Beleidslijn informatieveiligheid en privacy

Data classificatie

(BLD DATA)

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).

Informatieveiligheid is het geheel van maatregelen en procedures om informatie te beschermen. Het doel is: waarborgen van de continuïteit, integriteit en vertrouwelijkheid van informatie en de informatiesystemen en het beperken van de gevolgen van eventuele veiligheidsincidenten.

Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie:

- Vertrouwelijkheid: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden. De onderscheiden niveaus zijn: niet geklasseerd, gevoelig, geklasseerd, geheim.
- Integriteit: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). De onderscheiden niveaus zijn: niet zeker; beschermd; hoog en absoluut.
- Beschikbaarheid: hoeveel en wanneer data toegankelijk is en gebruikt kan worden. De onderscheiden niveaus zijn: niet nodig; noodzakelijk; belangrijk en essentieel.

Het toekennen van classificatieniveaus aan informatie en informatiesystemen is belangrijk, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt. Aan de hand hiervan kan worden bepaald welke vereisten gelden en welke maatregelen moeten worden genomen. Dit is bijvoorbeeld relevant voor beheerders die lang niet altijd bekend zijn met de inhoud en dus de waarde van data, maar wel worden geacht adequate veiligheidsmaatregelen te treffen. De volgende factoren oefenen invloed uit op de adequate veiligheidsmaatregelen: uitgangspunten, architectuurprincipes, veiligheidsvereisten.

Met een classificatiemethode kan bepaald worden hoeveel maatregelen nodig zijn. Indien de classificatie hoger dan vertrouwelijk is, dan zijn extra maatregelen nodig. Soms zijn deze maatregelen al genomen als binnen de procedure. Soms zijn deze extra maatregelen al uitgewerkt door een uitgevoerde risico-beoordeling van een andere instelling of er wordt binnen de instelling een risico-afweging gemaakt door het uitvoeren van een risico-beoordeling met als resultaat meer passende maatregelen.

Dit document geeft uitleg over het belang en de manier waarop data geklasseerd kan worden.

2. Data classificatie

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

1. De instelling moet voorziene bescherming of classificatie van informatie toepassen inclusief bijhorende informatieveiligheid- en privacy-maatregelen volgens een intern classificatieschema dat in lijn is met de specifieke wetgeving terzake alsook met de internationale regelgeving[1] en gebruik maken van het informatie classificatiemodel van de sociale zekerheid voor de onderlinge gegevensuitwisseling tussen de organisaties behorende tot de openbare instellingen van de sociale zekerheid. Indien de principes zoals beschreven in de wet- en regelgeving verschillend zijn van het interne classificatieschema van de instelling, zonder in tegenspraak te zijn, dan geldt de meest stringente regel. Indien het interne classificatieschema van de instelling in tegenspraak is met de van toepassing zijnde wet- en regelgeving, dan is de wet- en regelgeving van toepassing.
2. De instelling moet gepaste procedures en registers opstellen, valideren, implementeren, communiceren en onderhouden voor het labelen (etiketteren) en voor het verwerken van alle in beheer zijnde informatieverzamelingen, informatiedragers en informatiesystemen in overeenstemming met het interne classificatieschema.
3. Het object van classificatie is informatie. De classificatie die door de soort informatie bepaald wordt geldt ook voor het hogere niveau van informatiesystemen, dat wil zeggen dat, indien een systeem geheime informatie verwerkt, het hele systeem als geheim wordt aangemerkt, tenzij voor dat hogere niveau maatregelen genomen zijn binnen het informatiesysteem. Alle classificaties van alle kritische systemen zijn centraal vastgelegd door de eigenaren en dienen jaarlijks gecontroleerd te worden door de informatieveiligheidsconsulent (CISO) en/of de functionaris voor gegevensbescherming (DPO).
4. De verwerkingsverantwoordelijke van de informatie[2] bepaalt het vereiste beschermingsniveau (classificatie) op basis van het interne classificatieschema. Indien er sprake is van wettelijke vereisten, dan wordt dit expliciet aangegeven. De verwerkingsverantwoordelijke van de informatie bepaalt wie toegang krijgt tot welke informatie.
5. De verwerkingsverantwoordelijke van de informatie kan zich voor het classificeren laten ondersteunen door experten, zoals de informatieveiligheidsconsulent (CISO) en/of de functionaris voor gegevensbescherming (DPO).
6. Informatie kan meer of minder gevoelig of kritisch zijn. Voor bepaalde informatie kan een extra niveau van bescherming of een speciale verwerking nodig zijn. Als een informatiesysteem daarvoor maatregelen genomen heeft om delen van de systeeminformatie die hoger geclassificeerd is adequaat te beschermen, dan kan een systeem als geheel lager ingeschaald worden binnen de tabel en daarmee bijvoorbeeld alsnog binnen de norm vallen.
7. Er wordt gestreefd naar een zo ‘laag’ mogelijk classificatieniveau; te hoge classificatie leidt tot onnodige kosten. Bovendien dient informatie in beginsel voor zoveel mogelijk mensen beschikbaar zijn in het kader van een transparante overheid.
8. De controlemaatregelen moeten worden afgestemd op de risico’s, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van de te nemen maatregelen. Dit is situatie-afhankelijk. Naarmate de informatie een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen aan de veiligheid van die informatie te worden gesteld. Algemeen kan men stellen dat indien met geringe extra kosten meer veiligheid en privacy kan worden bewerkstelligd, dit als ‘gepast’ kan worden beschouwd. Extra veiligheid en privacy is niet meer “gepast” indien de kosten voor het mitigeren van deze risico’s disproportioneel hoog zijn. Risico’s en de te nemen controlemaatregelen dienen in balans te zijn.

[1] in het bijzonder de wetgeving van 11 december 1998 betreffende de classificatie en veiligheidsmachtigingen

[2] meestal de proceseigenaar

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2007		V2007	Eerste versie	10/10/2007	10/10/2007
2017		V2017	Integratie EU GDPR	07/03/2017	07/03/2017
2018		V2018	Update na controle policy werkgroep in 2017	09/01/2018	01/01/2019

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 veiligheidsconsulent van het eHealth platform.

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.
- ISO, “ISO/IEC 27010:2015 Information security management for inter-sector and inter-organizational communications”, november 2015, 32 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- ENISA, “Threat taxonomy: a tool for structuring threat information”, Januari 2016, 23 blz.
- NIST, SP800-60 volume II revision 1, “Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories”, Augustus 2008, 279 blz.

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

- http://www.iso.org/iso/iso27001
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=68427
- http://www.isaca.org/cobit
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf
- https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information
- https://www.cert.be/nl/het-traffic-light-protocol-tlp.html

Bijlage C: Richtlijnen classificatie van informatie

Toepassen van wet- en regelgeving

Richtlijnen
Alle persoonsgebonden informatie is door de wetgeving beschermd, los van elk expliciet classificatiesysteem. Persoonsgebonden gegevens worden sinds 27 april 2016 beschermd door de Europese verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens[3]. De principes van deze verordening moeten gerespecteerd worden, onafhankelijk van het door de instelling gedefinieerde interne classificatiesysteem.

Er moeten procedures opgesteld worden om toe te laten dat elke burger aanspraak kan maken op het recht administratieve documenten te raadplegen binnen de wet van 1 april 1994 betreffende de openbaarheid van bestuur. Deze procedures moeten toelaten toegangsaanvragen te evalueren, en die aanvragen te weigeren die niet voldoen aan de voorwaarden voorgeschreven door de wet. Op basis van de wet van 1 april 1994 betreffende de openbaarheid van bestuur kan, na verificatie van de geldigheid van een toegangsaanvraag tot administratieve documenten, afgeweken worden van de interne classificatieregels en de daaraan verbonden veiligheidsmaatregelen. Deze afwijking kan enkel op basis van een beslissing van een gemachtigd persoon of orgaan.

Voor informatie afkomstig uit andere landen of van in België gevestigde internationale instellingen waartoe de instelling toegang heeft, moet de instelling handelen “namens de instantie van oorsprong” (“eigenaar” van de informatie). In voornoemde gevallen moet de instelling in functie van het toegekende classificatieniveau van de betrokken informatie de overeenkomstig voorgeschreven beveiligingsmaatregelen toepassen.

Classificatie van door de instelling gecreëerde informatie

Richtlijnen
Al die informatie (en informatiemiddelen) die niet onder de wet- of regelgeving m.b.t. classificatie valt, moet door de instelling geclassificeerd worden. Het betreft informatie die:

- door de instelling zelf gecreëerd wordt
  én
- ofwel in haar naam opgeslagen wordt op analoge of digitale opslagmedia (al dan niet haar eigendom)
- of in haar naam op enige wijze fysiek verplaatst wordt of tussen eender welke opslagmedia op elektronische wijze uitgewisseld wordt.

Informatie die niet expliciet geclassificeerd wordt, zal als interne informatie worden beschouwd waarbij deze informatie:

- binnen de instelling vrij mag circuleren
- enkel aan het publiek of derde partijen mag gecommuniceerd worden op basis van een autorisatieprocedure
- aan contractanten of partners mag gecommuniceerd worden indien de informatie van belang is voor uitvoering van een opdracht en beveiliging van de informatie gewaarborgd wordt
- niet geclassificeerde informatie met betrekking tot personen en organisaties mogen aan de betrokken personen en organisaties gecommuniceerd worden, met uitsluiting van elk ander persoon of organisatie.

De classificatie moet het belang uitdrukken van de informatie voor de instelling op het vlak van de waarde ervan voor de instelling, kriticiteit, gevoeligheid (vertrouwelijkheid, integriteit, beschikbaarheid) en van wettelijke en/of contractuele vereisten. Informatie dient daarom toepasselijk geclassificeerd te worden zodat het een gepaste bescherming krijgt.

Verwerkingsverantwoordelijke van informatie en informatiemiddelen moeten verantwoordelijk gesteld worden voor de classificatie.

[3] http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&qid=1484310282035&from=NL

Een classificatieschema, bestaande uit verschillende classificatieniveaus, moet opgesteld worden met daarin afspraken voor classificatie en criteria voor geregeld nazicht van de classificatie. Het beschermingsniveau moet bepaald worden op basis van een analyse van de aspecten vertrouwelijkheid, integriteit en beschikbaarheid, en - voor zover nodig - op basis van bijkomende criteria.

Het classificatieschema moet consistent zijn doorheen de volledige organisatie zodat iedereen informatie op dezelfde wijze classificeert, een zelfde begrip heeft over beschermingsmaatregelen en over het toepassen van de gepaste bescherming.

Er mogen geen gegevens verwerkt worden zonder het akkoord van de eigenaar van de gegevens, of zonder een expliciete regel die het verwerken van de gegevens autoriseert[4].

Een instelling die informatie verwerkt en daarbij informatiesystemen gebruikt loopt bepaalde risico's doordat die informatie en informatiesystemen kwetsbaar zijn voor bedreigingen en problemen van binnen en van buiten.
Het uitvoeren van een degelijke risico-beoordeling ondersteunt bij het vaststellen van de risico's die worden gelopen en hoe groot die risico's zijn. Daarmee kan vervolgens bepaald worden welke veiligheidsmaatregelen getroffen moeten worden om de risico's terug te dringen tot een aanvaardbaar niveau. Vooral bij de vertaling van risico naar maatregel is classificatie een belangrijk hulpmiddel om de ernst van een risico en de reikwijdte van een maatregel te kunnen bepalen. Het voorgestelde interne classificatieschema kan beschouwd worden als een vereenvoudigde vorm van een risico-beoordeling. Bij een risico-beoordeling worden bedreigingen en problemen benoemd en in kaart gebracht. Per bedreiging en probleem wordt de kans van het optreden ervan bepaald en wordt vervolgens berekend wat de schade is die op zou kunnen optreden als een bedreiging of probleem zich daadwerkelijk voordoet (het inherente risico).
De bedoeling van een risico-beoordeling is dat er na de analyse wordt vastgesteld op welke wijze de risico's beheerst kunnen worden, of teruggebracht tot een aanvaardbaar niveau: met name via het treffen van informatieveiligheidsmaatregelen (het residuele risico). Naast de risico-beoordeling wordt ook een kosten-baten analyse uitgevoerd. Niet ieder risico kan of moet afgedekt worden: wanneer de kosten van de maatregelen om een risico te beperken hoger zijn dan de mogelijke schade, dan kan besloten worden om het residuele risico te aanvaarden.
Het is de verwerkingsverantwoordelijke van de informatie die bepaalt of de informatie classificatie juist is, maar ook of dat beargumenteerd van de aan deze classificatie gekoppelde maatregelen kan worden afgeweken, omdat het residuele risico aanvaardbaar is.

Informatie labelen

Richtlijnen

Procedures voor het labelen van informatie moeten zowel de informatie als de daaraan gerelateerde fysieke en elektronische middelen afdekken en richtlijnen geven in functie van het type medium over waar en hoe labels dienen aangebracht te worden.
De labeling moet het classificatieschema reflecteren en gerespecteerd worden voor al die informatie die een classificatie heeft van niveau hoger dan "intern".
Informatie die niet formeel geclassificeerd is, wordt als "interne" informatie beschouwd.
"Disclaimers" (bewijs van afstand) moeten aangeven dat:

- voor zover nodig, ingesloten informatie gevoelig is en, indien gecreëerd door de instelling, de informatie eigendom is van de instelling
- de ingesloten informatie enkel door de aangegeven bestemmeling(en) mag gelezen worden
- niet-geautoriseerd gebruik of vrijgave strikt verboden is
- iemand die ten onrechte de informatie verkregen heeft de afzender dient te contacteren
- indien het (zeer) vertrouwelijke informatie betreft via de post, dan dient een ingesloten disclaimer aan te geven dat de enveloppe enkel door de geadresseerde mag geopend worden.

[4] Wet van 11 april 1994 betreffende Openbaarheid van bestuur

Behandelen van informatiemiddelen

Richtlijnen

Procedures moeten opgesteld worden voor het behandelen, verwerken, stockeren en communiceren van informatie in overeenstemming met haar classificatie.

Volgende aspecten moeten beschouwd worden bij de behandeling van informatiebedrijfsmiddelen:

- toegangsbeperkingen in functie van het classificatieniveau en gebaseerd op het “need-to-have” principe voor de job
- registratie van geautoriseerde ontvangers van informatiebedrijfsmiddelen
- bescherming van tijdelijke of permanente kopijen van informatie op een niveau dat consistent is met het beschermingsniveau van de originele informatie
- markeren (labelen) van alle kopijen van informatiebedrijfsmiddelen ter attentie van de geautoriseerde ontvanger(s)
- stockeren van ICT bedrijfsmiddelen in overeenstemming met het classificatieniveau en/of van de productspecificaties van de leverancier

Overeenkomsten met andere externe organisaties waarmee informatie wordt uitgewisseld moeten procedures inhouden om de classificatie van informatie te identificeren en om de classificatie-labels/niveaus van andere organisaties te kunnen interpreteren. Zelfs indien benamingen van classificatie uit een classificatieschema van een andere organisatie identiek of vergelijkbaar zijn met die van de instelling, dan betekent dat nog niet dat de waarde die er aan gehecht wordt identiek of vergelijkbaar is.

Bijlage D: Voorbeeldmodellen van data classificatieschema's

1. Het informatie classificatiemodel van de Sociale Zekerheid

Informatie wordt gekenmerkt door de volgende parameters

- het type van gegeven: volgens de inhoudelijke domeinen waar het gegeven toe behoort eigen aan de context van de sociale zekerheid;
- de gevoeligheid: bepaalt de impact, in het algemeen, van het verlies of de verspreiding van de informatie.

Er worden 5 gevoeligheidsklassen onderkend :

- *Niveau 4 ter informatie (Top secret - Zeer geheim)*
  Onder de niveaus 'Top Secret' voor Europa en "Zeer geheim" voor België vallen gegevens, materiaal, technologieën, … waarvan de kennis of het gebruik de werking van Europa of België ernstig in gevaar brengt.
  Omwille van de coherentie met de positie van de instellingen binnen Europa en België wordt dit classificatieniveau niet gebruikt in de instellingen.
- *Niveau 3: geheim (Secret – High Classified – zeer vertrouwelijk)*
  Het niveau "Geheim" wordt toegekend wanneer ongepast gebruik van de informatie
  - een van de essentiële belangen van de instelling ernstig kan schaden.
  - er een impact is op de privacyrechten van een significante groep van mensen
- *Niveau 2: vertrouwelijk (Classified)*
  Het niveau "Vertrouwelijk" wordt toegekend wanneer ongepast gebruik van de informatie (als gevolg van bijvoorbeeld onvoldoende bescherming van gegevens)
  - een van de belangen van de instelling kan schaden of de werking van de dienst in gevaar brengt.
  - er een impact is op de privacyrechten van een groep van mensen of van kwetsbare personen en/of kinderen
- *Niveau 1: beperkt (Sensitive unclassified)*
  Het niveau "Beperkt" wordt toegekend wanneer ongepast gebruik van de informatie
  - een belang van een dienst kan schaden of het functioneren van een ambtenaar of een groep personen in het kader van hun functie binnen de instelling in gevaar brengt.
  - er een impact is op de privacyrechten van een (percentagegewijs) beperkte groep van mensen of van een individuele persoon
- *Niveau 0: niet geklasseerd (Unclassified – openbaar)*

  Dit niveau heeft tot gevolg dat de informatie zonder probleem verspreid mag worden omdat het niet het belang van de instelling, een dienst of het functioneren van een ambtenaar of een groep personen in het kader van hun functie binnen de instelling in gevaar brengt.

Opmerking : '**Gevoelige gegevens'** zijn gegevens met een gevoeligheidsklasse 'vertrouwelijk' en hoger.

De volgende type gegevens (informatie) worden onderscheiden :

I. Publieke gegevens

Als publieke gegevens worden alle gegevens beschouwd die openbaar zijn, algemene bekendheid hebben of vrij van vertrouwelijke inhoud zijn. Alle overige type gegevens zijn bijgevolg "Niet-publieke gegevens".

De standaard gevoeligheidsklasse van publieke gegevens is "niet geklasseerd".

Voorbeelden: website die toegankelijk is voor het grote publiek, papieren brochures of video's op sociale media voor de burgers.

II. Interne gegevens

Interne gegevens zijn alle gegevens waarvan het gebruik beperkt moet worden intern in de instelling. Deze gegevens zijn niet bestemd voor publieke bekendmaking zonder voorafgaande goedkeuring door de directie.

De standaard gevoeligheidsklasse van deze gegevens is "beperkt".

Voorbeelden: Interne telefoonlijst, notulen van een projectgroep.

III. Vertrouwelijke bedrijfsgegevens

Vertrouwelijke bedrijfsgegevens zijn alle gegevens die te maken hebben met de werking van de instelling en die binnen de context van de instelling - en mogelijk ook specifieke partners - een vertrouwelijk karakter hebben. Deze gegevens zijn niet bestemd voor mededeling zonder voorafgaande goedkeuring door de directie.

De standaard gevoeligheidsklasse van deze gegevens is “vertrouwelijk”.

Voorbeelden van vertrouwelijke gegevens: verslag van het directiecomité; boordtabellen, budgetramingen, begroting, lijsten van ziekenhuizen, lijsten van gezondheidsbeoefenaars, lijst van OCMW-voorzitters, … .

Synoniem : professionele gegevens

IV. Persoonsgegevens

Gegevens die betrekking hebben op een natuurlijke persoon die is of kan worden geïdentificeerd. Alle persoonsgegevens hebben een vertrouwelijk karakter en zijn gebonden aan de richtlijnen uit de Europese verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. (1)

De standaard gevoeligheidsklasse van deze gegevens is “vertrouwelijk

(1) (AVG regelgeving) "persoonsgegevens": 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;

V. Sociale persoonsgegevens

“Sociale gegevens van persoonlijke aard [(1)]” zijn alle persoonsgegevens die nodig zijn voor de toepassing van de sociale zekerheid met betrekking tot een natuurlijke persoon. Sociale gegevens die geen persoonsgegevens zijn dienen minstens als vertrouwelijke bedrijfsgegevens te worden behandeld.

De standaard gevoeligheidsklasse van deze gegevens is “vertrouwelijk”.

(1) Wet van 15 januari1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, art. 2, 6°.

Synoniem : sociale gegevens van persoonlijke aard

VI. Medische persoonsgegevens

“Sociale gegevens van persoonlijke aard die de gezondheid betreffen”[(1)] zijn alle sociale persoonsgegevens waaruit informatie kan afgeleid worden over de vroegere, huidige of toekomstige gezondheidstoestand, uitgezonderd louter administratieve of boekhoudkundige gegevens over geneeskundige behandelingen of verzorgingen. De behandeling, uitwisseling en bewaring van deze gegevens moet gebeuren onder toezicht en verantwoordelijkheid van een geneesheer[(2)].

De gevoeligheidsklasse van deze gegevens is “geheim”.

(1) Wet van 15 januari 1990 houdende oprichting van een Kruispuntbank van de sociale zekerheid, art.2, 7°

(2) [1] Wet van 15 januari 1990 houdende oprichting van een Kruispuntbank van de sociale zekerheid, art.26, §1

Opmerking :

- Definitie AVG (Art4) : "gegevens over gezondheid": persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;
- Zie ook NOTA MEDSEC

VII Administratief medische gegevens

Het zijn de louter administratieve of boekhoudkundige gegevens uit de wet van 21 augustus 2008 of dus alle medische gegevens niet behorende tot de ‘medische persoonsgegevens’ (zie ook BLD MEDSEC hoofdstuk 2)

De standaard gevoeligheidsklasse van deze gegevens is “vertrouwelijk”.

VIII Geclassificeerde gegevens (wet 11/12/1998)

De wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen legt de criteria vast voor de classificatie van de documenten die betrekking hebben op de veiligheid van het grondgebied, alsook de bevoegdheden en verantwoordelijkheden van de ambtenaren die ertoe gerechtigd zijn om ze te hanteren.

De gevoeligheidsklassen van deze gegevens zijn "zeer geheim", "geheim", "vertrouwelijk".

IX Privégegevens

Deze speciale categorie betreft privégegevens die door medewerkers opgeslagen kunnen worden op het netwerk van de instelling, doch geen enkele binding hebben met hun professionele activiteiten. Persoonlijke gegevens worden behandeld volgens de regels van de privacyverordening en het interne reglement van de instelling.

De standaard gevoeligheidsklasse van deze gegevens is "vertrouwelijk".

Voorbeeld: brief voor privédoeleinden, privé-e-mails, bestanden met betrekking tot het beheer van de persoonlijke loopbaan,

X Bijzondere categorieën van persoonsgegevens

(Art 9 AVG) Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

De gevoeligheidsklasse van deze gegevens is "geheim".

Synoniem : bijzondere persoonsgegevens'

XI Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

(Art 10 AVG) Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

De gevoeligheidsklasse van deze gegevens is "geheim".

XII. Zeer vertrouwelijke bedrijfsgegevens

Zeer vertrouwelijke bedrijfsgegevens zijn alle gegevens die te maken hebben met de werking van de instelling en die binnen de context van de instelling - en mogelijk ook specifieke partners - een zeer vertrouwelijk karakter hebben.

De standaard gevoeligheidsklasse van deze gegevens is "zeer vertrouwelijk".

Voorbeelden van zeer vertrouwelijke gegevens: de configuratie van de ICT infrastructuur bij data centers

Opmerking : **gevoelige persoonsgegevens** is de verzamelnaam voor medische persoonsgegevens, bijzondere categorieën van persoonsgegevens, persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.

Overzicht type gegeven en de default gevoeligheidsklasse

Type gegevens (informatie) groepen	Gevoeligheidsklasse
1. PUBLIEKE GEGEVENS **I Publieke gegevens**	niet geklasseerd
2. INTERNE GEGEVENS **II. Interne gegevens**	beperkt
3. VERTROUWELIJKE GEGEVENS VAN DE ONDERNEMING **III. Vertrouwelijke bedrijfsgegevens**	vertrouwelijk
4. PERSOONSGEGEVENS **IV. Persoonsgegevens**	vertrouwelijk
5. SOCIALE PERSOONSGEGEVENS **V. Sociale persoonsgegevens (sociale gegevens van persoonlijke aard)**	vertrouwelijk
6. GEVOELIGE PERSOONSGEGEVENS **VI. Medische persoonsgegevens** **X Bijzondere categorieën van persoonsgegevens** **XI Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten**	zeer vertrouwelijk
7. ADMINISTRATIEF MEDISCHE GEGEVENS **VII Administratief medische gegevens**	vertrouwelijk
8. GECLASSIFICEERDE GEGEVENS (WET VAN 11/12/1998) **VIII Geclassificeerde gegevens (wet 11/12/1998)**	zeer geheim, geheim, vertrouwelijk
9. PRIVÉGEGEVENS **IX Privé gegevens**	vertrouwelijk
10. ZEER VERTROUWELIJKE GEGEVENS VAN DE ONDERNEMING **XII. Zeer vertrouwelijke bedrijfsgegevens**	zeer vertrouwelijk

2. TLP

Hieronder volgt een voorbeeld van een classificatie naar type van gegevens, eigen aan de context van informatie uitwisseling tussen instellingen.

“Traffic Light Protocol” (of kortweg TLP) is ontworpen om het uitwisselen van informatie op een veilige, gecontroleerde manier te laten verlopen en aan te moedigen. Het fundamentele concept is voor de afzender om aan te geven hoever ze willen dat hun informatie verspreid wordt buiten de directe ontvanger van de informatie.

Het protocol vereist dat wie informatie verstuurt er een kleurcode toekent aan elke informatie. Deze kleur geeft aan of en op welke wijze deze informatie verder verspreid mag worden. Wie informatie ontvangt en meent dat bepaalde informatie op een grotere schaal verspreid moet kunnen worden, moet daarvoor eerst de expliciete toestemming aan de afzender vragen.

Het TLP zorgt voor een simpel en intuïtief schema om aan te duiden wanneer en hoe gevoelig bepaalde informatie kan gedeeld worden binnen een gemeenschap. Het delen van deze informatie zorgt voor een meer frequente en doeltreffende samenwerking tussen de instelling en haar partners.

De kleuren en hun betekenissen zijn als volgt:

ROOD	**Informatie uitsluitend bestemd voor de rechtstreeks geadresseerden.** Bijvoorbeeld: enkel voor de aanwezigen op een vergadering, een directe ontvanger van een sms, e-mail of post.
ORANJE	**Informatie voor een organisatie, eventueel beperkt tot bepaalde personen van de organisatie** Bijvoorbeeld: informatie mag binnen de organisatie verspreid worden op een 'need-to-know' basis. De afzender heeft het recht om de grenzen van deze verspreiding te bepalen.
GROEN	**Informatie voor een gemeenschap, maar niet te verspreiden op het internet.** Bijvoorbeeld: het delen van informatie enkel binnen een bepaalde sector zonder deze op internet of buiten de sector te verspreiden
WIT	**Informatie die vrij en onbeperkt verspreid mag worden, voor zover de verspreiding niet strijdig is met de wet (bijvoorbeeld de wet op het auteursrecht)**

3. Informatie veiligheid

Hieronder volgt een voorbeeld van een classificatie naar type van informatieveiligheidscriteria:

- vertrouwelijkheid,
- integriteit en
- beschikbaarheid.

De onderscheiden niveaus van vertrouwelijkheid zijn:

- Niet geklasseerd: Alle informatie die algemeen toegankelijk is voor een ieder. Er is geen schending van deze classificatie mogelijk.
- Intern: Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen instelling(en). Vertrouwelijkheid is gering. Schending van deze classificatie kan enige (in)directe schade toebrengen.
- Vertrouwelijk: Informatie die alleen toegankelijk mag zijn voor een beperkte groep personen. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- Geheim: Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote schade toebrengen.

Niveau	Authenticatie	Autorisatie	Monitoring	Veiligheid / Privacy
Niet geklasseerd	Geen	Geen	Geen	Geen
Intern	Authenticatie 'basis' vereist. Sessie-time out na 15 min inactiviteit. Absolute sessie-time out na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'basis' nodig voor deblokkeren.	Autorisatie vereist (lid van organisatie).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 6 maanden	Outputvalidatie. Versleuteling tijdens transport buiten netwerk van instelling via transport- of berichtveiligheid. Kopieën van gegevens moeten net zo goed beschermd worden. Gegevens uit productie-omgeving worden niet gebruikt in Ontwikkel-, Test- en

Niveau	Authenticatie	Autorisatie	Monitoring	Veiligheid / Privacy
				Acceptatie-omgevingen tenzij deze zijn geanonimiseerd en de informatie eigenaar toestemming heeft gegeven.
Vertrouwelijk	Authenticatie 'midden' vereist. Sessie-time out na 15 min inactiviteit. Voor klant absolute sessie-time out na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'midden' nodig voor deblokkeren.	Autorisatie vereist (specifieke rol).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 2 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations binnen en buiten netwerk van instelling via berichtveiligheid. Kopieën van gegevens moeten minimaal net zo goed beveiligd worden. Aantal kopieën minimaliseren. Gegevens uit productieomgeving worden niet gebruikt in Ontwikkel- Test en Acceptatie-omgevingen tenzij deze zijn geanonimiseerd en de informatie eigenaar toestemming heeft gegeven.
Geheim	Authenticatie 'hoog' vereist. Sessie-time out na 15 min inactiviteit. Voor klant absolute sessie-time out na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen. Authenticatie 'hoog' nodig voor deblokkeren. Geen SSO toegestaan.	Autorisatie vereist (specifieke rol).	Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 10 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations via berichtbeveiliging. Versleutelde opslag van gegevens. Transport van gegevens minimaliseren. Alleen transport en opslag binnen vaste netwerk van Gemeente <gemeentenaam>. Geen kopieën toegestaan behalve voor beschikbaarheid.' Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.

De onderscheiden niveaus van integriteit zijn:

- Niet zeker: Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
- Beschermd: Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits)fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van deze classificatie kan enige (in)directe schade toebrengen
- Hoog: Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- Absoluut: Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen

Niveau	Authenticatie	Autorisatie	Monitoring	Veiligheid / Privacy
Niet zeker	Geen	Geen	Geen	Geen
Beschermd	Authenticatie 'basis' vereist.	Autorisatie vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van 6 maanden	Inputvalidatie. Controleren op mutatie tijdens transport. Transport- of berichtveiligheid. Gegevens: Versie van gebruikte gegevens is bekend. Na uitvoering van een service blijven gewijzigde gegevens consistent.
Hoog	Authenticatie 'midden' vereist.	Autorisatie vereist. 4-ogen principe vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van maximaal 2 jaar of langer bij een vermoed beveiligingsincident.	Inputvalidatie. Controleren op mutatie tijdens transport. Berichtbeveiliging. Gegevens: Versie van gebruikte gegevens is bekend. Wijzigingen alleen op bron. Na uitvoering van een service blijven gewijzigde gegevens consistent.
Absoluut	Authenticatie 'hoog' vereist. Geen SSO toegestaan.	Autorisatie vereist. 4-ogen principe vereist.	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of service. Monitoring-gegevens bewaren voor periode van minimaal 3 jaar bij een vermoed beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.	Inputvalidatie. Controleren op mutatie tijdens transport. Berichtveiligheid. Informatie wordt niet buiten bron opgeslagen (behalve voor beschikbaarheid) en niet buiten bron gewijzigd. Na uitvoering van een service blijven gewijzigde gegevens consistent.

De onderscheiden niveaus van beschikbaarheid zijn:

- Niet nodig: De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn Schending van beschikbaarheid heeft geen gevolgschade.
- Noodzakelijk: De informatie of service mag incidenteel uitvallen, het proces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van deze classificatie kan enige (in)directe schade toebrengen
- Belangrijk: De informatie of service mag bijna nooit uitvallen, het proces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.
- Essentieel: De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het kritische proces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van integriteit kan (zeer) grote schade toebrengen.

Niet nodig: Toepassingen: 99,5% beschikbaarheid op werkdagen tussen 7:00 en 19:00 Intranet: 99,5% beschikbaarheid op werkdagen tussen 7:00 en 19:00

Noodzakelijk	
Werktijden	Van 08:00 tot 17:00 uur op maandag t/m vrijdag behoudens algemeen erkende feestdagen.
Beschikbaar tijdens werkuren	99.6%
Beschikbaar buiten werkuren	96.1%
Aantal storingen	
3 minuten of korter	4 per maand
Langer dan 3 minuten	1 per maand

Belangrijk	
Werktijden	Van 07:00 tot 21:00 uur op maandag t/m vrijdag behoudens algemeen erkende feestdagen.
Beschikbaar tijdens werkuren	99.6%
Beschikbaar buiten werkuren	96.1%
Aantal storingen	
3 minuten of korter	2 per maand
Langer dan 3 minuten	1 per 2 maanden

Essentieel	
Werktijden	24 uur per dag, 7 dagen per week, behoudens gepland onderhoud
Beschikbaar	99.9%
Aantal storingen	
3 minuten of korter	1 per maand
Langer dan 3 minuten	1 per 6 maanden

Bijlage E: 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	

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