GDPR en de beveiliging van (patiënten)gegevens: wat moet er gebeuren?


frank.robben@ksz.fgov.be


@FrRobben

https://www.ehealth.fgov.be
https://www.ksz.fgov.be
https://www.frankrobben.be

AVG of GDPR

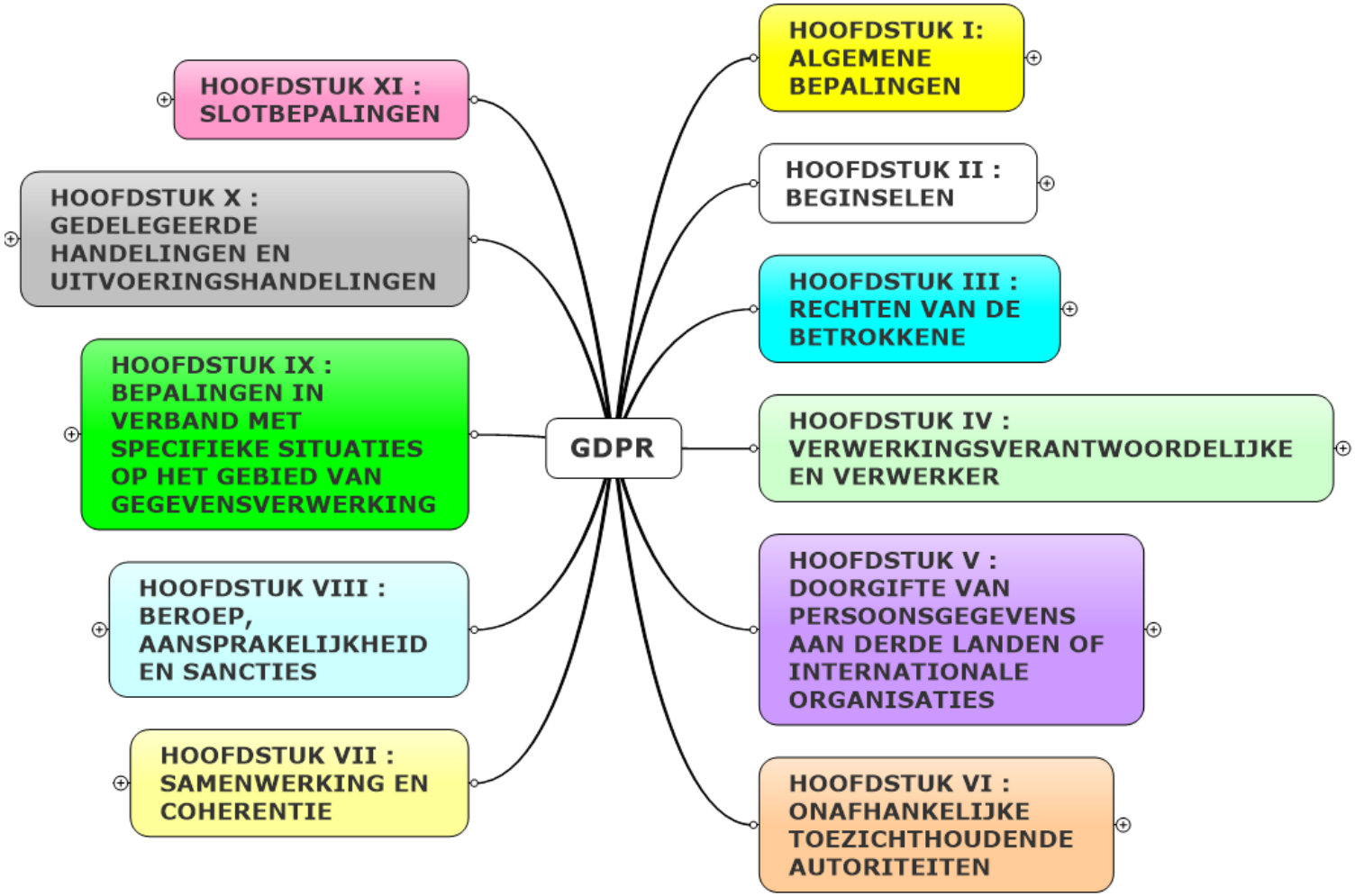
- Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016, afgekort als
  - Algemene Verordening Gegevensbescherming (AVG)
  - General Data Protection Regulation (GDPR)

- Verordening => rechtstreekse toepasselijk zonder dat omzetting in nationaal recht nodig is

- van toepassing vanaf 25 mei 2018

- wel aantal aanpassingen nodig in nationale regelgeving

Overzicht AVG of GDPR



Bevestiging geldende beginselen

- rechtmatige, eerlijke en transparante verwerking
- doelbindingsbeginsel
  - persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen niet verder op een met die doeleinden onverenigbare wijze worden verwerkt
- evenredigheidsbeginsel
  - persoonsgegevens moeten toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor het doeleinde waarvoor de gegevens worden verwerkt
  - de gegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren en niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt
- juistheidsbeginsel
  - persoonsgegevens moeten juist zijn en zo nodig bijgewerkt

Verwerking van gezondheidsgegevens

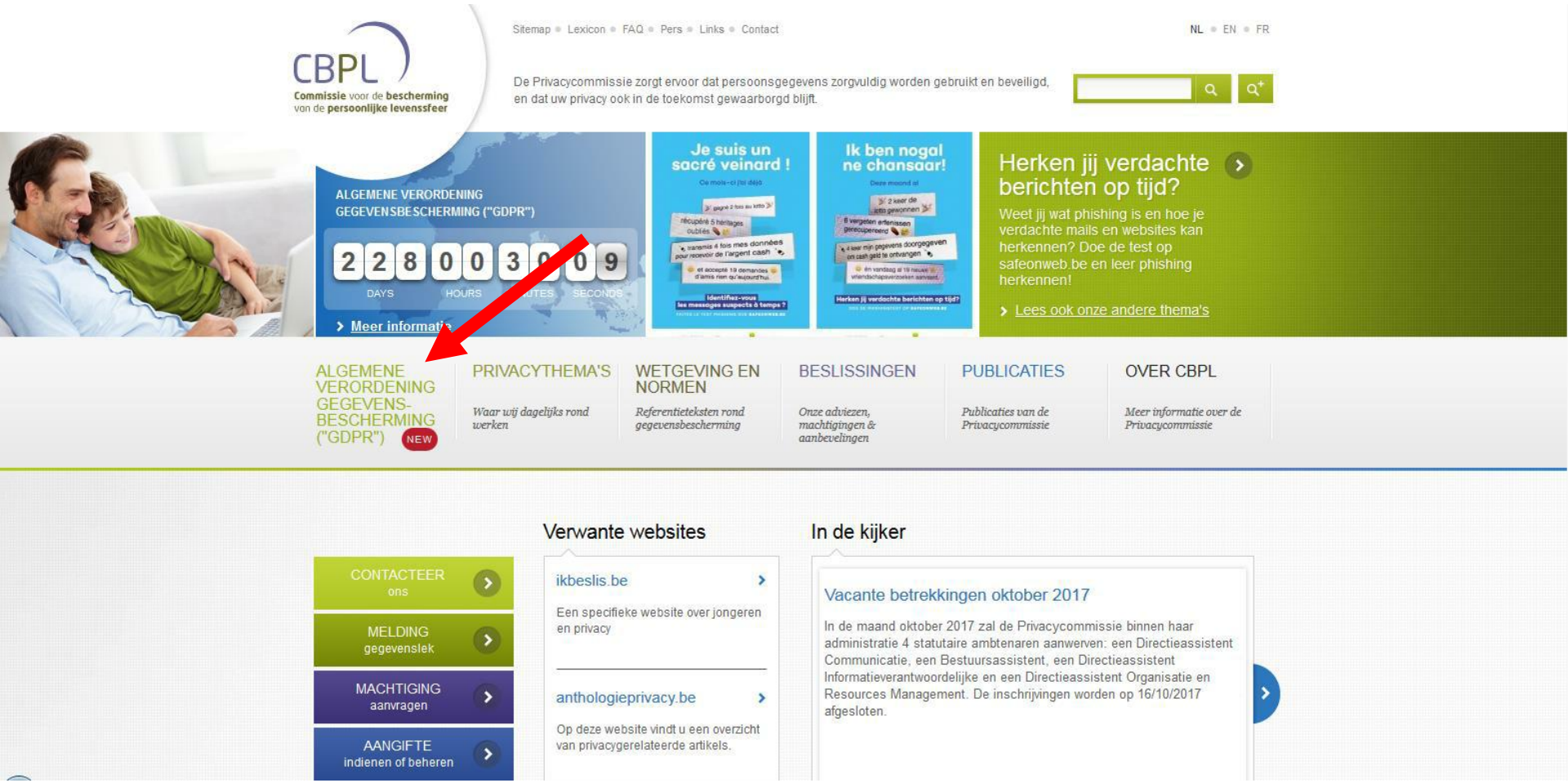
- ruime definitie, geen teleologische benadering
  - persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven
- verwerkingsgronden, onder meer
  - uitdrukkelijke toestemming van betrokkene
  - sociaalzekerheidsrechtelijke of arbeidsrechtelijke verplichtingen
  - redenen van zwaarwegend algemeen belang, waaronder volksgezondheid, sociale bescherming en beheer van gezondheidszorgdiensten
  - preventieve of arbeidsgeneeskunde, beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, verstrekken van gezondheidszorg of sociale diensten of behandelingen, beheren van gezondheidszorgstelsels en -diensten of sociale stelsels en diensten; in dit geval door of onder de verantwoordelijkheid van een beroepsbeoefenaar die aan het beroepsgeheim is gebonden

Aantal nieuwigheden

- risico-analyse als basis
- verantwoordingsplicht van de verwerkings-verantwoordelijke
  - register van verwerkingsactiviteiten
  - gegevensbeschermingseffectbeoordeling
- privacy by design
- privacy by default
- kennisgeving veiligheidsincidenten
- uitbreiding van de rechten van de betrokken
- functionaris van de gegevensbescherming
- mogelijkheid van gedragscodes en certificering
- sancties

Geen “one-size-fits-all” benadering

Voorstel van actieplan



https://privacycommission.be/

ALGEMENE VERORDENING GEGEVENSBESCHERMING

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

Roadmap & templates sociale sector

Links naar relevante bronnen

De originele tekst rond de EU GDPR

Verdere informatie van de Europese Commissie rond de EU GDPR

- EU GDPR factsheets
- Verduidelijking rond de overdraagbaarheid van gegevens
- Verduidelijking rond de functionaris voor gegevensbescherming (DPO)
- Verduidelijking rond identificatie van de 'verwerkingsverantwoordelijke' of 'leidende toezichthoudende autoriteit'
- Verduidelijking rond de gegevensbeschermingsimpactbeoordeling (DPIA)
- Publicatie van persoonlijke gegevens voor transparantiedoeleinden in de publieke sector
- Toolkit van EDPS rond beperkingen omtrent de bescherming van persoonlijke gegevens
- DPO Corner + suggesties (Engelstalig)
- Gegevensbescherming (Infographic)

Belgische commissie voor de bescherming van de persoonlijke levenssfeer (CBPL)

- specifieke pagina rond EU GDPR
- stappenplan voor de implementatie de EU GDPR
- ontwerp van aanbeveling uit eigen beweging uitgebracht met betrekking tot de gegevensbeschermingseffectbeoordeling ('data protection impact assessment' of 'DPIA')
- aanbeveling over de aanwijzing van de DPO en de toelaatbaarheid van de cumulatie van DPO met andere functies waaronder die van veiligheidsconsulent

KSZ

- roadmap voor de implementatie van de EU GDPR
- minimale normen voor informatieveiligheid aangepast en ook in overeenstemming gebracht met de EU GDPR

Templates

Ter inspiratie vindt u hier voorbeelden en templates bruikbaar bij de EU AVG (GDPR) compliance activiteiten. Het blijft uiteraard ten allen tijde de volledige verantwoordelijkheid van elke instelling om te voldoen aan de EU AVG (GDPR) regelgeving.

- Record registers 2017
- AVG Risk register 2017 (DPIA)

https://www.ksz-bcss.fgov.be/nl/veiligheid-en-privacy/general-data-protection-regulation

Meer gedetailleerde presentatie

KSZ BCSS

ALGEMENE VERORDENING GEGEVENSBESCHERMING

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

Hoofdlijnen voor de sociale- en gezondheidssector

Kruispuntbank van de Sociale Zekerheid
Willebroekkaai 38
B-1000 Brussel
Website KSZ: www.ksz-bcss.fgov.be

09/2015

https://www.frankrobben.be/wp-content/uploads/2016/08/20160610nl.pptx

1. Bewustmaking

Zorg dat de sleutelfiguren en beleidsmakers in je organisatie op de hoogte zijn van de nieuwe regelgeving. Zij moeten de gevolgen hiervan inschatten en aanwijzen welke domeinen vandaag mogelijks problematisch kunnen zijn in het licht van de AVG. Indien je organisatie over een risicoanalyse beschikt, kan dit een werkbaar vertrekpunt zijn.

Het implementeren van de AVG kan een behoorlijke invloed hebben op de beschikbare middelen, zeker voor wat betreft grote en meer complexe organisaties.

Gebruik de overgangsperiode dus allereerst om medewerkers te informeren over de aankomende veranderingen. Stel dit niet uit tot de laatste minuut.

2. Register van verwerkingsactiviteiten

Breng zorgvuldig in kaart welke persoonsgegevens je verwerkt, waar deze vandaan komen en met wie je deze deelt. Je doet er goed aan al je verwerkingen te registreren. Mogelijks dien je hiervoor een informatie-audit te organiseren in je organisatie of bepaalde afdelingen ervan.

De AVG introduceert enkele nieuwe verplichtingen, specifiek op maat van de netwerkwereld. Wanneer je bv. onnauwkeurige persoonsgegevens bijhoudt, en hebt gedeeld met andere organisaties, zal je deze laatsten moeten inlichten over de onnauwkeurigheid zodat deze een correctie kan aanbrengen in haar eigen verwerking.

De documentatieplicht helpt je de verantwoordingsplicht na te leven. Daarmee wordt de plicht bedoeld van een organisatie om te bewijzen dat ze handelt in overeenstemming met de gegevensbeschermingsprincipes.

3. Wettelijke grondslag voor verwerking

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en bepaal de wettelijke grondslag voor elk van hen. Ook dit helpt je te voldoen aan de verantwoordingsvereiste.

De rechten van de betrokkene variëren naargelang de wettelijke grondslag van de gegevensverwerking. Het meest voor de hand liggend voorbeeld is dat de betrokkene een sterker recht heeft om de verwijdering van zijn gegevens te vragen indien zijn toestemming aan de grondslag ligt van de verwerking.

Het is belangrijk om de gekozen wettelijke grondslag voor de gegevensverwerking te verduidelijken in de privacyverklaring en telkens wanneer je een toegangsverzoek beantwoordt. De wettelijke grondslagen in de AVG zijn quasi identiek aan deze in de huidige Privacywet.

Omschrijving verwerking	Vewerkende dienst (cel,…)	Doel van de verwerking	Bron(nen)		Toepassing/Databank/Platform
			Binnen de organisatie	Buiten de organisatie	

Over welk type gegevens gaat het?					
Persoonsgegevens		Gevoelige persoonsgegevens		Andere gegevens	
Over wie?	Welke gegevens?	Over wie?	Welke gegevens?	Waarover?	Welke?

Rechtsgrond van de verwerking		Met wie wordt de informatie gedeeld?	
Welke rechtsgrond (kies uit dropdown menu)	Verduidelijk (Welke wet, geef contract mee, …)	Binnen onze organisatie?	Buiten onze organisatie?

Bewaartermijn	Risicobeperkende maatregelen

4. Toestemming van betrokkene

Als de wettelijke grondslag voor de verwerking de toestemming van de betrokkene is, evalueer de wijze waarop je de toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

De toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig moet zijn. De toestemming moet ook blijken uit een actieve indicatie van akkoord. M.a.w. de toestemming kan niet worden afgeleid uit een stilzwijgen, een vooraf aangevinkt vakje of uit een niet-handelen.

Indien je rekent op de toestemming van de betrokkene om diens gegevens te verwerken, zorg dan zeker dat die toestemming voldoet aan de vereisten van de AVG.

Indien dit nu nog niet het geval is, wijzig dan je toestemmingsmechanisme of ga op zoek naar een alternatief voor toestemming als grondslag voor de gegevensverwerking.

4. Toestemming van betrokkene

Noteer dat de toestemming controleerbaar moet zijn en dat de betrokkene doorgaans meer rechten heeft wanneer je vertrouwt op toestemming als grondslag voor de gegevensverwerking.

De AVG verduidelijkt dat de verwerkingsverantwoordelijke in staat moet zijn om aan te tonen dat toestemming werd gegeven. Evalueer dus de huidige systemen die toestemming registreren, teneinde een audit trail (controlespoor) te verzekeren.

5. Toestemming namens kinderen

Als je organisatie gegevens over kinderen onder de 16 jaar verwerkt op basis van de toestemming van de betrokkene, moet een ouder of voogd deze toestemming geven opdat de gegevensverwerking rechtmatig zou zijn. De AVG biedt speciale bescherming aan gegevens van kinderen, o.a. in de context van commerciële internetdiensten als sociale netwerken.

Dit kan aanzienlijke gevolgen hebben als je organisatie gericht is op het aanbieden van diensten aan kinderen en daartoe hun persoonsgegevens verwerkt. Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder of voogd om toestemming vragen voor de verwerking van persoonsgegevens over kinderen.

Onthoud dat de toestemming controleerbaar moet zijn en dat desgevallend de privacyverklaring moet geschreven zijn in voor kinderen begrijpbare taal.

6. Transparantie tov de betrokkene

Wanneer je organisatie persoonsgegevens verwerkt, dient ze aan de betrokkene bepaalde informatie te verschaffen, zoals de doeleinden waarvoor de gegevens worden verwerkt. Doorgaans wordt deze informatie verstrekt in de vorm van een privacyverklaring.

Evalueer de bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

De AVG vereist dat deze privacyverklaring wordt aangevuld met nieuwe informatietypes. Zo zal je voortaan de wettelijke grondslag voor de gegevensverwerking moeten meedelen, de termijnen gedurende dewelke je de informatie zal bijhouden, of je de gegevens uitwisselt buiten de EU en de mogelijkheid voor de betrokkene om een klacht in te dienen bij de Privacycommissie indien deze meent dat zijn persoonsgegevens foutief worden verwerkt.

De AVG vereist dat deze informatie wordt verschaft in beknopte, begrijpbare en duidelijke taal.

7. Rechten van de betrokkene

Ga na of de huidige procedures in je organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld. De AVG voorziet o.a. in de volgende rechten voor de betrokkene

- informatie en toegang tot persoonsgegevens
- verbetering en uitwissing van de gegevens
- bezwaar tegen direct marketingpraktijken
- bezwaar tegen geautomatiseerde besluitvorming en profilering
- overdraagbaarheid van de gegevens (niet voor verwerking voor taak van algemeen belang of openbaar gezag)

7. Rechten van de betrokkene

De betrokkene geniet onder de AVG dezelfde rechten als onder de huidige Belgische Privacywet, mits enkele aanzienlijke verbeteringen. Het is een goed moment om je bestaande procedures te evalueren en na te gaan hoe je voortaan te werk zal gaan wanneer iemand zijn of haar recht wil uitoefenen.

Het recht op overdraagbaarheid van de gegevens is een nieuwigheid. Dit is een verbeterde vorm van toegang waarbij de betrokkene het recht heeft de persoonsgegevens die op hem van toepassing zijn in een gestructureerde, gangbare en elektronische vorm te verkrijgen.

8. Verzoek tot toegang

Voorzie een update van je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang zal behandelen onder de nieuwe termijnen in de AVG.

In de meeste gevallen zal gratis en binnen de 30 dagen (i.t.t. de huidige termijn van 45 dagen) gevolg moeten worden gegeven aan het verzoek tot toegang. Manifest ongegronde of overmatige verzoeken kunnen worden aangerekend of worden geweigerd.

Je dient de betrokkene die om toegang verzoekt bepaalde bijkomstige informatie te verschaffen, zoals de termijnen gedurende dewelke je informatie bijhoudt en het recht om onnauwkeurige gegevens te laten verbeteren. Het moet logistiek mogelijk zijn om alle verzoeken binnen de voorziene tijdspanne te verwerken en de betrokkene van de noodzakelijke informatie te voorzien.

Het kan kostenbesparend zijn een systeem te ontwikkelen dat de betrokkene in staat stelt de gegevens zelf online te raadplegen.

9. Privacy by design & PIA

Maak je vertrouwd met de begrippen “gegevensbescherming door ontwerp” en “gegevensbeschermingseffectbeoordeling”, beter gekend als Privacy by design en Privacy impact assessment (PIA). Ga na hoe je deze concepten in de werking van je organisatie kan implementeren. Deze kunnen worden gelinkt aan andere organisatorische processen zoals risicobeheer en projectbeheer. Beoordeel de situaties waarin het nodig is dergelijke beoordeling uit te voeren. Wie zal dit doen? Wie moet hierbij worden betrokken? Gebeurt de analyse centraal of lokaal?

Het behoort tot de “good practices” van een organisatie om gegevensbescherming van bij de start in te bouwen en als onderdeel hiervan een risicobeoordeling uit te voeren. Dit was voordien slechts een impliciete vereiste van de gegevens-beschermingsprincipes. De AVG maakt hiervan een duidelijke wettelijke vereiste.

9. Privacy by design & PIA

Noteer dat je niet steeds een gegevensbeschermingseffect-beoordeling moet uitvoeren. Deze is enkel vereist in hoge risicosituaties, bv. wanneer een nieuwe technologie wordt geïmplementeerd of wanneer een profileringsoperatie een aanzienlijk effect kan teweegbrengen voor de betrokkenen. Deze verplichting geldt niet voor individuele zorgprofessionals. Een nieuwe beoordeling is niet noodzakelijk wanneer verwerking gerechtvaardigd wordt door de noodzaak een wettelijke verplichting na te leven of wordt uitgevoerd in het algemeen belang indien deze reeds werd uitgevoerd bij de goedkeuring van de wettelijke basis.

Wanneer de PIA aangeeft dat de gegevensverwerking een hoog restrisico inhoudt, is het noodzakelijk het advies in te winnen van de Privacycommissie omtrent de rechtmatigheid van de verwerking in het licht van de AVG.

10. Melding van ‘data breaches’

Voorzie adequate procedures om veiligheidsincidenten met persoonsgegevens op te sporen, te rapporteren en te onderzoeken.

Beoordeel hiervoor de verscheidene verwerkingen die je uitvoert en documenteer welke binnen de meldingsplicht zouden vallen, ingeval zich een incident zou voordoen.

In sommige gevallen moet je de betrokkene die het voorwerp uitmaakt van het incident rechtstreeks verwittigen, bv. wanneer het incident aanleiding kan geven tot persoonlijke financiële verliezen.

Grotere organisaties zullen een beleid en procedures moeten ontwikkelen om incidenten te beheren – hetzij op centraal, hetzij op lokaal niveau.

10. Melding van ‘data breaches’

Niet alle incidenten zullen moeten worden gemeld aan de Privacycommissie – enkel deze waarbij het waarschijnlijk is dat de betrokkene enige vorm van schade zal leiden, bv. als gevolg van een identiteitsdiefstal of het schenden van een geheimhoudingsplicht.

Noteer dat de niet naleving van de meldplicht kan resulteren in een geldboete, bovenop de boete voor het datalek zelf.

11. Functionaris gegevensbescherming

Ga na of je een functionaris voor gegevensbescherming moet of wil aanduiden, die specifiek bijdraagt tot het naleven van de gegevensbeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van je organisatie.

De AVG vereist voor sommige organisaties dat zij een functionaris voor gegevensbescherming aanwijzen, bv. voor openbare overheden of verwerkers wiens taak bestaat uit het regelmatig en stelselmatig observeren van betrokkenen op grote schaal.

Algemeen is het van belang dat hetzij iemand in de organisatie, hetzij een externe adviseur bijdraagt tot en toeziet op het naleven van de gegevensbeschermingsprincipes. Hij/zij dient de kennis, medewerking, tijd en bevoegdheid te hebben om dit te doen.

12. Contracten met verwerkers

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de nodige veranderingen aan. De AVG creëert een intelligent systeem dat de verhouding tussen de verwerkingsverantwoordelijke en de verwerkers behelst. Het bepaalt zelfs de voorwaarden die van toepassing zijn op onderaannemingsactiviteiten. Opdat hieraan zou worden voldaan, moet je bestaande contracten beoordelen en de nodige wijzigingen aanbrengen.

De AVG benadrukt het belang van op gegevensverwerkingen toepasselijke veiligheidsmaatregelen. Ook in het geval van outsourcing of gebruik van clouddiensten is het belangrijk te beoordelen of de veiligheidsmaatregelen die werden voorzien in de bestaande contracten nog steeds toereikend zijn en voldoen aan de vereisten van de AVG.

13. Internationale aspecten

Indien je organisatie internationaal actief is, dien je te bepalen onder welke toezichthoudende autoriteit je valt.

De AVG voorziet een enigszins complexe regeling om te bepalen welke toezichthoudende autoriteit de leiding neemt bij het onderzoek naar een klacht met een internationaal karakter, bv. wanneer een gegevensverwerking betrekking heeft op inwoners van meerdere lidstaten. De leidende autoriteit wordt bepaald naargelang waar de organisatie haar hoofdvestiging heeft of de vestiging waar de beslissingen omtrent de gegevensverwerkingen worden genomen.

Voor een traditionele hoofdzetel is dit vrij eenvoudig vast te stellen. Moeilijker wordt het voor complexe, multi-site organisaties waarbij beslissingen omtrent diverse verwerkingsactiviteiten op verschillende plaatsen worden genomen.

13. Internationale aspecten

Om duidelijkheid te krijgen over welke toezichthoudende autoriteit de leiding heeft over je organisatie kan het raadzaam zijn in kaart te brengen waar jouw organisatie haar meest belangrijke beslissingen omtrent gegevensverwerkingen neemt. Dit zal je helpen bij het bepalen van de“hoofdvestiging” en dus ook van de bevoegde toezichthoudende autoriteit.

Concreet voor huisartsen

- bewustwording en ‘privacy by design’
- register van verwerkingsactiviteiten
- geen gebruik van persoonsgegevens buiten zorgverlening
- privacyverklaring op website, in wachtkamer, …
- contract met softwareleveranciers
- gebruik van diensten van eHealth-platform voor veilige gegevensuitwisseling
- respect van machtigingen van sectoraal comité gezondheid
- meldingsplicht bij data breaches
- nut van een gedragscode ?

frank.robben@ksz.fgov.be

@FrRobben

https://www.ehealth.fgov.be
https://www.ksz.fgov.be
https://www.frankrobben.be