Informatieveiligheid en privacy

Kernprincipes

(BLD KERN)

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 kernprincipes informatieveiligheid en privacy scheppen de nodige voorwaarden voor een betrouwbare uitvoering van informatieverwerking voor de openbare instellingen van sociale zekerheid (OISZ) die op het netwerk van de Kruispuntbank van de Sociale Zekerheid aangesloten zijn.

Het is voor de partners binnen de sociale zekerheid belangrijk om deze kernprincipes informatieveiligheid en privacy te kennen, te valideren, te communiceren en te integreren.

Dit document beschrijft de kernprincipes voor informatieveiligheid en privacy.

2. Kernprincipes van informatieveiligheid en privacy

De organisatie onderschrijft de volgende kernprincipes van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

1. Een duidelijk en helder beleid rond informatieveiligheid en privacy opzetten, valideren, communiceren en onderhouden om de beschikbaarheid, de integriteit, de vertrouwelijkheid te garanderen in lijn met de doelstellingen van de organisatie.
2. Conform de minimale normen informatieveiligheid en privacy en conform alle toepasselijke Belgische en Europese wetten en regelgevingen ageren om verplichtingen na te komen en boetes te vermijden.
3. Formele risico-aanpak rond informatieveiligheid en privacy opzetten, valideren, communiceren en onderhouden om relevante risico's tijdig, consistent en effectief aan te pakken in lijn met de verwachtingen van de organisatie.
4. Duidelijke rollen en verantwoordelijkheden rond informatieveiligheid en privacy van alle betrokken interne en externe personen en organisaties definiëren, valideren, communiceren en opvolgen.
5. De beleidslijnen informatieveiligheid en privacy omzetten in praktische gedocumenteerde procedures en richtlijnen in functie van de specifieke situatie van de organisatie en gebaseerd op de risico-beoordeling.
6. "Security en Privacy by design"[1] toepassen in de volledige levenscyclus van informatie in de organisatie om betrouwbare, kwalitatieve en efficiënte systemen te ontwikkelen: vanaf de creatie tot de verwijdering of de archivering van informatie.
7. Het niveau van informatieveiligheid en privacy continu verbeteren via een geactualiseerd meerjarenplan en regelmatige sensibiliseringscampagnes naar alle interne en externe betrokken personen en organisaties[2] om zo de kosten van inbreuken te verminderen en om de reputatie en het vertrouwen rond informatieverwerking te behouden.
8. Bij uitbesteding van informatieverwerking aan derde partijen de nodige controlemaatregelen opzetten, valideren, opvolgen en regelmatig controleren omdat de organisatie altijd verantwoordelijk blijft voor de informatieveiligheid en privacy.

[1] "Security en Privacy by design" betekent dat vanaf het begin van de ontwikkeling van een nieuw project of proces/dienstverlening steeds wordt nagedacht over de nodige maatregelen rond informatieveiligheid en privacy. Het is hierbij essentieel dat alle genomen maatregelen eenvoudig en gebruiksvriendelijk zijn en tegelijk verschillende beschermingslagen hebben. "Security en Privacy by design" is verschillend van "Security en Privacy by default" omdat in dit laatste geval steeds de veiligste of hoogste privacy optie gekozen wordt, wat niet altijd de meest gebruiksvriendelijke optie is.

[2] Het Sectoraal Comité van de Sociale Zekerheid kan hiervan een kopie opvragen.

9. Regelmatig rapporteren over de stand van informatieveiligheid en privacy om de toepasbaarheid, volledigheid, adequaatheid en effectiviteit van informatieveiligheid en privacy te valideren. Vastgestelde afwijkingen, problemen of incidenten zullen tijdig opgevolgd worden met gepaste acties/sancties in lijn met de interne procedures van de organisatie. Ernstige incidenten of inbreuken in verband met persoonsgegevens worden altijd tijdig geëscaleerd naar de bevoegde instanties[3].
10. Alle afwijkingen ten opzichte van de minimale normen informatieveiligheid en privacy met een significant risico voorafgaandelijk schriftelijk afstemmen en laten goedkeuren door het Sectoraal Comité van de Sociale Zekerheid[4].

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2017		V2017	Eerste versie inclusief 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 “Minimale Normen Definities informatieveiligheid en privacy”.

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

[3] Escalatie van incidenten kan altijd naar de veiligheidsdienst van de KSZ, naar CERT.BE. Escalatie is verplicht naar de privacy commissie binnen de 72 uur indien er persoonsgegevens betrokken zijn. http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&from=EN

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