**Vragenlijst gegevensbescherming voor wetenschappelijk onderzoek**

Deze vragenlijst dient om de naleving van de GDPR tijdens wetenschappelijke studies in GZA te garanderen.

De vragenlijst is zo eenvoudig mogelijk samengesteld. We schuiven één aandachtspunt naar voor wat betreft terminologie: *persoonsgegevens zijn alle gegevens (incl. beeld- en geluidsmateriaal) op basis waarvan een persoon kan worden geïdentificeerd of identificeerbaar is. In praktijk betekent dit dat alle gegevens die ooit aan een persoon waren gelinkt of gelinkt zijn, persoonsgegevens zijn.*

Ben je ervan overtuigd dat jouw dataset anoniem is en er derhalve geen persoonsgegevens zullen worden verwerkt, dan vragen we je daarover een motivering te schrijven waarin je aantoont dat elke identificatie onmogelijk is.

**Voorafgaandelijke vraag: worden tijdens dit onderzoek persoonsgegevens verwerkt?**

[ ]  **Ja**

*Vul onderstaande vragenlijst verder in.*

[ ]  **Nee, er worden enkel anonieme gegevens[[1]](#footnote-1)** **verwerkt:**

|  |
| --- |
| Motiveer en geef desgevallend de wijze waarop de persoonsgegevens worden geanonimiseerd. |

*Vul enkel Deel 6 van onderstaande vragenlijst in.*

# **Deel 1: Algemene toelichting van het onderzoek**

## Algemene informatie

* **Titel**: Geef de titel van het onderzoek.
* **Registratieloketnummer**: Geef bij het registratienummer verkregen van het Registratieloket

## Verwerkingsverantwoordelijke vs. Verwerker

* **Is er, naast ZAS, nog een andere partij betrokken bij het onderzoek?**

[ ]  Nee, het betreft een monocentrisch onderzoek van ZAS of een onderzoeker van ZAS, zonder betrokkenheid van een andere partij

[ ]  Ja

Wie bepaalt doel en middelen van het onderzoek (financiering alleen is onvoldoende)?

[ ]  ZAS of een onderzoeker van ZAS bepaalt dit (ZAS is verwerkingsverantwoordelijke; de andere partij betrokken bij het onderzoek, treedt op als verwerker of is een aparte verwerkingsverantwoordelijke)

[ ]  ZAS of een onderzoeker van ZAS bepaalt dit samen met een andere partij (gezamenlijke verwerkingsverantwoordelijken)

[ ]  ZAS of een onderzoeker van ZAS voert het onderzoek uit op instructie van een andere partij buiten ZAS (ZAS is verwerker)

[ ]  Dit wordt uitsluitend door een andere partij buiten ZAS bepaald, en ZAS of een onderzoeker van ZAS treedt niet op als verwerker (zuivere doorgifte van verwerkingsverantwoordelijke naar verwerkingsverantwoordelijke)

Werd met deze andere partij een overeenkomst afgesloten waarin bepaald wordt op welke wijze de persoonsgegevens moeten worden verwerkt?

 [ ]  Ja

*Gelieve de overeenkomst als bijlage toe te voegen bij deze vragenlijst.*

[ ]  Nee

## Uitvoering onderzoeksprotocol

* Is de persoon die het onderzoek uitvoert ook betrokken bij de zorg van de deelnemer (m.a.w. heeft de onderzoeker een therapeutische relatie met de deelnemer)?

[ ]  Ja

[ ]  Nee

* Zijn er personen of organisaties die onderzoeksactiviteiten uitvoeren die geen arbeidsrelatie hebben met het ziekenhuis (bv. zelfstandige onderzoekers of kwaliteitsmedewerkers, vertrouwde derde partij (*trusted third party*), etc.)?

[ ]  Ja, namelijk: Geef naam/namen

Werd met deze personen of organisatie een overeenkomst afgesloten waarin bepaald wordt op welke wijze zij de persoonsgegevens dienen te verwerken?

 [ ]  Ja

*Gelieve de overeenkomst als bijlage toe te voegen bij deze vragenlijst.*

[ ]  Nee

[ ]  Nee

## Voorafgaande controle inzake gegevensbescherming

Werd het onderzoek reeds extern voorgelegd voor een advies of besluitvorming inzake gegevensbescherming?

[ ]  Ja (bv. bij een (externe) DPO, een advocatenkantoor, een toezichthouder inzake gegevensbescherming zoals de Gegevensbeschermingsautoriteit of het Informatieveiligheidscomité, …)

*Gelieve het advies als bijlage toe te voegen bij deze vragenlijst.*

[ ]  Nee

## Welke (gepseudonimiseerde) persoonsgegevens worden verwerkt?

*Bespreek van wie (functies, geen namen) je gegevens verwerkt. Denk hierbij aan alle personen (ook wel betrokkene genoemd zoals aangegeven in onderstaande tabel). Ook de onderzoekers zelf bijvoorbeeld zijn ‘betrokkenen’. Vul onderstaande tabel 1.b in.*

Tabel 1.a: **Voorbeeld**



Tabel 1.b: **In te vullen tabel**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr. | Betrokkene (van wie zijn de gegevens) | Wie verwerkt deze gegevens? | Welke gegevens? | Wat is de bron van de gegevens? | Waarom? |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Worden (gepseudonimiseerde) persoonsgegevens doorgegeven aan derden[[2]](#footnote-2), tijdens en/of na afloop van het onderzoek

[ ]  Persoonsgegevens worden **niet doorgegeven aan derden**

[ ]  Persoonsgegevens worden doorgegeven aan **ontvangers in België of een ander land binnen de Europese Economische Ruimte (EER)[[3]](#footnote-3)**, namelijk:

* + - Het betreffen volgende gegevens: Geef de relevante nummers uit tabel 1.b.
		- Worden deze gegevens voorafgaandelijk aan de doorgifte beperkt (bv. worden identificatoren zoals naam, patiëntennummer, Rijksregisternummer verwijderd)?

[ ]  Ja, namelijk: Geef de (wijze van) beperking.

[ ]  Nee

* + - Wanneer zullen deze gegevens worden doorgegeven? Geef het moment van de doorgifte.
		- Wie is de ontvanger van deze gegevens? Geef de partij(en) aan wie de gegevens worden doorgegeven.
		- Is er een overeenkomst (*data transfer agreement*) afgesloten inzake de doorgifte?

[ ]  Ja, namelijk: Geef de partijen tussen wie deze overeenkomst werd afgesloten

*Gelieve de overeenkomst als bijlage toe te voegen bij de vragenlijst.*

[ ]  Nee

[ ]  Persoonsgegevens worden doorgegeven aan **ontvangers buiten de Europese Economische Ruimte (EER)[[4]](#footnote-4)**, namelijk:

* + - Het betreffen volgende gegevens: Geef de relevante nummers uit tabel 1.b.
		- Worden deze gegevens voorafgaandelijk aan de doorgifte beperkt (bv. worden identificatoren zoals naam, patiëntennummer, Rijksregisternummer verwijderd)?

[ ]  Ja, namelijk: Geef de (wijze van) beperking.

[ ]  Nee

* + - Wanneer zullen deze gegevens worden doorgegeven? Geef het moment van de doorgifte.
		- Wie is de ontvanger van deze gegevens? Geef de partij(en) aan wie de gegevens worden doorgegeven.
		- Is er een overeenkomst (*data transfer agreement*) afgesloten inzake de doorgifte?

[ ]  Ja, namelijk: Geef de partijen tussen wie deze overeenkomst werd afgesloten

*Gelieve de overeenkomst als bijlage toe te voegen bij de vragenlijst.*

[ ]  Nee

## Beheer van incidenten

|  |
| --- |
| Bespreek op welke manier incidenten m.b.t. de verwerking van persoonsgegevens – zoals het verlies van gegevens – zullen worden gemeld vóór, tijdens en na het onderzoek. Vb. voor het studiepersoneel van het ziekenhuis zal dit steeds dienen te gebeuren via iProva. |

# **Deel 2: Inzamelen van persoonsgegevens met het oog op onderzoek**

## Gegevensbronnen tijdens de selectie van deelnemers, vóór de start van het onderzoek

*Duid aan hoe de selectie van deelnemers zal plaatsvinden.*

[ ]  De **behandelend arts kijkt manueel in het EPD** om geschikte deelnemers te vinden.

[ ]  Een door de behandelend arts **aangewezen persoon kijkt in het EPD** om geschikte deelnemers te vinden.

[ ]  Er wordt een vraag gesteld aan het **datawarehouse** team van het ziekenhuis, domeinexperten of rapportbouwers voor een selectie van patiëntengegevens uit het EPD.

[ ]  **Patiënten** met een bepaalde pathologie worden gevraagd om deel te nemen. Er worden geen gegevensbronnen geconsulteerd.

[ ]  **Anders**, namelijk: Licht dit kort toe.

## Gegevensbronnen tijdens de uitvoering van het onderzoek

*Wat is de bron van de onderzoeksgegevens? Duid aan wat van toepassing is en vul verder aan.*

[ ]  Er worden tijdens het onderzoek gegevens **uit het EPD** van de deelnemer gehaald. (*zie ook vraag 11*)

[ ]  Er worden gegevens verzameld tijdens het onderzoek, **in interactie met de deelnemer**: Verklaar op welke wijze dit gebeurt. Bv. vragenlijsten, bloedstalen, medisch onderzoek, …

[ ]  **Andere bronnen** (dan het EPD en de deelnemer), namelijk: Licht dit kort toe.

## Gegevensverzameling uit het EPD

*Duid aan wat van toepassing is met betrekking tot de gegevensverzameling uit het EPD*

[ ]  Er worden **op geen enkel moment** gegevens uit het EPD gehaald.

[ ]  Er worden gegevens uit het EPD gehaald **in het kader van retrospectief onderzoek**.

[ ]  Er worden gegevens uit het EPD gehaald of geconsulteerd **bij de selectie van deelnemers voor het onderzoek.**

* + Volgende personen hebben hierbij toegang tot het EPD: Geef de functie van deze personen. Bv. “behandelend arts”.
	+ Het betreffen volgende gegevens: Geef de relevante nummers uit tabel 1.b.

[ ]  Er worden gegevens uit het EPD gehaald **na ondertekening van het ICF.**

* + Volgende personen hebben hierbij toegang tot het EPD: Geef de functie van deze personen. Bv. “behandelend arts”.
	+ Het betreffen volgende gegevens: Geef de relevante nummers uit tabel 1.b.

# **Deel 3: Pseudonimiseren van de persoonsgegevens**

## Persoonsgegevens in het onderzoeksdossier

*Welke identificatiegegevens (zoals naam, patiëntennummer, Rijksregisternummer, …) zijn aanwezig in het onderzoeksdossier? Vul onderstaande tabel aan:*

Tabel 2.a: **Voorbeeld**



Tabel 3.b: **In te vullen tabel**

|  |  |  |
| --- | --- | --- |
| Identificatiegegeven | In welke dataset | Waarom is deze informatie nodig? |
|  |  |  |
|  |  |  |
|  |  |  |

## Sleutelbeheerder

*Wanneer er voor de gepseudonimiseerde gegevens opgesomd in tabel 2.b met een sleutelbestand wordt gewerkt, antwoord dan op de volgende vragen.*

* Welk *format* heeft het sleutelbestand? Licht toe, bv. Word, Excel, …)
* Welke velden worden voorzien in het sleutelbestand? Licht toe.
* Wie is de beheerder van het sleutelbestand (niet nominatief, vb “de studiecoördinator”, “de kwaliteitsmedewerker van het ziekenhuis”, “een derde partij met name…”) Geef de functie van de beheerder, bv. “studiecoördinator, “kwaliteitsmedewerker van het ziekenhuis”, “een derde partij met name…”, …
* Wanneer wordt het sleutelbestand aangemaakt? Geef het moment van aanmaak tijdens het onderzoek, bv. voorafgaandelijk, tijdens, ...
* Wie vult het sleutelbestand in? Geef de naam/namen.
* Wie heeft toegang tot het sleutelbestand? Geef de functies en/of namen.
* Waar wordt het sleutelbestand bewaard? Licht toe, bv. cloud, lokale schijf, …
* Hoe wordt het sleutelbestand beveiligd? Licht toe, bv. d.m.v. een wachtwoord
* Hoe lang wordt het sleutelbestand bewaard? Geef tijdsaanduiding.

# **Deel 4: Verwerken van de onderzoeksgegevens**

## Tools voor de onderzoeker

*Welke ICT tools worden ingezet tijdens het onderzoek door de onderzoeker, wie levert deze en werd er met de leverancier een contract afgesloten inzake het verwerken van persoonsgegevens?*

Tabel 4.a: **Voorbeeld**



Tabel 5.b: **In te vullen tabel**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tool | Waarvoor dient de tool? | Wie levert de tool aan? | Contract tussen partijen inzake gegevensbescherming? | Wie gebruikt de tool |
|  |  |  |  |  |
|  |  |  |  |  |

## Tools voor de deelnemer

*Welke ICT tools worden ingezet tijdens het onderzoek voor de deelnemer, wie levert deze en werd er met de leverancier een contract afgesloten inzake het verwerken van persoonsgegevens?*

Tabel 4.a: **Voorbeeld**



Tabel 4.b: **In te vullen tabel**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tool | Waarvoor dient de tool? | Wie levert de tool aan? | Contract tussen partijen over gegevensbescherming? | Wie heeft toegang tot de (gegevens in deze) tool |
|  |  |  |  |  |
|  |  |  |  |  |

# **Deel 5: Verwerken van de onderzoeksgegevens na het onderzoek**

## Het verwerken van persoonsgegevens na het onderzoek

* Hoe lang worden de gegevens na het onderzoek bewaard? Geef de bewaartermijn.
* Verklaar deze bewaartermijn? Licht toe.
* Door wie worden de gegevens bewaard? Geef de functies en/of namen.
* Welke garanties worden geboden opdat de gegevens niet langer worden bewaard dan voorzien? Licht de procedure toe.

# **Deel 6: Afsluitende informatie**

*Volgende verplichtingen gelden onverkort voor elk onderzoek:*

* Onderzoeksgegevens mogen in geen geval voor andere doeleinden gebruikt worden dan weergegeven in deze vragenlijst zonder dat hiervoor een goedkeuring van een medisch ethische commissie werd verkregen.
* Deelnemers aan het onderzoek die via een ICF worden ingelicht, dienen een goed begrip te hebben over welke persoonsgegevens worden verwerkt en waarom. Zie *Annex 2* voor een checklist voor het ICF met het oog op het verwerken van persoonsgegevens.
* De persoonsgegevens die worden ingezameld tijdens het onderzoek zijn beperkt tot die gegevens die strikt noodzakelijk zijn om het onderzoek uit te voeren.
* Tijdens het onderzoek dienen maximale inspanningen te worden geleverd om de juistheid van de persoonsgegevens te garanderen.
* Persoonsgegevens worden niet langer dan nodig verzameld en bewaard. De bewaartermijnen zijn naar waarheid toegelicht in deze vragenlijst.
* De noodzakelijke technische en organisatorische maatregelen dienen te worden genomen met het oog op een veilige verwerking van persoonsgegevens. Deze maatregelen worden toegelicht in *Annex 3*.
* Na afloop van het onderzoek dient de medisch ethische commissie hiervan op de hoogte te worden gebracht.
* De adviezen van de DPO’s van alle betrokken organisaties dienen steeds nauwgezet te worden opgevolgd.
* Alle partijen - zowel onderzoekspartners, personeel als onderaannemers - zijn gebonden om de regels inzake gegevensbescherming na te leven.

|  |
| --- |
| ***Deze vragenlijst is naar waarheid ingevuld****Naam:* Geef je naam.*Functie:* Geef je functie.*Contactgegevens:* Geef je contactgegevens, bij voorkeur een e-mailadres.*Handtekening:* |

# *Annex 1: Minimale inhoud verwerkersovereenkomst (art. 28 GDPR)*

Wat de relatie verwerker – verwerkingsverantwoordelijke betreft, vereist art. 28 GDPR dat volgende zaken in een overeenkomst worden opgenomen:

* het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven
* De verwerkersovereenkomst bepaalt met name dat de verwerker:
	+ de persoonsgegevens uitsluitend verwerkt op basis van schriftelijke instructies van de verwerkingsverantwoordelijke, onder meer met betrekking tot doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, tenzij een op de verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de verwerker de verwerkingsverantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt
	+ waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden
	+ alle overeenkomstig artikel 32 GDPR vereiste maatregelen neemt (beveiligingsmaatregelen)
	+ geen andere verwerker in dienst neemt zonder voorafgaande specifieke of algemene schriftelijke toestemming van de verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht de verwerker de verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers, waarbij de verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.
	+ Wanneer een verwerker een andere verwerker in dienst neemt om voor rekening van de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst of een andere rechtshandeling krachtens Unierecht of lidstatelijk recht dezelfde verplichtingen inzake gegevensbescherming opgelegd als diegene die tussen de verwerkingsverantwoordelijke en de verwerker zijn opgenomen, met name de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de verwerking aan het bepaalde in deze verordening voldoet. Wanneer de andere verwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de eerste verwerker ten aanzien van de verwerkingsverantwoordelijke volledig aansprakelijk voor het nakomen van de verplichtingen van die andere verwerker
	+ rekening houdend met de aard van de verwerking, de verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand verleent bij het vervullen van diens plicht om verzoeken om uitoefening van de rechten van de betrokkene te beantwoorden
	+ rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen m.b.t. beveiliging, melding van inbreuken, het uitvoeren van gegevensbeschermingseffectbeoordelingen en het voorafgaand raadplegen van de toezichthoudende overheid
	+ na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt, en bestaande kopieën verwijdert, tenzij opslag van de persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht;
	+ de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om de nakoming van de in dit artikel neergelegde verplichtingen aan te tonen en audits, waaronder inspecties, door de verwerkingsverantwoordelijke of een door de verwerkingsverantwoordelijke gemachtigde controleur mogelijk maakt en eraan bijdraagt.

De verwerker stelt de verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op deze verordening of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

# *Annex 2: Informatieplicht aan betrokkenen (art. 13 – 14 GDPR)*

**Indien de gegevens rechtstreeks bij de deelnemers zelf worden verzameld (primaire verwerking)**, moet volgende informatie worden meegedeeld aan de betrokkenen:

* Contactgegevens van de verwerkingsverantwoordelijke(n) (en diens DPO)
* Het doel waarvoor hun persoonsgegevens verwerkt zullen worden
* De wettelijke basis voor de verwerking van hun persoonsgegevens
* Indien de verwerking gebaseerd is op de rechtsgrond ‘gerechtvaardigde belangen’: een argumentatie van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke
* Indien de verwerking gebaseerd is op de rechtsgrond ‘toestemming’: de vermelding dat de betrokkene het recht heeft de toestemming ten allen tijde in te trekken
* De personen of organisaties waarmee de persoonsgegevens gedeeld zullen worden
* Of er een transfer zal gebeuren van hun persoonsgegevens naar een derde land of een internationale organisatie. Indien er een transfer plaatsvindt, moet aangegeven worden welke waarborgen genomen worden om de privacy van de betrokkenen te beschermen
* Hoe lang de persoonsgegevens bewaard zullen worden
* Wat de rechten van de betrokken zijn en hoe deze uitgeoefend kunnen worden
* Dat de betrokkenen het recht heeft om klacht in te dienen bij de toezichthoudende autoriteit

**Indien de persoonsgegevens niet rechtstreeks van de betrokkenen verkregen zijn (een secundaire verwerking)**, moet daarnaast ook nog de volgende informatie worden meegegeven:

* De bron waar de persoonsgegevens vandaan komen
* Indien van toepassing: het bestaan van geautomatiseerde besluitvorming

**Indien de rechten van de betrokkenen tijdens de studie worden beperkt (bij primaire of secundaire verwerking)**, bv. omdat het om een (dubbel)blinde studie gaat en de betrokkene niet mag weten of hij al dan niet in de placebogroep zit, dan moet bijkomend ook nog de volgende informatie worden meegedeeld aan de betrokkene:

* Dat de persoonsgegevens al dan niet worden geanonimiseerd

De redenen waarom de uitoefening van de rechten van de betrokkene de verwezenlijking van de doeleinden onmogelijk dreigt te maken of ernstig dreigt te belemmeren.

# *Annex 3: Principes van informatieveiligheid*

De indiener van het onderzoek zorgt minstens voor de volgende beveiligingsmaatregelen:

(a) fysieke toegang tot de kantoren en informatieverwerkingsfaciliteiten beperken tot werknemers, personeel en goedgekeurde bezoekers;

(b) bewaking van de ontvangstruimten voor kantoren en informatieverwerkingsfaciliteiten door een receptionist of bewaker; toegang buiten openingstijden controleren;

(c) het verstrekken van toegangskaarten en sleutels aan datacenters, server- en back-upruimtes uitsluitend aan bevoegde personen; regelmatige beoordelingen van toegangsrechten uitvoeren;

(d) ervoor te zorgen dat geen ongeautoriseerde personen toegang hebben tot en / of de ontgrendelde schermen kunnen zien van de computerapparatuur die door medewerkers en personeel van de instelling worden gebruikt voor gegevensinvoer op het moment van gegevensinvoer;

(e) het implementeren van een verbod om de persoonlijke gegevens op te slaan op mobiele apparaten of mediakaarten van apparaten, tenzij gecodeerd met 128-bits of hogere codering en apparaten te beheren via gecentraliseerde apparaatbeheersoftware die op afstand kan vergrendelen en wissen verloren / gestolen apparaten;

(f) accounts met een individuele login en wachtwoord toewijzen aan geautoriseerde gebruikers; het voorzien van procedures voor account creatie, verandering, verwijdering controle; implementeren van op rollen gebaseerde toegangscontrole in gegevensverwerkingssystemen; en differentiëren toegangsniveaus voor gebruikers en geprivilegieerde toegang;

Het creëren van toegang voor de werknemer gebeurt op basis van documenten waaruit de identiteit van de persoon blijkt.

(g) zorgen voor duurzame identificatie en authenticatie in een virtuele omgeving; centraal vastleggen van gebruikerstoegang in virtuele omgeving;

(h) implementeren van een wachtwoordbeleid dat wachtwoorden van ten minste 8 (acht) tekens vereist, geen overeenkomst met vorige 5 (vijf) wachtwoorden; verplichte regelmatige wijziging van wachtwoorden;

(i) het implementeren van regels voor verzending via openbare of draadloze netwerken van wachtwoorden, los van informatie over accounts en / of beschermde gegevensbestanden, tenzij gecodeerd met ten minste 128-bit codering of verzonden via het gecodeerde communicatiekanaal;

(j) implementatie van netwerk-, applicatie-, databasebeveiliging door middel van firewalls en antivirus / anti-malware;

(k) zorgen voor detectie van malware die is bedoeld voor ongeoorloofde verwijdering, blokkeren, kopiëren van informatie, uitschakelen van beveiligingsmaatregelen; en reactie op dergelijke aanvallen;

(l) vastlegging van beveiligingsgebeurtenissen / incidenten in informatiesystemen; het implementeren van procedures voor rapportage, analyse, monitoring en oplossing van beveiligingsincidenten;

(m) het configureren van computersystemen voor het automatisch ontvangen van besturingssysteempatches en updates van een gecentraliseerde service die updates beheert en verspreidt;

(n) zorgen voor een back-up van informatiesystemen, computers en software die betrokken zijn bij de uitvoering van het onderzoek;

(o) gegevens van de interne en externe actoren (sponsor, CRO, andere onderzoeken, …) scheiden van elkaar, zodat vermenging van gegevens wordt vermeden en extractie en teruggave aan de juiste partij kan worden gegarandeerd;

(p) het implementeren van procedures en praktijken voor de veilige vernietiging van papieren documenten die persoonsgegevens bevatten;

(q) het implementeren van bedrijfscontinuïteitsprocedures die ervoor zorgen dat de onderzoeksdiensten kunnen gegarandeerd blijven;

(r) passende gegevensbeschermings- en informatiebeveiligingstrainingen bieden aan de werknemers en personeel.

1. Anonieme gegevens zijn gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Anonieme gegevens onderscheiden zich van pseudonieme gegevens. Dergelijke pseudonieme gegevens zijn persoonsgegevens die niet meer aan specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt die apart worden bewaard en waarvoor technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat zij niet rechtstreeks aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. [↑](#footnote-ref-1)
2. Een derde is *“een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken*”, m.a.w.: een andere partij dan de opdrachtgever (sponsor) van het onderzoek, het ziekenhuis en de onderzoekers betrokken bij het onderzoek. [↑](#footnote-ref-2)
3. Alle EU-landen, plus Liechtenstein, Noorwegen en IJsland. [↑](#footnote-ref-3)
4. Zie voetnoot 3. [↑](#footnote-ref-4)