Informatieveiligheid en privacy

Definities

(MNM DEF)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de minimale normen 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).

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in dit document.

2. Definities

A

Address spoofing: Techniek die het misbruik van IP adressen mogelijk maakt om firewall filters te omzeilen

Actieve sessie: Is een specifieke online omgeving waarin een gebruiker met zijn toepassing/transactie aan het werken is. Een gebruiker kan gelijktijdig in meerdere online omgevingen (of sessies) werken.

Analoge drager: Op een analoge drager worden gegevens op een niet-digitale manier opgeslagen. De meest voor de hand liggende analoge drager is papier.

B

Bedrijfscontinuïteitsbeheer (Business Continuity Management : BCM)

Bedrijfscontinuïteitsbeheer streeft ernaar om de bedrijfsprocessen (bedrijfsactiviteiten) te beschermen tegen onderbrekingen en om, wanneer er zich een onderbreking zou voordoen, te zorgen voor een positieve en effectieve reactie hierop.

Beheersmaatregelen: De maatregelen die getroffen worden voor het verzekeren van de integriteit, vertrouwelijkheid en beschikbaarheid van informatie.

Beschikbaarheid van informatie: Eigenschap dat informatie toegankelijk en bruikbaar is op verzoek van een bevoegde entiteit.

Beveiligde ruimten: Ruimten die fysiek beschermd zijn (bijv. data centers).

D

Data: Elektronische informatie verwerkt door of opgeslagen op informatiesystemen.

Declassificatie: Het wegnemen van de eerder aan informatie toegekende classificatie, waardoor de betreffende informatie vrij toegankelijk wordt.

Denial of service: Een situatie waarin een computersysteem onbedoeld niet beschikbaar is voor de verwachte dienstverlening.

Derde partij: Persoon of organisatie vreemd aan de organisatie, die voor of met de organisatie werken uitvoert, of goederen of diensten levert, met uitzondering van klanten (bijv. burgers, ondernemingen). Een eerstelijns derde partij is die derde partij waarmee de organisatie rechtsreeks onderhandelt en een overeenkomst afsluit.

Digitale drager: Wanneer gegevens op een elektronische manier opgeslagen worden (een representatie van de gegevens in een binaire omzetting) spreken we van een digitale drager.

Distributielijst: Een distributielijst is een de lijst van personen aan wie een document geheel of gedeeltelijk verstuurd of gecommuniceerd mag worden. Personen kunnen fysieke individuele personen zijn of groepen van personen die zich door een specifiek verifieerbaar kenmerk onderscheiden.

E

Eigenaar van informatie (informatie-eigenaar): Informatie moet toegekend worden aan een 'eigenaar' die kennis heeft van het gebruik en de waarde van de informatie voor de organisatie, nodig om het classificatieniveau van de informatie te bepalen. Een 'eigenaar' van informatie is verantwoordelijk voor het :

- Beschermen van informatie
- Bepalen van de waarde van de informatie voor de organisatie
- Bepalen van het classificatieniveau van informatie
- Labelen van informatie
- Toepassen van de nodige beheersmaatregelen op basis van de classificatie.

Een 'eigenaar' van informatie heeft echter niet het eigendomsrecht in de strikt juridische zin van het woord.

EU GDPR: European General Data Protection Regulation

F

Forensisch (onderzoek): Met betrekking tot rechtszaken, gerechtelijk onderzoek.

Fysieke perimeter: Een fysieke perimeter is een fysieke barrière, die verhindert dat ongeoorloofde personen deze barrière binnendringen. Het bestaan van een fysieke perimeter gaat dus samen met het verlenen van toegang aan bevoegde personen. Dit kan op verschillende manieren, bijv. door een sleutel of een badgesysteem. In het kader van dit beleid wordt ervan uit gegaan dat de fysieke perimeter afdoende beveiligd is tegen indringing door onbevoegden.

G

Gecompromitteerde sleutel: Een sleutel waarvan niet gegarandeerd kan worden dat deze enkel geautoriseerd gebruikt kan worden.

Gebruikers van informatiesystemen: Alle interne en externe medewerkers, geautomatiseerde diensten en applicaties en externe partijen (bv. andere organisaties) en klanten (bv. personen, ondernemingen, instellingen).

Gegevensbeschermingseffectbeoordeling: analyse van onderdelen van processen en het effect dat een onderbreking van activiteiten daarop kan hebben .

Geprivilegieerde toegangsrechten: De toegangsrechten die benodigd zijn om wijzigingen binnen het RBAC-model uit te voeren of om systeemwijzingen uit te voeren (systeembeheer).

Gevoelige gegevens: Gevoelige gegevens zijn die gegevens die door de eigenaar van de gegevens als dusdanig geclassificeerd worden. Algemeen beschouwd mogen gevoelige gegevens niet aan het publiek gecommuniceerd worden maar uitsluitend aan de betrokken persoon of onderneming. In functie van de classificatie zijn deze gevoelige gegevens duidelijk gedefinieerd, zijn er gebruiksregels gedefinieerd, en worden zij slechts gebruikt door een relatief beperkte groep van de medewerkers.

Gevoelige persoonsgegevens: De gegevens worden in dit beleid als "gevoelige gegevens" beschouwd op basis van de artikelen 6 (waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de verwerking van persoonsgegevens die het seksuele leven betreffen, 7 (gezondheid) en 8 (geschillen) van de wet van 8/12/1992 (Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens). Zolang niet in tegenstrijd met de wetgeving ter zake kan de eigenaar van de gegevens beslissen om persoonsgegevens, andere dan diegene expliciet vermeld in voornoemde wetgevingen, als "niet gevoelige persoonsgegevens" te beschouwen.

H

Hoge risico omgeving: Omgevingen die een hoger risico lopen op vlak van informatieveiligheid. Bv. omgevingen die een gegevenstrafiek genereren over een publiek netwerk (zoals VPN verbindingen).

I

ICT Continuïteitsbeheer: ICT Continuïteitsbeheer verzekert dat vereiste informatie- en communicatietechnologie en diensten weerbaar zijn en kunnen hersteld worden tot op vooraf gedefinieerde niveaus, én binnen tijdschalen zoals vereist door de business. ICT Continuïteitsbeheer ondersteunt het overkoepelend Bedrijfscontinuïteitsbeheerproces (Business Continuity Management (BCM)) van een organisatie.

Informatie: Informatie is een bedrijfsmiddel dat, zoals elk ander belangrijk bedrijfsmiddel, gepast beschermd/beveiligd moet worden. Informatie kan verschillende vormen aannemen, zoals geschreven, gedrukte, elektronische of gesproken informatie.

Informatiemiddel: alle elementen/middelen die bij het creëren, ontvangen, verwerken, opslagen, verdelen, verzenden, dupliceren, en vernietigen van informatie van waarde zijn voor de organisatie; informatie die kan opgeslagen worden op verschillende informatiedragers en in verschillende informatiesystemen.

Informatieveiligheidsgebeurtenis: Een waargenomen verandering in de normale werking van een systeem, omgeving, proces of persoon, die gerelateerd is aan een mogelijke inbreuk van het informatieveiligheid, het falen van controle maatregelen, een voordien nog onbekende situatie die relevant kan zijn in het kader van informatieveiligheid.

Informatieveiligheidsincident: Een of meerdere niet gewenste informatieveiligheidsgebeurtenissen met een significante kans om de dienstverlening van de organisatie te verstoren en de informatieveiligheid in gedrang te brengen.

Informatiesystemen: Alle netwerken en ICT systemen, inclusief applicaties, onder het beheer van de organisatie.

Informatieveiligheid: Informatieveiligheid is het beschermen van informatie tegen een breed scala van dreigingen. De integriteit, vertrouwelijkheid en beschikbaarheid van informatie zijn drie aspecten die hierin centraal staan.

Inherent risico: de waarschijnlijkheid dat een negatieve impact zich zal voordoen wanneer er geen beschermingsmaatregelen genomen worden

Integriteit van informatie: Eigenschap dat de nauwkeurigheid en volledigheid van informatie wordt beveiligd.

Interne gegevens: alle gegevens waarvan het gebruik beperkt moet worden tot binnen de eigen organisatie. Deze gegevens zijn niet bestemd voor publieke bekendmaking zonder voorafgaande goedkeuring door een bevoegd personeelslid van de organisatie.

Intrusion Detection System (IDS): Een geautomatiseerd systeem dat pogingen of voorvallen van niet geautoriseerde toegang tot een informatie systeem of netwerk detecteert.

Intrusion Prevention System (IPS): Een geautomatiseerd systeem dat pogingen of voorvallen van niet-geautoriseerde toegang tot een netwerk blokkeert.

K

Kritieke IT- of informatiesystemen: Op basis van een risico analyse moet bepaald worden of een IT- of informatiesysteem als kritiek beschouwd moet worden. Kritiek dient beschouwd te worden vanuit het belang van een IT- of informatiesysteem in het vrijwaren van vertrouwelijkheid, integriteit of beschikbaarheid van gegevens en IT dienstverlening.

Kritische toepassingen: Zonder de kritische toepassingen is een organisatie niet in staat om de dagdagelijkse activiteiten uit te voeren.

L

Logische perimeter: Een logische perimeter is een barrière op het niveau van informatiesystemen, die verhindert dat ongeoorloofde personen of applicaties deze barrière binnendringen. Het bestaan van een logische perimeter vereist dus het verifiëren van de identiteit, het controleren van de autorisatie en het filteren van de gegevens.

M

Mobiele apparaten: De verzamelnaam voor smartphones, tablets, notebooks en laptops.

Mobile device management (MDM): Software die het mogelijk maakt om apparaten op afstand uit te schakelen, informatie te wissen of te blokkeren in geval van diefstal of misbruik

N

Naleving: Niet-naleving van deze beleidslijnen kan ernstige veiligheidsrisico's met zich meebrengen met betrekking tot de vertrouwelijkheid, integriteit en beschikbaarheid van (gevoelige) gegevens, en het imago en reputatie van de organisatie. De vaststelling dat het beleid en de bijhorende procedures niet gerespecteerd worden, kan leiden tot sancties of zelfs juridische vervolging.

O

Operationeel informatiebeheerder: Een operationele beheerder van informatie is een persoon, of een departement, aangeduid door ofwel de organisatie of door de proceseigenaar, die verantwoordelijk is voor het implementeren en operationeel beheren van de nodige beveiligingsmaatregelen in functie van het classificatieniveau bepaald door de proceseigenaar. In de praktijk kan een operationele beheerder van informatie bijvoorbeeld een ICT systeembeheerder zijn, een toepassingsontwikkelaar, een verantwoordelijke voor gebouwenbeheer, enz.

Opslag: het bewaren van gegevens op een drager (opslagmedium). Vanuit de opslag kan een verwerking gebeuren.

Overeenkomst: Schriftelijke afspraken tussen de organisaties en een derde partij over werken, leveringen en diensten die geleverd worden door derde partijen aan de organisatie en/of omgekeerd.

P

Patch: een aanpassing/update van ofwel een bestaande software op basis van een programmacode ter correctie en/of verbetering van zwakheden of fouten, ofwel van netwerkapparatuur en/of netwerkbekabeling.

Permissies: bepalen welke acties de gebruiker kan uitvoeren in een applicatie of systeem.

Privacy Risk Assessment (PRA) : zie gegevensbeschermingseffectbeoordeling

Procedures: ondersteunen de specifieke beleidsdocumenten door de desbetreffende beleidslijnen om te zetten naar specifieke operationele taken (hoe er beveiligd moet worden).

R

Recovery Point Objective (RPO): De maximale periode waarin het aanvaardbaar is om data te verliezen.

Recovery Time Objective (RTO): Het tijdbestek na uitval van een systeem waarin systemen en data moeten worden teruggezet naar een eerder vastgesteld punt.

Relatiebeheer: Het beheren van de relatie met een derde partij die toegang heeft (of zal verkrijgen) tot informatie en/of informatiebedrijfsmiddelen van de organisatie, en/of informatie en/of informatiebedrijfsmiddelen aanlevert (of zal aanleveren) aan de organisatie.

Residuele risico: de waarschijnlijkheid dat een negatieve impact zich zal voordoen, ondanks de maatregelen die genomen worden om het (inherent) risico te beïnvloeden (beperken)

Risico: de kans (“waarschijnlijkheid”) dat een bepaalde bedreiging zich voordoet met een welbepaalde impact (“ernst”) tot gevolg

Risico-beoordeling: het geheel van procedures dat er toe strekt om risico’s te identificeren, analyseren en beoordelen

Risicoprofiel: het resultaat van de risico analyse van de organisatie. Binnen de risico analyse worden - op basis van de impact en waarschijnlijkheid van bedreigingen op vlak van informatieveiligheid - de risico’s bepaald. Alle risico’s samen vormen het risicoprofiel van de organisatie.

Role-based access control (RBAC): Een methode waarmee op een effectieve en efficiënte wijze toegangscontrole voor informatiesystemen kan worden ingericht, waarbij gebruikers gekoppeld worden aan voor-gedefinieerde bedrijfsfuncties, die bestaan uit diverse rollen, waarvan elk een specifieke set permissies heeft.

Roleigenaar: Verantwoordelijke voor een rol in het RBAC-model, bestaande uit een specifieke set permissies en gekoppeld aan één of meerdere functies.

S

Security Incident en Event management (SIEM): Een term voor software producten en diensten die data over gebeurtenissen en incidenten, die een invloed op de veiligheid kunnen hebben, verzamelen in een centraal overzicht en deze analyseren.

Security Incident Response Team (SIRT): Team van medewerkers dat moet optreden wanneer er bepaalde informatiebeveiligingsincidenten zich voordoen. In functie van het type informatiebeveiligingsincident kan dit team telkens uit verschillende personen bestaan.

Systeemeigenaar: Verantwoordelijke voor een of meerdere informatiesystemen onder het beheer van organisatie.

Systemen van gebruikers: Alle systemen die toegekend zijn aan een individuele gebruiker en uitsluitend gebruikt worden door deze persoon.

T

Token: Een authenticatiemiddel dat gebruikt wordt om de identiteit van de gebruiker te controleren. Een token bestaat meestal uit reeks cijfers die onderdeel uit maken van een wachtwoord. (bv. token die burgers zelf kunnen aanvragen, de elektronische token die aan de medewerkers van de organisatie verstrekt wordt).

Transactie: Een transactie is een automatische uitwisseling van data tussen IT systemen zonder tussenkomst van een gebruiker. Vb. uitwisseling van data met andere overheidsinstellingen.

Transport: Onder fysiek transport van gegevens wordt het verplaatsen van de drager (dus zowel analoge als digitale opslagmedia) bedoeld of het verplaatsen van de apparatuur waarin deze drager zou geïntegreerd zijn. Impliciet is er dan automatisch ook sprake van mobiele opslagmedia. Onder elektronisch transport wordt het kopiëren of het behandelen van dat via een telecommunicatienetwerk bedoeld. Bij elektronisch transport gaat het uitsluitend over digitale gegevens. Eigen aan elektronisch transport is dat men niet het opslagmedium zelf, maar een kopie van de data verplaatst.

Twee-factor authenticatie (TOTP) : Een authenticatie methode die gebruik maakt van een combinatie van twee verschillende manieren om de identiteit van de gebruiker te bevestigen (bv. Geld afhalen door gebruik te maken van een bankkaart en een pincode).

V

Veiligheidsconsulent: een functie verantwoordelijk voor het onderhoud en ontwikkeling van de beveiligingsstrategie van de organisatie en dit in overeenstemming met de geldende wetgeving en de minimale normen waarop de organisatie zich baseert. Hij/zij rapporteert verplicht formeel één keer per jaar aan de directie

Veiligheidsmatrix: Een model dat gebruikt wordt voor het beheren van de toegangsrechten op basis van de permissies, rollen en functies voor applicaties.

Vernietiging: zeker stellen dat elk spoor van data of informatie op een gegevensdrager verdwenen is, of de gegevensdrager zelf in voldoende mate vernietigd is, en de data of informatie van dezelfde bron niet terug zichtbaar of leesbaar kan gemaakt worden. Vernietiging van bijvoorbeeld documenten kan door versnippering, of door het verzamelen in speciale ‘containers’. De inhoud van deze containers wordt door een gespecialiseerde firma vernietigd. Vernietiging van originele gegevens kan uitsluitend met medeweten van de eigenaar en rekening houdend met de wettelijke bepalingen die erop van toepassing zijn. De actie van de vernietiging moet het voorwerp uitmaken van een autorisatie.

Vertrouwelijke informatie/gegevens: In de classificatie van gegevens moeten alle categorieën als vertrouwelijk worden beschouwd, met uitzondering van de interne bedrijfsgegevens en publieke gegevens. Er moet opgemerkt worden dat sommige interne bedrijfsgegevens, hoewel zij niet echt vertrouwelijk zijn, toch minimaal beveiligd worden.

Vertrouwelijkheid van informatie: Eigenschap dat informatie niet beschikbaar wordt gesteld of wordt ontsloten aan onbevoegde personen, entiteiten of processen.

Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt (Bron AVG).

Verwerking: elke bewerking of elk geheel van bewerkingen met betrekking tot informatie, al dan niet uitgevoerd met behulp van geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.

Verwerkingverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (Bron AVG).

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
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.

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