Koninklijk Nederlands Genootschap voor Fysiotherapie

Dataprotocol Landelijke Database Fysiotherapie (LDF)

Versiebeheer

Versie	Status	Datum	Auteur(s)	Opmerkingen
1.0	Concept	2 februari 2016	SOLV	
2.0	Concept	mei 2019	Immix	
3.0	Definitief	september 2019	Immix	
4.0	Definitief	maart 2020	JEAN Legal	
5.0	Definitief	November 2020	JEAN Legal	
6.0	Definitief	April 2021	JEAN Legal	

Inhoud

1. Inleiding

1.1 Achtergrond

Het Koninklijk Nederlands Genootschap voor Fysiotherapie (hierna te noemen: “KNGF”) heeft in het kader van haar kwaliteitsbeleid in 2013 een landelijke database ontwikkeld, genaamd de Landelijke Database Fysiotherapie (hierna te noemen: “LDF”). In de LDF worden gegevens verzameld die de medewerkers van een fysiotherapiepraktijk gedurende het zorgproces van een patiënt vastleggen in het elektronische patiëntendossier (hierna te noemen: “EPD”). Wanneer een fysiotherapiepraktijk is aangesloten bij de LDF worden gegevens vanuit het EPD eens per maand aan de LDF geleverd door de fysiotherapiepraktijk. Het betreft gepseudonimiseerde gegevens over de patiënt, gegevens over de behandeling, de fysiotherapeut en de fysiotherapiepraktijk. Hieronder vallen ook (bijzondere) persoonsgegevens (hierna te noemen: “persoonsgegevens van patiënten en fysiotherapeuten”).

De gegevens in de LDF worden verzameld met de volgende drie doelen:

1. Kwaliteitsborging
2. Wetenschappelijk onderzoek
3. Beleidsontwikkeling

Om deze doelen te kunnen bereiken, worden de in de LDF verzamelde gegevens (data) omgezet in informatie die teruggekoppeld wordt aan de eindgebruiker(s). Deze informatie gaat onder andere over de dossiervoering, de behaalde behandelresultaten en het behandelgemiddelde. Deze terugkoppeling van informatie wordt met name gedaan via het LDF-Dashboard waarop de fysiotherapeut via een webapplicatie kan inloggen, maar kan ook worden gedaan in wetenschappelijke publicaties of in beleidsrapporten.

1.2 Doel Dataprotocol LDF

Het doel van dit Dataprotocol LDF is het geven van een duidelijke beschrijving over de wijze van verkrijging en verwerking van persoonsgegevens van patiënten en fysiotherapeuten, die in de LDF worden opgenomen. Aanvullend wordt in dit Dataprotocol LDF beschreven op welke wijze uitvoering wordt gegeven aan de wettelijke verplichtingen die voortvloeien uit onder andere de Algemene Verordening Gegevensbescherming (Verordening (EU) nr. 2016/679). In hoofdstuk 2 wordt eerst het wettelijk kader dat geldt voor de in de LDF verzamelde persoonsgegevens toegelicht. In hoofdstuk 3 worden de betrokken partijen en de rolverdeling toegelicht. Hoofdstuk 4 bevat een beschrijving van het proces van de verzameling en verwerking van de persoonsgegevens. Hoofdstuk 5 beschrijft het beheer en de beveiliging van de persoonsgegevens. Tot slot gaat hoofdstuk 6 over controle en rapportage.

De laatst geldende versie van het Dataprotocol wordt gepubliceerd op https://www.kngf.nl/ldf.

2. Wettelijk kader

Binnen Europa zijn de voorwaarden waaronder persoonsgegevens van natuurlijke personen[1] mogen worden verwerkt geregeld in de Algemene Verordening Gegevensbescherming (hierna: de "AVG"). De AVG hanteert de volgende begrippen:

> ***Verwerking***[2]*: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen wissen of vernietigen van gegevens.*
>
> ***Persoonsgegevens***[3]*: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.*
>
> ***Bijzondere persoonsgegevens***[4]***:*** *persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.*

De verantwoordelijke voor de gegevensverwerking, de verwerkingsverantwoordelijke, dient ervoor te zorgen dat de verwerking in overeenstemming met de AVG plaatsvindt. Daarbij kan de verwerkingsverantwoordelijke de feitelijke verwerking laten uitvoeren door een derde. Deze derde, de verwerker, dient de persoonsgegevens te verwerken in overeenstemming met het doel en de middelen die de verwerkingsverantwoordelijke bepaalt. De verwerker mag de persoonsgegevens dus niet gebruiken voor andere doeleinden.

In de LDF zijn persoonsgegevens van fysiotherapeuten en patiënten opgenomen. Het KNGF bepaalt het doel en de middelen voor het verwerken van de persoonsgegevens. De data in de LDF zijn afkomstig van derden, namelijk fysiotherapiepraktijken. Fysiotherapiepraktijken verschaffen deze data

[1] De betrokkene: degene op wie een persoonsgegeven betrekking heeft (artikel 4 lid 1 AVG).
[2] Artikel 4 lid 2 AVG.
[3] Artikel 4 lid 1 AVG.
[4] Artikel 9 lid 1 AVG.

zonder dat zij inspraak hebben in wat hier vervolgens mee gebeurt. Daarom sluiten zij door middel van algemene voorwaarden verwerkersovereenkomsten met het KNGF. De fysiotherapiepraktijk is en blijft verwerkingsverantwoordelijk voor de aangeleverde data ten aanzien van het eigen gebruik van data. Het KNGF wordt verwerkingsverantwoordelijk voor de data zodra deze in de LDF zijn opgenomen. Dit staat los van de verwerkingsverantwoordelijkheid van de fysiotherapiepraktijken. De gegevens van patiënten zijn enkel herleidbaar voor de EPD-leverancier.

De EPD-leverancier beheert de sleutel die de gepseudonimiseerde informatie in de LDF herleidbaar maakt tot de persoon (zie ook hoofdstuk 4). Op die manier kunnen het KNGF en haar partners en Andere Partijen niet beschikken over deze gegevens. Dat betekent dat deze gegevens niet geanonimiseerd zijn, maar wel ‘gepseudonimiseerd’. In dit Dataprotocol noemen wij de gepseudonimiseerde (bijzondere) persoonsgegevens van patiënten verder ‘patiëntgegevens’. Voordat de patiëntgegevens gepseudonimiseerd aan het KNGF worden verstrekt, verleent de patiënt hiervoor expliciete toestemming aan de fysiotherapiepraktijk. Deze toestemming voldoet aan de wettelijke vereisten.

Het KNGF laat de verwerking binnen de LDF uitvoeren door haar partner Mediquest B.V. Deze partij is aan te merken als verwerker. Ook is het in de toekomst mogelijk dat een of meer andere daartoe geschikte partij(en) ingezet wordt/ worden als verwerker.

Andere Partijen ontvangen ook patiëntgegevens, die zij gebruiken voor wetenschappelijk onderzoek, kwaliteitsborging of beleidsontwikkeling. Zij zijn aan te merken verwerkingsverantwoordelijke en soms ook als verwerker. Het KNGF en deze Andere Partijen hebben (samenwerkings)overeenkomsten gesloten die - afhankelijk van de feitelijke situatie - in de voorwaarden van de verwerking en de verwerkingsverantwoordelijkheid voorziet.

3. Partijen en rolverdeling

De bij dit Dataprotocol LDF betrokken partijen zijn:

KNGF: De vereniging met volledige rechtsbevoegdheid **Koninklijk Nederlands Genootschap voor Fysiotherapie**, gevestigd te (3817BA) Amersfoort aan de Stadsring 159 B is verwerkingsverantwoordelijke voor de verwerking van de persoonsgegevens van de fysiotherapeuten en de patiëntgegevens in het kader van de LDF.

Mediquest: De besloten vennootschap **Mediquest B.V.**, gevestigd te (3581KP) Utrecht aan de Burgemeester Reigerstraat 89 is als ICT dienstverlener verwerker van de persoonsgegevens van de fysiotherapeuten en de patiëntgegevens in het kader van de LDF in opdracht van het KNGF.

Bovenstaande partijen worden in dit Dataprotocol LDF tevens individueel “Partij” en tezamen “Partijen” genoemd. Naast deze Partijen spelen de volgende partijen een rol in het kader van de LDF:

Betrokkenen: De patiënten en fysiotherapeuten van wie persoonsgegevens worden verstrekt aan het KNGF.

Fysiotherapiepraktijk: De fysiotherapiepraktijk die deelneemt aan de LDF en daartoe, met toestemming van zijn medewerkers persoonsgegevens over hen aan het KNGF verstrekt, alsook met toestemming van de patiënt patiëntgegevens aan het KNGF verstrekt.

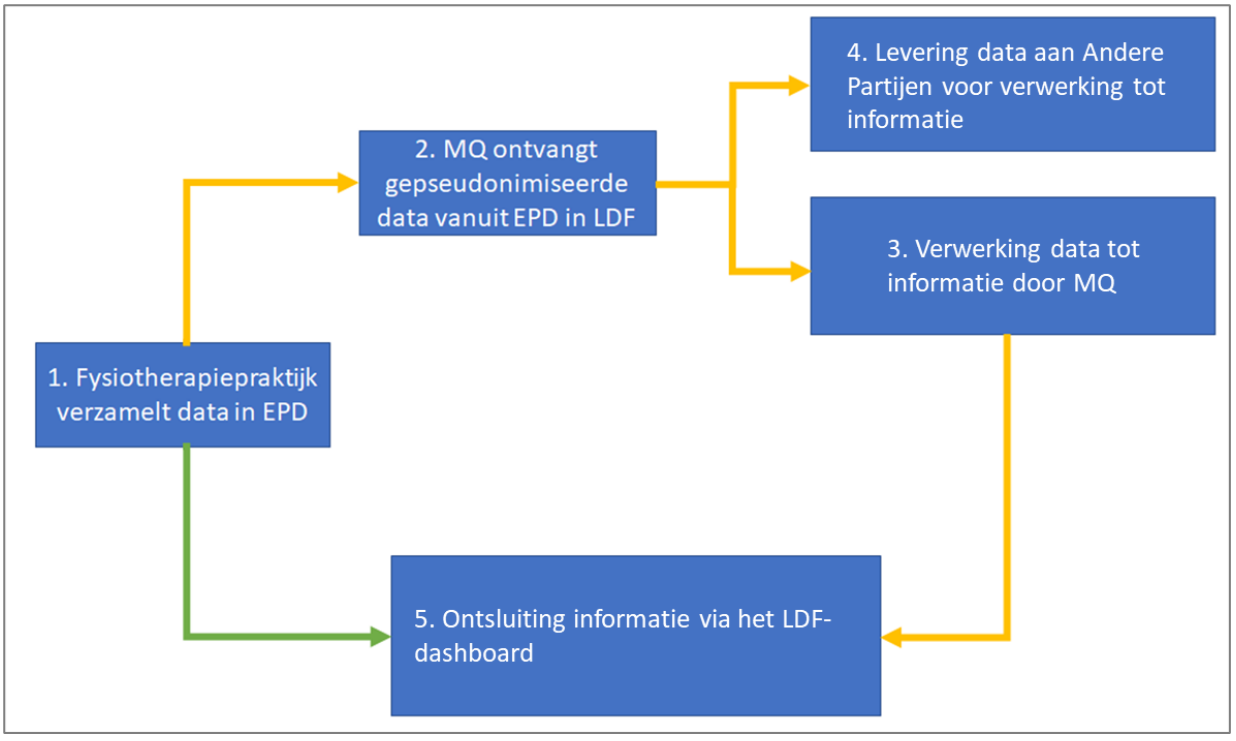
EPD Leverancier: De aanbieder van een ICT-omgeving voor het inrichten en onderhouden van elektronische patiëntendossiers (EPD’s), waaruit migratie van data plaatsvindt naar de LDF van het KNGF in opdracht van de fysiotherapiepraktijken.

Andere Partijen: Onderzoeksinstituten en/of andere derden, waaronder (netwerken van) fysiotherapeuten, die binnen het kader en onder de voorwaarden van dit Dataprotocol LDF gegevens uit de LDF verkrijgen ten behoeve van kwaliteitsborging, wetenschappelijk onderzoek of beleidsontwikkeling. Een actueel overzicht van Andere Partijen is te vinden op: https://www.kngf.nl/article/vak-en-kwaliteit/kwaliteit/ldf/juridische-informatie.

4. Dataproces

Schematische weergave van de dataflow

Het dataproces ten aanzien van de verwerking van de persoonsgegevens van fysiotherapeuten en patiëntgegevens in het kader van de LDF kan als volgt schematisch worden weergegeven:



Figuur 1 Schematische weergave dataflow

1. Fysiotherapiepraktijk legt persoonsgegevens van patiënten en fysiotherapeuten vast in het EPD

   Medewerkers van fysiotherapiepraktijken houden voor iedere patiënt een patiëntendossier bij, waarin o.a. persoonsgegevens zoals naam, adres, geboortedatum, klachtenbeeld en behandelresultaat worden bijgehouden. Hiertoe zijn ze verplicht conform wet- en regelgeving. De fysiotherapeut kan, indien hij digitaal werkt, deze patiëntgegevens vastleggen in een EPD. Het opnemen van deze persoonsgegevens in een EPD is de verantwoordelijkheid van de fysiotherapeut en staat los van de LDF. Het valt daarom buiten de scope van dit Dataprotocol LDF.

2. Mediquest ontvangt persoonsgegevens van patiënten en fysiotherapeuten uit het EPD in de LDF

   De fysiotherapiepraktijk exporteert maandelijks een selectie van de gegevens over de fysiotherapeuten en patiënten van de betreffende praktijk uit het EPD naar de LDF. Voordat de gegevens van een patiënt geëxporteerd kunnen worden, dient de patiënt daar uitdrukkelijk

toestemming voor te geven (opt-in)[5]. Deze toestemming vormt de grondslag voor de verwerking. De toestemming wordt ten tijde van het verkrijgen en invoeren van de patiëntgegevens in het EPD (punt 1) gevraagd. Voor het uitvragen van deze toestemming kan gebruik gemaakt worden van de Informatie voor de patiënten (**Bijlage 1**). Een beschrijving van de patiëntgegevens die vanuit het EPD worden geleverd aan de LDF is te raadplegen via: https://kngf.nl/ldf.

In de export van de gegevens uit het EPD naar de LDF worden de patiëntgegevens voor verzending door de EPD leverancier versleuteld. Dit betekent dat de aan de LDF geleverde patiëntgegevens gepseudonimiseerd zijn. De gegevens zijn hierdoor niet direct naar een persoon te herleiden. Alleen met behulp van een sleutel kan de pseudonimisering teruggedraaid worden. De EPD-leverancier beschikt over deze sleutel en beheert deze voor haar klant, de fysiotherapiepraktijk. Betrokken partijen (KNGF, Mediquest, en andere Andere Partijen) kunnen door deze versleuteling de gegevens niet naar een persoon herleiden.

Voordat de het leveren van patiëntgegevens aan de LDF mogelijk is, dient een fysiotherapiepraktijk zich aan te melden bij de LDF. De aanmeldprocedure staat beschreven op: https://www.kngf.nl/ldf.

3. Verwerking van persoonsgegevens van patiënten en fysiotherapeuten tot informatie door Mediquest

   Om de verzamelde gegevens van data in te zetten om de drie doelstellingen van de LDF te bereiken, dienen deze omgezet te worden in relevante informatie. Mediquest is als ICT partij de samenwerkingspartner van het KNGF voor het verwerken van gegevens tot informatie, o.a. door het uitvoeren van data-analyses en door data te preparen voor weergave in het LDF-dashboard.

4. Levering persoonsgegevens van patiënten en fysiotherapeuten aan Andere Partijen voor verwerking tot informatie

   KNGF werkt ook met Andere Partijen om de verzamelde data om te zetten in relevante informatie, om de drie doelstellingen van de LDF te bereiken. Andere Partijen zijn samenwerkingspartners van het KNGF voor o.a. het opzetten van onderzoeken en de verwerking van gegevens tot informatie.

5. Ontsluiting van informatie via het LDF-dashboard

   De informatie die door Mediquest wordt opgeleverd, wordt gepresenteerd in het LDF-Dashboard van het KNGF. Dit is de visuele weergave die op basis van feedback uit het werkveld tot stand komt (meer informatie: https://www.kngf.nl/article/vak-en-kwaliteit/kwaliteit/ldf/ontdek-het-ldf-

[5] Als (delen van) een patiëntendossier elektronisch beschikbaar worden gesteld voor anderen, dan moet de zorgverlener vooraf uitdrukkelijk toestemming vragen aan de patiënt. Die uitdrukkelijke toestemming wordt "**opt-in"** genoemd.

dashboard).

Uitvoering van de dataprocessen door verwerkers

Mediquest en Andere Partijen zijn verplicht om de persoonsgegevens van patiënten en fysiotherapeuten uitsluitend te verwerken in lijn met de doelstellingen van de LDF, zoals opgesteld door het KNGF (zie hoofdstuk 1). Voorts voeren Mediquest en de Andere Partijen alleen verwerkingen uit volgens instructie van het KNGF of in samenwerking met het KNGF, of om te voldoen aan wettelijke verplichtingen.

Mediquest en de Andere Partijen mogen geen gebruik maken van de via het KNGF verkregen gegevens voor eigen doeleinden of voor doeleinden van derden zonder uitdrukkelijke en schriftelijke toestemming van het KNGF. Hiervoor heeft het KNGF een Verwerkersovereenkomst gesloten met Mediquest. Afhankelijk van de rol van de Andere Partij is een Verwerkersovereenkomst en/of een Samenwerkingsovereenkomst overeengekomen (zie hierna).

Uitvoering van de dataprocessen door Andere Partijen

Op basis van de tussen het KNGF en een of meerdere Andere Partijen gesloten Samenwerkings-overeenkomsten en/of Verwerkersovereenkomsten ontvangen deze Andere Partijen van het KNGF persoonsgegevens van patiënten en fysiotherapeuten. De mogelijkheid bestaat dat Andere Partijen verwerkingen op de gegevens uit de LDF verrichten. De Andere Partijen en het KNGF stellen samen de doeleinden van de gegevensverwerking vast. De Andere Partijen mogen alleen gebruik maken van via het KNGF verkregen persoonsgegevens als de doelen waarvoor deze worden verwerkt schriftelijk zijn overeengekomen tussen partijen. In voorkomend geval sluit het KNGF met die Andere Partij(en) een overeenkomst, waarin de rechtmatige verwerking van persoonsgegevens geborgd is.

5. Beheer en beveiliging van Persoonsgegevens

Beheer

De data die worden geleverd aan de LDF staan opgeslagen bij Mediquest en worden enkel geleverd aan verwerkers en verwerkingsverantwoordelijken die zich committeren aan dit Dataprotocol LDF en met wie een Verwerkersovereenkomst en/of Samenwerkingsovereenkomst gesloten is. Mediquest beschikt over ISO-27001 en NEN7510-certificeringen. Dat betekent dat zij voldoet aan de ISO-27001 en NEN7510 normen en gecertificeerd is voor de uitvoering van al haar bedrijfsactiviteiten. De normen worden jaarlijks getoetst door een extern bevoegde audit organisatie.

Verzoeken van patiënt of fysiotherapeut

Een patiënt of fysiotherapeut kan verzoeken om inzage in de van hem/haar verwerkte persoonsgegevens en/of een verzoek doen tot verbetering, aanvulling, verwijdering of afscherming. Deze rechten van de betrokkene zijn als volgt opgenomen in de AVG en betreffen:

- het recht op inzage[6];
- het recht op rectificatie[7];
- het recht op gegevenswissing[8];
- het recht op beperking van de verwerking[9];
- het recht op overdraagbaarheid van gegevens[10] en
- het recht van bezwaar[11].

Om ervoor te zorgen dat tijdig aan de verzoeken van een patiënt of fysiotherapeut kan worden voldaan, dienen Partijen in een voorkomend geval het Protocol Verzoeken Betrokkene nauwgezet te volgen. Het Protocol Verzoek Betrokkene is opgenomen in **bijlage 2** bij dit Dataprotocol LDF.

Beveiliging van patiëntgegevens en persoonsgegevens van fysiotherapeuten

Alle Partijen die betrokken zijn bij de verwerking van de patiëntgegevens en persoonsgegevens van fysiotherapeuten in het kader van de LDF en die hiertoe een Samenwerkingsovereenkomst en/of Verwerkersovereenkomst hebben gesloten met KNGF, nemen adequate technische en organisatorische maatregelen om de patiëntgegevens en persoonsgegevens van fysiotherapeuten te beschermen tegen verlies en beschadiging, alsmede tegen onrechtmatige verwerking van de gegevens.

De verdere uitwerking van de door Partijen getroffen maatregelen, behaalde certificeringen en/of (interne) voorschriften die worden nageleefd ten aanzien van de beveiliging van (persoons)gegevens, is geborgd in de individuele Verwerkeringsovereenkomsten en Samenwerkingsovereenkomsten met als basis de in ISO 27001 en NEN 7510 vastgelegde beveiligingsnormen.

De beveiliging van de EPD's en de ICT systemen bij de fysiotherapeuten en/of EPD leveranciers valt buiten de reikwijdte van dit Dataprotocol LDF. Hiertoe dienen die (aanleverende) partijen zelf adequate maatregelen te treffen.

Beveiligingsbeheer

Voor het geval zich - ondanks de getroffen beveiligingsmaatregelen - bij een Partij of bij meerdere Partijen een beveiligingsincident voordoet, hebben Partijen een Procedure Meldplicht Datalekken Landelijke Database Fysiotherapie geïmplementeerd. Deze Procedure Meldplicht Datalekken Landelijke Database Fysiotherapie is bijgevoegd als **bijlage 4** bij dit Dataprotocol LDF. In het geval zich een beveiligingsincident voordoet, zullen Mediquest en of de Andere Partijen daarvan direct melding maken bij het KNGF.

[6] Artikel 15 AVG
[7] Artikel 16 AVG
[8] Artikel 17 AVG
[9] Artikel 18 AVG
[10] Artikel 20 AVG
[11] Artikel 21 AVG

6. Controle en rapportage

Vaststellen van het Dataprotocol LDF

Het KNGF stelt jaarlijks de inhoud van het Dataprotocol vast.

Evalueren en wijzigen van het Dataprotocol LDF

Partijen zullen de verwerking van persoonsgegevens evalueren en van deze evaluatie schriftelijke documentatie bijhouden, een en ander volgens onderstaande tabel.

Rapport type	Periodiciteit	Wijze	Verantwoordelijke
• Beveiligingsincidenten. • Ongeautoriseerde mutaties aan sourcecode, data, databases, servers en netwerkcomponenten. • Fails van continuïteit, back-up en recovery. • (Indicatie van) Onbevoegde toegang. • Lekken van informatie en (patiënt)gegevens. • Overtreding van fysieke en logische beveiligings-maatregelen. • Verbetermaatregelen indien bovenstaande daar aanleiding toe geeft.	Wanneer zich één of meerdere van de situatie zich voordoet, alsmede maandelijks.	Schriftelijk	Betrokken partij(en)
• Review Dataprotocol LDF	Jaarlijks	Schriftelijk	KNGF
• Review beveiligingsbeleid van Partijen. • Review Procedure Meldplicht Datalekken Landelijke Database Fysiotherapie	Jaarlijks of na belangrijke wijzigingen in informatiesystemen/ernstige beveiligingsincidenten en/of relevante wetswijziging.	Schriftelijk	Betrokken partij(en)
• Review bewerkersovereenkomst. • Review informatiebrief. • Review protocol verzoeken betrokkene.	Jaarlijks of na een relevante wetswijziging of wijziging in de verwerking ten aanzien van de LDF	Schriftelijk	Betrokken partij(en)

In het geval zich een beveiligingsincident voordoet, zullen Mediquest en of de Andere Partijen daarvan direct melding maken bij het KNGF in overeenstemming met bijlage 4 bij dit Dataprotocol LDF. In de maandelijkse rapportages worden de incidenten die zich in de vorige maand hebben voorgedaan beschreven.

Partijen zullen jaarlijks tezamen de uitkomsten van de individuele evaluaties bespreken. Voorstellen tot wijzigingen van dit Dataprotocol LDF of één van de bijlagen worden op initiatief van één of meerdere Partijen ter inhoudelijke besluitvorming voorgelegd aan de overige partijen bij dit Dataprotocol LDF.

Bijlage 1: Informatie voor patienten

LANDELIJKE DATABASE FYSIOTHERAPIE

Informatie voor patiënten

1. Inleiding

Wat is de Landelijke Database Fysiotherapie?

Uw fysiotherapeut heeft u gevraagd om hem of haar toestemming te geven om enkele gegevens over u en uw behandeling op te nemen in de Landelijke Database Fysiotherapie (LDF). De LDF is een initiatief van de beroepsgroep van fysiotherapeuten, het KNGF. In de Landelijke Database Fysiotherapie worden bepaalde gegevens verzameld die de medewerkers van een Fysiotherapiepraktijk gedurende het zorgproces van een patiënt vastleggen.

Welke gegevens worden verzameld in de LDF en hoe gaat dit in zijn werk?

Het gaat om zogeheten gepseudonimiseerde[12] gegevens over de patiënt, om gegevens over de fysiotherapeut en van de fysiotherapiepraktijk. Hieronder vallen ook (bijzondere) persoonsgegevens, die worden verkregen uit het elektronische patiëntendossier. U kunt hierbij denken aan de gepseudonimiseerde verslaglegging van de behandeling, het behandelgemiddelde en de behaalde behandelresultaten.

Wanneer een fysiotherapiepraktijk is aangesloten bij de Landelijke Database Fysiotherapie worden deze (bijzondere) persoonsgegevens vanuit het elektronisch patiëntendossier (“EPD”) eens per maand aan de Landelijke Database Fysiotherapie geleverd door de fysiotherapiepraktijk.

Wat gebeurt er vervolgens met deze gegevens?

Met de gegevens wordt wetenschappelijk onderzoek verricht om de zorgverlening te optimaliseren. De uitkomst hiervan wordt via de Landelijke Database Fysiotherapie teruggekoppeld aan de aangesloten fysiotherapeuten. Dit gebeurt via het LDF-Dashboard waarop de aangesloten fysiotherapeut via een webapplicatie kan inloggen. Hierdoor kan fysiotherapeut bijvoorbeeld zien welke behandelmethodes het beste werken en wat het gemiddelde resultaat van die behandelmethode is. Verder worden de gegevens (niet herleidbaar tot de patiënt) gebruikt voor wetenschappelijke publicaties of in beleidsrapporten.

[12] “Pseudonimisering”: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

2. Om welke gegevens gaat het?

De volgende gegevens over u en uw behandeling worden in de LDF opgenomen:

- Geslacht;
- Geboortejaar;
- Het identificatienummer van uw zorgverzekeraar;
- De behandelgegevens.

Voor gedetailleerde informatie over de behandelgegevens die worden gedeeld, kunt u kijken op:

https://www.kngf.nl/article/vak-en-kwaliteit/kwaliteit/ldf/wat-lever-je-aan

Gegevens zoals uw naam, adres, telefoonnummer, e-mailadres, geboortedatum, Burgerservicenummer en medische voorgeschiedenis zijn **niet** relevant voor de LDF en worden daarom **niet** opgenomen.

De behandelgegevens worden voor onbepaalde tijd bewaard omdat de medische waarde van behandelgegevens aanzienlijk toeneemt naarmate er meer van dergelijke gegevens beschikbaar zijn. Daardoor kunnen namelijk nauwkeuriger berekeningen en vergelijkingen worden gemaakt ten aanzien van de het behandelgemiddelde en de behaalde behandelresultaten.

1. Hoe werkt het precies?

Uw fysiotherapeut houdt een elektronisch patiëntendossier (EPD) over u bij. Als u daarvoor toestemming geeft, worden maandelijks enkele gegevens uit uw EPD over de daaraan voorafgaande drie maanden via een beveiligde koppeling naar de LDF verstuurd en daarin verzameld. Op basis van de gegevens die uw fysiotherapeut bij de LDF aanlevert, ontvangt hij of zij een terugkoppeling in het LDF-Dashboard die vergelijking met de resultaten van andere fysiotherapeuten mogelijk maakt. Uw fysiotherapeut wordt daarmee gestimuleerd om, waar nodig, zijn of haar handelen aan te passen om de kwaliteit van zijn of haar zorg te verbeteren. De verzamelde gegevens worden ook gebruikt om wetenschappelijk onderzoek te doen naar fysiotherapeutische zorg en om het landelijke zorgbeleid te beïnvloeden.

2. Welke partijen zijn betrokken?

Het KNGF werkt met betrekking tot de LDF samen met Mediquest B.V. te Utrecht. Mediquest zorgt voor de techniek die veilige levering, opslag en beheer van data mogelijk maakt. Daarnaast is een aantal onderzoeksinstituten en/of andere derden, waaronder (netwerken van) fysiotherapeuten, betrokken bij het gebruik van de gegevens, zogeheten Andere Partijen. Een actueel overzicht van de Andere Partijen is te vinden op: https://www.kngf.nl/article/vak-en-kwaliteit/kwaliteit/ldf/juridische-informatie.

3. Hoe worden uw gegevens beveiligd?

Het KNGF vindt de bescherming van uw privacy zeer belangrijk. Om de veiligheid van uw gegevens te waarborgen heeft zij technische en organisatorische maatregelen genomen die zijn vastgelegd in het *"LDF Dataprotocol"* en hierover specifieke afspraken gemaakt met Mediquest. Andere Partijen hebben afspraken gemaakt via samenwerkingsovereenkomsten en verwerkingsovereenkomsten. Deze documenten zijn allen te vinden op: https://www.kngf.nl/article/vak-en-kwaliteit/kwaliteit/ldf/juridische-informatie.

Het KNGF verwerkt de betreffende gegevens geheel in overeenstemming met de hiervoor geldende wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG) (Verordening 2016/679).

4. Wat als u toestemming geeft en later van gedachten verandert?

Uw fysiotherapeut registreert uw toestemming voor het verstrekken van uw gegevens aan de LDF. Mocht u onverhoopt uw toestemming op enig moment willen intrekken, dan kunt u dit aangeven bij uw fysiotherapeut. Hij of zij zal ervoor zorgen dat uw gegevens vanaf dat moment niet meer worden aangeleverd aan de LDF. | Meer informatie: https://www.kngf.nl/article/vak-en-kwaliteit/kwaliteit/ldf/informatie-voor-patienten.

Verder hebt u recht op:

(i) het inzien van uw gegevens;

(ii) een verzoek tot verwijdering of correctie van uw persoonsgegevens/ het recht om bezwaar te maken tegen de gegevensverwerking;

(iii) bewijs dat uw persoonsgegevens zijn verwijderd of gecorrigeerd naar aanleiding van een verzoek;

(iv) een verzoek tot rectificatie en aanvulling van uw persoonsgegevens;

(v) een verzoek tot het overdragen van persoonsgegevens aan een andere partij;

(vi) een verzoek tot het laten verwerken van minder persoonsgegevens;

(vii) een verzoek tot een menselijke interventie van geautomatiseerde besluitvorming en profilering;

(viii) Het recht op duidelijke informatie over wat het LDF met uw persoonsgegevens doet.

5. Meer informatie

Meer informatie is te vinden op https://www.kngf.nl/ldf. Met vragen kunt u terecht bij uw fysiotherapeut of de afdeling Ledenvoorlichting (033-4672929 en ledenvoorlichting@kngf.nl) van het KNGF.

Bijlage 2: Werkinstructie Verzoek Betrokkene

Het KNGF is de verwerkingsverantwoordelijke en rechthebbende tot de gegevens die worden verzameld in de Landelijke Database Fysiotherapie ("LDF"), waaronder gegevens van de fysiotherapiepraktijk, de fysiotherapeut en gepseudonimiseerde (bijzondere) persoonsgegevens van patiënten (in deze context allen aangeduid met "de Betrokkene"). Een gedetailleerd overzicht van de (persoons)gegevens die in de LDF worden verzameld is te vinden op https://www.kngf.nl/article/vak-en-kwaliteit/kwaliteit/ldf/wat-lever-je-aan. Gegevens die zijn terug te herleiden naar een natuurlijke persoon worden aangeduid met "Data" van de Betrokkene.

Soorten verzoeken

Een verzoek van een Betrokkene kan verschillende soorten wijzigingen betreffen, afhankelijk van op welk recht ten aanzien van de Data de Betrokkene een beroep doet. De AVG benoemt expliciet de volgende rechten van de Betrokkene:

(i) het voldoen aan een inzageverzoek van een Betrokkene;
(ii) een verzoek tot verwijdering of correctie van de Data van een Betrokkene/ het recht om bezwaar te maken tegen de gegevensverwerking;
(iii) aantonen dat Data zijn verwijderd of gecorrigeerd naar aanleiding van een verzoek;
(iv) een verzoek tot rectificatie en aanvulling van de Data van een Betrokkene;
(v) een verzoek tot het overdragen van Data aan een andere partij van een Betrokkene;
(vi) een verzoek tot het laten verwerken van minder Data van een Betrokkene;
(vii) een verzoek tot een menselijke interventie van geautomatiseerde besluitvorming en profilering van een Betrokkene;
(viii) Het recht op duidelijke informatie over wat het LDF met Data van Betrokkenen doet.

Wijze waarop een aanvraag van een Betrokkene dient te worden ingediend

Een verzoek vanuit de Betrokkene moet schriftelijk zijn ingediend of schriftelijk zijn bevestigd (bijvoorbeeld bevestiging van een telefoongesprek via e-mail). Een telefonisch akkoord alleen is niet voldoende, want daar is achteraf geen bewijs van. Ook zal de Betrokkene zich op enige wijze moeten identificeren om misbruik te voorkomen. Alle verzoeken dienen te worden doorgestuurd aan het projectteam (e-mailadres: ldf@kngf.nl).

Het projectteam

Het projectteam bestaat uit:

- Chantal Weymans – KNGF – Beleidsmedewerker – c.weymans@kngf.nl – 033 467 29 63
- Floortje Diephuis – Mediquest – Projectleider – fdiephuis@Mediquest.nl – 088 126 39 90

De rollen in het Projectteam zijn gekoppeld aan de functies binnen de betreffende organisatie, zodat de continuïteit is gewaarborgd.

Het Projectteam zorgt voor alle interne en externe coördinatie, afhandeling, het bewaken van termijnen/ follow-up en alle communicatie met betrekking tot verzoeken van Betrokkenen. Zij overlegt maandelijks met als vaste agendapunten:

- Lopende verzoeken van Betrokkenen/ follow-up vanuit ieders rol/ verantwoordelijkheden;
- Evaluatie/ updaten van processen;

Stappen Projectteam bij ieder verzoek.

Bij ieder verzoek van een Betrokkene zal het Projectteam de volgende stappen doorlopen:

1. Het projectteam bevestigt aan de Betrokkene dat zij het verzoek in behandeling neemt, alsook de verwachte responstijd en email/telefoonnummer van KNGF. Indien het verzoek niet rechtstreeks van de Betrokkene afkomstig is maar via een fysiotherapeut/praktijk is ingediend dan wordt de fysiotherapeut/praktijk geïnformeerd dat het verzoek in behandeling is genomen, en dat het verdere inhoudelijke contact rechtstreeks met de Betrokkene plaatsvindt.

2. Het verzoek (de e-mail of gescande brief) moet worden gearchiveerd in de daarvoor bestemde map op de LDF Sharepoint omgeving (https://kngf365.sharepoint.com/:f:/r/sites/LDF/Gedeelde%20%20documenten/Mediquest/Verzoek%20Betrokkene%20(gedeelde%20map)?csf=1&web=1&e=TeliKc), waarbij de naamgeving plaatsvindt volgens methode JJJJMMDD_nummerverzoek_onderwerp email).

3. Het verzoek wordt geregistreerd in een registratiebestand in dezelfde map. De andere leden van het Projectteam worden geïnformeerd dat registratie heeft plaatsgevonden en dat zij aan de slag kunnen.

4. Het Projectteam stelt al dan niet samen met de Betrokkene vast of het verzoek betrekking heeft op Data in de LDF en/of Data in het EPD-systeem van de fysiotherapeut/praktijk.
    a. Als een verzoek geen betrekking heeft op Data in de LDF, maar uitsluitend op Data in het EPD. In dat geval valt de verwerking van het verzoek niet onder de verantwoordelijkheid van het Projectteam. Het verzoek dient door Betrokkene rechtstreeks te worden ingediend bij de fysiotherapeut of praktijk. Betrokkene wordt

hierover geïnformeerd, en het verzoek wordt niet verder in behandeling genomen door het Projectteam.

b. Als een verzoek zowel betrekking heeft op Data in de LDF als op Data in het EPD, dan is de fysiotherapeut/praktijk is verantwoordelijk voor de uitvoering van het gedeelte van het verzoek wat betrekking heeft op het EPD. De Betrokkene kan hierover zelf contact opnemen met de fysiotherapeut/praktijk. Het Projectteam kan als de Betrokkene dat wenst faciliteren in het leggen van contact met de fysiotherapeut/praktijk. Het Projectteam is verantwoordelijk voor de uitvoering van het gedeelte van het verzoek wat betrekking heeft op de LDF. Het verzoek wordt verder verwerkt.

c. Als het verzoek uitsluitend betrekking heeft op data in de LDF dan wordt dit verzoek door het Projectteam in behandeling genomen, en verzoek wordt verder verwerkt.

5. Het Projectteam stelt al dan niet samen met de Betrokkene vast op welke recht van de Betrokkene het verzoek betrekking heeft, en per soort recht is hieronder aangegeven hoe gehandeld dient te worden in geval van een verzoek:

(i) *Het voldoen aan een inzageverzoek*: de gevraagde en/of beschikbare Data wordt doorgezonden aan de Betrokkene. Dit gebeurt in een met wachtwoord beveiligd bestand in gangbaar digitaal format (zoals Microsoft Excel of Microsoft Word).

(ii) *Een verzoek tot verwijdering of correctie van de Data/ het recht om bezwaar te maken tegen de gegevensverwerking*:

- <u>Correctie</u>: als een verzoek om correctie van de Data wordt gedaan, kan Betrokkene een vragenlijst toegestuurd krijgen die hij met de correcte Data kan invullen. De bestaande Data worden vervangen met de nieuwe Data.
- <u>Verwijdering/bezwaar</u>: de Data van Betrokkene worden vernietigd en worden niet meer meegenomen in nieuwe data-analyses in de LDF. De verwijdering dient integraal te geschieden.

In beide gevallen kan een aanvullende actie van de behandelend fysiotherapeut in het EPD nodig zijn (het uitzetten van de toestemming voor datalevering aan de LDF). Als dat van toepassing is, zal het Projectteam hierover namens de patiënt contact opnemen met de behandelend fysiotherapeut. Dit contact zal schriftelijk zijn of wordt schriftelijk bevestigd, met een CC naar de Betrokkene.

(iii) *Aantonen dat Data zijn verwijderd of gecorrigeerd naar aanleiding van een verzoek*;
als de Betrokkene dat wenst dan moet ten aanzien van punt (ii) bewijs worden meegestuurd;

Correctie: de correctie kan worden aangetoond door inzage te geven in de beschikbare Data, zoals bij een inzageverzoek (i).
Verwijdering/bezwaar: het is niet aan te tonen dat iets er niet is. In dit geval zal moeten worden volstaan met een schriftelijke bevestiging van Mediquest dat de actie is uitgevoerd.

(iv) *Een verzoek tot rectificatie en aanvulling van de Data van een Betrokkene*; de Betrokkene wordt in de gelegenheid gesteld kenbaar te maken welke Data hij gerectificeerd en/of aangevuld wens te zien. De bestaande Data worden vervangen door de gerectificeerde Data en/of aangevuld met nieuwe Data.

In dit geval kan een aanvullende actie van de behandelend fysiotherapeut in het EPD nodig zijn (het uitzetten van de toestemming voor datalevering aan de LDF). Als dat van toepassing is, zal het Projectteam hierover namens de patiënt contact opnemen met de behandelend fysiotherapeut. Dit contact zal schriftelijk zijn of wordt schriftelijk bevestigd, met een CC naar de Betrokkene.

(v) *Een verzoek tot het overdragen van Data aan een andere partij*: als de Betrokkene dat wenst dan zal zijn Data worden overgedragen aan een andere partij. Dit gebeurt in een met wachtwoord beveiligd bestand in gangbaar digitaal format (zoals Microsoft Excel of Microsoft Word).

(vi) *Een verzoek tot het laten verwerken van minder Data*: de Betrokkene wordt in de gelegenheid gesteld toe te lichten welke Data hij niet langer verwerkt wil hebben. Vervolgens zullen deze data niet meer worden verwerkt.

(vii) In dit geval kan een aanvullende actie van de behandelend fysiotherapeut in het EPD nodig zijn (het uitzetten van de toestemming voor datalevering aan de LDF). Als dat van toepassing is, zal het Projectteam hierover namens de patiënt contact opnemen met de behandelend fysiotherapeut. Dit contact zal schriftelijk zijn of wordt schriftelijk bevestigd, met een CC naar de Betrokkene.

(viii) *Een verzoek tot een menselijke interventie van geautomatiseerde besluitvorming en profilering*; niet van toepassing.

(ix) *Het recht op duidelijke informatie over wat het LDF met Data van Betrokkenen doet*: de Betrokkene wordt in de gelegenheid gesteld zijn concrete vraag of vragen te stellen. Als leidraad kan de patiëntinformatie op de LDF webpagina van de KNGF website worden gebruikt, eventueel aangevuld met uitleg van het KNGF, Mediquest, en/of overige verwerkers.

6. Als de actie moet plaatsvinden in de LDF zal het Projectteam contact opnemen met de fysiotherapeut/praktijk en EPD-leverancier om hen te informeren over het verzoek en te achterhalen met welk PatientID de gegevens van de Betrokkene aan de LDF zijn geleverd. Hierna kan het verzoek worden ingewilligd.

7. Het Projectteam bevestigt per e-mail (met ontvangstbevestiging) aan Betrokkene dat diens verzoek is volbracht. Desgevraagd wordt daarvan bewijs meegestuurd, voor zover dat hierboven is bepaald en dit redelijkerwijs mogelijk is. Als de Betrokkene weigert de ontvangst van de e-mail te bevestigen, dient het voornoemde in het uiterste geval per aangetekende brief te worden verstuurd.

8. Het Projectteam legt de afronding van het verzoek vast in het registratiebestand.

Bijlage 3: Procedure Meldplicht Datalekken Landelijke Database Fysiotherapie

Document historie

Versie	Wijziging	Datum	Auteur
0.1	Concept	16-04-2018	Gerrit Verrips
1.0		20-05-2018	Gerrit Verrips
2.0	Aanpassing KNGF naar generiek	november 2020	JEAN Legal/ KNGF

1. Inleiding

Definities

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming (EU) 2016/679
Betrokkene	de persoon van wie Data worden verwerkt als bedoeld in de AVG
Data	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon
Datalek	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de beschadiging, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte (persoons)gegevens
LDF	Landelijke Database Fysiotherapie
Partijen	De partijen op wie het Dataprotocol op dat moment van toepassing is (ten tijde van het opstellen van deze versie van het PMD: Mediquest en Partijen, zie: https://www.kngf.nl/article/vak-en-kwaliteit/kwaliteit/ldf).
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van een Verwerkingsverantwoordelijke Data verwerkt en van wie de Functionaris Gegevensbescherming (FG) en de Security Officer de contactpersonen zijn.
Verwerkingsverantwoordelijke	Degene die de doelen voor de verwerking van Data vaststelt en van wie de Functionaris Gegevensbescherming (FG) en de Security Officer de contactpersonen zijn.
PMD	Deze Procedure Meldplicht Datalekken

Doel PMD

Het doel van de PMD is om Partijen in staat te stellen op gecontroleerde wijze om te gaan met de gevolgen van een Datalek. Aan de hand van een stappenplan wordt bepaald of er sprake is van een Datalek, of hier melding van moet worden gemaakt aan de AP, door wie, hoe dit moet gebeuren en of het Datalek moet worden gemeld aan de Betrokkene.

Werkingssfeer

De PMD is van toepassing op alle werknemers, ZZP'ers, bestuurders en toezichthouders die werkzaam zijn bij/voor Partijen, in ieder geval voor zover een Datalek verband houdt met de LDF. Ook in dit geval dient de PMD te worden gevolgd.

Verantwoordelijke / contactpersonen PMD

KNGF

Functionaris Gegevensbescherming (FG):	Betty Kroes E-mail: ldf@kngf.nl Telefoon: 033 467 2903
Security Officer:	Erik Tetteroo E-mail: ldf@kngf.nl Telefoon: 06 52 68 3360
Primair LDF-contactpersoon voor Partijen:	Femke Driehuis E-mail: ldf@kngf.nl Telefoon: 06 42 44 98 84

Voor contactgegevens Partijen, zie: www.kngf.nl/ldf

MELDINGEN AAN DE AP EN/ OF BETROKKENEN DIENEN ALTIJD UITSLUITEND DOOR DE FUNCTIONARIS GEGEVENSBESCHERMING OF DE SECURITY OFFICER TE WORDEN GEDAAN. DEZE PROCEDURE IS SLECHTS EEN LEIDRAAD OM VAST TE STELLEN OF MOGELIJK SPRAKE IS VAN EEN DATALEK EN/OF MELDPLICHT AAN BETROKKENEN EN HOE TE HANDELEN IN EEN DERGELIJKE SITUATIE.

2. Wat is een Datalek?

Datalekken worden opgedeeld in drie situaties/ subcategorieën, te weten:

1. "*Inbreuk op de vertrouwelijkheid*" – als sprake is van ongeoorloofde of onbedoelde verstrekking van of toegang tot Data.

   Bijvoorbeeld:
   - papieren met Data die op straat belanden;
   - een kwetsbaarheid in een applicatie waardoor Data worden gelekt.

2. "*Inbreuk op de integriteit*" – als sprake is van een ongeoorloofde of onopzettelijke wijziging van Data.

   Bijvoorbeeld:
   - een hack waarbij Data worden gewijzigd.

3. "*Inbreuk op de beschikbaarheid*" – als sprake is van een onopzettelijk of ongeoorloofd verlies van toegang tot Data of een onopzettelijke of ongeoorloofde vernietiging van Data.

   Bijvoorbeeld:
   - een kwijtgeraakte USB-stick waar zich Data op bevinden;
   - een gestolen laptop;
   - een email met Data naar een verkeerd adres;
   - een DDoS-aanval;
   - een besmetting met ransomware.

Vaak gaat het om een combinatie van bovenstaande situaties/ subcategorieën.
Het is niet van belang of het gaat om een tijdelijke of definitieve situatie.

Het is essentieel dat direct alle relevante Partijen worden betrokken bij omgang met (potentiële) Datalekken via de bovenstaande e-mailadressen/ contactgegevens.

3. Stappenplan ter identificatie van Datalekken

Introductie

Het is niet altijd even eenvoudig vast te stellen of sprake is van een Datalek dat dient te worden gemeld aan de AP en/of Betrokkenen. Hieronder volgt een stappenplan om je op weg te helpen een Datalek te identificeren en hoe daarmee om te gaan.

Stap 1: Gaat het hier om Data?

Zijn de gegevens, waar het incident verband mee houdt, aan te merken als Data?
Voorbeelden zijn: namen, mobiele nummers en (e-mail)adressen van natuurlijke personen. Gepseudonimiseerde Data (zoals in de LDF) vallen hier ook onder, omdat Betrokkenen nog altijd identificeerbaar zijn met behulp van de sleutel van de EPD-leverancier. Onomkeerbaar geanonimiseerde gegevens vallen hier echter niet onder.

JA: ga naar stap 2
NEE: er hoeft geen melding te worden gedaan.

Stap 2: Verwerkingsverantwoordelijke of Verwerker?

Wat is de hoedanigheid van de betrokken Partijen?
Een verwerkingsverantwoordelijke is degene die de doelen van de verwerking van de Data bepaalt. Hij is in die hoedanigheid verplicht een Datalek te melden bij de AP. Een Verwerker heeft de plicht om een Datalek dat plaatsvindt onder diens feitelijke toezicht te melden aan de Verwerkingsverantwoordelijke. Waar nodig ondersteunt de Verwerker de Verwerkingsverantwoordelijke bij de afhandeling van een Datalek, maar hij hoeft daar doorgaans zelf geen melding van te doen bij de AP.

Verwerkingsverantwoordelijke: Ga naar stap 3.
Verwerker: De Verwerker heeft de plicht het (potentiële) Datalek direct te melden aan de Verwerkingsverantwoordelijke, zodat deze tijdig melding kan maken bij de AP en/of Betrokkenen. Een Verwerker neemt bij (het vermoeden van) een Datalek direct contact op met de Verwerkingsverantwoordelijke om het (potentiële) Datalek te melden en te bezien of ondersteuning nodig is.

Stap 3: Is sprake van een Datalek?

Stap 3A: is sprake van beschadiging van Data?
Beschadiging van Data betekent dat de deze zijn gewijzigd, gecorrumpeerd of niet langer volledig zijn (zie Hoofdstuk 2 voor meer details).

JA, beschadiging: er kan alsnog sprake zijn van een Datalek, ga naar stap 3B.
NEE, geen beschadiging: ga naar stap 3B.

Stap 3B: zijn Data verloren gegaan?
Verlies houdt in dat de Data niet langer bestaan, of niet langer bestaan in een vorm die van nut is of de oorspronkelijke vorm.

JA, wel verloren: dit is een Datalek, ga naar stap 4.
NEE, niet verloren: er kan toch sprake zijn van een Datalek, ga naar stap 3C.

Stap 3C: kan redelijkerwijs worden uitgesloten dat Data onrechtmatig zijn verwerkt?
Onder onrechtmatige vormen van verwerking vallen aantasting van Data, onbevoegde kennisneming, wijziging, of verstrekking daarvan.

JA, kan uitgesloten worden: dit is geen Datalek. Er hoeft geen melding te worden gedaan.
NEE, kan niet uitgesloten worden: er is sprake van een Datalek, ga naar stap 4.

Stap 4: Melding AP?

In deze stap zijn er twee vragen om rekening mee te houden:

Stap 4a: zijn *bijzondere* Data gelekt?
Bij een aantal categorieën Data kan verlies of onrechtmatige verwerking onder meer leiden tot stigmatisering of uitsluiting van Betrokkene(n), schade aan de gezondheid, financiële schade of tot (identiteits-) fraude. Tot deze categorieën van Data moeten in ieder geval worden gerekend:

- *Bijzondere Data;* Data over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke Data en Data over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

- *Gegevens over de financiële of economische situatie van de Betrokkene;* Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de Betrokkene;* Hieronder vallen bijvoorbeeld gegevens over verslavingen, prestaties op school en/ of werk of relatieproblemen.

- *Gebruikersnamen, wachtwoorden en andere inloggegevens;* De mogelijke gevolgen voor Betrokkenen hangen af van de verwerkingen en van de Data waar de inloggegevens toegang toe geven.

- *Gegevens die kunnen worden misbruikt voor (identiteits-)fraude;* Het gaat hierbij onder meer om biometrische gegevens. Ook gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen (bijvoorbeeld het medisch beroepsgeheim) moeten als Data van gevoelige aard worden aangemerkt.

JA, gevoelige gegevens: dit moet gemeld worden bij de AP. Ga naar stap 5.
NEE, geen gevoelige gegevens: ga naar stap 4B.

Stap 4b: leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?
De aard en omvang van de getroffen verwerking is medebepalend voor de beantwoording van de vraag of er bij een Datalek sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de bescherming van Data.

Naarmate de gevolgen van de beslissingen, die op basis van de verwerkte Data kunnen worden genomen, potentieel ingrijpender kunnen zijn, is ook de impact van verlies of onrechtmatige verwerking groter. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen, zijn de gevolgen van verlies en onbevoegde wijziging van de gegevens ingrijpender dan bij gebruik van dezelfde gegevens voor bijvoorbeeld marketingdoeleinden.

Als de aard en omvang van de getroffen verwerking voldoen aan het bovenstaande, dan moet ervan uit worden gegaan dat (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte Data aanwezig kunnen zijn.

JA, wel ernstige gevolgen: dit moet gemeld worden bij de AP. Mogelijk moet dit ook gemeld worden aan de Betrokkenen, ga daarna naar stap 6.
NEE, geen ernstige gevolgen: dit Datalek hoeft niet gemeld te worden aan de AP.

Stap 5: Hoe melden bij AP?

Wie moet een Datalek melden bij de AP?

Het is van groot belang een Datalek **direct** te melden aan Verwerkingsverantwoordelijke. De eerste en uitsluitende verantwoordelijkheid voor melding van een Datalek aan de AP en/ of Betrokkenen ligt bij de Verwerkingsverantwoordelijke. In geval van een beoogde melding van een Datalek zal de Functionaris

Gegevensbescherming of Security officer bovendien onmiddellijk actie ondernemen om corrigerende maatregelen te nemen.

Voordat melding van een Datalek wordt gemaakt bij de AP, *informeert* de Verwerkingsverantwoordelijke de andere Partijen schriftelijk.

De volgende zaken maken in ieder geval altijd deel uit van de melding aan de AP:

- de aard van het Datalek, waar mogelijk onder vermelding van de categorieën Betrokkenen, de persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en contactgegevens van de Functionaris voor Gegevensbescherming, Security Officer of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van het Datalek;
- de maatregelen die de Verwerkingsverantwoordelijke heeft voorgesteld of genomen om het Datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

In sommige gevallen kan het raadzaam zijn aangifte te doen bij de politie.

Mogelijk moet er naast een melding bij de AP, ook gemeld worden aan Betrokkenen. Ga door naar stap 6.

Stap 6: Impact op privéleven?

Heeft het Datalek (waarschijnlijk) ongunstige gevolgen voor het privéleven van Betrokkenen?

Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik van Data ernstig in hun belangen worden geschaad. Het Datalek moet dan ook direct aan de Betrokkene worden gemeld als dit waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

De belangrijkste aanleiding op grond waarvan een Datalek ook aan Betrokkenen moet worden meegedeeld, is als het waarschijnlijk is dat het Datalek een hoog risico voor de rechten en vrijheden van Betrokkenen met zich meebrengt. Dit risico bestaat als het Datalek kan leiden tot lichamelijke, materiële of immateriële schade voor de Betrokkenen wier Data het voorwerp van de inbreuk zijn.

Voorbeelden van dergelijke schade zijn: discriminatie, identiteitsdiefstal of -fraude, financieel verlies en reputatieschade. Wanneer de inbreuk betrekking heeft op Data waaruit ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, of op Data die genetische gegevens of gegevens met betrekking tot de gezondheid of het seksleven, of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen omvatten, moet dergelijke schade als waarschijnlijk worden beschouwd.

Bij de concrete beoordeling van ieder afzonderlijk Datalek, dienen de volgende zaken te worden betrokken:

De aard van de inbreuk
Indien Data door derden worden buitgemaakt, legt dit bijvoorbeeld meer gewicht in de schaal dan indien diezelfde Data verloren zijn gegaan.

De aard, gevoeligheid en omvang van de Data
De aard en gevoeligheid van de gegevens hebben betrekking op het soort gegevens. Iemands NAW-gegevens zullen in de regel minder zwaar wegen dan iemands' strafblad. In het geval van bijzondere Data als omschreven in stap 4A is het zeer waarschijnlijk dat de Betrokkenen hierover zullen moeten worden geïnformeerd. Ook is van belang dat samenstelling en onderlinge verhouding worden afgewogen. Zo kan bekendmaking van NAW-gegevens sec doorgaans relatief weinig kwaad aanrichten. Indien het gaat om NAW-gegevens in combinatie met het tijdelijk stopzetten van een krantenabonnement vanwege vakantie, terwijl deze gegevens in handen van inbrekers zijn gekomen, is dit vanzelfsprekend anders.

Gemak waarmee personen kunnen worden geïdentificeerd
Identificatie kan direct of indirect mogelijk zijn op basis van de gecompromitteerde Data, maar kan ook afhankelijk zijn van de specifieke context van de inbreuk en de publieke beschikbaarheid van gerelateerde Data. Data met een passend niveau van versleuteling zullen doorgaans ontoegankelijk zijn voor onbevoegden die niet over de decodeersleutel beschikken. Daarnaast kan een goed uitgevoerde pseudonimisering (zoals bij de LDF) ook de kans verkleinen dat personen in het geval van een inbreuk worden geïdentificeerd.

Ernst van gevolgen voor personen
Als het Datalek betrekking heeft op kwetsbare personen, kunnen zij een groter risico op schade lopen. Ook het feit dat de Verwerkingsverantwoordelijke zich er al dan niet van bewust is dat Data in handen zijn van personen van wie de intenties onbekend of mogelijk kwaadwillig zijn, kan van invloed zijn op het niveau van het potentiële risico. Ook moet rekening worden gehouden met het blijvende karakter van de gevolgen voor Betrokkenen, waarbij de gevolgen als groter kunnen worden beschouwd indien langetermijneffecten optreden. Een misdrijf dat blijvend vindbaar is op het internet, kan bijvoorbeeld zo een situatie opleveren.

Bijzondere kenmerken van de Betrokkene
Een inbreuk kan betrekking hebben op Data van kinderen of andere kwetsbare personen, die als gevolg daarvan een groter risico of gevaar lopen. Verder kunnen andere bijzondere factoren met betrekking tot de Betrokkene van invloed zijn op de mate waarin de inbreuk voor hem gevolgen heeft.

Bijzondere kenmerken van de Verwerkingsverantwoordelijke
De aard en rol van de Verwerkingsverantwoordelijke en zijn activiteiten kunnen ook van invloed zijn op het risico dat een inbreuk voor personen inhoudt. Indien bijvoorbeeld de server van het OM wordt gehackt, heeft dit vanzelfsprekend andere consequenties dan wanneer de LDF wordt binnengedrongen.

Het aantal getroffen Betrokkenen
Een inbreuk kan slechts één Betrokkene treffen of kan een paar Betrokkene, enkele duizenden Betrokkenen of nog veel meer Betrokkenen treffen. Over het algemeen kan een inbreuk grotere gevolgen hebben naarmate er meer Betrokkenen bij betrokken zijn. Een inbreuk kan echter zelfs voor één Betrokkene ernstige gevolgen hebben, afhankelijk van de aard van de Data en de context waarin deze zijn gecompromitteerd. Ook hier komt het erop aan te kijken naar de waarschijnlijkheid en ernst van de gevolgen voor de Betrokkene/ de hoeveelheid Betrokkenen.

Algemene punten
De Verwerkingsverantwoordelijke dient bij de beoordeling van het risico dat waarschijnlijk uit een inbreuk zal voortvloeien, rekening te houden met een combinatie van de ernst van de mogelijke gevolgen voor de rechten en vrijheden van Betrokkenen en de waarschijnlijkheid dat deze zich voordoen.

Het is duidelijk dat wanneer de gevolgen van een inbreuk ernstiger zijn, het risico groter is en dat wanneer de waarschijnlijkheid dat deze zich voordoen groter is, het risico ook groter is. In geval van twijfel dient de Verwerkingsverantwoordelijke het zekere voor het onzekere te nemen en de inbreuk te melden.

Het is aan Verwerkingsverantwoordelijke om (eventueel met behulp van specialisten, zoals gespecialiseerde ICT'ers of juristen, etc.) deze afweging te maken en te beslissen of melding moet worden gemaakt aan de Betrokkenen.

JA, hoog risico voor de rechten en vrijheden van Betrokkenen: ga naar stap 7.
NEE, geen gevolgen voor hoog risico voor de rechten en vrijheden van Betrokkenen: er hoeft alleen aan de AP en niet aan de Betrokkenen gemeld te worden.

Stap 7: Melding Betrokkenen

De Betrokkene(n) moet(en) 'onverwijld' (d.w.z. zo spoedig mogelijk) worden geïnformeerd. Bij melding wordt ten minste de volgende informatie verstrekt:

- een beschrijving van de aard van het Datalek;
- de naam en contactgegevens van de Functionaris voor Gegevensbescherming, Security Officer of een ander contactpunt van Verwerkingsverantwoordelijke;
- een beschrijving van de waarschijnlijke gevolgen van het Datalek; en
- een beschrijving van de maatregelen die de Verwerkingsverantwoordelijke heeft voorgesteld

of genomen om de inbreuk aan te pakken, met inbegrip van, in voorkomend geval, maatregelen om de mogelijke nadelige gevolgen ervan te beperken.

4. Ten slotte

Alle Datalekken moeten worden bijgehouden in een overzicht. Ook inbreuken/ situaties die niet worden gemeld aan de AP, dienen te worden vastgelegd, omdat de AP moet kunnen nagaan hoe Partijen omgaan met dergelijke situaties.

Per Datalek/ inbreuk bevat het overzicht in ieder geval de volgende zaken:

- feiten en omtrent de inbreuk in verband met Data;
- de gevolgen daarvan; en
- de genomen corrigerende maatregelen;
- (eventueel) de tekst van de kennisgeving aan de Betrokkene(n).

Het overzicht hoeft niet openbaar te worden gemaakt. Het overzicht moet minstens één jaar bewaard worden. In afwijking hiervan, moeten gegevens minimaal drie jaar worden bewaard als geen melding aan de Betrokkene is gedaan of omdat voldoende technische beschermingsmaatregelen zijn genomen.