SAMENWERKINGSOVEREENKOMST TUSSEN EEN MAMMOGRAFISCHE EENHEID EN HET CENTRUM VOOR KANKEROPSPORING BETREFFENDE DE ORGANISATIE VAN HET VLAAMS BEVOLKINGSONDERZOEK NAAR BORSTKANKER

Tussen enerzijds het centrum voor kankeropsporing, gevestigd te Ruddershove 4, 8000 Brugge vertegenwoordigd door dr. Patrick Martens , directeur van vzw Centrum voor Kankeropsporing

en anderzijds

de mammografische eenheid ……,

gevestigd …… (straat en nummer)

in …… (postcode) ……,

vertegenwoordigd door ……,

(de eindverantwoordelijke van de mammografische eenheid, hierna ME genoemd),

WORDT OVEREENGEKOMEN WAT VOLGT:

Artikel 1. Voor de toepassing van deze overeenkomst wordt verstaan onder:

1° agentschap: het Vlaams Agentschap Zorg en Gezondheid;

2° besluit van de Vlaamse Regering van 16 maart 2012: besluit van de Vlaamse Regering van 16 maart 2012 betreffende aspecten van het Vlaams bevolkingsonderzoek naar borstkanker;

3° centrum: Centrum voor Kankeropsporing;

4° doelgroep: alle asymptomatische vrouwen zonder familiaal verhoogd risico van de leeftijdsgroep 50 t.e.m. 69 jaar, ongeacht hun taal, als ze zich wenden tot een door de Vlaamse overheid erkende mammografische eenheid;

5° draaiboek: het draaiboek Vlaams bevolkingsonderzoek naar borstkanker;

6° eenheid: mammografische eenheid;

7° Vlaamse werkgroep: de Vlaamse werkgroep Bevolkingsonderzoek naar borstkanker.

Art. 2. Het centrum en de eenheid voeren de aanbevelingen uit en volgen de procedures die in de Vlaamse werkgroep worden gemaakt en die hun neerslag vinden in het draaiboek.

Het draaiboek wordt gepubliceerd op de website over het Vlaams bevolkingsonderzoek naar borstkanker. Het centrum brengt de eenheid via e-mail op de hoogte van alle wijzigingen van het draaiboek. Het centrum en de eenheid verbinden zich ertoe altijd de laatste versie van de aanbevelingen en procedures te hanteren.

Art. 3. Het centrum en de eenheid registeren en wisselen de gegevens uit over de radiologen die screeningsmammografieën uitvoeren en beoordelen.

De eenheid bezorgt het centrum en het agentschap de lijst met de namen en RIZIV-nummers van de radiologen die in de eenheid analoge screeningsmammografieën uitvoeren en/of een lijst met dezelfde gegevens voor de radiologen die digitale screeningsmammografieën uitvoeren. In die lijsten, waarvan de modellen opgenomen zijn in het draaiboek, vult de eenheid ook de contactgegevens van de administratie in en indien van toepassing de contactgegevens van de IT-verantwoordelijke voor de digitale screeningsmammografieën. De eenheid brengt het centrum en het agentschap op de hoogte van elke wijziging in die lijsten.

Het centrum voert de gegevens uit die lijsten, alsook alle wijzingen daaraan, in het borstkankerregistratiesysteem in.

Art. 4. De eenheid en het centrum hanteren gezamenlijk een klantgericht afsprakensysteem. Bij problemen wordt de procedure gevolgd, vermeld in het draaiboek.

De mammografische eenheid biedt voldoende en toegankelijke afspraaktijdstippen aan om de vrouwen die in aanmerking komen voor het Vlaams bevolkingsonderzoek naar borstkanker te kunnen uitnodigen.

Art. 5. De eenheid benadert de vrouw op een respectvolle en klantvriendelijke wijze en verstrekt haar informatie over het verloop en de voor- en nadelen van het bevolkingsonderzoek naar borstkanker.

De eenheid vult samen met de vrouw het aanvraagformulier in, neemt de screeningsmammografie en voert een eerste beoordeling uit.

In het kader van het Vlaams bevolkingsonderzoek naar borstkanker mag er maar één screeningsmammografie per twee opeenvolgende kalenderjaren genomen worden en mogen er bij de screeningsmammografie geen bijkomende onderzoeken (onder meer echografie en borstpalpatie) worden uitgevoerd.

De eenheid vult altijd de mutualiteitgegevens van de deelnemende vrouw in alsook het RIZIVnummer en de correcte naam- en adresgegevens van de opgegeven arts(en) in op het aanvraagformulier tweede lezing of de digitale versie, waarvan het model is opgenomen in het draaiboek. De vrouw moet na het invullen van alle gegevens, het formulier ter goedkeuring ondertekenen. Bij het gebruik van de digitale versie wordt het papieren formulier met de handtekening van de vrouw door de eenheid bewaard. Als de wettelijke vereisten (elektronische handtekening) het toelaten, is het rechtstreeks invoeren of het gestructureerd doorsturen van het aanvraagformulier tweede lezing en/of het registratieformulier eerste lezing mogelijk.

Als er al een screeningsmammografie of een diagnostische mammografie genomen is bij de deelnemende vrouw door de eenheid, moet de nieuwe screeningsmammografie vergeleken worden met de vorige mammografie(ën). Als die mammografie (screening of diagnostisch) uitgevoerd is door een andere radiologische dienst en in het bezit is van de deelnemende vrouw, moet aan de vrouw gevraagd worden om die mammografie aan de eenheid te bezorgen, zodat de nieuwe screeningsmammografie daarmee vergeleken kan worden.

De mammografieën waarmee de eenheid vergeleken heeft moeten altijd meegestuurd worden naar het centrum zodat de tweede lezer over dezelfde informatie beschikt als de eerste lezer voor de beoordeling van de nieuwe screeningsmammografie.

Op vraag worden alle screeningsmammografieën kosteloos bezorgd aan een andere mammografische eenheid of aan de dame in kwestie. Digitale screeningsmammografieën kunnen bij het centrum opgevraagd worden.

Het resultaat van de beoordeling wordt door de eenheid genoteerd op het registratieformulier eerste lezing of de digitale versie, waarvan het model is opgenomen in het draaiboek, volgens de richtlijnen vermeld in het draaiboek. De eenheid vult op het registratieformulier of de digitale versie altijd het INSZ-nummer van de deelnemende vrouw in en vermeldt indien van toepassing duidelijk de initialen van de laborant die de screeningsmammografie heeft genomen.

De eenheid wacht het screeningsresultaat af en brengt de vrouw niet op de hoogte (mondeling of schriftelijk) van het resultaat van de eerste lezing.

Art. 6. De eenheid bezorgt het centrum het screeningsdossier, al dan niet in digitale vorm, waarin de volgende gegevens van de deelnemende vrouw zijn opgenomen:

1° de nieuwe screeningsmammografie (voor digitale screeningsmammografieën in DICOM standaard for presentation; uitprints van de digitale screeningsmammografieën worden niet toegestaan); 2° indien van toepassing, de vorige screenings- of diagnostische mammografie(ën);

3° het door de deelnemende vrouw ondertekende aanvraagformulier tweede lezing of bij digitale registratie een bevestiging dat de eenheid het aanvraagformulier tweede lezing heeft ingevuld en bewaart;

4° het registratieformulier eerste lezing of de digitale versie.

Alleen de documenten die relevant zijn voor het huidige screeningsdossier mogen verstuurd worden naar het centrum.

De gegevens, vermeld in het eerste lid, worden binnen een termijn van vijf werkdagen (zeven kalenderdagen) aan het centrum bezorgd. De eenheid beslist zelf op welke manier ze het screeningsdossier aan het centrum bezorgt. Het dossier wordt als volledig beschouwd en geregistreerd op het ogenblik dat alle vereiste gegevens tijdens de kantooruren in het centrum worden afgeleverd. De eenheid wordt minstens 1 week op voorhand op de hoogte gebracht van geplande sluitingsdagen van het centrum.

Bij digitale screeningsmammografieën volgt de eenheid de hardware-vereisten en de manier van werken zoals vastgelegd door het centrum bij de radiologische controle digitale mammografie. Bij gebruik van CAD software in de eenheid moet de CAD-informatie op een gestructureerde manier meegestuurd worden met de beelden naar het centrum.

Art 7. Het centrum laat een tweede beoordeling uitvoeren van de screeningsmammografie, zonder inzage van het besluit van de eerste lezing. De tweede lezer registreert het besluit op het registratieformulier tweede lezing of digitale versie, waarvan het model is opgenomen in het draaiboek.

Als de tweede lezer niet tot hetzelfde besluit komt als de eenheid (afwijkend of niet afwijkend), gebeurt er een derde lezing waarbij de screeningsmammografie een derde maal wordt beoordeeld, deze keer met kennis van het resultaat van de vorige lezingen. Die derde lezing wordt uitgevoerd door een derde radioloog, verbonden aan het centrum, of gebeurt in een consensuslezing tussen de eenheid en het centrum.

Het centrum bezorgt aan de deelnemende vrouw en aan de door haar opgegeven arts(en) het screeningsresultaat:

1° bij een niet afwijkend screeningsresultaat ontvangen de deelnemende vrouw en de door haar opgegeven arts(en) op hetzelfde tijdstip een bericht met het screeningsresultaat;

2° bij een afwijkend screeningsresultaat ontvangt de deelnemende vrouw later dan de opgegeven arts(en), maar niet later dan zeven kalenderdagen, een bericht met de vraag om contact op te nemen met één van de door haar opgegeven artsen.

Het centrum verwerkt het screeningsdossier en verstuurt het screeningsresultaat binnen de twee weken (14 kalenderdagen), na ontvangst van het dossier van de eenheid. Het centrum bezorgt maandelijks het agentschap een analyse van de aanlevertijden van de eenheden en de verwerkingstijd van het centrum. Als de verwerkingstermijn uitzonderlijk niet wordt gehaald, moet het centrum dit verantwoorden aan het agentschap.

Art. 8. De eenheid en de radiologen die er werken, passen de derdebetalersregeling toe voor alle screeningsmammografieën en volgen de bepalingen van de RIZIV-nomenclatuur die betrekking hebben op screeningsmammografieën.

Als de radioloog die de tweede of derde beoordeling van de screeningsmammografie uitvoert, vaststelt dat om fysisch-technische of medisch-radiologische redenen de kwaliteit onvoldoende is, dan verbindt de eenheid er zich toe om een nieuwe screeningsmammografie uit te voeren. Die screeningsmammografie wordt niet aan de deelnemende vrouw en ook niet aan de ziekteverzekering aangerekend. De kost van die medische prestatie wordt gedragen door de eenheid.

Art. 9. De bewaring van het screeningsdossier (inclusief de analoge en de digitale screeningsmammografieën) valt onder de verantwoordelijkheid van de eenheid.

Het centrum bezorgt daartoe het screeningsdossier (inclusief eventuele analoge screeningsmammografieën) en een kopie van de resultaatsbrief aan de eenheid. Het centrum bewaart een kopie van de digitale screeningsmammografieën. De screeningsmammografieën en de gegevens in de DICOM headers mogen voor wetenschappelijke doeleinden gebruikt worden. De persoonsgegevens zullen in dit geval worden geanonimiseerd.

Bij een positief screeningsresultaat bezorgt het centrum op vraag kosteloos een kopie van de digitale screeningsmammografieën, de resultaatsbrief en de registratieformulieren eerste, tweede en eventueel derde lezing aan de arts die instaat voor het uitvoeren van het vervolgonderzoek.

Art. 10. Het centrum registreert en wisselt alle gegevens uit die noodzakelijk zijn voor de voortgangscontrole en de kwaliteitsbewaking van het Vlaams bevolkingsonderzoek naar borstkanker in het algemeen en voor de werking van de eenheid en de radiologen die er werken, in het bijzonder.

De gegevens die noodzakelijk zijn voor de fysisch-technische en de medisch-radiologische kwaliteit van de analoge en digitale screeningsmammografieën omvatten minstens die gegevens die vermeld staan in het draaiboek.

De gegevens die bijkomend noodzakelijk zijn voor de voortgangscontrole en kwaliteitsbewaking van de digitale screeningsmammografie omvatten minstens de DICOM header-gegevens, vermeld in het draaiboek. Dit omvat, maar is niet beperkt tot, de vereiste dat het Identificatienummer Sociale Zekerheid (INSZ) van de vrouw opgenomen in de DICOM header op de locatie: Other Patient ID (0010,1000) en dat steeds als acquisition date (0008,0022) de datum van de mammografie genomen worden. Dezelfde datum wordt vermeld op het registratieformulier van de eerste lezing.

De eenheid en het centrum wisselen zoveel als mogelijk de gegevens elektronisch uit.

Bij elke update/upgrade van hardware/software ter hoogte van een digitaal mammografietoestel of ter hoogte van de PACS omgeving, moet de eenheid het centrum daarvan onmiddellijk op de hoogte stellen zodat de nodige stappen kunnen ondernomen worden om de kwaliteit van de mammografieën te herevalueren volgens de procedures, opgenomen in het draaiboek.

Art. 11. Het centrum is verantwoordelijk voor de terugkoppeling en de advisering over de kwaliteit van de werking van de eenheid en de radiologen.

De procesindicatoren en -parameters die geregistreerd worden en die dus kunnen geëvalueerd worden in het Vlaams bevolkingsonderzoek naar borstkanker zijn beschreven in het draaiboek.

Het centrum bezorgt aan de eenheid een evaluatierapport m.b.t. tot de kwaliteitsparameters en volgens de frequentie, vermeld in bijlage 3 punt 2 van het besluit van de Vlaamse Regering van 16 maart 2012.

De eenheid werkt mee aan de continue evaluatie en bijsturing om een optimaal kwaliteitsniveau te bereiken van de screeningsmammografieën en de lezingen.

Bij vaststelling van een fysisch-technisch kwaliteitsprobleem wordt de procedure gevolgd, vermeld in bijlage 4, punt 1 van het besluit van de Vlaamse Regering van 16 maart 2012.

Bij vaststelling van een medisch-radiologisch kwaliteitsprobleem wordt de procedure gevolgd, vermeld in bijlage 4, punt 2 van het besluit van de Vlaamse Regering van 16 maart 2012.

Art. 12. Het centrum registreert alle klachten aan de hand van een registratieformulier, waarvan het model is opgenomen in het draaiboek, en volgens de procedure, vermeld in het draaiboek.

Art. 13. Deze samenwerkingsovereenkomst wordt afgesloten voor onbepaalde duur en houdt op van kracht te zijn op de datum van intrekking of opheffing van de erkenning van een van beide partijen of als het Vlaams bevolkingsonderzoek naar borstkanker stopgezet wordt.

Indien een partij zijn verplichtingen krachtens deze samenwerkingsovereenkomst niet nakomt en deze partij in gebreke blijft met het nakomen van deze verplichtingen gedurende een periode van dertig (30) werkdagen na de aangetekende ingebrekestelling door de andere partij, zal de laatstgenoemde partij de overeenkomst na afloop van voormelde termijn van rechtswege en zonder verdere ingebrekestelling bij aangetekend schrijven kunnen verbreken.

De partijen verbinden zich ertoe om elke gebeurtenis of omstandigheid die gevolgen kan hebben op de zorgvuldige uitvoering van de samenwerkingsovereenkomst aan de andere partij te melden. Indien een partij zich in deze situatie bevindt, zal hij de andere partij binnen de vijf (5) werkdagen op de hoogte brengen van de aard van deze onvoorzienbare en buiten zijn wil ontstane situatie, en zal de uitvoering van de overeenkomst worden geschorst. Indien de schorsing langer duurt dan dertig (30) werkdagen, dan zullen de partijen onderhandelingen voeren met het oog op de passende amendering of beëindiging van de samenwerkingsovereenkomst.

Opgemaakt te …… in twee exemplaren, op …… .

Voor het centrum,

Voor de eenheid,

(de samenwerkingsovereenkomst moet ondertekend worden door de eindverantwoordelijke van de eenheid)

ADDENDUM BIJ DE SAMENWERKINGSOVEREENOMST TUSSEN EEN MAMMOGRAFISCHE EENHEID EN HET CENTRUM VOOR KANKEROPSPORING BETREFFENDE DE ORGANISATIE VAN HET VLAAMS BEVOLKINGSONDERZOEK BORSTKANKER:VERWERKERSOVEREENKOMST – GDPR

Tussen enerzijds het centrum voor kankeropsporing, gevestigd te Ruddershove 4, 8000 Brugge vertegenwoordigd door dr. Patrick Martens , directeur van vzw Centrum voor Kankeropsporing

en anderzijds

de mammografische eenheid ……,

gevestigd …… (straat en nummer)

in …… (postcode) ……,

vertegenwoordigd door ……,

(de eindverantwoordelijke van de mammografische eenheid, hierna ME genoemd),

Rekening houdend met het feit dat

- de "General Data Protection Regulation" (GDPR) van kracht is sinds 25/05/2018;
- Het Vlaams Agentschap Zorg en Gezondheid de verwerkingsverantwoordelijke is
- Het CvKO optreedt als verwerker van de gegevens van de bevolkingsonderzoeken in opdracht van het Vlaams Agentschap Zorg en Gezondheid;
- de mammografische eenheid optreedt als subverwerker

WORDT OVEREENGEKOMEN WAT VOLGT:

Art. 1. In het kader van het bevolkingsonderzoek naar Borstkanker handelt de ME uitsluitend in opdracht van CvKO en conform de instructies van het CvKO en licht het CvKO onmiddellijk in ingeval bepaalde instructies zouden indruisen tegen de voorschriften zoals voorzien in de GDPR.

Art. 2. De ME is verplicht tot geheimhouding van de persoonsgegevens die hij van het CvKO ontvangt, behoudens voor zover een wettelijk voorschrift de ME tot mededelen verplicht en behoudens de gegevensverstrekking die plaatsvindt in opdracht van het CvKO. Dit houdt de principiële verplichting in om de gegevens enkel intern te gebruiken en geenszins mee te delen aan derden, op welke wijze ook.

Art. 3. De ME zal er over waken dat de toegang tot de te verwerken medische en verwerkte medische gegevens beperkt is tot personeel in dienst van de ME die de gegevens nodig hebben om de taken uit te voeren die de ME hen in uitvoering van deze overeenkomst toewijst. De ME verbindt zich ertoe en maakt zich sterk dat de tot het verwerken van medische gegevens gemachtigde

personen zich ertoe verbonden hebben de vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting tot vertrouwelijkheid zijn gebonden.

Art. 4. Beveiliging
De ME verbindt zich ertoe de gepaste maatregelen te nemen om de persoonsgegevens en de verwerking ervan te beveiligen.

De ME verbindt zich ertoe de passende technische en organisatorische maatregelen te nemen om de persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking of toegang. Deze maatregelen dienen, rekening houdend met de stand van de techniek en de daarmee gemoeide kosten, een passend beveiligingsniveau te garanderen, gelet op de risico's van de verwerking van persoonsgegevens. Deze maatregelen worden verder omschreven in het document "referentiemaatregelen GDPR".

Het document "referentiemaatregelen GDPR" moet gezien worden als een leidraad.

De opsomming van de referentiemaatregelen moet op elke pagina geparafeerd worden en moet eveneens voorafgegaan zijn door het aangevuld en ondertekend informatieblad.

https://borstkanker.bevolkingsonderzoek.be/nl/professionelen/mammografische-eenheden

Tevens verbinden het CvKO en de ME zich ertoe om alle in artikel 32 GDPR opgesomde vereiste maatregelen te nemen in het licht van de beveiliging van de verwerking, meer bepaald passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, het volgende omvatten:

4.1. de pseudonimisering en versleuteling van persoonsgegevens;

4.2. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

4.3. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

4.4. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Art. 5. Fysische toegangsbeperking

De ME zal ervoor zorgen dat de plaatsen waar ten behoeve van het CvKO persoonsgegevens worden verwerkt, niet toegankelijk zijn voor onbevoegden. Daartoe zal hij onder meer de nodige organisatorische maatregelen nemen.

Art. 6. Functionele toegangsbeperking

De ME zal de toegang tot de verwerkte persoonsgegevens beperken tot die personeelsleden die de gegevens nodig hebben om de taken uit te oefenen die de ME hen in uitvoering van deze overeenkomst toewijst.

Art. 7. Bijstand aan CvKO

7.1. De ME verbindt zich ertoe rekening houdende met de aard van de verwerking, het CvKO door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand te verlenen bij het vervullen van diens plicht om verzoeken om uitoefening van de in Hoofdstuk III van de GDPR vastgestelde rechten van de betrokkene wier persoonsgegevens worden verwerkt te beantwoorden. De betrokkenen hebben recht op informatie aangaande het doel van de verwerking, de gegevens die worden verwerkt, de duurtijd van de bewaring, inzage, correctie, rectificatie en verwijdering van hun persoonsgegevens, evenals recht op overdraagbaarheid van deze persoonsgegevens aan een andere verwerkingsverantwoordelijke en recht van bezwaar tegen de verwerking.
In het verlengde van bovenstaande verbindt de ME zich ertoe het CvKO onverwijld in te lichten indien hij van een betrokkene één van voormelde verzoeken krijgt. De ME beantwoordt de verzoeken en aanvragen van de betrokkenen niet zelf, behoudens eventuele andersluidende schriftelijke afspraken tussen de ME en CvKO.

7.2. De ME verbindt zich ertoe rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie het CvKO bijstand te verlenen bij het doen nakomen van de verplichtingen in hoofde van de art. 33 t.e.m. 36 van de GDPR :

De ME dient het CvKO bij te staan indien het CvKO een melding moet maken van een inbreuk aan haar verwerkingsverantwoordelijke. In het verlengde hiervan licht de ME het CvKO omstandig en onmiddellijk in over een (vermoedelijke) inbreuk in verband met persoonsgegevens alsook over elk gegevenslek zodra de ME hiervan kennis heeft genomen. De kennisgeving gebeurt op een dergelijke wijze dat het CvKO tijdig kan voldoen aan haar wettelijke verplichtingen tegenover haar verwerkingsverantwoordelijke onder de GDPR. De ME vrijwaart het CvKO conform artikel 11 van deze overeenkomst. Voor de melding gebruikt de ME het modelformulier melding gegevenslek https://borstkanker.bevolkingsonderzoek.be/nl/professionelen/mammografische-eenheden

De ME dient het CvKO bij te staan ingeval van nood aan een gegevensbeschermingseffecten-beoordeling en voor zover van toepassing een voorafgaande raadpleging van de verwerkingsverantwoordelijke telkens wanneer een verwerking van persoonsgegevens een hoog risico inhoudt gegeven de aard, context, omvang en doeleinden van deze verwerking;

Art. 8. Onderaanneming van bepaalde verwerkingsactiviteiten

De ME kan bepaalde verwerkingsactiviteiten van medische gegevens uitbesteden aan een subverwerker voor zover de ME het CvKO hiervan op voorhand inlicht. Het CvKO heeft telkens de mogelijkheid om hier bezwaar tegen te maken.

Wanneer de ME een subverwerker in dienst neemt om voor het CvKO specifieke verwerkingsactiviteiten te verrichten, worden aan deze subverwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als deze bedoeld in huidige overeenkomst. Wanneer deze

subverwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de ME tov het CvKO volledig aansprakelijk voor het nakomen van de verplichtingen van de subverwerker.

Art. 9. Register van verwerkingsactiviteiten
De ME houdt een register bij van alle verwerkingsactiviteiten die zij ten behoeve van het CvKO heeft verricht. Dit register bevat de in artikel 30, punt 2. GDPR vermelde gegevens. Naast de contactgegevens van de ME en van het CvKO worden tevens de categorieën van uitgevoerde verwerkingen opgenomen in dit register. Het register wordt opgesteld in schriftelijke vorm, waaronder elektronisch.
Dit register wordt op verzoek van de GBA aan deze laatste overhandigd.

Art. 10. Controle door het CvKO

Het CvKO heeft het recht om de naleving van deze overeenkomst te controleren. Daartoe kan het zich, na afspraak, ter plaatse begeven in de lokalen of plaatsen waar de ME de gegevensverwerking uitvoert en de back-up bewaart.
Op eenvoudig verzoek van het CvKO is de ME ertoe gehouden alle inlichtingen die van belang zijn bij de uitvoering van deze overeenkomst over te maken aan het CvKO.

Art. 11. Aansprakelijkheid
ME en CvKO zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen. De in dit artikel geregelde aansprakelijkheid heeft uitsluitend betrekking op de aansprakelijkheid ten gevolge van een inbreuk op de GDPR en dit addendum, onverminderd de aansprakelijkheid op grond van andere regels.

Indien het CvKO door een betrokkene wordt aangesproken in schadevergoeding, zal de ME tussenkomen in de procedure. Indien het CvKO voor de verwerking aansprakelijk wordt gehouden, kan deze op de ME regres nemen indien de ME toerekenbaar is tekortgeschoten in de naleving van de in de bij of krachtens de GDPR gegeven voorschriften en onderhavige Verwerkersovereenkomst. Zo zal de ME het CvKO vergoeden en vrijwaren voor alle claims, acties, aanspraken van derden en voor alle schade en verliezen (waaronder ook boetes van de GBA) die rechtstreeks of onrechtstreeks voortvloeien uit een verwerking van persoonsgegevens wanneer bij de verwerking niet is voldaan aan de bepalingen van de GDPR dan wel in strijd met de rechtmatige instructies van het CvKO werd gehandeld.

Opgemaakt te …… in drie exemplaren, op ……. .

Voor het CvKO, dr. Patrick Martens, directeur van vzw Centrum voor Kankeropsporing.

..

Voor de ME,
de eindverantwoordelijke van de mammografische eenheid.

..

Bijlage 1 : document referentiemaatregelen (pagina 12 t/m pagina 18)

Het document moeten gezien worden als een leidraad. Mogelijk is de uitvoering van de maatregelen nog in progress.
De opsomming van de referentiemaatregelen moet op elke pagina geparafeerd worden en moet eveneens voorafgegaan zijn door het aangevuld en ondertekend informatieblad.

Bijlage 2 : modelformulier melding gegevenslekken (pagina 19 t/m pagina 24)

BIJLAGE 1 : Referentie maatregelen voor de beveiliging van elke verwerking van persoonsgegevens informatieblad

Benaming mammografische eenheid:

Adres :

Ondernemingsnummer (KBO):

Voornaam, Naam & email adres van de verantwoordelijke voor informatieveiligheid (verplicht)

Voornaam, Naam & email adres van het aanspreekpunt voor informatieveiligheid (CISO) (optioneel)

Voornaam, Naam & email adres van de functionaris voor gegevensbescherming (DPO) (verplicht)

Voornaam, Naam & email adres van het lokale aanspreekpunt voor gegevensbescherming (adjunct DPO of vertegenwoordiger, optioneel)

Voornaam, Naam & email adres van de persoon belast met het dagelijks bestuur (CEO, verplicht)

Datum en handtekening van de verantwoordelijke voor informatieveiligheid of functionaris voor gegevensbeheer van de mammografische eenheid (optioneel)

Datum en handtekening van de persoon belast met het dagelijks bestuur van de mammografische eenheid **(verplicht)**

Referentiemaatregelen voor de beveiliging van elke verwerking van persoonsgegevens[1]

Het voorliggend document bevat een lijst met elf actiedomeinen in verband met de informatiebeveiliging waarvoor elke instelling – rechtspersoon[2], onderneming of administratie – die persoonsgegevens bewaart, gebruikt, verwerkt of mededeelt, maatregelen moet nemen.

De extreme diversiteit van concrete situaties maakt het onmogelijk om voor elk voorkomend geval heel precies de te ondernemen acties te omschrijven.

Elke hiernavolgende referentiemaatregel zal dus aan de context en aan het specifieke karakter van elke instelling aangepast moeten worden en impliceert de uitvoering van praktische oplossingen waarvan het detailniveau of de complexiteit proportioneel moet zijn ten opzichte van de reële behoeften van de instelling. Hiervoor moet rekening worden gehouden met:

- de aard van de verwerkte persoonsgegevens en de verwerkingen ervan evenals de vereisten inzake vertrouwelijkheid, integriteit en beschikbaarheid;
- de wettelijke of reglementaire vereisten die van toepassing zouden zijn;
- de grootte van de instelling (daarbij inbegrepen het aantal personen die toegang tot de gegevens zouden kunnen hebben);
- het belang en de complexiteit van de betrokken informatiesystemen, toepassingsprogramma's en informaticasystemen;
- de mate waarin de instelling openstaat voor de buitenwereld evenals de mate waarin er toegang is vanuit de buitenwereld;
- de risico's waaraan de instelling zelf of de personen wiens persoonsgegevens worden verwerkt zich blootstellen;
- alsook de 'stand van de techniek terzake en de kosten voor het toepassen van de maatregelen'[1].

Informatiebeveiliging is een materie die blijvend onderhevig is aan evolutie en daarom zullen deze referentiemaatregelen ook systematisch worden aangepast in functie van de ontwikkelingen van de regelgeving, de techniek of andere aspecten.

1 Het voorliggend document is bestemd voor de verantwoordelijken van een verwerking en wil als hulp dienen bij de implementatie van een degelijke beveiliging overeenkomstig de verplichting opgelegd in de "Verordening (EU) 2016/379 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 de Richtlijn 95/46/ eg (algemene verordening gegevensbescherming)"

2 Dit stelt natuurlijke personen niet vrij van de verplichting zich te voegen naar de bovengenoemde Europese verordening, die aan elke verantwoordelijke voor de verwerking verplichtingen oplegt inzake beveiliging.

1. Informatiebeveiligingsbeleid

Elke instelling die persoonsgegevens gebruikt/verwerkt moet een geschreven document opstellen – het informatiebeveiligingsbeleid – waarin de strategieën en de weerhouden maatregelen voor gegevensbeveiliging nauwkeurig worden omschreven.
Vooraleer deze beveiligingsstrategieën en -maatregelen bepaald worden, moet de instelling nadenken over de potentiële dreigingen die wegen op de gebruikte/verwerkte persoonsgegevens en de reële risico's waaraan deze gegevens blootstaan evalueren.

Het informatiebeveiligingsbeleid bestaat uit:

- een toelichting over de uitgevoerde analyse en het risicobeheer van de persoonsgegevens;
- de prioriteiten die werden weerhouden en de beheersmaatregelen die ingevolge deze risicoanalyse werden of worden aangebracht;
- de planning van de inwerkingstelling;
- de beschrijving van de verschillende verantwoordelijkheden en de ingestelde organisatorische regels;
- de beschrijving van het beheersproces bij beveiligingsincidenten;
- de beschrijving van het sensibiliseringsproces van de instelling voor dit beleid;
- de weerhouden maatregelen om het beveiligingssysteem te actualiseren eens het werd geïnstalleerd.

Dit informatiebeveiligingsbeleid moet door de hoogste hiërarchie en de diverse verantwoordelijken worden goedgekeurd en opdat dit beleid bij iedereen gekend zou zijn, moet het binnen de instelling voldoende verspreid worden.

Dit beleid moet ten minste een keer per jaar of na wijziging of herevaluatie worden bijgewerkt.

2. Organisatie van informatiebeveiliging

Al naargelang van de aard van de gebruikte/verwerkte persoonsgegevens en de termen van de verleende machtiging moet binnen de instelling een veiligheidsconsulent worden aangesteld die verantwoordelijk is voor de uitvoering van het informatiebeveiligingsbeleid.

De veiligheidsconsulent rapporteert rechtstreeks aan de directie van de instelling, en moet kunnen beschikken over voldoende middelen (tijd, human resources, uitrusting en budget) en vrijuit toegang hebben tot de informatie die noodzakelijk is voor zijn functie en voor zover hij binnen het kader van het informatiebeveiligingsbeleid blijft.

Hij zal erop toezien dat de verschillende verantwoordelijkheden inzake informatiebeveiliging (preventie, toezicht, opsporing en verwerking) duidelijk in kaart zijn gebracht en dat de personen belast met de informatiebeveiliging in alle onafhankelijkheid kunnen handelen en ervan gevrijwaard blijven dat ze voor persoonlijke of tegenstrijdige belangen onder druk worden gezet.

De veiligheidsconsulent zal moeten beschikken over de noodzakelijke competenties en opleidingen en zal geen functie(s) kunnen uitoefenen of verantwoordelijkheden hebben die onverenigbaar zijn met die van veiligheidsconsulent.

3. Organisatie en menselijke aspecten van de informatiebeveiliging

De instelling moet duidelijk de verantwoordelijkheden en het beheersproces inzake beveiliging van persoonsgegevens omschrijven en die op gepaste wijze integreren in de algemene organisatiestructuur en werking.

Om de informatiebeveiliging te organiseren, moeten er voldoende en aangepaste organisatorische, technische en financiële middelen beschikbaar worden gesteld.

Om de persoonsgegevens op een doeltreffende wijze te beveiligen moet de instelling erop toezien dat er procedures worden opgesteld voor classificatie[3] van informatie. Dit maakt de inventarisatie en lokalisatie van alle gebruikte/verwerkte persoonsgegevens mogelijk, ongeacht het soort drager.

Omdat het welslagen van een beveiliging van een informatiesysteem sterk afhangt van een correcte informatieverstrekking aan de verschillende actoren, moet de instelling de nodige maatregelen nemen opdat elke persoon (intern of extern) die tussenkomt in de verwerking van persoonsgegevens, voldoende en constant geïnformeerd wordt over zijn verplichtingen en verantwoordelijkheden tijdens deze verwerking en voldoende en juist opgeleid is voor de uitoefening van zijn functies en verantwoordelijkheden inzake informatiebeveiliging.

Er moet eventueel in tuchtrechtelijke gevolgen worden voorzien ingeval de voorgeschreven regels niet worden nageleefd, en wanneer de risico's dit rechtvaardigen is een geheimhoudingsverklaring vereist.

Wanneer de instelling deze verwerkingen van persoonsgegevens geheel of gedeeltelijk in onderaanneming geeft, moet ze erop toezien dat in het contract van onderaanneming dezelfde verplichtingen inzake informatiebeveiliging opgenomen worden als die van de instelling zelf.

4. Fysieke beveiliging van de omgeving

De instelling moet de nodige maatregelen nemen om de fysieke bescherming van de persoonsgegevens te garanderen.

Hiertoe moet de instelling zich ervan verzekeren dat de dragers van persoonsgegevens en de informaticasystemen die deze gegevens gebruiken/verwerken overeenkomstig hun classificatie geplaatst worden in geïdentificeerde en beschermde lokalen waarvan de toegang beperkt is tot de hiertoe gemachtigde personen en tot de uren waarin zij hun functie uitoefenen.

Wanneer een continuïteit van diensten noodzakelijk blijkt, moeten er apparaten geïnstalleerd worden ter preventie, opsporing en aanpak van fysieke bedreigingen zoals branden of overstromingen. Deze apparaten moeten regelmatig gecontroleerd worden. De instelling moet ook back-upmaatregelen nemen om het verlies of de toevallige verandering van de persoonsgegevens te verhinderen.

[3] De term "classificatie" dient hier te begrepen volgens de klassieke bewoording van ordening van gegevens zoals het genoegzaam wordt aangewend bij beveiliging van informatiesystemen, d.w.z. kwalificatie van de informatie en niet zoals voorzien in de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

5. Beveiliging van de netwerken

De instelling moet zich ervan vergewissen dat de netwerken waarmee de apparatuur verbonden is en die betrokken is bij een gebruik/verwerking van persoonsgegevens, de vertrouwelijkheid en de integriteit van de gegevens garanderen.

Indien het interne netwerk van de instelling verbonden is met een openbaar extern netwerk dan moet de instelling de noodzakelijke maatregelen nemen om het (de) netwerk(en) tijdens de verwerkingen te beschermen tegen elke onrechtmatige toegang (inbraken, virussen, kwaadaardige software, enz.).

6. Logische beveiliging van de toegang

De instelling moet zich ervan vergewissen dat de persoonsgegevens overeenkomstig hun classificatie slechts toegankelijk zijn voor de personen en toepassingsprogramma's die hiertoe uitdrukkelijk gemachtigd zijn.

De instelling bewaart een bijgewerkte lijst van de verschillende personen die gemachtigd zijn om tot deze gegevens toegang te hebben en ze te gebruiken/verwerken, en van hun respectievelijke machtigingen.

Deze verschillende machtigingen moeten vertaald worden in technische voorzieningen en toegangscontroles tot de verschillende informaticaonderdelen (programma's, procedures, opslag, telecommunicatie-uitrusting) die tussenkomen in een verwerking van persoonsgegevens.

Deze technische voorzieningen moeten zowel vervat zitten in de activiteiten van de beginfase (ontwikkeling van de toepassingsprogramma's) als in die van de eindfase (back-upbeheer).

Indien het beveiligingsniveau het noodzakelijk maakt, zal de identificatie van de intervenanten vervolledigd worden met een authenticatie.

7. Logging, opsporing en analyse van toegang

De instelling moet loggings- en opsporingsmechanismen installeren.

Hiermee moet wanneer nodig de identiteit kunnen worden teruggevonden van iedere persoon die toegang had tot de persoonsgegevens of ze bewerkt heeft. De registratie van deze controle-informatie kan naargelang het geval betrekking hebben op fysieke toegang, logische toegang of beide.

De fijnheid van de registraties, de lokalisatie en de bewaarduur van deze gegevens, evenals de frequentie van de bewerking en het type bewerkingen, hangen af van de context. Bijkomende

mechanismen voor opsporing van inbraak zouden kunnen vereist zijn. De verantwoordelijke voor de verwerking moet in staat zijn de gemaakte keuzes te rechtvaardigen.

Omdat opsporingsgegevens persoonsgegevens zijn, moet elke verwerking van deze gegevens gepaard gaan met gepaste beheersmaatregelen.

8. Toezicht, nazicht en onderhoud

De instelling moet zich ervan vergewissen dat de technische of organisatorische beheersmaatregelen gevalideerd zijn en regelmatig nagekeken worden.

Om te bepalen hoe de informatiebeveiliging op een passend niveau kan worden gehouden, moet er toezicht worden gehouden op de verwerkingen, de evolutie van de bronnen en de analyse van de loggings.

Aangezien de informatiesystemen en de risico's waaraan zij blootstaan constant evolueren, dient de instelling er zich regelmatig van te vergewissen (minstens één keer per jaar) dat de aanvankelijk nagestreefde doelen en de maatregelen die daarna werden ingesteld nog actueel zijn, opdat ze indien nodig verbeteringen zouden kunnen aanbrengen.

Bij elke reorganisatie van de instelling of wijziging van haar infrastructuur moet er een actualisering van de beheersmaatregelen doorgevoerd worden.

9. Beheer van beveiligingsincidenten en continuïteit

De instelling moet beschikken over een beheersplan voor beveiligingsincidenten.

Wanneer er zich incidenten voordoen die de vertrouwelijkheid en de integriteit van de persoonsgegevens in gevaar brengen, is de snelheid van een interventie primordiaal om de gevolgen van een dergelijke situatie in de dijken. Hiertoe moet de instelling in procedures voorzien die nauwkeurig omschrijven welke de te ondernemen stappen zijn bij ontdekking van een beveiligingsincident van persoonsgegevens alsook welke personen verantwoordelijk zijn om dit incident aan te pakken en zo een gezonde toestand te herstellen.

Bovendien moeten de omstandigheden van het incident geanalyseerd worden, zodat er daaruit preventieve maatregelen of bijsturingen kunnen worden gefilterd om een herhaling van dit soort incidenten te vermijden of om zo snel mogelijk naar de normale toestand te kunnen terugkeren.

Instellingen die verplicht zijn om de continuïteit van hun diensten te verzekeren moeten:

- voorzien in een herstel- en continuïteitsplan om zich bij beveiligingsincidenten in te dekken tegen een dienstenonderbreking die de aanvaardbare termijn overschrijdt;
- er in het bijzonder op toezien dat tijdens de uitvoering van de diverse plannen de vertrouwelijkheid en de integriteit van de persoonsgegevens steeds gegarandeerd zijn.

10. Naleving

Elke instelling moet steeds alle van toepassing zijnde regels en wetten naleven met betrekking tot de verwerking en de bescherming van persoonsgegevens. Deze wetgeving is steeds raadpleegbaar op de website van de Gegevensbeschermingsautoriteit "Wetgeving en normen".

Zo bepaalt de Europese Regelgeving heel nauwkeurig de voorwaarden en de omstandigheden voor een verwerking of doorgifte van persoonsgegevens. Elke instelling is verplicht om voorafgaand aan de verwerking na te gaan of de uitvoering van de verwerking, gelet op het delicate karakter van de gegevens, niet onderworpen is aan een machtiging en moet er steeds over waken dat de voorwaarden van de machtiging gerespecteerd blijven.

De instelling moet op regelmatige basis een audit organiseren met betrekking tot de beveiliging van de gebruikte/verwerkte persoonsgegevens.

11. Documentatie

De instelling moet beschikken over volledige, gecentraliseerde documentatie en die met betrekking tot informatiebeveiliging regelmatig bijwerken.

De instelling moet voor het goed beheer van beveiligde persoonsgegevens alle nodige documentatie aanleggen. Deze documentatie moet volledig en geformaliseerd zijn, proportioneel ten opzichte van de informatiebeveiligingsbehoeften, voortdurend worden bijgewerkt en geïnventariseerd zodat ze te gelegener tijd beschikbaar is voor de bevoegde persoon.

Deze documentatie moet ten minste het volgende bevatten:

- het informatiebeveiligingsbeleid;
- de identiteit van de veiligheidsconsulent of van de verantwoordelijke voor de informatiebeveiligingscel;
- de implementatie van de beheersmaatregelen;
- de inventaris van de gebruikte/verwerkte persoonsgegevens, hun lokalisaties en uitgevoerde verwerkingen;
- de nominatieve lijst van de organen of aangestelden die toegang hebben tot de gegevens;
- de configuratie van de systemen en netwerken;
- de technische documentatie over de ingestelde beheersmaatregelen;
- de agenda van geplande operaties;
- het opsporingsbeleid;
- de testplannen van de beheersmaatregelen;
- verslagen betreffende incidenten;
- eventuele auditverslagen.

Bijlage 2 : modelformulier melding gegevenslekken

contactpunten van de afdelingen van het CvKO	e-mail	telefoon
ANTWERPEN	sofie.vanroosbroeck@uantwerpen.be	0477 48 45 48
BRUGGE	els.vandemaele@vobvzw.be	050 32 70 65
BRUSSEL	stephanie.vandervorst@uzbrussel.be	02 477 54 21
GENT	marjan.vangurp@ugent.be	09 332 83 33
LEUVEN	nadja.torel@uzleuven.be	016 33 25 13

Datum :
Bedrijfsnaam :
Adres:
Postcode:
BTW-nummer
Wie heeft de inbreuk geconstateerd?
Naam:
Functietitel:
Wanneer is de inbreuk geconstateerd:
Datum:
Tijd:

Omschrijf het beveiligingsincident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan:
Wanneer heeft de inbreuk plaatsgevonden?
a. Op (datum + tijd)
b. Tussen (datum + tijd) en (datum + tijd)
c. Is nog niet vastgesteld
d. Er is sprake van een anonieme melding door een derde
Vastleggen context van de data betrokken bij de inbreuk :
Classificatie van de data :
a. Geen, de gegevens zijn niet herleidbaar tot een individu
b. NAW-gegevens
c. Telefoonnummers
d. E-mailadressen, Facebook ID's, Twitter ID's etc.

e. Gebruikersnamen, wachtwoorden of andere inloggegevens, klantnummers
f. Financiële gegevens : rekeningnummers, creditcardnummers
g. rijksregisternummer
h. Kopieën van identiteitsbewijzen
i. Geslacht, geboortedatum, en/of leeftijd
j. Gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid of lidmaatschap van een vakvereniging
k. Gegevens over iemands gezondheid of seksuele geaardheid
l. Strafrechtelijke persoonsgegevens of persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag
m. Gegevens over iemand financiële of economische situatie, gegevens over schulden, salaris- en betalingsgegevens
n. Afgeleide financiële data (inkomenscategorie, huizenbezit, autobezit)
o. Lifestyle kenmerken (o.a. gezinssamenstelling, woonsituatie, interesses, demografische kenmerken (leeftijd, geslacht, nationaliteit, beroep, onderwijs)
p. Data verkregen uit (openbare) sociale profielen (Facebook-, LinkedIn- en Twitteraccounts, …)
q. Overig, namelijk :
Classificatie van de context betrokken bij de inbreuk :
Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
a. Geen, de gegevens zijn niet herleidbaar tot een individu
b. Nog niet vastgesteld
c. Ten minste …… (aantal), maar niet meer dan ……..(aantal) betrokkenen
Omschrijf de groep mensen waarvan persoonsgegevens zijn betrokken bij de inbreuk:

Omstandigheden van de gegevenslek :
a. Alleen lezen (een niet geautoriseerde derde heeft (vertrouwelijke) data kunnen inzien. Verwerker heeft de data nog in zijn bezit.) - confidentialiteit is in gevaar
b. Kopiëren (een niet-geautoriseerde derde heeft data kunnen kopiëren. De data is ook nog in het bezit van Verwerker.) - confidentialiteit is in gevaar
c. Wijzigen (een niet-geautoriseerde derde heeft data (kunnen) wijzigen in systemen van Verwerker - Integriteit is in gevaar
d. Verwijderen of vernietigen (een niet-geautoriseerde derde heeft data verwijderd uit de systemen van Verwerker of data vernietigd.) - Beschikbaarheid is in gevaar
e. Diefstal - Beschikbaarheid is in gevaar
f. Nog niet bekend
Zijn de Persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt voor ongeautoriseerde derden, bijvoorbeeld door encryptie en hashing ?
Ja
Nee
Deels, namelijk

Zo ja, op welke manier zijn de Persoonsgegevens versleuteld:
Heeft de inbreuk betrekking op personen uit andere EU-landen?
Ja
Nee
Zo ja, welke EU-landen:
Welke beveiligingsmaatregelen (technisch en organisatorisch) zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Wie kan benaderd worden voor meer informatie over de inbreuk?
Naam contactpersoon van de leverancier
E-mail :
Telefoonnummer: