EU GDPR Roadmap Belgium

ACTIEPUNT 1 : screening en aanpassing regelgeving in het algemeen

CONTEXT EN DOELSTELLINGEN

- de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en andere relevante regelgeving in overeenstemming brengen met de Europese verordening (GDPR) en (gevolgen na te kijken door sociale inspectiediensten) richtlijn 216/80;
- indien nodig redactie van wettelijke bepalingen waarbij bijkomende uitzonderingen voor de publieke sector worden opgenomen (zie artikel 23 GDPR).

ACTIES EN TIMING

Acties **Rood: strategisch cruciaal om actie tijdig uit te voeren**	**Tijdsas**	**R**esponsible **C**onsulted **S**upportive **I**nformed
○ waar nodig aanpassing van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (verordening heeft directe werking) - de schrapping van de aangifte - de kennisgeving van veiligheidsincidenten - de controle- en sanctiebevoegdheid - de documentatieplicht inzake inventaris en gegevensbeschermingseffectbeoordeling - de bepalingen inzake raadpleging van en overleg en medewerking met de toezichthoudende autoriteit - het mechanisme van gedragscode en eventuele certificering - het statuut van de verantwoordelijke coördinator voor de persoonsgegevensbescherming (DPO) (behoud huidige cumul met de veiligheidsconsulent) - onderzoek en in voorkomend geval redactie van bijkomende wettelijke uitzonderingen voor de publieke sector en regels m.b.t. het (niet) opleggen van administratieve geldboeten voor de publieke sector - de mogelijkheid om bijkomende voorwaarden vast te stellen met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid....	K3 2017 (sommige aspecten vroeger?)	**R: FOD Justitie** C/S: CBPL / KSZ (algemeen bestuur & afdeling I&B) I: OISZ
○ de redesign van de CBPL en de sectorale comités (zie nota Ministerraad): versterking van de onafhankelijkheid, de taken en bevoegdheden van de toezichthoudende autoriteit & eventueel bijkomende bevoegdheden bij wet	K1 2018	**R: FOD Justitie** C/S: CBPL / KSZ (algemeen bestuur & afdeling I&B) I: OISZ

EU GDPR Roadmap Belgium

ACTIEPUNT 2 : screening en aanpassing regelgeving sociale en gezondheidssector

CONTEXT EN DOELSTELLINGEN

- relevante regelgeving in overeenstemming brengen met GDPR;
- indien nodig redactie van wettelijke bepalingen waarbij bijkomende uitzonderingen voor de sociale- en gezondheidssector worden opgenomen.

ACTIES EN TIMING

Acties	**Timing**	**Verantwoordelijk**
○ onderzoek conformiteit bestaande regelgeving en uitzonderingen; wijziging wettelijke referenties ○ screening/inventaris van te wijzigen artikelen/reglementering ○ intern/extern overleg over opportuniteit tot wijziging ○ redactie aanpassingen beëindigd ○ procedure doorlopen (adviezen, publicatie)	**K4 2017** Okt 2016 Nov 2016 Juni 2017 Dec 2017	**R: OISZ & KSZ afdeling I&B (elk voor eigen regelgeving)** S: KSZ/OISZ I: CBPL
○ onderzoek opportuniteit om artikel 23 van de GDPR toe te passen: de reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan (…) worden beperkt (…); dergelijke wettelijke uitzonderingen moeten specifieke bepalingen bevatten, zoals voorgeschreven in de GDPR ○ inventaris van mogelijke uitzonderingen ○ intern/extern overleg over opportuniteit tot wijziging ○ desgevallend redactie van bijkomende wettelijke uitzonderingen voor de sociale- en gezondheidssector, zoals inzake - de beperking van het recht op overdraagbaarheid; - **de kennisgeving van veiligheidsincidenten aan betrokkene.** ○ redactie aanpassingen beëindigd ○ procedure doorlopen (adviezen, publicatie)	**K4 2017** Okt 2016 Nov 2016 Juni 2017 Dec 2017	**R: KSZ afdeling I&B** C: CBPL I: OISZ
○ aanpassing van het koninklijk besluit van 12 augustus 1993 houdende de organisatie van de informatieveiligheid bij de instellingen van sociale zekerheid en van het koninklijk besluit van 20 september 2012 houdende de organisatie van de informatieveiligheid bij het eHealth-platform en houdende vaststelling van de opdrachten en de bevoegdheden van de geneesheer onder wiens toezicht en verantwoordelijkheid de verwerking van persoonsgegevens betreffende de gezondheid door het eHealth-platform gebeurt ○ inventaris van te wijzigen artikelen ○ intern/extern overleg over opportuniteit tot wijziging ○ redactie aanpassingen beëindigd ○ procedure doorlopen (adviezen, publicatie)	**K1 2018** Jan 2017 Feb 2017 Sep 2017 Maart 2018	**R: KSZ afdeling I&B** C: CBPL I: OISZ

EU GDPR Roadmap Belgium

ACTIEPUNT 3 : draaiboek voor alle instellingen in de sociale-en gezondheidssector

CONTEXT EN DOELSTELLINGEN

- opzetten/voorbereiden/aanpassen van geheel aan maatregelen om de nieuwe regelgeving tijdig en volledig te kunnen toepassen binnen de ganse sociale- en gezondheidssector;
- de verantwoordelijke voor de verwerking zal voortaan op een objectieve wijze de waarschijnlijkheid en de ernst moeten inschatten van de risico's voor de rechten en vrijheden van personen wanneer hij een verwerking uitvoert ; hij staat ten volle in voor de effectieve naleving van de regels en is aansprakelijk ten opzichte van de controleautoriteiten alsook van de betrokkenen voor de daartoe genomen maatregelen.

ACTIES EN TIMING

Acties	**Timing**	**Verantwoordelijk**
○ **de sensibilisering van de stafleden van betrokken instellingen (privacy awareness)** ○ **Rol van DPO** ▪ **Link tussen veiligheidsconsulent (CISO) en privacy officer (DPO)** ○ **"EU GDPR for dummies"** ○ **Meldingsplicht**	K1 – K4 2017	**R: KSZ (algemeen bestuur & afdeling I&B) & OISZ**
○ **concretisering van de nieuwe benadering gebaseerd op risico; vaststellen van het risiconiveau van de verwerkingen binnen de sector** ○ **Privacy Risk Management minimale aanpak**	K1 2017 Feb 2017	**R: KSZ afdeling Veiligheid** S: OISZ (overleg binnen werkgroep informatieveiligheid) C: CBPL (overleg binnen Europees Comité voor gegevensbescherming)
○ **CBPL moet een lijst opstellen van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling verplicht is en kan een lijst opstellen van het soort verwerking waarvoor geen gegevensbeschermingseffectbeoordeling is vereist** ○ **een template en instructies m.b.t. de gegevensbeschermingseffectbeoordeling (met inachtname van de in de GDPR opgenomen uitzonderingen)** **accent op de verplichting van een voorafgaande gegevensbeschermingseffectbeoordeling voor bepaalde verwerkingen die beschouwd worden als gevoeliger en op de maatregelen die kunnen worden genomen om deze risico's te verminderen; ingeval deze voorafgaande analyse leidt tot het detecteren van bijzondere risico's zal de verantwoordelijke ertoe gehouden zijn de CBPL te raadplegen alvorens van start te gaan met de verwerking** **Met een template en instructies voor de documentatieplicht**	K3 2017 K1 2018 Eerste draft eind dec 2016 Finale versie eind dec 2017	**R: CBPL** I: KSZ/ OISZ **R: KSZ afdeling Veiligheid** S: OISZ (overleg binnen werkgroep informatieveiligheid) I: CBPL
○ **in voorkomend geval actualiseren/redactie policies inzake het verzamelen, vernietigen, opslaan en opzoeken van persoonsgegevens en verdere verwerking voor andere doeleinden(nieuw!) in overeenstemming met de beginselen van de GDPR**	K1 2018 Eerste drafts eind	**R: KSZ afdeling Veiligheid & OISZ (werkgroep informatieveiligheid:**

○ **in voorkomend geval actualiseren veiligheidspolicies (waaronder policies m.b.t. loggings, testen, monitoring, helpdesk)** **enkele voorbeelden van beveiligingsmaatregelen die door de GDPR gegeven worden zijn de pseudonimisering, versleuteling, het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen, het vermogen om bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen en procedures voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen** ○ **actualiseren richtlijnen en referentiemaatregelen CBPL**	dec 2017 Finale versie eind april 2018	**taakverdeling op basis van de policies, waarop de EU GDPR een impact** **R: CBPL** I: KSZ
○ **een policy inzake de beheersing, behandeling en de kennisgeving van inbreuken in verband met persoonsgegevens (rekening houdend met evt bijkomende wettelijke uitzonderingen t.a.v. betrokkene; zie actiepunten 1 en 2) – te integreren in een ruimere benadering rond veiligheidsincidenten** **indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de bevoegde toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen** **indien een inbreuk in verband met persoonsgegevens waarschijnlijk <u>een hoog risico</u> inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de <u>betrokkene</u> de inbreuk in verband met persoonsgegevens onverwijld mee (met diverse uitzonderingen)** ○ **een policy inzake het beheer van verwerkers** ○ **een template met instructies voor de contractuele bepalingen** ○ **een template met instructies voor het uitvoeren van een simulatie van inbreuk** ○ **een policy inzake leveranciersbeheer en controle** ○ **template met instructies voor het contacteren van externe leveranciers die toegang hebben tot persoonsgegevens** ○ **principes en regels inzake de melding en de bijstand bij inbreuken in verband met persoonsgegevens**	K2 2018 Eerste draft eind dec 2017 Finale versie eind april 2018	**R: KSZ afdeling Veiligheid** S: OISZ (overleg binnen werkgroep informatieveiligheid) I: CBPL
○ **het vastleggen van principes en regels om een privacy audit uit te voeren om de zwakkere schakels te ontdekken en concrete acties voor te dragen aan beslissingsnemers.** **Samen uit te werken met de contractuele bepalingen inzake verwerkers**	K2 2018 Finale versie eind mei 2018	**R: KSZ afdeling Veiligheid & OISZ (taakverdeling binnen werkgroep informatieveiligheid)**
Pro memorie ○ **het desgevallend opstellen van gedragscode**	K2 2018 Te beoordelen	**R: KSZ afdeling Veiligheid & OISZ (taakverdeling binnen werkgroep informatieveiligheid)**

EU GDPR Roadmap Belgium

ACTIEPUNT 4 : specifieke maatregelen door elke instelling in de sociale-en gezondheidssector

CONTEXT EN DOELSTELLINGEN:

- in overleg met DPO opzetten/voorbereiden/aanpassen van geheel aan maatregelen om de nieuwe regelgeving tijdig en volledig te kunnen toepassen binnen betrokken instelling.

ACTIES EN TIMING:

Acties	**Timing**	**Verantwoordelijk**
○ lopende verwerkingen in lijn brengen met de GDPR	K1 2018	**R: OISZ**
○ **voorbereiden van een policy hoe kan bewezen worden dat voldaan wordt aan de vereiste standaarden (verantwoordingsplicht)** **de verantwoordelijke voor de verwerking is verantwoordelijk voor de conformiteit met de beginselen van de GDPR en moet die conformiteit ook kunnen aantonen**	K1 2018 Eerste draft eind dec 2016 Finale versie eind dec 2017	**R: OISZ (overleg binnen werkgroep informatieveiligheid)** S: KSZ afdeling Veiligheid
○ implementeren van de documentatie/register (inventaris van persoonsgegevens in processen en inventaris van de gegevensbeschermingseffectbeoordelingen), die kan opgevraagd worden door de toezichthoudende autoriteit	K1 2018	**R: OISZ/KSZ**
○ voorbereiden van een procescultuur met interne beleidsmaatregelen die voldoen aan de beginselen van persoonsgegevensbescherming ("privacy by design") passende technische en organisatorische maatregelen nemen rekening houdend met aard en risico's van verwerking en alleen persoonsgegevens verwerken die noodzakelijk zijn voor de doeleinden; maatregelen zouden onder meer kunnen bestaan in het minimaliseren van de verwerking van persoonsgegevens, het zo spoedig mogelijk pseudonimiseren van persoonsgegevens, transparantie met betrekking tot de functies en de verwerking van persoonsgegevens, het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking en uit het in staat stellen van de verwerkingsverantwoordelijke om beveiligingskenmerken te creëren en te verbeteren	K1 2018	**R: OISZ/KSZ**
○ documenteren van alle inbreuken in verband met persoonsgegevens, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen	K2 2018	**R: OISZ/KSZ**
○ aanduiding van een verantwoordelijke coördinator voor persoonsgegevensverwerking (DPO) - continuïteit	K2 2018	**R: OISZ/KSZ**

ACTIEPUNT 5 : beleid voor communicatie met betrokkenen

CONTEXT EN DOELSTELLINGEN

- het moet voor burgers transparant zijn dat de hen betreffende gegevens zijn ingezameld, gebruikt, geraadpleegd of anders verwerkt. Het transparantiebeginsel vereist dat alle informatie of communicatie met betrekking tot een gegevensverwerking gemakkelijk toegankelijk moet zijn en gemakkelijk te begrijpen. Er moet dus gebruik gemaakt worden van een duidelijke en eenvoudige taal. Dit gaat in het bijzonder over de verstrekte informatie over de identiteit van de verantwoordelijke voor de verwerking en de doeleinden van de verwerking. Dit gaat eveneens over de bijkomende informatie die kan verstrekt worden zodat een gerechtvaardigde en transparante verwerking verzekerd is;
- de burgers moeten verwittigd worden van de risico's, de regels, garanties en rechten die verband houden met de verwerking alsook de manier om hun rechten uit te oefenen.

ACTIES EN TIMING

Acties	**Timing**	**Verantwoordelijk**
○ **Onderzoek impact en methodologie vastleggen** (rekening houdend met uitzonderingen verordening en eventuele bijkomende wettelijke uitzonderingen; zie actiepunten 1 en 2) versterking rechten van betrokkene (recht op informatie en toegang, recht op rechtzetting en gegevensverwijdering, recht op beperking van de verwerking, recht op overdraagbaarheid van de gegevens, recht van bezwaar)	K4 2017	**R: OISZ (geval per geval)**
○ voorbereiden van een policy voor communicatie met betrokkenen meer volledige informatieverstrekking en kennisgevingsplicht, evenals gewijzigde termijnen onderscheid naargelang rechtstreekse/onrechtstreekse inzameling en gevallen van informatievrijstelling of collectieve informatieverstrekking	K1 2018	**R: OISZ (geval per geval)**
○ vastleggen informatie en procedures gestandaardiseerde iconen	K4 2018	**R: gedelegeerde handelingen Europese Commissie?** I: CBPL, KSZ &OISZ

ACTIEPUNT 6 : aanpassing antwoorden / formulieren / contracten

CONTEXT EN DOELSTELLINGEN:

- de bestaande antwoorden, formulieren, contracten aanpassen aan nieuwe bepalingen GDPR.

ACTIES EN TIMING:

Acties	**Timing**	**Verantwoordelijk**
o aanpassing modelantwoorden aan burgers	K2 2018	**R: OISZ (geval per geval)**
o elektronisch klachtenformulier	K2 2018	**R: CBPL** I: KSZ &OISZ
o voorstel of goedkeuring modelcontractbepalingen tussen verwerkingsverantwoordelijke en verwerker (art. 28.3 verordening)	K2 2018	**R: OISZ**