Beleidslijn informatieveiligheid en privacy

Veilig uitbesteding aan derden

(BLD OUTS)

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).

Dit document beschrijft de beleidslijnen rond informatieveiligheid in relatiebeheer met derde partijen (leveranciers).

2. Veilig uitbesteden aan derden

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

In geval van onderaanneming moet de organisatie zich van het volgende vergewissen dat

1. de verplichtingen[1] inzake de verwerking van persoonsgegevens moeten contractueel vastgelegd zijn
2. de vereisten rond informatieveiligheid en privacy moeten overeengekomen worden met derde partijen en gedocumenteerd worden om risico's te reduceren met betrekking tot toegang van derde partijen tot informatiemiddelen
3. alle relevante vereisten rond informatieveiligheid en privacy moeten opgesteld en overeengekomen worden met elk van die derde partijen die informatie van de organisatie lezen, verwerken, stockeren, communiceren of ICT infrastructuurcomponenten aanleveren
4. overeenkomsten met derde partijen moeten alle vereisten omvatten om risico's van informatieveiligheid en privacy behandelen die geassocieerd zijn met ICT diensten
5. de organisatie moet regelmatig de dienstverlening van derde partijen monitoren, evalueren en auditeren
6. wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatieveiligheid en privacy, moeten beheerd worden. Bij het beheren dient er rekening gehouden te worden met het kritieke karakter van de betrokken systemen en processen en met her-evaluatie van risico's

1 De organisatie blijft altijd aansprakelijk voor de informatieveiligheid en de privacy van de verwerking, met inbegrip van de verwerking bij de onderaannemer(s).

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2003		V2003	Eerste versie	10/09/2003	01/10/2003
2004		V2004	Tweede versie	11/02/2004	01/12/2004
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.
- SANS, “A security guide for acquiring outsourced service”, April 2017, 20 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 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.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.isaca.org/cobit
- https://www.sans.org/reading-room/whitepapers/services/a-security-guide-for-acquiring-outsourced-service-1241
- https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx
- http://www.isaca.org/Knowledge-Center/Research/Documents/Governance-of-Outsourcing_res_Eng_0105.pdf

Bijlage C: Richtlijnen rond veilig uitbesteding aan derde partijen

Informatieveiligheid en privacy bij relatiebeheer met derde partijen

1. Er dienen specifieke richtlijnen opgesteld te worden voor (logisch en fysiek) toegangsbeheer van derde partijen
2. De verschillende types derde partijen die toegang krijgen tot informatie of informatiesystemen van de organisatie (zoals leveranciers, nutsbedrijven), moeten geïdentificeerd en gedocumenteerd worden
3. Voor uitvoering van een opdracht moet een standaard proces en cyclus voor relatiebeheer met derde partijen opgesteld worden om informatieveiligheid en privacy te verzekeren
4. Indien een derde partij werkt met onderaannemers, dan blijft de derde partij (hoofdaannemer) verantwoordelijk voor het naleven van de informatieveiligheid- en privacy-vereisten door de onderaannemer
5. De verschillende types toegang tot informatie (raadplegen, schrijven, wijzigen, verwijderen) die door de organisatie toegestaan worden aan de verschillende derde partijen moeten gedefinieerd zijn, en de toegangen moeten bewaakt en gecontroleerd worden volgens vastgelegde processen en procedures
6. Beleidslijnen informatieveiligheid en privacy moeten voor elk type informatie en toegang een basis vormen voor individuele overeenkomsten met derde partijen. Deze overeenkomsten moeten gebaseerd zijn op vereisten en risicoprofiel van de organisatie
7. Medewerkers van de organisatie die rechtsreeks interageren met derde partijen moeten bewust gemaakt worden over geëigende regels en gedrag, gebaseerd op het type derde partij (zoals nutsbedrijf of leverancier) en op hun toegangsniveau tot de (informatie)systemen van de organisatie

Informatieveiligheid en privacy behandelen in overeenkomsten met derde partijen

Er moeten individuele overeenkomsten met elke eerstelijns derde partij opgesteld worden om te verzekeren dat er geen misverstanden bestaan over de verantwoordelijkheden van beide partijen m.b.t. informatieveiligheid en privacy. Volgens de aard van “derde partij”, kan de relatie met de organisatie als volgt gedefinieerd worden:

1. Een wet- of regelgeving die een samenwerking oplegt of autoriseert met andere publieke instellingen, nationaal of internationaal
2. Een overeenkomst tussen publieke instellingen die de voorwaarden voor samenwerking regelt
3. De clausules van een bestek
4. Een expliciete overeenkomst tussen twee partijen.

In deze overeenkomsten moeten de hieronder volgende richtlijnen in acht genomen worden

1. Continue transparantie en communicatie van de derde partij naar de organisatie omtrent het verder uitbesteden aan andere partijen van activiteiten gerelateerd aan de opdracht met de organisatie, met inbegrip van de genomen maatregelen rond informatieveiligheid en privacy.
2. Hoe met incidenten met betrekking tot toegang van een derde partij omgegaan moet worden door zowel de organisatie als de derde partij.
3. Regelingen voor weerbaarheid en, indien nodig, herstel om beschikbaarheid van informatie of informatiesystemen van een van beide partijen te verzekeren.
4. Hoe overdracht van informatie, informatiesystemen of andere informatiemiddelen die verplaatst worden, beheerd moet worden en hoe de veiligheid en privacy van de informatie verzekerd moet worden tijdens de overdrachtsperiode.
5. Er moet een duidelijke beschrijving zijn van informatie die verstrekt of benaderd wordt alsook de manier(en) waarop informatie verstrekt of benaderd wordt.

6. De gegevens moet volgens het classificatieschema van de organisatie beschreven worden waarbij, indien nodig geacht, de classificatieschema's en respectieve informatieveiligheid- en privacy-maatregelen van beide partijen in samenspraak op elkaar afgestemd en vastgelegd worden.
7. Regelgevende en wettelijke vereisten, inclusief cybersecurity, privacy, intellectuele eigendomsrechten en auteursrechten moeten beschreven zijn met bovendien een beschrijving van hoe aan deze vereisten voldaan zal worden.
8. Verplichting van elke contractuele partij om overeengekomen controlemaatregelen te implementeren zoals toegangscontrole, nazicht van niveaus, monitoren, rapporteren en audit.
9. Verplichtingen van derde partijen voor het naleven van de informatieveiligheid- en privacy-vereisten van de organisatie zoals regels voor aanvaardbaar gebruik van informatie en, indien nodig, onaanvaardbaar gebruik van informatie.
10. Er moeten procedures of voorwaarden zijn voor autorisatie en het verwijderen van autorisatie voor toegang tot, of ontvangen van, informatie van de organisatie, bijvoorbeeld door een expliciete lijst op te stellen van medewerkers van derde partijen die geautoriseerde toegang krijgen tot informatie van de organisatie of deze informatie ontvangen.
11. Informatieveiligheidsvereisten en procedures voor het beheer van incidenten rond informatieveiligheid en privacy, voornamelijk notificatie en samenwerking tijdens het remediëren van een incident.
12. Training- en bewustmakingsvereisten over specifieke procedures en vereisten rond informatieveiligheid en privacy, zoals behandeling van incidenten en autorisatieprocedures.
13. Relevante contactpersonen, inclusief de contactpersoon voor informatieveiligheid en voor privacy.
14. Voor zover nodig, screening-vereisten voor medewerkers van derde partijen
15. Het recht van de organisatie om processen en procedures van derde partijen, die verband houden met de overeenkomst, te (laten) auditeren.
16. Verplichting van de derde partij om periodiek een onafhankelijk rapport af te leveren over de effectiviteit van de controles en een akkoord over tijdige oplossingen van eventuele relevante problemen vermeld in een auditrapport.
17. Proces voor het oplossen van defecten, conflicten en voor een uitstapregeling (exit strategie).

In het kader van overheidsopdrachten moeten de algemene principes van de overeenkomst gedefinieerd worden in een bestek.

ICT keten

Volgende richtlijnen moeten in acht genomen worden in overeenkomsten met betrekking tot informatieveiligheid en privacy in de ICT keten (supply chain):

1. Naast de algemene informatieveiligheid- en privacy-vereisten moeten ook specifieke informatieveiligheid- en privacy-vereisten gedefinieerd worden die van toepassing zijn op het aanschaffen van ICT gerelateerde producten en diensten.
2. ICT gerelateerde diensten en producten van derde partijen, die vereisen dat deze derde partijen de informatieveiligheid- en privacy-vereisten van de organisatie eventueel verder moeten doorgeven aan hun onderaannemers.
3. Er moet een monitoringproces en aanvaardbare validatiemethoden geïmplementeerd worden om na te gaan of ICT producten en diensten voldoen aan gespecificeerde informatieveiligheid- en privacy-vereisten.
4. Een proces voor het identificeren van product- of dienstverleningscomponenten die cruciaal zijn voor het onderhoud van de functionaliteit, moet geïmplementeerd worden. Er moet extra aandacht geschonken worden aan product- of dienstencomponenten wanneer die door een leverancier verder worden uitbesteed.

5. Derde partijen moeten aan de organisatie verzekeren dat kritieke onderdelen en diensten doorheen de ganse distributieketen getraceerd kunnen worden. Verder moeten ze ook verzekeren dat de geleverde ICT producten functioneren zoals verwacht, zonder enige onverwachte of ongewenste functies.
6. Er moeten regels gedefinieerd worden m.b.t. het delen van informatie over de ICT keten en over mogelijke problemen tussen de organisatie en de derde partijen.
7. Specifieke processen voor het beheren van de levenscyclus, beschikbaarheden en bijhorende informatieveiligheid- en privacy-risico's van onderdelen van ICT moeten vastgelegd worden. Hierbij moet rekening gehouden worden met onderdelen die niet meer beschikbaar zijn vanwege een productiestop, bijvoorbeeld door faillissement van een derde partij of door verouderde niet meer leverbare technologie (componenten).

Monitoring en evaluatie van dienstverlening van derde partijen

Er moeten processen opgesteld en geïmplementeerd worden voor het beheer van de dienstverlening tussen de organisatie en derde partijen. Hierbij moeten volgende aspecten in acht genomen worden:

1. De prestatieniveaus van de dienstverlening moeten gecontroleerd worden op conformiteit met de overeenkomsten
2. Dienstverleningsrapporten die door een derde partij opgesteld zijn moeten door de organisatie nagekeken worden, en bovendien moeten er regelmatig vergaderingen over de voortgang georganiseerd worden, zoals overeengekomen
3. Informatie over incidenten van informatieveiligheid of privacy moeten verstrekt worden. Deze informatie moet beoordeeld worden door de derde partij en de organisatie zoals vereist in overeenkomsten en in ondersteunende richtlijnen en procedures
4. Auditsporen en registraties van gebeurtenissen, operationele problemen, mislukkingen, opsporing van storingen, en onderbrekingen die verband houden met de geleverde diensten, moeten beoordeeld worden
5. Afspraken betreffende informatieveiligheid en privacy die een derde partij heeft met onderaannemers moeten geëvalueerd worden
6. Derde partijen moeten verzekeren dat zij kunnen blijven voldoen aan het overeengekomen prestatieniveau in geval van ernstige incidenten of rampen
7. De organisatie moet ervoor zorgen dat zijn medewerkers technisch bekwaam zijn en over voldoende middelen beschikken voor het monitoren van vereisten uit een overeenkomst. Indien nodig moeten er gepaste trainingen voorzien worden

Beheer van wijziging van dienstverlening van derde partijen

Wijzigingen in de dienstverlening door derde partijen, inclusief onderhoud en verbetering van het informatieveiligheidsbeleid, -procedures en -controles moeten beheerd worden rekening houdend met het kritieke karakter van de betrokken bedrijfsinformatie, -systemen, –processen en producten, en met een her-evaluatie van risico's. De volgende aspecten moeten hierbij in acht genomen worden

1. Wijzigingen aan overeenkomsten met derde partijen
2. Wijzigingen aan relevante wet- en regelgeving
3. Wijzigingen door de organisatie ter implementatie van
    a. Verbeteringen aan de huidig geleverde diensten.
    b. Ontwikkeling van nieuwe applicaties en systemen.
    c. Wijzigingen of updates aan beleidsdocumenten en procedures.

   d. Nieuwe of gewijzigde controlemaatregelen om incidenten rond informatieveiligheid of privacy op te lossen en te verbeteren.

4. Wijzigingen aan de dienstverlening door derde partijen ter implementatie van
   a. Wijzigingen en uitbreidingen aan netwerken.
   b. Gebruik van nieuwe technologieën.
   c. Nieuwe producten of nieuwe versies van bestaande producten.
   d. Nieuwe ontwikkelingstools en -omgevingen.
   e. Verandering van fysieke locaties.
   f. Verandering van leverancier.
   g. Uitbesteding aan andere onderaannemer.

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.	
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	**Ja**
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

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