Beleidslijn informatieveiligheid en privacy

Gedragscode voor informatiebeheerders

(BLD ETHICS)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

Niemand twijfelt er vandaag de dag aan dat de informatie- en communicatietechnologie (ICT) een belangrijke rol speelt in het economisch leven. Het behoorlijk functioneren van de informatiesystemen inclusief hardware en software is van groot belang voor overheden, organisaties en burgers die in grote mate afhankelijk zijn van deze systemen en bijgevolg van hun informatiebeheerders[1].

Alvorens de rollen en de verantwoordelijkheden van de informatiebeheerders verder toe te lichten blijkt het nuttig om de opdrachten van de informatieveiligheidsconsulent binnen het netwerk van de sociale zekerheid in herinnering te brengen. De informatieveiligheidsconsulent is immers ertoe gehouden de wetten met betrekking tot de bescherming van persoonlijke levenssfeer te doen naleven. Hij/zij heeft ook een adviserende, stimulerende, documenterende, controlerende en bevorderende opdracht inzake naleving van de informatieveiligheidsregels die door een wettelijke of reglementaire bepaling of krachtens dergelijke bepaling zijn opgelegd. Hij/zij moet er ook voor zorgen dat alle medewerkers een veiligheidsbevorderende houding aannemen. In dat opzicht is de informatieveiligheidsconsulent een bevoorrechte partner van de informatiebeheerders. De informatieveiligheidsconsulent is ertoe gehouden een ethische gedragscode na te leven.

De informatiebeheerder is iedere persoon die in het kader van verantwoordelijkheden met betrekking tot een ICT-systeem over toegangsrechten beschikt die ruimer zijn dan het louter functioneel gebruik van de informatie ("superusers" of "powerusers"). Het gaat onder meer om systeembeheerders, databank administrators (DBA), informatieveiligheidsconsulenten (CISO), functionarissen voor de gegevensbescherming (DPO), software-ontwikkelaars en –beheerders, netwerk-beheerders, consultants, externe IT dienstenleveranciers[2], en onderaannemers.

Deze gedragscode heeft niet de ambitie om de precieze taak van de informatiebeheerder te omschrijven of om een technische handleiding te zijn voor informatiebeheerders. Dat is immers al gebeurd in andere documenten zoals de beleidslijnen, job-omschrijvingen of arbeidsreglementen. Deze gedragscode biedt ook geen concrete oplossingen voor elk ethisch of beleidsprobleem waarmee een informatiebeheerder bij de uitvoering van zijn functie geconfronteerd kan worden.

Deze gedragscode wil de informatiebeheerders bewust maken van het belang om hun bevoegdheden op een ethisch verantwoorde manier uit te oefenen: de integriteit van een informatiebeheerder maakt integraal deel uit van zijn/haar professionaliteit. De informatiebeheerders kunnen deze gedragscode gebruiken als beleidslijn voor de dagdagelijkse werkzaamheden. Bovendien kan de informatiebeheerder deze gedragscode zien als een voortdurende uitnodiging om alle professionele handelingen ethisch te toetsen en waar nodig aan te passen. Voor alle overige medewerkers van de organisatie is het nuttig te weten dat de uitoefening van de bevoegdheden van informatiebeheerder ingebed is in regels. Voor de directie is het nuttig om te preciseren hoe de informatiebeheerder gebruik moet maken van zijn/haar bevoegdheden in het belang van de organisatie.

Deze gedragscode voor informatiebeheerders gaat uit van drie basisbegrippen: integriteit, informatiebescherming en informatie/documentatieplicht. Bij integriteit gaat het zowel over ethische integriteit van de informatiebeheerder als over integriteit van informatiesystemen. Informatiebescherming handelt over privacybescherming en het omgaan met vertrouwelijke informatie. Informatie/documentatieplicht gaat over het informeren van medewerkers en het documenteren van informatiesystemen.

[1] In het engels wordt dikwijls de term « data custodian » gebruikt en niet te verwarren met « data steward ». Data stewards zijn verantwoordelijk voor gegevens inhoud, context en bijbehorende bedrijfsregels. Data custodians zijn verantwoordelijk voor de bewaring, het vervoer, de opslag van de gegevens en de uitvoering van zakelijke regels. Met andere woorden, data stewards zijn verantwoordelijk voor wat is opgeslagen in een gegevensveld, terwijl data custodians verantwoordelijk zijn voor de technische omgeving en database structuur zijn.

[2] Voorbeelden van externe IT dienstenleveranciers zijn internet service providers (ISP), application service providers (ASP), cloud service providers (CSP) of cloud service brokers (CSB)

Dit document beschrijft de beleidslijnen met betrekking tot de regels die in acht moeten worden genomen door de informatiebeheerders die werkzaam zijn binnen de instellingen die deel uitmaken van het netwerk van de sociale zekerheid.

2. Gedragscode

Elke organisatie onderschrijft de volgende beleidslijnen van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

1. De directie van de organisatie moet een gedragscode voor informatiebeheerders rond integriteit, informatiebescherming en informatie/documentatieplicht opzetten, valideren, communiceren en onderhouden.
2. De directie van de organisatie behoudt zich het recht voor om de gedragscode te controleren.
3. De organisatie moet een formele meldingsprocedure hebben en een formeel gevalideerd disciplinair proces hebben voor medewerkers die inbreuk op de gedragscode hebben gepleegd.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2005		V2005	Eerste versie	29/06/2005	01/07/2005
2005		V2005	Tweede versie	12/09/2005	01/10/2005
2017		V2017	Integratie EU GDPR	07/03/2017	07/03/2017

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- ADM, “Gedragscode voor informatiebeheerders”, September 2010, 7 blz.

Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.isaca.org/certification/code-of-professional-ethics/pages/default.aspx
- https://www.sans.org/security-resources/ethics
- https://en.wikibooks.org/wiki/Ethics_for_IT_Professionals/Professional_Code_of_Ethics
- http://ethics-wg.org/framework.html
- https://digital-forensics.sans.org/certification/ethics
- https://www.ksz-bcss.fgov.be/nl
- http://www.ccb.belgium.be/nl

Bijlage C: Uitgewerkte gedragscode

I. De ethische integriteit van de informatiebeheerder

I.1. De informatiebeheerder stelt zich objectief en onpartijdig op tijdens de uitoefening van zijn/haar functie.

Toelichting: deze algemene richtlijn omschrijft de houding van de informatiebeheerder. De informatiebeheerder vervult deze functie op een kritische en verantwoorde manier. Hi/zij tracht zoveel mogelijk rekening te houden met de verschillende in het spel zijnde belangen en baseert zijn beslissingen op een rationele beoordeling van alle relevante beschikbare informatie.

I.2. De informatiebeheerder streeft ernaar (de perceptie van) persoonlijke belangenconflicten te vermijden. Wanneer deze zich toch voordoen, zal hij zijn oversten daarover onmiddellijk inlichten en hierover een formele beslissing vragen.

Toelichting: het gaat hier om persoonlijke belangen die onverenigbaar zijn met het belang van de organisatie, bijvoorbeeld de positie binnen de organisatie veilig stellen via praktijken en gedragingen die niet correct zijn. De informatiebeheerder zal geen geschenken, giften of uitnodigingen aanvaarden van derde partijen of externe consultants of tijdelijke medewerkers zonder expliciete voorafgaandelijke communicatie naar en goedkeuring van de persoon belast met het dagelijks bestuur van de organisatie.

I.3. De informatiebeheerder stelt zijn vaardigheden op gepaste wijze ten dienste van de organisatie en van de medewerkers van de informatiesystemen.

Toelichting: een informatiebeheerder beschikt over een zeer waardevolle kennis en expertise, en moet ervoor zorgen dat deze kennis en expertise op gepaste wijze wordt gebruikt in het belang van (het bereiken van de doelstellingen van) de organisatie.

I.4. De informatiebeheerder streeft ernaar in de best mogelijke verstandhouding samen te werken met alle medewerkers van de organisatie.

Toelichting: de informatiebeheerder mag geen buitenstaander worden ten opzichte van de eigen organisatie of een dergelijke houding gaat aannemen ten koste van de belangen of doelstellingen van de organisatie. Ook de externe consultants en tijdelijke medewerkers worden beschouwd als zijnde werkzaam binnen de organisatie.

I.5. De informatiebeheerder zal zijn technische vaardigheden eerlijk voorstellen en doet een beroep op bijkomende professionele (technische) bijstand indien nodig.

I.6. De informatiebeheerder krijgt de middelen en levert voldoende inspanningen om op de hoogte te blijven van de evoluties binnen zijn/haar domein.

I.7. De informatiebeheerder zal steeds respectvol omgaan en samenwerken met alle medewerkers (intern en extern).

I.8. De informatiebeheerder zal met de (toezichthoudende) autoriteiten samenwerken.

II. De integriteit en de beschikbaarheid van de informatie

II.1. De informatiebeheerder waakt over het behoorlijk functioneren van het systeem en stelt de handelingen die nodig zijn om de integriteit en de beschikbaarheid van het informatiesysteem te garanderen.

Toelichting: de informatiebeheerder verricht geen enkele handeling voor enig ander doel dan het garanderen van de goede werking van het informatiesysteem in het belang van de organisatie .

II.2. De informatiebeheerder waakt erover dat de handelingen niet het verlies, de onbeschikbaarheid of de vernietiging van de gegevens of van de toepassingen tot gevolg hebben.

II.3. Aangezien bepaalde handelingen van medewerkers schade kunnen berokkenen aan de integriteit of de beschikbaarheid van het computersysteem of –netwerk, of de gegevens, moet de informatiebeheerder in het kader van zijn verantwoordelijkheden toezien op de naleving van het beleid van toepassing in de organisatie en indien nodig zijn hiërarchische meerderen op de hoogte brengen. Indien hij vaststelt dat bepaalde van deze acties niet onder het toepassingsgebied van de bestaande minimale normen vallen, brengt hij de informatieveiligheidsconsulent hiervan op de hoogte. De informatieveiligheidsconsulent zal dan de nodige maatregelen treffen in het belang van de organisatie.

II.4. De informatiebeheerder zorgt ervoor dat de toegang tot het systeem gegarandeerd wordt aan de personen die dergelijke toegang nodig hebben in het kader van hun functie en dat de toegang tot die personen beperkt blijft.

III. Informatiebescherming

Naleving van de privacy verordening[3] en de bescherming van de gevoelige gegevens

III.1. De informatiebeheerder is zich bewust van het feit dat hij/zij toegang heeft tot grote hoeveelheden persoonsgegevens en gevoelige gegevens waarop de bepalingen inzake bescherming van het privéleven en van persoonsgegevens van toepassing zijn.

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

III.2. De informatiebeheerder is zich bewust van het feit dat de persoonsgegevens en gevoelige gegevens moeten worden beschermd.

III.3. De informatiebeheerder wijst op de risico's eigen aan zijn domein, dringt er bij de directie op aan om gepaste instructies te krijgen met betrekking tot die risico's en past technische, procedurele, communicatieve en organisatorische maatregelen toe waardoor de persoonsgegevens en gevoelige gegevens beveiligd en beschermd zijn tegen elke niet toegelaten gegevensverwerking. De informatiebeheerder houdt naast de aan verwerkingen verbonden risico's, ook rekening met de aard, de omvang, de context en de verwerkingsdoeleinden.

Toelichting : om te bepalen wat « passende » instructies zijn, wordt rekening gehouden met de stand van de techniek terzake en de kosten voor het toepassen van de controlemaatregelen enerzijds, en de aard van de te beveiligen informatie en de potentiële risico's anderzijds.

III.4. De informatiebeheerder waakt erover dat ook derden en externe medewerkers de bepalingen met betrekking tot de bescherming van persoonsgegevens en gevoelige gegevens naleven.

Toelichting: bijvoorbeeld bij onderhoud of herstelling van informatiesystemen door derden en externe medewerkers moeten ook deze op de hoogte zijn van de relevante verplichtingen inzake de bescherming van persoonsgegevens en gevoelige gegevens.

Controle van on-line communicatie en toegang tot bestanden

III.5. De informatiebeheerder mag on-line communicatie en toegangen tot bestanden controleren binnen het kader van zijn/haar bevoegdheden en mits de naleving van de wettelijke en reglementaire bepalingen.

Toelichting : In principe mag de controle op de elektronische on-line communicatiegegevens geen inmenging in de persoonlijke levenssfeer van de medewerker tot gevolg hebben. Als de controle toch een inmenging in de persoonlijke levenssfeer van de medewerker tot gevolg heeft, moet deze inmenging tot een minimum beperkt worden. Geheime controles zijn verboden. Daarenboven mag er enkel gecontroleerd worden voor: 1° het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden; 2° de bescherming van economische, handels- en financiële belangen van de organisatie die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken; 3° de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de organisatie, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de organisatie; 4° het te goeder trouw naleven van de in de organisatie geldende beginselen en regels voor het gebruik van on-line technologieën.

Vertrouwelijke gegevens

III.6. De informatiebeheerder gaat ervan uit dat alle informatie van de organisatie vertrouwelijk is en als dusdanig behandeld moet worden, door zichzelf als door alle medewerkers van de organisatie.

Toelichting: het gaat naast persoonsgegevens (waaronder ook sociale en medische gegevens) ook over beroepsgeheimen, know-how en andere gevoelige informatie. Geen enkele informatiebeheerder mag misbruik maken van deze informatie.

[3] **EU GDPR** http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

IV. Informatie- en documentatie-plicht

IV.1 De informatiebeheerder licht alle betrokken medewerkers duidelijk en regelmatig in over hun verantwoordelijkheden bij het toegelaten gebruik van informatiesystemen via bewustmaking, opleiding en evaluaties (audits).

IV.2. De informatiebeheerder licht naar aanleiding van een interventie zijn/haar handelingen tijdig en op een begrijpelijke manier toe opdat de betrokken medewerker(s) voldoende geïnformeerd zou zijn over de gevolgen op (het gebruik van) de informatiesystemen.

Toelichting: het gaat om de interventies van de informatiebeheerder, bijvoorbeeld in het kader van de aanpassing van een systeem.

IV.3. De informatiebeheerder waakt erover dat er steeds een geactualiseerde documentatie voorhanden is waarin het informatiesysteem (zoals ontwikkeling, hard- en software, infrastructuur) op zodanige wijze wordt beschreven dat elke betrokken persoon zich een precies en volledig totaalbeeld zou kunnen vormen. De bedoeling ervan is een continu beheer van het informatiesysteem te garanderen. De gegevensbeschermingseffect-beoordeling maakt hier integraal deel van uit.

Toelichting: indien de informatiebeheerder om de een of andere reden zijn/haar functie niet meer kan uitoefenen, dan moet een andere informatiebeheerder het informatiesysteem verder doeltreffend kunnen beheren. Om de kennisoverdracht te vergemakkelijken is een precieze en volledige inventaris van de informatiesystemen een vertrekpunt.

IV.4. De informatiebeheerder kan vragen of problemen bespreken met andere informatiebeheerders in de organisatie en indien nodig ook in vertrouwen bespreken met de dienst informatieveiligheid van de KSZ.

Bijlage D: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	
Organisatie van de informatieveiligheid.	**Ja**
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	**Ja**

***** EINDE VAN DIT DOCUMENT *****