegevens. Deze verantwoordelijke moet verschillend zijn van de persoon die de toegangsrechten op technisch niveau in de systemen toekent, aanpast of verwijdert.

6.3 VERANTWOORDELIJKHEDEN VAN GEBRUIKERS ***(zie ISO 27002 – 9.3 Verantwoordelijkheden van gebruikers)***	
A-6.3.1	De gebruikers moeten worden ingelicht over hun verantwoordelijkheid in een doeltreffende toegangsbeveiliging, onder meer inzake het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur waarop persoonsgegevens gebruikt/verwerkt worden.
6.4 TOEGANGSBEVEILIGING VAN SYSTEMEN EN TOEPASSINGEN ***(zie ISO 27002 – 9.4 Toegangsbeveiliging van systemen en toepassingen)***	
A-6.4.1	Uw organisatie moet de gepaste beveiligingsmaatregelen bepalen om de toegang tot persoonsgegevens te beperken.
A-6.4.2	Uw organisatie moet de toegang beperken voor informatiebeheerders (systeembeheerders, ook wel "superusers" genoemd) tot systemen en toepassingen waarop persoonsgegevens gebruikt/verwerkt worden.

7 CRYPTOGRAFIE ***(zie ISO 27002 – 10 Cryptografie)***	
7.1 CRYPTOGRAFISCHE BEHEERSMAATREGELEN ***(zie ISO 27002 – 10.1 Cryptografische beheersmaatregelen)***	
A-7.1.1	Afhankelijk van de resultaten van de risicobeoordeling moet uw organisatie een beleid ontwikkelen voor een correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van persoonsgegevens te beschermen.
A-7.1.2	Uw organisatie moet een beleid ontwikkelen voor het gebruik, de bescherming en de levensduur van cryptografische sleutels tijdens hun gehele levenscyclus.

8 FYSIEKE BEVEILIGING ***(zie ISO 27002 – 11 Fysieke beveiliging en beveiliging van de omgeving)***	
8.1 BEVEILIGING VAN DE OMGEVING ***(zie ISO 27002 – 11.1 Beveiligde gebieden)***	
A-8.1.1	Op basis van de resultaten van de risicobeoordeling moeten beveiligde zones en de gepaste toegangsbeveiligingen bepaald worden om alle ruimten te beveiligen waarin zich informatie en informatieverwerkende faciliteiten met persoonsgegevens bevinden.
A-8.1.2	Uw organisatie moet de nodige maatregelen bepalen met betrekking tot de beveiligde zones om elke vorm van schade te vermijden die de persoonsgegevens in gevaar kunnen brengen.
8.2 BEVEILIGDE APPARATUUR ***(zie ISO 27002 – 11.2 Apparatuur)***	
A-8.2.1	Uw organisatie behoort op basis van de risicobeoordeling de gepaste beheersmaatregelen te bepalen betreffende de apparatuur, de bekabeling en de ondersteunende voorzieningen om verlies, schade, diefstal en het ongewenst veranderen van persoonsgegevens te voorkomen. Hierbij dient bijzondere aandacht te worden besteed aan apparatuur die zich buiten het terrein van de organisatie bevindt of wordt gebruikt.
A-8.2.2	Uw organisatie moet een specifieke procedure uitwerken voor het verwijderen of hergebruiken van alle apparatuur met opslagmedia waarop persoonsgegevens worden gebruikt/verwerkt.

9 OPERATIONELE BEVEILIGING ***(zie ISO 27002 – 12 Beveiliging van bedrijfsactiviteiten)***	
9.1 OPERATIONELE PROCEDURES EN VERANTWOORDELIJKHEDEN OMTRENT INFORMATIEBEVEILIGING ***(zie ISO 27002 – 12.1 Bedieningsprocedures en verantwoordelijkheden)***	
A-9.1.1	Uw organisatie moet de nodige procedures en verantwoordelijkheden bepalen bij veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging van persoonsgegevens.
A-9.1.2	Uw organisatie moet voorzien in een functiescheiding om te voorkomen dat één enkele persoon de exclusieve controle zou verwerven over een verwerking van persoonsgegevens.

9.2 BESCHERMING TEGEN MALWARE ***(zie ISO 27002 – 12.2 Bescherming tegen malware)***	
A-9.2.1	Uw organisatie moet beschikken over geschikte procedures en richtlijnen ter bescherming tegen malware en om het bewustzijn van de systeem- en de eindgebruikers te vergroten. Enkele voorbeelden van mogelijke richtlijnen en procedures zijn: • gebruik van ongeautoriseerde programmatuur verbieden; • beleid bepalen inzake het ontvangen van bestanden en programmatuur vanuit of via externe netwerken of via enig ander medium; • vastleggen van de verantwoordelijkheden inzake de bescherming tegen malware.
9.3 BACK-UP ***(zie ISO 27002 – 12.3 Back-up)***	
A-9.3.1	Uw organisatie dient een geschikt back-up beleid op te stellen en op te volgen om een adequaat herstel te waarborgen na verlies, schade, diefstal of het ongewenst veranderen van persoonsgegevens.

10 COMMUNICATIEBEVEILIGING ***(zie ISO 27002 – 13 Communicatiebeveiliging)***	
10.1 NETWERKBEVEILIGING ***(zie ISO 27002 – 13.1 Beheer van netwerkbeveiliging)***	
A-10.1.1	Netwerkbeveiliging moet een onderdeel vormen van uw globaal informatiebeveiligingsplan waarbij bijzondere aandacht moet besteed worden aan de informatiestromen waarbij persoonsgegevens uw organisatie kunnen verlaten.
10.2 INFORMATIETRANSPORT ***(zie ISO 27002 – 13.2 Informatietransport)***	
A-10.2.1	Uw organisatie moet over een formeel, geactualiseerd en door het hoogste beslissingsorgaan van uw organisatie goedgekeurd beleid beschikken inzake communicatiemiddelen (zoals e-mail, internet, video, fax en telefoon) dat op regelmatige basis naar alle relevante partijen gecommuniceerd wordt en waarin bijzondere aandacht wordt gegeven aan het gebruik van persoonsgegevens. Wij verwijzen hierbij ook naar aanbeveling nr. 8/2012 van de Privacycommissie betreffende de controle door de werkgever op het gebruik van elektronische communicatie-instrumenten op de werkvloer.

A-10.2.2	Uw organisatie moet de eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van uw organisatie betreffende het beschermen van persoonsgegevens weerspiegelen, vastleggen, regelmatig beoordelen en documenteren.

11 AANSCHAFFEN, ONTWIKKELEN EN ONDERHOUDEN VAN INFORMATIESYSTEMEN ***(zie ISO 27002 – 14 Verwerving, ontwikkeling en onderhoud van informatiesystemen)***	
11.1 BEVEILIGINGSEISEN VOOR INFORMATIESYSTEMEN ***(zie ISO 27002 – 14.1 Beveiligingseisen voor informatiesystemen)***	
A-11.1.1	Uw organisatie dient erover te waken dat de beveiligingsvereisten voor de persoonsgegevens onverminderd gegarandeerd blijven bij de aanschaf of ontwikkeling van nieuwe informatiesystemen of bij uitbreidingen van bestaande informatiesystemen. Onder informatiesystemen worden toepassingen, diensten, IT-middelen of andere informatieverwerkende onderdelen verstaan.
11.2 BEVEILIGING IN ONTWIKKELINGS- EN ONDERSTEUNINGSPROCESSEN ***(zie ISO 27002 – 14.2 Beveiliging in ontwikkelings- en ondersteuningsprocessen)***	
A-11.2.1	Uw organisatie moet over procedures beschikken voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen zodat door de projectverantwoordelijke rekening wordt gehouden met de noodzakelijke beveiligingsvereisten met betrekking tot de bescherming van persoonsgegevens.
A-11.2.2	Uw organisatie moet duidelijke formele wijzigingsprocedures toepassen zodat de kans op onterechte wijzigingen of het lekken van persoonsgegevens tot een minimum beperkt wordt.

12 LEVERANCIERSRELATIES ***(zie ISO 27002 – 15 Leveranciersrelaties)***	
12.1 INFORMATIEBEVEILIGING IN LEVERANCIERSRELATIES ***(zie ISO 27002 – 15.1 Informatiebeveiliging in leveranciersrelaties)***	
A-12.1.1	In geval van samenwerking met leveranciers dient uw organisatie zich ervan te vergewissen dat de leverancier voldoende waarborgen biedt m.b.t. de informatiebeveiliging van persoonsgegevens en dat de verplichtingen inzake het gebruik en de verwerking van persoonsgegevens contractueel zijn vastgelegd (cfr. Privacywet Art.16 §1).

A-12.1.2	In het geval uw organisatie voor de opslag, het gebruik en/of de verwerking van persoonsgegevens overweegt gebruik te maken van de diensten van een cloudprovider dient uw organisatie een risicobeoordeling uit te voeren met betrekking tot de overeenstemming inzake de voorgestelde informatiebeveiliging en onderhavige richtsnoeren, en de contractuele voorwaarden (inzonderheid een eventuele toegang tot de persoonsgegevens door derden en minimale contractuele garanties met betrekking tot bijvoorbeeld auditregels, de continuïteit en kwaliteit van de dienstverlening, interoperabiliteit en omkeerbaarheid/overdraagbaarheid).

13 INFORMATIEBEVEILIGINGSINCIDENTEN ***(zie ISO 27002 – 16 Beheer van informatiebeveiligingsincidenten)***	
13.1 BEHEER VAN INFORMATIEBEVEILIGINGSINCIDENTEN EN –VERBETERINGEN ***(zie ISO 27002 – 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen)***	
A-13.1.1	De verantwoordelijkheden en de procedures moeten vastgelegd worden inzake de detectie en de behandeling van informatiebeveiligingsincidenten en zwakke plekken rond persoonsgegevens die gerapporteerd worden.
A-13.1.2	Uw organisatie moet er voor zorgen dat de informatiebeveiligingscel/verantwoordelijke voor de verwerking steeds direct op de hoogte gesteld wordt van gebeurtenissen en incidenten die de informatiebeveiliging van persoonsgegevens in het gedrang kunnen brengen of gebracht hebben.
A-13.1.3	Uw organisatie moet er voor zorgen dat de informatiebeveiligingscel/verantwoordelijke voor de verwerking steeds direct op de hoogte gesteld wordt van de gedetecteerde of vermeende zwakke plekken in de beveiliging in de systemen of de diensten die verband houden met de persoonsgegevensverwerking.
A-13.1.4	Uw organisatie dient te beschikken over een formele en geactualiseerde procedure voor het rapporteren van informatiebeveiligingsgebeurtenissen in combinatie met een reactie- en een escalatieprocedure voor incidenten rond persoonsgegevens. In het geval van een openbaar incident strekt het tot de aanbeveling melding te doen bij de bevoegde instanties conform aanbeveling nr 01/2013 van de Privacycommissie. Meer in het bijzonder geldt, conform de wet van 13 juni 2005 betreffende de elektronische communicatie, de meldingsplicht indien het een openbaar incident betreft in de telecomsector.
A-13.1.5	De informatiebeveiligingscel/verantwoordelijke voor de verwerking moet systematisch geïnformeerd worden over alle maatregelen die genomen worden om aan informatiebeveiligingsincidenten en zwakke plekken rond persoonsgegevens het hoofd te bieden.

14 BEDRIJFSCONTINUITEIT ***(zie ISO 27002 – 17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer)***	
14.1 INFORMATIEBEVEILIGINGSCONTINUITEIT ***(zie ISO 27002 – 17.1 Informatiebeveiligingscontinuïteit)***	
A-14.1.1	Uw organisatie moet op basis van een risicobeoordeling de nodige maatregelen bepalen om de continuïteit van de informatiebeveiliging van persoonsgegevens te waarborgen.
14.2 REDUNDANTE COMPONENTEN	
A-14.2.1	Naargelang de eisen van uw organisatie dienen informatieverwerkende faciliteiten met voldoende redundantie te worden voorzien om de beschikbaarheid van persoonsgegevens te waarborgen. Bijkomende informatiebeveiligingsrisico's als gevolg van redundantie moeten hierbij in acht te worden genomen.

15 NALEVING ***(zie ISO 27002 – 18 Naleving)***	
15.1 NALEVING VAN WETTELIJKE VOORSCHRIFTEN ***(zie ISO 27002 – 18.1 Naleving van wettelijke en contractuele eisen)***	
A-15.1.1	Uw organisatie moet steeds alle van toepassing zijnde wetten en regels over de verwerking en de bescherming van persoonsgegevens naleven. Minimaal moeten de bepalingen opgenomen in de wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (Privacywet) en haar uitvoeringsbesluit (KB van 13 februari 2001) worden nageleefd. In functie van de gegevensverwerking wordt dit wettelijk kader aangevuld met specifieke wetgeving: • *Koninklijk Besluit van 17 december 2003 tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van bepaalde sectorale comités opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer;* • *Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen;* • *Wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de Sociale Zekerheid;* • *Wet van 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen;* • *Wet van 4 juli 1962 betreffende de openbare statistiek;* • *Wet van 13 juni 2005 betreffende de elektronische communicatie;* • *Wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator;*

	• *Wet van 5 mei 2014 houdende verankering van het principe van de unieke gegevensinzameling in de werking van de diensten en instanties die behoren tot of taken uitvoeren voor de overheid en tot vereenvoudiging en gelijkschakeling van elektronische en papieren formulieren;* • *Koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid;* • *Koninklijk besluit van 17 maart 2013 betreffende de veiligheidsadviseurs ingevoerd door de wet van 15 augustus 2012 houdende oprichting en organisatie van een federale dienstenintegrator;* • *Koninklijk besluit van 7 juni 2007 tot vaststelling van de nadere regels met betrekking tot de samenstelling en de werking van het Statistisch Toezichtscomité opgericht binnen de Commissie voor de bescherming van de persoonlijke levenssfeer;* • *Omzendbrief van 9 januari 2002 betreffende de toegang tot de informatiegegevens die in het Rijksregister van de natuurlijke personen opgenomen zijn. Maatregelen ter beveiliging van de gegevens;* • *Omzendbrief van 24 september 2007 betreffende de verplichtingen voor de verantwoordelijken van gegevensverwerking;* • *Omzendbrief van 12 maart 2008 betreffende de bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens- Toegang tot de informatiegegevens van het Rijksregister – Veiligheidsmaatregelen die ertoe strekken de vertrouwelijkheid en de integriteit van de gegevens, de authenticatie van de gebruikers en het spoor van de activiteiten die uitgevoerd werden op de informatiesystemen, te waarborgen;* • *Omzendbrief van 10 juli 2008 betreffende de bescherming van de persoonlijke levenssfeer t.o.v. de verwerking van persoonsgegevens -Toegang tot de informatiegegevens van het Rijksregister – Respect voor de doeleinden waarvoor toestemming werd gegeven om toegang te krijgen tot de informatiegegevens in het Rijksregister of om er mededeling van te bekomen.*
A-15.1.2	Uw organisatie moet op een systematische wijze nagaan of een machtiging (al dan niet onder de vorm van een aansluiting) vereist is voor het aanschaffen of ontwikkelen van een systeem dat persoonsgegevens gebruikt/verwerkt. Indien die vereist is moet zij maatregelen nemen om aan alle verplichten te voldoen inzonderheid de melding van de identiteit van de veiligheidsconsulent en de beschrijving van het beveiligingsbeleid ter attentie en door middel van de formulieren voorgeschreven door het instrumenterende sectoraal comité.
A-15.1.3	Uw organisatie moet over geactualiseerde procedures beschikken voor de uitwerking en onderhoud van documentatie die betrekking heeft op de verleende machtiging(en).
A-15.1.4	Uw organisatie moet over een goedgekeurde aanpak beschikken om na te gaan dat de machtiging gerespecteerd blijft bij iedere wijziging aan de toepassing/applicatie die persoonsgegevens gebruikt/verwerkt waarvoor deze machtiging verleend is.

15.2 INFORMATIEBEVEILIGINGSBEOORDELINGEN ***(zie ISO 27002 – 18.2 Informatiebeveiligingsbeoordelingen)***	
A-15.2.1	Uw organisatie moet op regelmatige basis een degelijke audit organiseren met betrekking tot informatiebeveiliging van persoonsgegevens. Deze audit moet betrekking hebben op de volgende domeinen uit de onderhavige richtsnoeren: - risicobeoordeling; - beleid i.v.m. informatiebeveiliging; - organisatie van de informatiebeveiliging; - beveiligingsvereisten m.b.t. personeel; - beheer van bedrijfsmiddelen; - logische toegangsbeveiliging; - cryptografische beheersmaatregelen - fysieke beveiliging; - operationeel beheer; - onderhoud en ontwikkeling van informatiesystemen; - informatiebeveiliging in leveranciersrelaties - beheersen van informatiebeveiligingsincidenten; - beheersproces bedrijfscontinuïteit; - naleving.

DEEL B – SPECIFIEKE/TECHNISCHE IMPLEMENTATIENORMEN

3 ORGANISATIE ***(zie ISO 27002 – 6 Organisatie van informatiebeveiliging)***	
3.2 Mobiel werken ***(zie ISO 27002 – 6.2 Mobiele apparatuur en telewerken)***	
B-3.2.1	De nodige beheersmaatregelen om mobiel computergebruik (inclusief andere mobiele media) en telewerken op een veilige manier toe te laten, moeten ingevoerd worden. Deze maatregelen kunnen onder meer betrekking hebben op: • cryptografische technieken; • back-ups; • bescherming tegen malware; • toegangsbeveiliging bij de externe toegang tot persoonsgegevens; • fysieke beveiliging van draagbaar computerapparatuur (inclusief mobiele media) en van de telewerklocatie tegen diefstal.

4 PERSONEELSBELEID ***(zie ISO 27002 – 7 Veilig personeelsbeleid)***	
4.2 INFORMATIEBEVEILIGING TIJDENS HET DIENSTVERBAND **(zie ISO 27002 – 7.2 Tijdens het dienstverband)**	
B-4.2.1	Alle gepaste maatregelen moeten geïmplementeerd worden om te verhinderen dat persoonsgegevens ongecontroleerd uw organisatie verlaten en in ongeoorloofde handen vallen. Met name door: - bedrijfsmiddelen te beschermen tegen ongeoorloofde toegang, openbaarmaking, wijziging, vernietiging of verstoring; - bepaalde beveiligingsprocessen of –activiteiten uit te voeren; - te waarborgen dat de verantwoordelijkheid van genomen handelingen steeds duidelijk wordt toegewezen aan een persoon; - beveiligingsgebeurtenissen of potentiële gebeurtenissen of andere beveiligingsrisico's te rapporteren.

4.3 INFORMATIEBEVEILIGING BIJ BEEINDIGING OF WIJZIGING VAN DIENSTVERBAND ***(zie ISO 27002 – 7.3 Beëindiging en wijziging van dienstverband)***	
B-4.3.1	Bij wijziging van verantwoordelijkheden aan deelname in de gegevensverwerking moeten de noodzakelijke aanpassingen aan de informatiebeveiligingsmaatregelen getroffen worden zoals opgenomen in de punten 5.1.3 en 6.1.2.

5 BEDRIJFSMIDDELEN ***(zie ISO 27002 – 8 Beheer van bedrijfsmiddelen)***	
5.1 VERANTWOORDELIJKHEID VOOR BEDRIJFSMIDDELEN ***(zie ISO 27002 – 8.1 Verantwoordelijkheid voor bedrijfsmiddelen)***	
B-5.1.1	Een geactualiseerde inventaris van relevante bedrijfsmiddelen met betrekking tot persoonsgegevensverwerkingen moet in samenwerking met de betrokken operationele diensten worden opgesteld. Relevante bedrijfsmiddelen zijn onder andere: - informatie; - software programma's; - fysieke middelen; - diensten; - alle gebruikers (inclusief toegangsrechten).
B-5.1.2	In deze inventaris moet elk relevant bedrijfsmiddel met betrekking tot een persoonsgegevensverwerking gekoppeld zijn aan een welbepaalde functie/persoon binnen uw organisatie (verantwoordelijkheid).
B-5.1.3	Bij beëindiging van dienstverband, contract of overeenkomst moet een formele procedure toegepast worden voor het teruggeven van alle relevante verstrekte bedrijfsmiddelen (zoals programmatuur, bedrijfsdocumenten, apparatuur en toegangskaarten). In geval van gebruik van persoonlijke apparatuur moeten er gepaste maatregelen toegepast worden voor de overdracht van alle relevante informatie aan de organisatie en het correct verwijderen van de informatie van de apparatuur.
5.2 CLASSIFICATIE VAN INFORMATIE ***(zie ISO 27002 – 8.2 Classificatie van informatie)***	
B-5.2.1	Bij het gebruik en de verwerking van persoonsgegevens moet duidelijk rekening gehouden worden met het onderscheid tussen de volgende gegevenstypes: • anonieme gegevens;

	• persoonsgegevens; • gevoelige persoonsgegevens; • gecodeerde al dan niet gevoelige persoonsgegevens.
5.3 BEHANDELEN VAN MEDIA ***(zie ISO 27002 – 8.3 Behandelen van media)***	

B-5.3.1	Bij gebruik van verwijderbare of andere media waarop persoonsgegevens worden opgeslagen dienen de gepaste beheersmaatregelen genomen te worden. Enkele voorbeelden zijn:
	• indien de media de beveiligingsperimeter verlaten:
	  o moeten de opgeslagen persoonsgegevens verwijderd worden indien ze niet meer nodig zijn,
	  o met persoonsgegevens, moet vooraf goedkeuring worden verkregen en wordt een register bijgehouden;
	• stations voor verwijderbare media enkel vrijgeven als dit om bedrijfsredenen noodzakelijk is;
	• het bewaren van persoonsgegevens op verwijderbare media moet in lijn zijn met de levensduur van de media. Indien de bewaartermijn de levensduur overstijgt, moeten de gegevens ook elders opgeslagen worden.

B-5.3.2	De gepaste maatregelen om fysieke media (inclusief papieren documenten) die persoonsgegevens bevatten tijdens het transport te beschermen tegen onbevoegde toegang, misbruik of corruptie behoren uitgevoerd te worden. Mogelijke maatregelen zijn: • betrouwbare transport- of koerierdiensten gebruiken; • procedures ontwikkelen om de identificatie van koeriers te verifiëren; • toereikende verpakking gebruiken om de inhoud te beschermen tegen fysieke schade tijdens het transport; • registraties bijhouden omtrent het vervoer, de ontvangst en de identificatie van de inhoud en toegepaste bescherming van de media.

6 TOEGANG TOT PERSOONSGEGEVENS **(zie ISO 27002 – 9 Toegangsbeveiliging)**	
6.1 EISEN VOOR TOEGANGSBEVEILIGING ***(zie ISO 27002 – 9.1 Bedrijfseisen voor toegangsbeveiliging)***	
B-6.1.1	Uw netwerkbeheerders moeten de vastgestelde beveiligingsmaatregelen implementeren indien toegang wordt verleend tot persoonsgegevens via netwerken of netwerkdiensten.

B-6.1.2	De toegangsrechten van alle medewerkers en externe gebruikers tot informatie en informatieverwerkende faciliteiten moeten verwijderd of aangepast worden bij respectievelijk beëindiging of wijziging van hun dienstverband, contract of overeenkomst.
6.4 TOEGANGSBEVEILIGING VAN SYSTEMEN EN TOEPASSINGEN ***(zie ISO 27002 – 9.4 Toegangsbeveiliging van systemen en toepassingen)***	
B-6.4.1	Uw informaticadienst moet per bedrijfstoepassing op basis van de beveiligingseisen de nodige beveiligingsmaatregelen nemen om de toegang tot de persoonsgegevens te beperken. Dit dient te gebeuren door middel van een: - identificatiesysteem- (wie bent u?); - authenticatiesysteem- (hoe maakt u duidelijk wie u bent?); - en een autorisatiesysteem (wat mag u doen?).
B-6.4.2	De toegang voor uw informatiebeheerders (systeembeheerders, ook wel "superusers" genoemd) tot informaticasystemen waarop de persoonsgegevens gebruikt/verwerkt worden, moet beperkt worden door middel van: - identificatie (wie bent u?); - authenticatie (hoe maakt u duidelijk wie u bent?); - en autorisatie (wat mag u doen als superuser?).

7 CRYPTOGRAFIE ***(zie ISO 27002 – 10 Cryptografie)***	
7.1 CRYPTOGRAFISCHE BEHEERSMAATREGELEN ***(zie ISO 27002 – 10.1 Cryptografische beheersmaatregelen)***	
B-7.1.1	De vastgestelde cryptografische beheersmaatregelen dienen geïmplementeerd te worden om de vertrouwelijkheid, authenticiteit en/of integriteit van persoonsgegevens te beschermen.
A-7.1.2	Het beleid met betrekking tot het beheer van cryptografische sleutels moet over de gehele levenscyclus zorgvuldig worden toegepast.

8 FYSIEKE BEVEILIGING ***(zie ISO 27002 – 11 Fysieke beveiliging en beveiliging van de omgeving)***	
8.1 BEVEILIGING VAN DE OMGEVING ***(zie ISO 27002 – 11.1 Beveiligde gebieden)***	
B-8.1.1	De toegang tot beveiligde ruimtes (waarin zich persoonsgegevens bevinden of gebruikt/verwerkt worden) moet strikt beperkt worden tot de bevoegde personen door uw organisatie aangeduid door het aan brengen van de vastgestelde toegangsbeveiligingen. Hierop moet door de aangeduide verantwoordelijke regelmatige controle uitgeoefend worden, zowel tijdens als buiten de normale werkuren (logboek of logfile).
B-8.1.2	De gepaste maatregelen moeten genomen worden om schade door brand, wateroverlast, explosie, … kortom elke vorm van natuurlijke of door mensen veroorzaakte calamiteiten te vermijden. Enkele voorbeelden van maatregelen zijn: • de brandcompartimentering laten aansluiten met de detectie van beveiligde ruimtes; • de gepaste branddetectie en brandblusapparatuur voorzien en de werking ervan op geregelde tijdstippen controleren; • opslag van media voor back-ups en reserveapparatuur scheiden van de beveiligde ruimte.
8.2 BEVEILIGDE APPARATUUR ***(zie ISO 27002 – 11.2 Apparatuur)***	
B-8.2.1	Apparatuur moet beschermd worden tegen fysieke bedreigingen en gevaren van buitenaf. Hierbij dient bijzondere aandacht te worden besteed aan apparatuur die zich buiten het terrein van organisatie bevindt of wordt gebruikt. Er dient onder meer aandacht te zijn voor: • de plaatsing en de bescherming van apparatuur zodat het beschermd is tegen risico's van schade en storing van buitenaf en de toegang door onbevoegden wordt vermeden; • de bescherming tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen; • het beveiligen van voedings- en telecommunicatiekabels tegen interceptie of beschadiging; • het onderhoud van de apparatuur.
B-8.2.2	Alle apparatuur met opslagmedia moet voor verwijdering of hergebruik gecontroleerd worden zodat alle persoonsgegevens veilig overschreven of verwijderd zijn. Indien deze apparatuur gevoelige persoonsgegevens bevat moeten specifieke maatregelen genomen worden om deze apparatuur fysiek te vernietigen of de informatie zodanig te verwijderen met technieken die het onmogelijk maken deze terug te halen.

9 OPERATIONELE BEVEILIGING ***(zie ISO 27002 – 12 Beveiliging van bedrijfsactiviteiten)***	
9.1 OPERATIONELE PROCEDURES EN VERANTWOORDELIJKHEDEN OMTRENT INFORMATIEBEVEILIGING **(zie ISO 27002 – 12.1 Bedieningsprocedures en verantwoordelijkheden)**	
B-9.1.1	Om een correcte en veilige bediening van informatieverwerkende faciliteiten die persoonsgegevens gebruiken/verwerken te waarborgen moeten bedieningsprocedures gedocumenteerd en beschikbaar gesteld worden aan alle gebruikers die ze nodig hebben.
B-9.1.2	Conform aanbeveling nr 01/2013 van de Privacycommissie moet er een strikte scheiding zijn tussen de ontwikkelings-, test-, aanvaardings-/integratie- en productieomgevingen om het risico op onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen. Dit impliceert onder meer. dat er geen testen of ontwikkelingen mogen plaatsvinden in de productieomgeving. Slechts in uitzonderlijke gevallen kan voor testdoeleinden van deze regel afgeweken worden op voorwaarde dat de gepaste maatregelen getroffen worden.
9.2 BESCHERMING TEGEN MALWARE **(zie ISO 27002 – 12.2 Bescherming tegen malware)**	
B-9.2.1	Ter bescherming tegen malware (voorkomen, ontdekken en verwijderen/herstellen) behoort uw informaticadienst anti-malware- en herstelsoftware te installeren en regelmatig te updaten, waarbij computers en media als voorzorgsmaatregel of routematig worden gescand. De uitgevoerde scan behoort onder meer: - alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware te scannen; - bijlagen en downloads vóór gebruik op malware te scannen en dit op verschillende cruciale plaatsen in uw netwerkconfiguratie (mailservers, computers, netwerktoegang…); - internetpagina's op malware te scannen. Nauwkeurige en informatieve waarschuwingsberichten in het geval van een reële bedreiging kunnen het bewustzijn van de gebruikers vergroten.
9.3 BACK-UP ***(zie ISO 27002 – 12.3 Back-up)***	
B-9.3.1	Uw verantwoordelijken voor het back-upbeheer moeten op regelmatige basis volledige en gecontroleerde back-ups van de persoonsgegevens nemen en moeten op regelmatige basis controleren of ze in staat zijn om deze back-ups terug te gebruiken ("*restore*").

B-9.3.2	Uw verantwoordelijken voor het back-upbeheer moeten de nodige maatregelen nemen om de vertrouwelijkheid, integriteit en toegankelijkheid m.b.t. de back-up gegevens te garanderen.
9.4 MONITORING ***(zie ISO 27002 – 12.4 Registreren en monitoren)***	
B-9.4.1	Voor het gebruik en de verwerking van persoonsgegevens moeten, conform de referentiemaatregelen van de Privacycommissie, duidelijke afgeschermde logbestanden aangemaakt worden. De logbestanden behoren onder meer activiteiten, uitzonderingen en gebeurtenissen te omvatten.
B-9.4.2	De door uw organisatie aangeduide verantwoordelijke moet over een geactualiseerde lijst beschikken met alle personen en hun respectievelijke toegangsniveaus tot de persoonsgegevens.
9.5 OVERWEGINGEN BIJ AUDITS VAN INFORMATIESYSTEMEN ***(zie ISO 27002 – 12.7 Overwegingen betreffende audits van informatiesystemen)***	
B-9.5.1	De gepaste beheers- en beveiligingsmaatregelen moet genomen worden om gegevenslekken, verlies aan persoonsgegevens, gegevensbeschadiging en verstoringen van bedrijfsprocessen te vermijden tijdens informatiesysteem-audits.

10 COMMUNICATIEBEVEILIGING ***(zie ISO 27002 – 13 Communicatiebeveiliging)***	
10.1 NETWERKBEVEILIGING ***(zie ISO 27002 – 13.1 Beheer van netwerkbeveiliging)***	
B-10.1.1	Uw netwerkbeheerders moeten beveiligingsmaatregelen nemen ter bescherming van de verschillende netwerken waarmee de apparatuur (die de persoonsgegevens verwerkt) verbonden is.
B-10.1.2	Uw netwerkbeheerders moeten de nodige beheersmaatregelen nemen op het niveau van de informatienetwerken om: - de vertrouwelijkheid en de integriteit m.b.t. de persoonsgegevens te garanderen, en - ongeoorloofde toegang te voorkomen; - tegemoet te komen aan de vereisten van beschikbaarheid en capaciteit.

B-10.1.3	Uw netwerkbeheerders moeten een geactualiseerde cartografie bijhouden van de gegevensstromen op netwerkniveau, en deze steeds ter beschikking stellen van de veiligheidsconsulent.

11 AANSCHAFFEN, ONTWIKKELEN EN ONDERHOUDEN VAN INFORMATIESYSTEMEN ***(zie ISO 27002 – 14 Verwerving, ontwikkeling en onderhoud van informatiesystemen)***	
11.1 BEVEILIGINGSEISEN VOOR INFORMATIESYSTEMEN ***(zie ISO 27002 – 14.1 Beveiligingseisen voor informatiesystemen)***	
B-11.1.1	Uw beveiligingseisen moeten voorafgaand aan de aanschaf en/of de ontwikkeling en/of de verbetering van het informatiesysteem formeel en duidelijk vastgesteld, overeengekomen en gedocumenteerd worden. Deze documentatie moet steeds bijgewerkt worden in het kader van het lanceren van een nieuwe of een verbeterde versie van uw informatiesysteem.
11.2 BEVEILIGING IN ONTWIKKELINGS- EN ONDERSTEUNINGSPROCESSEN ***(zie ISO 27002 – 14.2 Beveiliging in ontwikkelings- en ondersteuningsprocessen)***	
B-11.2.1	De projectverantwoordelijke moet, vooraleer nieuwe of belangrijke evoluties van bestaande systemen in productie genomen worden, nagaan of aan de beveiligingsvereisten die aan het begin van de ontwikkelingsfase vastgesteld zijn, voldaan is.

12 LEVERANCIERSRELATIES ***(zie ISO 27002 – 15 Leveranciersrelaties)***	
12.1 INFORMATIEBEVEILIGING IN LEVERANCIERSRELATIES ***(zie ISO 27002 – 15.2 Beheer van dienstverlening van leveranciers)***	
B-12.1.1	De dienstverlening van leveranciers moet op regelmatige basis gemonitord, beoordeeld en geaudit worden.

13 INFORMATIEBEVEILIGINGSINCIDENTEN ***(zie ISO 27002 – 16 Beheer van informatiebeveiligingsincidenten)***	
13.1 BEHEER VAN INFORMATIEBEVEILIGINGSINCIDENTEN EN –VERBETERINGEN ***(zie ISO 27002 – 16.1 Beheer van informatiebeveiligingsincidenten en –verbeteringen)***	
B-13.1.1	Een procedure moet geïnstalleerd worden die toelaat om informatiebeveiligingsgebeurtenissen m.b.t. de gebruikte/verwerkte persoonsgegevens: - op te sporen; - te beoordelen, en indien van toepassing: - op te volgen; - en te herstellen.
B-13.1.2	De door uw organisatie aangeduide veiligheidsconsulent treedt op als contactpunt voor het opsporen en rapporteren van beveiligingsincidenten.
B-13.1.3	Indien een informatiebeveiligingsincident de grenzen van de organisatie overschrijdt moeten alle getroffen externe partijen op een gecoördineerde wijze tijdig en afdoende geïnformeerd worden door de veiligheidsconsulent.

14 BEDRIJFSCONTINUITEIT ***(zie ISO 27002 – 17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer)***	
14.1 INFORMATIEBEVEILIGINGSCONTINUITEIT ***(zie ISO 27002 – 17.1 Informatiebeveiligingscontinuïteit)***	
B-14.1.1	De nodige procedures moeten geïmplementeerd worden voor het herstel van uw bedrijfsprocessen, het waarborgen van het vereiste niveau van informatiebeveiliging en het opnieuw beschikbaar stellen van de persoonsgegevens binnen een vooraf bepaalde tijdspanne. De procedures kunnen omvatten: procedures voor noodsituaties, uitwijkprocedures, herstartprocedures, … Deze procedures moeten gedocumenteerd zijn, regelmatig getest en aangepast worden en de betrokken personen moeten opgeleid zijn. De procedures rond bedrijfscontinuïteit dienen eveneens beveiligd te worden tegen lekken en beschadiging gezien de gevoelige informatie die erin aanwezig is (met name hoe de organisatie zal reageren bij een ernstig incident of ramp).

B-14.1.2	Uw maatregelen voor de continuïteit van de informatiebeveiliging van persoonsgegevens moeten op regelmatige basis getest en indien nodig geüpdatet worden.

15 NALEVING ***(zie ISO 27002 – 18 Naleving)***	
15.1 NALEVING VAN WETTELIJKE VOORSCHRIFTEN ***(zie ISO 27002 – 18.1 Naleving van wettelijke en contractuele eisen)***	
B-15.1.1	De veiligheidsconsulent communiceert tijdig aan alle personen die betrokken zijn bij het verwerken van persoonsgegevens over de relevante na te leven wet- en regelgeving.