Beleidslijn informatieveiligheid en privacy

Verwerking van persoonsgebonden gegevens

(BLD PRIV)

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).

De basis voor dit beleid wordt gevormd door de 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 (Europese Algemene Verordening Gegevensbescherming). [1]

Deze beleidslijnen zijn van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van de organisatie, alsmede op de verwerking van persoonsgegevens[2] die in bestanden zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Dit document heeft betrekking op de beleidslijnen voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrij verkeer van persoonsgegevens.

2. Verwerking van persoonsgebonden gegevens

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

- De organisatie brengt regelmatig alle risico's in kaart in verband met de conformiteit met de Europese verordening[3]. De geplande acties als gevolg van een hoog "residueel" risico op non-conformiteit dienen opgenomen te worden in het informatieveiligheid- en privacy-plan van de organisatie.
- In functie van de rol voor een specifieke (groep) verwerking (verwerker of verwerkings-verantwoordelijke), zal de organisatie minimaal de volgende activiteiten uitvoeren:
    - de opname van de verwerking in het centraal register van de verwerkingsverantwoordelijke of van de verwerker;
    - een formele verantwoording voor het niet-realiseren van controlemaatregelen gericht op de naleving van de Europese verordening[4].

[1] Beter bekend als European General Data Protection Regulation (afgekort "EU GDPR") http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] Onder informatieverwerking wordt verstaan: 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. Dit is de definitie uit de Europese verordening voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens van 27 april 2016.

[3] https://www.privacycommission.be/sites/privacycommission/files/documents/CO-AR-2016-004_NL.pdf

[4] pas toe of leg uit principe ("comply or explain principle")

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2017		V2017	Eerste versie	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 documenten, 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:

- 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)
- 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.
- ISO, “ISO/IEC 29100:2012 Security Techniques – Privacy framework”, december 2012, 21 blz.

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

- http://eur-lex.europa.eu/eli/reg/2016/679/oj
- https://www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-0
- https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- https://www.enisa.europa.eu/topics/data-protection
- 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
- https://www.iso.org/standard/45123.html
- http://www.isaca.org/privacy

Bijlage C: Bijhorende richtlijnen en templates

Voor het realiseren van deze beleidslijnen kan de organisatie gebruik maken van de volgende procedures:

1. de informatie aanvraag procedure en de gegevensbeschermingseffectbeoordelingsprocedure ("Privacy Impact Assessment") met bijhorende risicolijst uit de beleidslijn 'risicobeoordeling'
2. het register van verwerker en verwerkingsverantwoordelijke van de beleidslijn 'data classificatie'
3. de inbreuk en bezwaar procedure uit de beleidslijn 'Incidentenbeheer'
4. de functieomschrijving voor de functionaris voor gegevensbescherming uit de beleidslijn 'personeelsgerelateerde aspecten'
5. de contractuele bepalingen inzake gegevensbescherming uit de beleidslijn 'veilig uitbesteden aan derde partijen' en de beleidslijn 'personeelsgerelateerde aspecten'
6. de communicatie met betrokkene ("privacy verklaring") uit de beleidslijn 'aankopen, ontwerpen, ontwikkelen en onderhouden van informatiesystemen'.

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	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	**Ja**

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