HICT

Gegevensbeschermingsbeleid

[Updated: 23/12/2019]

OPTIMISING HEALTHCARE

1 Het belang van gegevensbescherming

Hict hecht grote waarde aan het juist beschermen van de gegevens die zij verwerkt, in het bijzonder persoonsgegevens. Middels dit beleid wil Hict op strategisch niveau vastleggen op welke wijze gegevens beschermd worden, welke verantwoordelijkheden hierrond zijn toegewezen en welke prioriteiten Hict heeft bepaald rond de bescherming van gegevens.

In het bijzonder wilt Hict de gegevens van klanten en de persoonsgegevens die zij ter beschikking stellen, beschermen tegen:

- Verlies: gegevens zijn niet meer beschikbaar
- Lekken: gegevens komen in verkeerde handen terecht
- Fouten: gegevens zijn niet correct, bijvoorbeeld verouderd of onvolledig
- Niet toegankelijk: op het moment van de zorg zijn gegevens niet toegankelijk
- Onterecht inkijken: ingekeken door personen die hiertoe niet gemachtigd zijn
- Het niet kunnen nagaan wie de gegevens inkeek, wijzigde of verwijderde

Verwerkingen die niet in lijn liggen met regelgeving, richtlijnen en normen

De directie wil in dit beleid een beroep doen op iedereen die betrokken is bij de elektronische en papieren verwerking om samen, vanuit een gemeenschappelijke visie én vanuit onze gezamenlijke wil om kwaliteitsvolle dienstverlening aan te bieden, de verwerking van persoonsgegevens van onze correct te laten verlopen.

Dit beleidshandboek gaat dieper in op de bescherming van de persoonlijke levenssfeer van en meer in het bijzonder, de informationele privacy. Dit beleidshandboek dient als norm voor het verwerken van de persoonsgegevens van de klanten en hun verzekerden door Hict. Het is een leidraad voor alle verwerkingsprocessen en biedt een referentienorm voor audit en controle. Het beleidshandboek biedt elke belanghebbende, medewerker of betrokken externe een inzage in het gegevensbeschermingsbeleid en de manier waarop we omgaan met gevoelige persoonsgegevens.

Het handboek is tevens geschreven voor iedereen die een functie heeft binnen Hict waarbij persoonsgegevens verwerkt worden. Ze gebruiken (delen van) dit beleidshandboek voor het ontwerpen van procedures en richtlijnen voor medewerkers en externen, zoals ICT-leveranciers. De relevante onderdelen van dit beleidshandboek worden verwerkt in overeenkomsten met personeel en leveranciers.

2 De organisatie van gegevensbescherming

Bevoegdheid

Als verantwoordelijke voor de verwerking, ligt de bevoegdheid van dit beleid bij Hict, vertegenwoordigd door haar directeur. De directeur is verantwoordelijk voor het formuleren en vaststellen van, en het toezien op, de naleving van de beleidsprincipes binnen Hict, hierbij ondersteund door de Directiecomité/ managementteam/ etc..

Verantwoordelijke uitvoerder

Het directiecomité fungeert als formeel beslissingsplatform voor gegevensbescherming. Het directiecomité is bevoegd om beslissingen te nemen die betrekking hebben op volgende aspecten:

- De risicoanalyse en bijhorende methodiek;
- Het ontwikkelen van het gegevensbeschermingsbeleid en de bijhorende richtlijnen;
- De implementatie van beveiligingsmaatregelen (i.e. de inhoud van het veiligheidsplan)
- De structurele reactie op gegevensbeschermingsproblemen en –adviezen (binnen de 3 maanden);

De DPO

De inhoudelijke opvolging van het gegevensbeschermingsbeleid ligt bij de Data Protection Officer (DPO). Hij/zij voert deze taak uit volgens de bepalingen in de GDPR . Hict geeft de identiteit (en eventuele wijzigingen) van de DPO door aan de gegevensbeschermingsautoriteit. De DPO rapporteert aan de directeur van Hict en is meer in het bijzonder belast met:

- Adviezen en aanbevelingen voorleggen aan het directiecomité
- Bevorderen van de bewustwording van alle actoren binnen Hict
- Ziet toe op de naleving van het gegevensbeschermingsbeleid binnen Hict
- Documenteert het nodige rond gegevensbescherming, zoals een veiligheidsplan en het verwerkingsregister
- Voert de specifieke taken uit die aan de DPO zijn toegekend in het kader van de GDPR
- Registreert overtredingen en maakt deze, samen met een advies, over aan het directiecomité.

De medewerker

Iedereen (intern of extern) die gegevens verwerkt (bijvoorbeeld inkijkt, registreert, wijzigt, ...), doet dit volgens de beleidsprincipes uit dit beleidshandboek. De gebruiker verwerkt gegevens in overeenstemming met de discretieplicht, en conform volgende principes:

- Is verantwoordelijk voor de gegevens van bewoners die hij/zij verwerkt
- Voert de veiligheidsrichtlijnen uit tijdens zijn/haar verwerkingsopdracht.
- Verwerkt enkel die gegevens die horen bij de taak
- Draagt zorg voor de gegevens
- Meldt inbreuken
- Leeft artikel 458 van het Strafwetboek na: De gebruiker respecteert het beroepsgeheim.

ICT medewerker of key user

De ICT-medewerker of key user zijn, bovenop de verantwoordelijkheden voor de gebruiker, verantwoordelijk voor:

- De implementatie van de technische maatregelen
- De veiligheidsinstellingen te implementeren in lijn met dit beleidshandboek.
- De veiligheidsproblemen die ontstaan voor, tijdens of na de implementatie van ICT-middelen te melden aan de DPO
- Te fungeren als expert. Vanuit deze rol neemt hij/zij deel aan de identificatie zowel als aan de remediëring van de gegevensbeschermingsrisico's
- De gedragscode na te leven.

ICT leverancier

De ICT-leverancier heeft dezelfde verantwoordelijkheden als deze van een ICT-medewerker. Bijkomstig:

- Wijst hij op veiligheidsrisico's van geleverde toepassingen

- Wijst de leverancier op de op te nemen veiligheidstaken
    - Streeft de leverancier een transparant gegevensbeschermingsbeleid na door te communiceren over het eigen actuele veiligheidsniveau en bij de afhandeling van veiligheidsincidenten.

3 Scope van het gegevensbeschermingsbeleid

Dit beleid is van toepassing voor de gehele levensduur van informatie binnen Hict, van het verkrijgen van informatie tot de uiteindelijke verwijdering van informatie binnen de organisatie.

Dit beleid geldt voor geheel Hict:

- Het kantoor van Hict
- Alle personeelsleden van Hict, zowel interne medewerkers als externen die tewerkgesteld zijn binnen Hict voor bepaalde of onbepaalde duur.
- Alle bedrijfsmiddelen en informatieverwerkende systemen beheerd door Hict evenals systemen beheerd door externen ten behoeve van informatieverwerkingen voor Hict zoals databases, informatie ongeacht de drager ervan, netwerken, datacenters, etc.
- Ale verwerkingsactiviteiten, zowel als verwerkingsverantwoordelijke als verwerker.

Voor bepaalde domeinen of processen binnen Hict kunnen aanvullende richtlijnen of procedures worden uitgewerkt die in detail omschrijven welke maatregelen genomen worden om het gewenste niveau van gegevensbescherming te bereiken. Dit beleid is de kapstok waar alle andere richtlijnen of procedures onder vallen.

Gezien de belangrijke rol van de ICT-leveranciers bij het opzetten van de ICT-omgeving om gegevens te verwerken, legt het beleidshandboek hiervoor ook de beleidsprincipes vast.

4 Het beheer van risico's

Hict brengt de risico's inzake gegevensbescherming in kaart aan de hand van een risico analyse, die voor het eerst werd uitgevoerd in het 1e kwartaal van 2018. De risico analyse werd uitgevoerd op basis van volgende criteria (toetsingskader):

- De richtsnoeren met betrekking tot de informatiebeveiliging van persoonsgegevens, zoals deze werden gepubliceerd door de Commissie voor de Bescherming van de Persoonlijke Levenssfeer
- De Algemene Verordening Gegevensbescherming
- De ISO 27001 norm rond informatiebeveiliging

De analyse bracht operationele en tactische risico's in kaart. Deze risico's werden besproken samen met de directie op 03/05/2018. De bevindingen uit de risico analyse werden besproken en worden opgenomen in een actieplan om de gevonden risico's te behandelen. Hierin onderkent Hict vier mogelijk risicobehandelingen:

- Accepteren: een risico wordt geaccepteerd, er worden geen aanvullende maatregelen genomen. Hict streeft er naar zo min mogelijk risico's te accepteren.
- Overdragen: een risico wordt overgedragen waardoor de verantwoordelijkheid ten aanzien van het risico niet langer bij Hict rust.

- Beperken: Hict neemt de noodzakelijke maatregelen om een risico te beperken zodat het risico wordt teruggebracht tot een niveau waarop het te accepteren is.
- Uitsluiten: Hict neemt maatregelen om te voorkomen dat een risico zich überhaupt kan voordoen.

Het doel is dat de risico analyse minstens jaarlijks wordt herzien. Dit maakt onderdeel uit van de werkzaamheden van de DPO.

De actiepunten die momenteel prioritair zijn in functie van de uitgevoerde risico analyse vindt u terug in het hoofdstuk 6.

5 Beleidsdoelstellingen voor gegevensbescherming

Hict, zowel in haar rol als verwerkingsverantwoordelijke als verwerker:

- Is transparant over de persoonsgegevens die het verwerkt en het verwerkingsdoel, zowel naar de betrokkene, de klanten als naar de toezichthouders. De gevoerde communicatie is eerlijk, eenvoudig toegankelijk en begrijpelijk. Het transparantieprincipe is ook van toepassing wanneer de persoonsgegevens worden uitgewisseld.

- Verwerkt enkel de gegevens die relevant zijn voor het uitvoeren van haar taken. Elke taak waarbij persoonsgegevens worden verwerkt, is rechtmatig. Dit betekent onder meer dat de verwerking in overeenstemming is met de wettelijke en statutaire doelen van Hict. Dit wordt telkens geëvalueerd bij een nieuw verwerkingsdoel, waar nodig aan de hand van een gegevensbeschermignseffectbeoordeling.

- Verwerkt enkel de persoonsgegevens die strikt noodzakelijk voor de uitvoering van de activiteiten. Zo worden identificatoren die horen bij de persoonsgegevens tot een minimum herleid.

- Kijkt toe op de integriteit van de persoonsgegevens gedurende de ganse verwerkingscyclus.

- Bewaart gegevens niet langer dan noodzakelijk. De noodzakelijkheid is afgetoetst tegenover wettelijke verplichtingen en de rechten en vrijheden van de betrokkene.

- Voorkomt inbreuken die voortvloeien uit het verwerken van persoonsgegevens. Informatieveiligheid, gegevensbescherming bij ontwerp en privacy-vriendelijke standaardinstellingen zijn hiervoor hulpmiddelen. Wanneer een inbreuk plaatsvindt, wordt hierover gerapporteerd in lijn met de regelgeving ter zake.

- Is in staat om alle geldende rechten van een betrokkene, zoals het recht op inzage, afschrift en eventueel ook schrapping uit te voeren. Hict bewaakt hierbij over de eventuele beperkingen die op deze rechten van toepassing zijn.

- Waakt er actief over dat bij het verwerken van de persoonsgegevens voor een welbepaald doel, de rechten en vrijheden (bijvoorbeeld recht op verzekerbaarheid, recht op zorg) van de betrokkene gevrijwaard blijven.

- Verwerkt gegevens in lijn met de rechten en vrijheden die gelden in de Europese Economische Ruimte en controleert de toepassing hiervan wanneer de gegevens worden uitgewisseld daarbuiten. Hict leeft bijgevolg alle wettelijke en normerende kaders na (i.e. zowel Vlaamse, Federale als Europese regels) bij het verwerken van persoonsgegevens en heeft daartoe haar verantwoordelijkheid over de persoonsgegevens en die van andere duidelijk in kaart gebracht. Hict monitort daarenboven ook de in de sector geldende gedragscodes en past deze toe.

- Kan aantonen dat het alle beleidsdoelstellingen naleeft, conform de wettelijke bepalingen. Deze verantwoordingsplicht wordt bewaakt door interne toezicht en controle en is uitvoerbaar volgens de wettelijk geldende principes.

6 Prioritaire actiepunten uit de risico analyse

Onderstaand zijn de verschillende prioritaire actiepunten die naar voren zijn gekomen uit de risico analyse. Het gaat hier om de bevindingen met een score Hoog of Kritiek.

NVT