

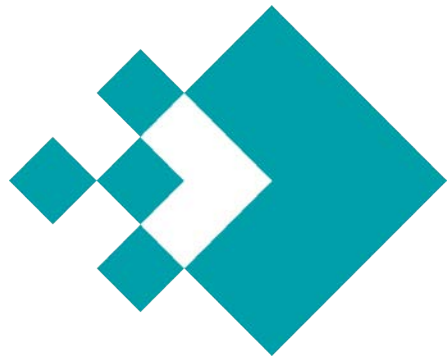
Gegevensbescherming bij MRDM in het kader van AVG

Paul Crauwels

Informatiebijeenkomst MRDM

17 mei 2018

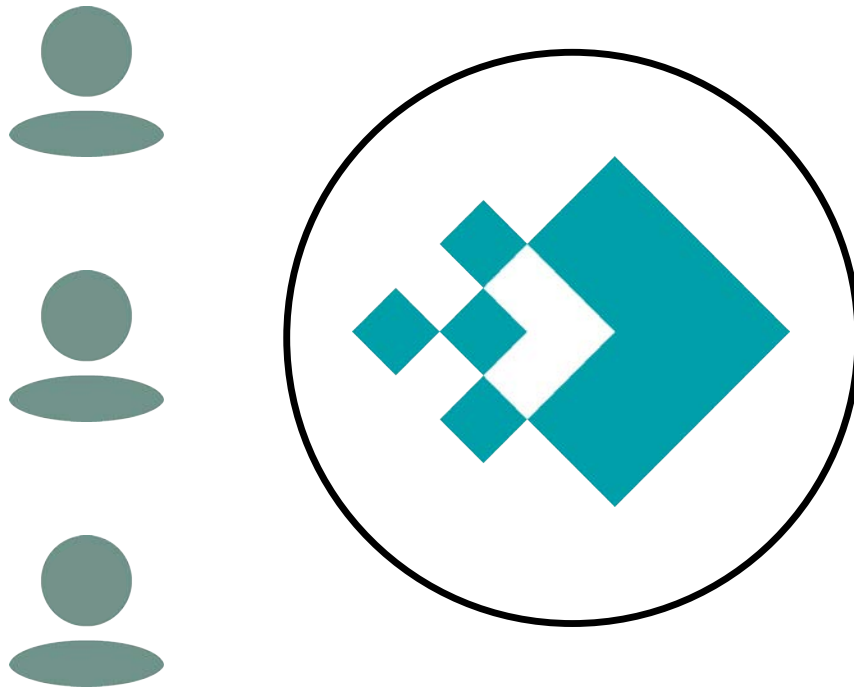




MRDM verzamelt medische gegevens
van zorginstellingen, patiënten en
andere leveranciers van medische
data...

en verwerkt en distribueert deze
IN OPDRACHT VAN de verantwoordelijke partij

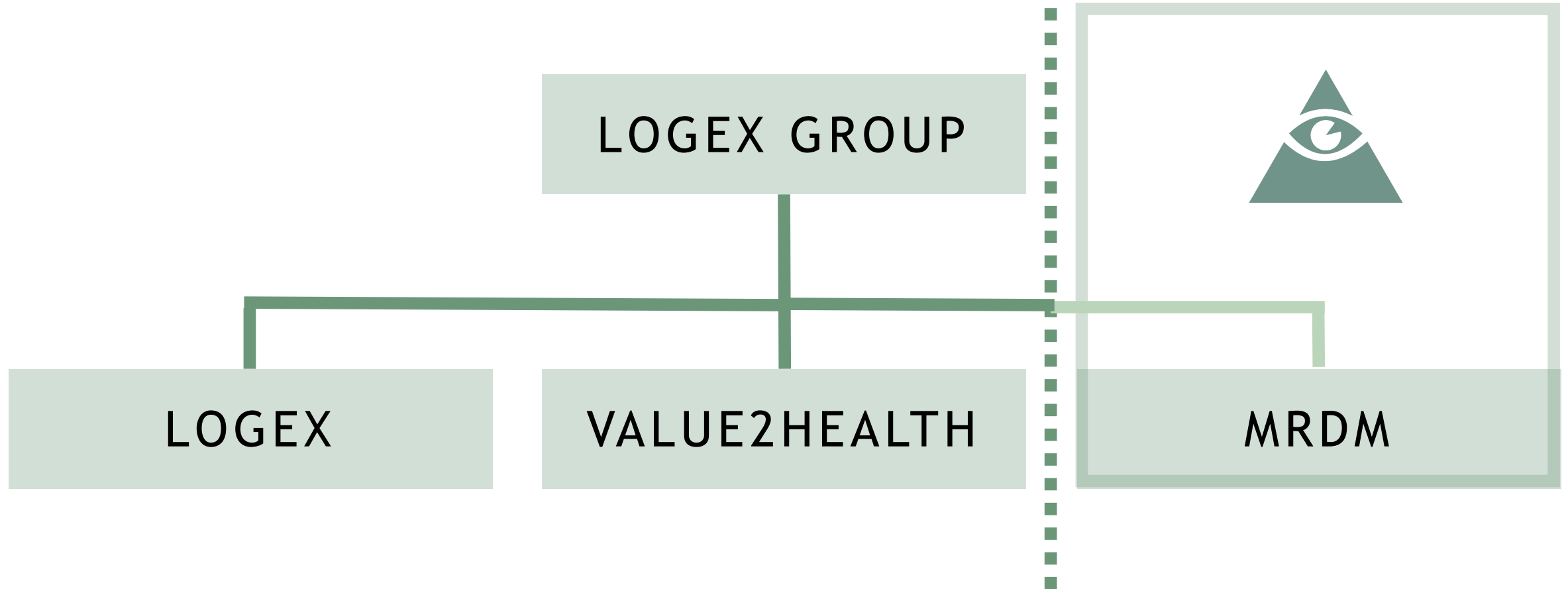
MRDM is een onafhankelijke partij



MRDM is een GEGEVENSVERWERKER

...en UITSLUITEND de verwerkingsverantwoordelijken
zijn onze OPDRACHTGEVERS

MRDM



De AVG in een notendop



Gegevensbescherming (AVG)

Persoonsgegevens

*‘alle informatie’ over een ‘geïdentificeerde-
of identificeerbare’ ‘natuurlijke persoon’*

Bijzondere persoonsgegevens: verwerken verboden tenzij ...

Door de aard van deze persoonsgegevens kan verwerking leiden

tot significante risico's voor de fundamentele rechten en vrijheid

van betrokkenen

*ras - etniciteit - politieke opvatting - vakbond -
religieuze of levensbeschouwelijke overtuiging - seksuele gerichtheid*



genetische-, biometrische- en gezondheidsgegevens

De AVG in een notendop (1)

(bron: website Autoriteit Persoonsgegevens)

Op basis hiervan mag je persoonsgegevens verzamelen

De grondslag



Toestemming
van de gebruiker



Vitale
belangen



Wettelijke
verplichting



Overeenkomst



Algemeen
belang



Gerechtvaardigd
belang



De AVG in een notendop (2)

(bron: website Autoriteit Persoonsgegevens)

Het begint aan de tekentafel Zorgvuldigheid



Functionaris
gegevensbescherming



Privacy
by design



Impact
assessment



De AVG in een notendop (3)

(bron: website Autoriteit Persoonsgegevens)

Technische en organisatorische maatregelen Verplichtingen



Register met alle
verwerkingen



Gegevens-
beschermingsbeleid



(Digitale)
beveiliging



De AVG in een notendop (4)

(bron: website Autoriteit Persoonsgegevens)

Mensen moeten controle kunnen uitoefenen Rechten van de betrokkenen



Recht om
in te zien



Recht om
te wijzigen



Recht om vergeten
te worden



Recht om gegevens
over te dragen



Recht op
informatie

Twee niet genoemde rechten van betrokkenen:

- *recht op bezwaar tegen verwerking, en*
- *recht op bezwaar tegen automated decision making*

Verantwoordingsplicht (accountability)

- Kunnen aantonen dat de verwerking voldoet aan de regels van de AVG:
 - *Rechtmatigheid*
 - *Transparantie*
 - *Doelbinding*
 - *Juistheid*
- Inzicht in genomen organisatorische en technische maatregelen om de persoonsgegevens te beschermen

Noodzakelijkheid

- Verwerkingsverantwoordelijken moeten beoordelen of de te verwerken persoonsgegevens geschikt en in overeenstemming zijn met het specifieke doel
 - *Bij elke gegevensverwerking moet de vraag gesteld worden of het doel ook bereikt kan worden met anonieme data en/of met minder data*
 - *Data worden ook als overbodig gezien als doel ook bereikt kan worden door bijv. alleen het geboortjaar of leeftijdsgroepen te registreren i.p.v. volledige geboortedatum*

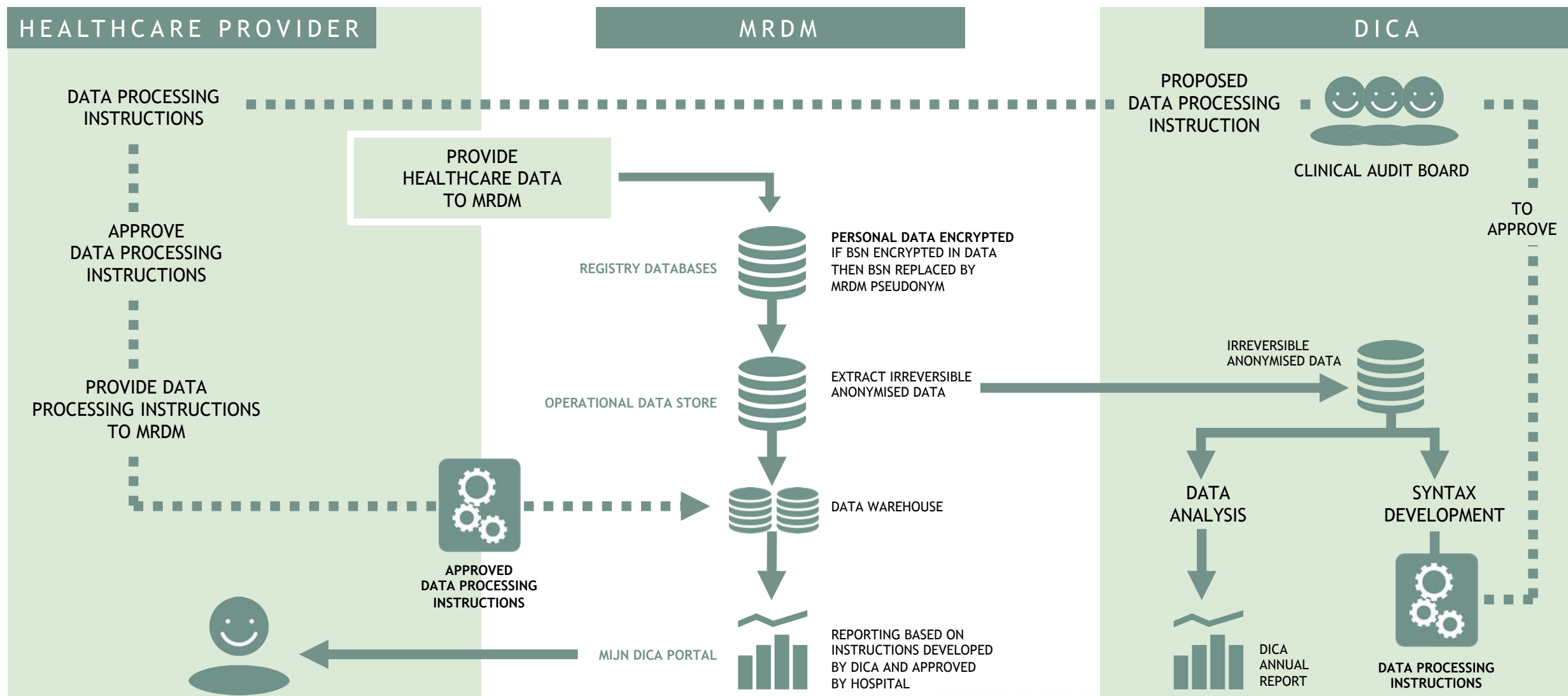
Verplichte maatregelen

- Het bijhouden van een register van verwerkingsactiviteiten
- Het uitvoeren van een data protection impact assessment (DPIA)
- Het bijhouden van een register van datalekken die zijn opgetreden
- Het kunnen aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor een gegevensverwerking wanneer voor die verwerking toestemming vereist is

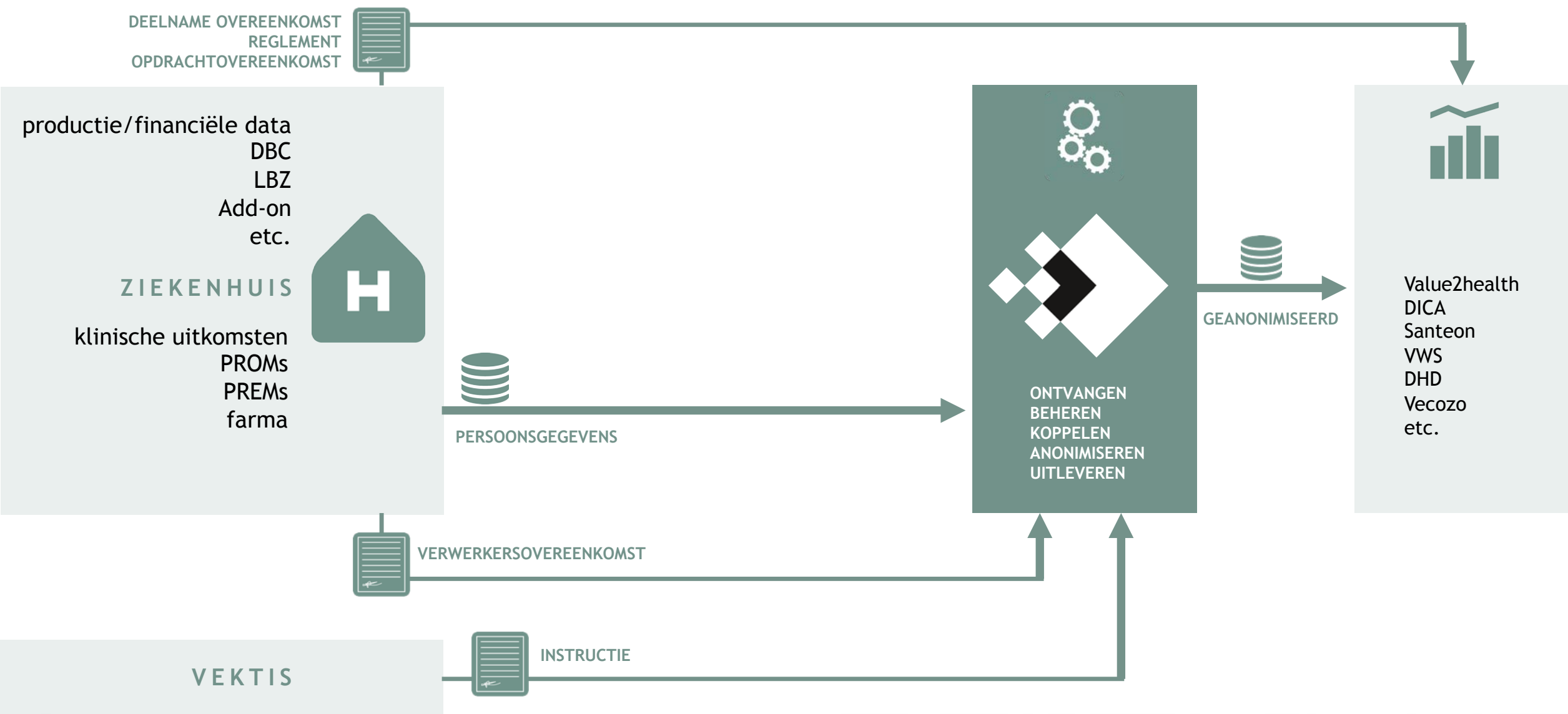
Data processing MRDM



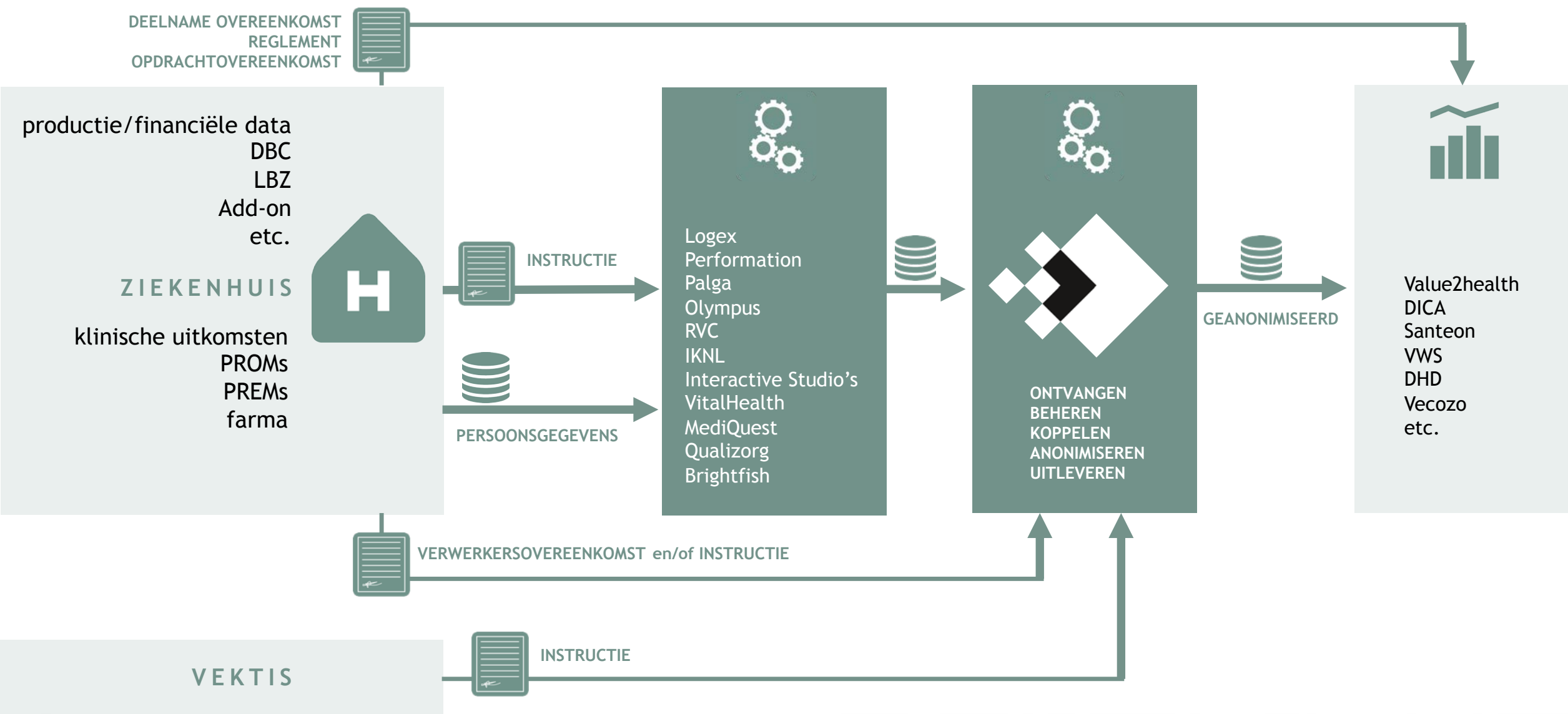
Data processing DICA clinical audits



Data processing MRDM



Data processing MRDM



Model Verwerkersovereenkomst Brancheorganisaties Zorg



verenigd in



Nieuwsbericht

MRDM verwerkersovereenkomst - positief advies NVZ

Op 8 mei 2018 geplaatst door  **Trudy Boshuizen**

Alle ziekenhuizen hebben aangepaste contracten van MRDM ontvangen waarbij het model BOZ-verwerkersovereenkomst is gebruikt. MRDM heeft de BOZ-verwerkersovereenkomst integraal overgenomen met slechts een enkele aanpassing opgenomen in Bijlage 4.

Deze aanpassingen zijn besproken met MRDM. De verwijzingen naar diverse bijlagen in de Opdrachtovereenkomst matchen niet met de aparte pdf-bijlagen. Dat is enigszins verwarrend maar niet noodzakelijk om aan te passen en alle contracten te herzien.

Er is slechts een kleine inhoudelijke wijziging afgesproken:

De afwijkende bepaling artikel 8.6a in Bijlage 4 van de Verwerkersovereenkomst wordt apart onder artikel 8.8 opgenomen en daarmee niet gekoppeld aan de bepaling over het vervallen van aansprakelijkheid in geval van opzet of grove schuld aan de zijde van de betreffende Partij (artikel 8.6).

Artikel 8.8 - Toevoeging:

De aansprakelijkheid van Verwerker ingevolge de leden 2 en 3 van dit artikel is beperkt tot Euro 2.500.000 per gebeurtenis en per jaar.

De ziekenhuizen krijgen een brief waarin deze aanpassing wordt beschreven. De brief dient vervolgens als bijlage bij de contracten te worden bewaard.

Instructie (1)

DEELNAMEOVEREENKOMST CLINICAL AUDIT

PARTIJEN:

1. De stichting **Dutch Institute for Clinical Auditing**, statutair gevestigd te Leiden en aldaar kantoorhoudende aan de Rijsburgerweg 10, hierbij rechtsgeldig vertegenwoordigd door dr. E.H. Eddes, hierna te noemen: "DICA",

en

2. De/Het statutair gevestigd te kantoorhoudende te aan de/het hierbij rechtsgeldig vertegenwoordigd door hierna te noemen: "Deelnemer";

Partijen sub 1 en sub 2 zullen hierna ieder afzonderlijk ook worden aangeduid als Partij en gezamenlijk als Partijen;

IN AANMERKING NEMENDE DAT:

- A. DICA een systeem heeft ontwikkeld voor het uitvoeren van clinical audits die bijdragen aan kwaliteitsborging, transparantie en verantwoording van de zorg en het tevens mogelijk

REGLEMENT DICA CLINICAL AUDIT

Toelichting

De DICA clinical audits dragen er zorg voor dat de deelnemende zorgaanbieders over betrouwbare informatie beschikken ten behoeve van kwaliteitsborging en verantwoording van de zorg.

Deelnemende zorgaanbieders kunnen daarmee voldoen aan de eisen die de Wet kwaliteit, klachten en geschillen in de zorg oplegt. Voor betrouwbare kwaliteitsinformatie is het noodzakelijk dat de zorg aan de patiënt op uniforme en wetenschappelijk verantwoorde wijze wordt geregistreerd. Op deze wijze kan 'spiegelinformatie' worden gegenereerd voor de deelnemende zorgaanbieders en de daaraan verbonden artsen. Zorgaanbieders kunnen deze spiegelinformatie gebruiken voor kwaliteitsverbetering en als verantwoordingsinformatie tegenover bijvoorbeeld zorgverzekeraars.

De gegevens die geregistreerd worden als gevolg van de clinical audits zijn voorts van grote waarde voor wetenschappelijk onderzoek. Binnen de grenzen van het Reglement, kan DICA op basis van een aanvraag van een wetenschapper besluiten om bepaalde gegevens voor dit doel ter beschikking te stellen.

In het kader van de uitvoering van de clinical audits, wordt gezondheidsinformatie van patiënten verwerkt. Zowel de Wet inzake de geneeskundige behandelingsovereenkomst (Wgbo) als de Wet bescherming persoonsgegevens (Wbp) is op die verwerking van toepassing. In opdracht van de zorgaanbieders bewerkt de bewerker (MRDM) deze gegevens zodanig dat DICA alleen Gecodeerde gegevens over de patiënten ontvangt die door haar niet meer direct tot een individuele patiënt te herleiden zijn. Als gevolg hiervan kunnen de deelnemende zorgaanbieders en DICA clinical audits uitvoeren die tot doel hebben om onderzoek naar kwaliteit van zorg en wetenschappelijk onderzoek

Instructie (2)

Instructie aan MRDM in de zin van artikel 3 lid 1 onder b van de met MRDM gesloten verwerkersovereenkomst

[Vul hier de naam van uw organisatie in] gevestigd te [vestigingsplaats], hierbij rechtsgeldig vertegenwoordigd door [naam en functie rechtsgeldige vertegenwoordiger], (hierna te noemen: Opdrachtgever)

Overwegende dat:

- Opdrachtgever met Value2Health BV is overeengekomen dat Value2health voor Opdrachtgever het product [De naam van het project, het informatieproduct of de dienst die Value2Health voor u gaat uitvoeren], (hierna te noemen: het Product) zal uitvoeren;
- Het Product samenvattend inhoudt dat [Omschrijving van het project, het informatieproduct of de dienst];
- Ten behoeve van het Product gegevens van de Opdrachtgever moeten worden verwerkt;
- Dit in de eerste fase van het Product het verwerken van persoonsgegevens omvat;
- MRDM BV en Logex BV bij deze eerste fase betrokken zijn;
- MRDM BV een deel van deze gegevens al verwerkt krachtens de op [Datum ondertekenen verwerkersovereenkomst met MRDM] gesloten verwerkersovereenkomst met de Opdrachtgever;
- Deze gegevens gecombineerd moeten worden met gegevens die Logex BV krachtens een verwerkersovereenkomst met de Opdrachtgever verwerkt;
- De bewerkingen voor het Product in de eerste fase van het Product door MRDM zullen worden uitgevoerd, waarna MRDM deze gegevens geanonimiseerd uitvoert naar Value2Health ten behoeve van verdere analyses en rapportages in het kader van het

Instructie aan VitalHealth in de zin van artikel 3 lid 1 onder b van de met VitalHealth gesloten verwerkersovereenkomst

[Vul hier de naam van uw organisatie in] gevestigd te [vestigingsplaats], hierbij rechtsgeldig vertegenwoordigd door [naam en functie rechtsgeldige vertegenwoordiger], (hierna te noemen: Opdrachtgever)

Overwegende dat:

- Opdrachtgever met Value2Health BV is overeengekomen dat Value2health voor Opdrachtgever het product [De naam van het project, het informatieproduct of de dienst die Value2Health voor u gaat uitvoeren], (hierna te noemen: het Product) zal uitvoeren;
- Het Product samenvattend inhoudt dat [Omschrijving van het project, het informatieproduct of de dienst];
- Ten behoeve van het Product gegevens van de Opdrachtgever moeten worden verwerkt;
- Dit in de eerste fase van het Product het verwerken van persoonsgegevens omvat;
- MRDM BV en Logex BV bij deze eerste fase betrokken zijn;
- MRDM BV een deel van deze gegevens al verwerkt krachtens de op [Datum ondertekenen verwerkersovereenkomst met MRDM] gesloten verwerkersovereenkomst met de Opdrachtgever;
- Deze gegevens gecombineerd moeten worden met gegevens die Logex BV krachtens een verwerkersovereenkomst met de Opdrachtgever verwerkt;
- De bewerkingen voor het Product in de eerste fase van het Product door MRDM zullen worden uitgevoerd, waarna MRDM deze gegevens geanonimiseerd uitvoert naar Value2Health ten behoeve van verdere analyses en rapportages in het kader van het

Instructie aan MediQuest in de zin van artikel 3 lid 1 onder b van de met MediQuest gesloten verwerkersovereenkomst

[Vul hier de naam van uw organisatie in] gevestigd te [vestigingsplaats], hierbij rechtsgeldig vertegenwoordigd door [naam en functie rechtsgeldige vertegenwoordiger], (hierna te noemen: Opdrachtgever)

Overwegende dat:

- Opdrachtgever met Value2Health BV is overeengekomen dat Value2health voor Opdrachtgever het product [De naam van het project, het informatieproduct of de dienst die Value2Health voor u gaat uitvoeren], (hierna te noemen: het Product) zal uitvoeren;
- Het Product samenvattend inhoudt dat [Omschrijving van het project, het informatieproduct of de dienst];
- Ten behoeve van het Product gegevens van de Opdrachtgever moeten worden verwerkt;
- Dit in de eerste fase van het Product het verwerken van persoonsgegevens omvat;
- MRDM BV en Logex BV bij deze eerste fase betrokken zijn;
- MRDM BV een deel van deze gegevens al verwerkt krachtens de op [Datum ondertekenen verwerkersovereenkomst met MRDM] gesloten verwerkersovereenkomst met de Opdrachtgever;
- Deze gegevens gecombineerd moeten worden met gegevens die Logex BV krachtens een verwerkersovereenkomst met de Opdrachtgever verwerkt;
- De bewerkingen voor het Product in de eerste fase van het Product door MRDM zullen worden uitgevoerd, waarna MRDM deze gegevens geanonimiseerd uitvoert naar Value2Health ten behoeve van verdere analyses en rapportages in het kader van het

Instructie aan IKNL in de zin van artikel 3 lid 1 onder b van de met IKNL gesloten verwerkersovereenkomst

[Vul hier de naam van uw organisatie in] gevestigd te [vestigingsplaats], hierbij rechtsgeldig vertegenwoordigd door [naam en functie rechtsgeldige vertegenwoordiger], (hierna te noemen: Opdrachtgever)

Overwegende dat:

- Opdrachtgever met Value2Health BV is overeengekomen dat Value2health voor Opdrachtgever het product [De naam van het project, het informatieproduct of de dienst die Value2Health voor u gaat uitvoeren], (hierna te noemen: het Product) zal uitvoeren;
- Het Product samenvattend inhoudt dat [Omschrijving van het project, het informatieproduct of de dienst];
- Ten behoeve van het Product gegevens van de Opdrachtgever moeten worden verwerkt;
- Dit in de eerste fase van het Product het verwerken van persoonsgegevens omvat;
- MRDM BV en Logex BV bij deze eerste fase betrokken zijn;
- MRDM BV een deel van deze gegevens al verwerkt krachtens de op [Datum ondertekenen verwerkersovereenkomst met MRDM] gesloten verwerkersovereenkomst met de Opdrachtgever;
- Deze gegevens gecombineerd moeten worden met gegevens die Logex BV krachtens een verwerkersovereenkomst met de Opdrachtgever verwerkt;
- De bewerkingen voor het Product in de eerste fase van het Product door MRDM zullen worden uitgevoerd, waarna MRDM deze gegevens geanonimiseerd uitvoert naar Value2Health ten behoeve van verdere analyses en rapportages in het kader van het

Instructie aan Logex in de zin van artikel 3 lid 1 onder b van de met Logex gesloten verwerkersovereenkomst

[Vul hier de naam van uw organisatie in] gevestigd te [vestigingsplaats], hierbij rechtsgeldig vertegenwoordigd door [naam en functie rechtsgeldige vertegenwoordiger], (hierna te noemen: Opdrachtgever)

Overwegende dat:

- Opdrachtgever met Value2Health BV is overeengekomen dat Value2health voor Opdrachtgever het product [De naam van het project, het informatieproduct of de dienst die Value2Health voor u gaat uitvoeren], (hierna te noemen: het Product) zal uitvoeren;
- Het Product samenvattend inhoudt dat [Omschrijving van het project, het informatieproduct of de dienst];
- Ten behoeve van het Product gegevens van de Opdrachtgever moeten worden verwerkt;
- Dit in de eerste fase van het Product het verwerken van persoonsgegevens omvat;
- Logex BV een deel van deze gegevens al verwerkt krachtens de op [Datum ondertekenen verwerkersovereenkomst met Logex] gesloten verwerkersovereenkomst met de Opdrachtgever;
- Deze gegevens in de eerste fase van het product door MRDM gecombineerd moeten worden met gegevens die MRDM BV krachtens een verwerkersovereenkomst met de Opdrachtgever verwerkt;
- De bewerkingen voor het Product in de eerste fase van het Product door MRDM zullen worden uitgevoerd, waarna MRDM deze gegevens geanonimiseerd uitvoert naar Value2Health ten behoeve van verdere analyses en rapportages in het kader van het

Informed consent



Informed consent clinical audits?

Grondslag voor verwerken persoonsgegevens is contract:

BEHANDELOVEREENKOMST

Doel clinical audits is verenigbaar met oorspronkelijk doel:

**GÉÉN CONSENT NODIG
WEL MOGELIJKHEID BIEDEN TOT BEZWAAR (OPT-OUT)**

Informed consent data processing



INFORMATIE



+

GEÏNFORMEERDE
PATIËNT

=

INFORMED CONSENT



KETENREGISTRATIE



ONDERZOEKSDOELEINDEN



ANDERE ZORGVERLENER



...

Voorwaarden voor consent

- Verantwoordelijke moet toestemming kunnen aantonen!
- Verzoek om toestemming moet
 - vrijelijk gegeven kunnen worden
 - begrijpelijk en in een gemakkelijk toegankelijke vorm, en
 - in duidelijke eenvoudige taal gepresenteerd worden,
 - Waarbij duidelijk is waar overal (dus uitputtende opsomming) toestemming voor gegeven wordt
- Voorziening om toestemming te allen tijde te kunnen intrekken, net zo simpel als het geven daarvan

Privacy Programma management



Gegevensbeschermingsbeleid (*verwerkersdomein*)

Contractmanagement

Register verwerkingen

Privacy functionarissen

Maatregelen

- ✓ *Verwerkersovereenkomsten*
 - *Verwerkersverantwoordelijken*
 - ✓ *Subverwerkers*
- ✓ *Instructies*
- ✓ *Actueel en raadpleegbaar*
- ✓ *Functiescheiding FG/PO/SO*
- ✓ *Organisatorische maatregelen*
- ✓ *Training en bewustwording*
- ✓ *VOG en geheimhouding*
- ✓ *Procedure meld(plicht)*
 - ✓ *Datalekken*
 - ✓ *Incidenten*
- ✓ *ISMS o.b.v. ISO27001 / NEN7510*

Data processing MRDM

Privacy by design



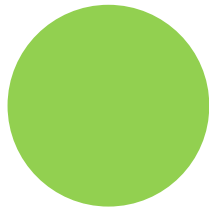
Privacy by design

Start bij verzamelen data

- Hergebruik bestaande informatie
- Zorginformatie eenmalig en eenduidig vastleggen
- Meervoudig gebruik voor verschillende doelen
- Versleutelen aan de bron

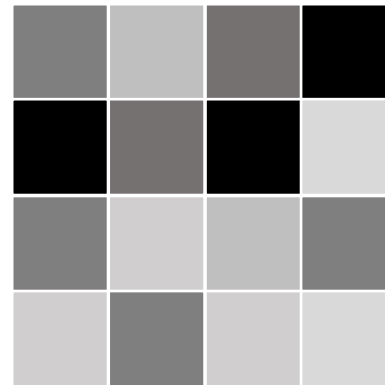
Focus op verwerkingsverantwoordelijke

VERWERKINGS
VERANTWOORDELIJKE



Gegevensbescherming op organisatieniveau

Focus op verwerkingsverantwoordelijke



Meerdere data typen:
HL7 FHIR / CDA
CSV, XML, TXT en XLS

Pseudonimisatie voorafgaand aan aanleveren van data aan MRDM

Focus op verwerkingsverantwoordelijke

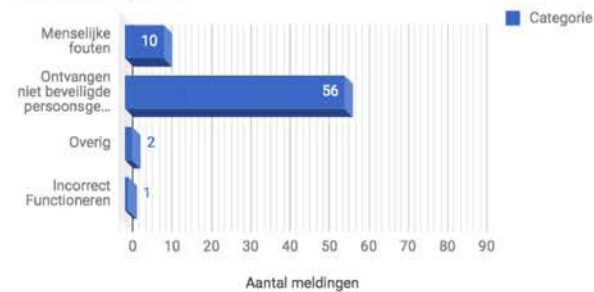
Verwerkingsverantwoordelijke
in control

- Volledig afgeschermd, eigen datakluis met secure inbox en secure outbox
- Volledige controle over eigen datakluis
- Managementinformatie over eigen datakluis
- Managementinformatie over gegevensverwerking

Incident monitoring

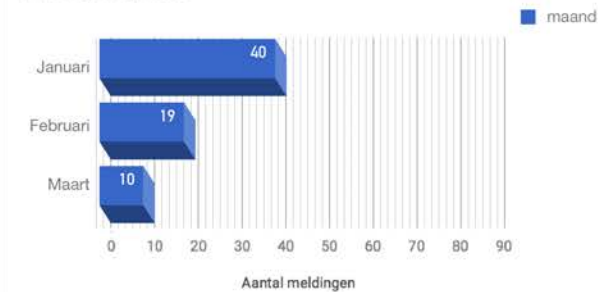
Aantal meldingen per categorie

Vanaf begin registratie

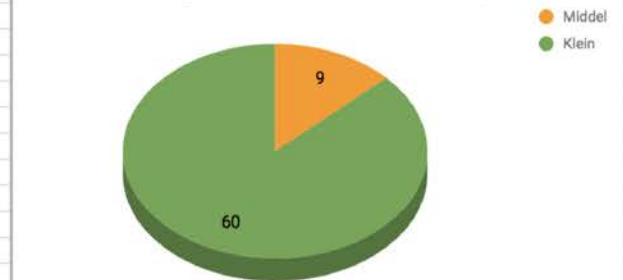


Aantal meldingen per maand

Vanaf begin registratie

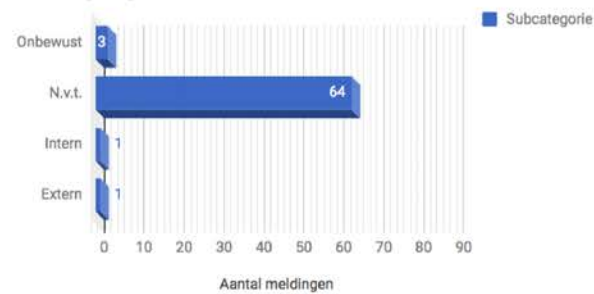


Aantal meldingen onderverdeeld naar Scope



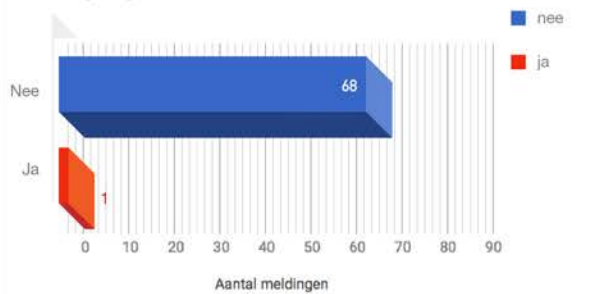
Aantal meldingen per subcategorie

Vanaf begin registratie



Aantal meldingen die een datalek zijn

Vanaf begin registratie



Aantal meldingen onderverdeeld naar Impact



Bent u klaar voor de AVG?
Hoe klaar bent u voor de AVG?

