

# De GDPR in 10 stappen

Stap 2- Breng in kaart hoe u gegevens  
verwerkt

# De GDPR in 10 Stappen

## Stap 2 – Breng in kaart hoe u gegevens verwerkt

### Inleiding

In de vorige stap heeft u in kaart gebracht welke gegevens u juist verwerkt. In stap 2 gaan we vervolgens na *hoe* u deze gegevens verwerkt. Onder de GDPR volstaat het immers niet om louter een overzicht te maken van de gegevens die u verwerkt, u moet ook kunnen aantonen dat u deze gegevens op een correcte manier verwerkt. Om na te gaan hoe u gegevens verwerkt, en of dat wel op een correcte manier gebeurt, moeten we 7 vragen overlopen:

1. [Zijn de gegevens die u verwerkt proportioneel?](#)
2. [Verwerkt u de gegevens enkel voor de doeleinden die u meedeelt?](#)
3. [Zijn de gegevens die u verwerkt correct?](#)
4. [Op welke juridische basis verwerkt u deze gegevens?](#)
5. [Vraagt u op een correcte manier toestemming?](#)
6. [Hoe lang bewaart u de gegevens die u verzamelt?](#)
7. [Geeft u gegevens door aan derde partijen?](#)

Dit is de langste en misschien ook moeilijkste stap van het Stappenplan. Neem dus de tijd om deze stap zorgvuldig te doorlopen.

Hou er ook rekening mee u er sowieso niet in zal slagen 100% in orde te zijn met de GDPR. Niemand kan dat. Maar eigenlijk verwacht de GDPR dat ook niet. Wat wel verwacht wordt is dat u de keuzes die u in de onderstaande vragen zal maken, kan verantwoorden. Met andere woorden: dat u op een redelijke manier kan argumenteren waarom u op die bepaalde manier met gegevens omgaat. Denk er daarom goed over na, en documenteer ook waarom u een bepaalde beslissing neemt.

Vooraleer we aan de vragen beginnen: ‘Privacy by design’ en ‘privacy by default’

Dit zijn twee moeilijke termen om aan te geven dat u zowel bij het bepalen van de manier waarop u gegevens zal verwerken en de middelen die u daarvoor zal inzetten (‘privacy by design’) als bij de effectieve verwerking zelf (‘privacy by default’) voldoende maatregelen moet nemen om de beginselen van de GDPR te waarborgen.

Eén van de kernbeginselen van deze twee termen is dat u enkel gegevens mag verwerken die noodzakelijk zijn voor elk specifiek doel van de verwerking, en dan meer bepaald op het vlak van:

- De hoeveelheid gegevens die u verzamelt;
- De mate waarin ze worden verwerkt;
- De termijn voor bewaring van de gegevens;
- De toegankelijkheid van de gegevens.

### Wat betekent dat concreet?

- ✓ Als u zelf programma's of toepassingen ontwikkelt waarin persoonsgegevens worden verwerkt, zorg dan dat de standaardinstellingen zo zijn bepaald dat de betrokken gegevens maximaal worden beschermd, door bijvoorbeeld:
  - Niet te veel open velden te voorzien
  - Niet te werken met vooraf aangekruiste vakjes
  - Te voorzien in een verplichting voor de betrokkene om vooraf aan te geven dat hij uw informatieclausules heeft gelezen
- ✓ Als u programma's of toepassingen aankoopt, moet u navragen (én controleren) of de leverancier deze twee principes wel heeft voorzien, en dus of hun producten wel in overeenstemming zijn met de GDPR.

### 1<sup>e</sup> vraag: zijn de gegevens die u verwerkt proportioneel?

Zoals al aangegeven, **is het doeleinde waarvoor u gegevens verwerkt, cruciaal om te weten wat u juist met de gegevens mag doen**. Binnen elk doeleinde mag u immers volgens de GDPR enkel die gegevens verwerken die 'toereikend, ter zake dienend en niet overmatig' zijn.

Het komt er dus op neer dat u enkel gegevens mag verwerken die nodig en relevant zijn voor het doeleinde waarvoor ze verwerkt worden.

Bijvoorbeeld: in het kader van het doeleinde 'loonadministratie' zijn de detailgegevens van een personeelsevaluatie niet proportioneel. Daar is in beginsel enkel het resultaat van de evaluatie relevant en dus proportioneel omdat deze (wellicht) leidt tot een bonus. Het detail van de evaluatie is enkel relevant en dus proportioneel in de verwerking "personeelsbeheer".

#### TO DO

Een gegeven dat binnen een doeleinde niet proportioneel is, mag niet langer verwerkt worden binnen dat doeleinde. Indien u de proportionaliteit niet kan verantwoorden binnen een doeleinde, moet u er voor zorgen dat u binnen dat doeleinde dergelijke gegevens niet meer verwerkt.

### 2<sup>e</sup> Vraag: verwerkt u de gegevens enkel voor de doeleinden die u meedeelt?

De GDPR legt niet alleen op dat u enkel gegevens mag verwerken die proportioneel zijn binnen een bepaald doeleinde, u mag de gegevens die u binnen dat doeleinde verwerkt bovendien ook *alleen maar* voor dat doeleinde verwerken.

Bijvoorbeeld: als u bij de informatie aan de patiënt het identificatienummer van de sociale zekerheid van de patiënt enkel hebt vermeld in het doeleinde 'patiëntenbeheer', mag u dat gegeven niet verwerken voor het doeleinde 'patiëntenregistratie'. Zorg er dan ook voor dat u de categorie van gegevens vermeldt onder alle doeleinden waarvoor u die categorie van gegevens wenst te gebruiken.

U moet met andere woorden, vooraleer u aan de verwerking van een persoonsgegeven begint, aan de betrokkene laten weten voor welk(e) doeleinde(n) u die gegevens verwerkt. U kan later die gegevens niet gaan verwerken voor andere doeleinden dan degene die u op voorhand had aangegeven, tenzij de betrokkene daar toestemming voor geeft.

Dit vraagt, zoals wel vaker bij de GDPR, wat 'gezond verstand'. U zal moeten inschatten welke verwerkingsprocessen binnen een bepaald doeleinde 'redelijk te verwachten vallen'.

Bijvoorbeeld: het is niet meer dan logisch dat u binnen het doeleinde 'loonadministratie' de loongegevens van uw medewerkers moet doorgeven aan de RSZ en de FOD Financiën. Dat moet niet beschouwd worden als een afzonderlijk 'doeleinde'.

In Stap 4 verduidelijken we hoe u op een correcte manier deze informatie aan de betrokkene kan geven.

### 3<sup>e</sup> Vraag: zijn de gegevens die u verwerkt correct?

Ga na of u er zeker van bent dat de gegevens die u bijhoudt en verwerkt, wel correct zijn. Als u er aan twijfelt of de gegevens die u bijhoudt nog wel correct zijn, doet u er best aan dat te controleren bij de betrokkene. Let op: u moet niet kunnen garanderen dat alle persoonsgegevens juist zijn. U moet wel kunnen aantonen dat u alle redelijke maatregelen heeft genomen om er voor te zorgen dat de gegevens (zo) juist (mogelijk) zijn.

- ⇒ Dit is één van de redenen waarom u de laatste weken overstelpt wordt met mails van bedrijven die u vragen om uw gegevens te controleren. U kan er voor kiezen ook zo'n mail te sturen naar uw adressenbestanden, maar eigenlijk geeft u daarmee aan dat u niet zeker bent dat alle gegevens correct zijn. En dat komt natuurlijk ook niet altijd professioneel over... .

Let op: als zorgverlener werkt u met veel gevoelige gegevens. Voor dit soort gegevens is het des te belangrijker om voldoende mogelijkheden te bieden aan de betrokkene om na te kijken of zijn/haar gegevens wel correct zijn. U moet dus met andere woorden maatregelen nemen om er voor te zorgen dat de gegevens up – to – date blijven. Meestal zal dit een IT-oplossing vragen, zodat u zich hierover best informeert bij een leverancier.

### 4<sup>e</sup> Vraag: op welke juridische basis verwerkt u deze gegevens?

Het zal u al opgevallen zijn dat, wanneer men over de GDPR spreekt, vaak naar boven komt dat men nu voor alles toestemming moet vragen. Dat klopt echter niet. Wat wel klopt, is dat de GDPR vereist dat u enkel gegevens mag verwerken als u daar een geldige juridische grondslag voor heeft. Toestemming is echter slechts één van die juridische grondslagen. In totaal voorziet de GDPR nog vijf andere mogelijke grondslagen:

- 1) De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of om vóór de sluiting van de overeenkomst, op verzoek van de betrokkene, maatregelen te nemen;
- 2) De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting (die op de verwerkingsverantwoordelijke rust) (denk bijvoorbeeld aan de verplichting om te factureren, of loon te betalen aan personeel);
- 3) De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derden, mits de belangen of grondrechten en fundamentele vrijheden van de betrokkene niet zwaarder (door)wegen;

- 4) De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meerdere specifieke doeleinden;
- 5) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- 6) De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Let wel op: bijzondere categorieën van persoonsgegevens ( zoals gegevens over gezondheid, ras, seksuele geaardheid, ...), is zoals gezegd in principe verboden. De GDPR staat dit enkel in uitzonderlijke gevallen toe. We besparen u de juridische achtergrond, maar voor u als zorgverstrekker komt het er op neer dat u deze bijzondere categorieën van gegevens enkel mag verwerken in één van de twee volgende gevallen:

- a. De verwerking is noodzakelijk voor doeleinden van gezondheidszorg én gebeurt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die gebonden is door het beroepsgeheim én u mag de gegevens verwerken op grond van één van de bovenstaande 6 rechtsgronden; gegevens worden verwerkt onder u één van bovenstaande juridische grondslagen kan toepassen<sup>1</sup>; én
- b. Als u niet aan de voorwaarden van a) voldoet ( bijvoorbeeld omdat de gegevens niet worden verwerkt door of onder de verantwoordelijkheid van een beroepsbeoefenaar die gebonden is aan het beroepsgeheim), dan mag u de gegevens enkel verwerken als u daar toestemming voor heeft van de betrokkene.

Bovendien is de verwerking van dergelijke bijzondere categorieën van persoonsgegevens onder de huidige regelgeving onderworpen aan enkele bijzondere voorwaarden (zie artikel 25 tot en met 27 van het KB van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, BS 13 maart 2001, 7839). Omdat deze voorwaarden zinvol zijn, is het aangewezen ze te behouden en toe te passen. Het gaat om de volgende voorwaarden:

- 1) de categorieën van personen die de persoonsgegevens kunnen (en mogen) raadplegen, moeten worden aangewezen waarbij hun hoedanigheid ten opzichte van de verwerking van de betrokken gegevens nauwkeurig moet worden omschreven;
- 2) de lijst of het bestand van de aldus aangewezen categorieën van personen moet ter beschikking worden gehouden van toezichthoudende autoriteit;
- 3) de aldus aangewezen personen moeten er door een wettelijke of statutaire verplichting dan wel een evenwaardige contractuele bepaling toe gehouden zijn het vertrouwelijk karakter van de betrokken gegevens in acht te nemen;
- 4) in het (intern) register moet vermeld worden op grond van welke wet of bepaling de verwerking van de bijzondere categorieën van persoonsgegevens is toegestaan.

Vanuit die wetenschap, geeft dat, toegepast op de verwerkingsdoeleinden die we u in de 1<sup>e</sup> stap hebben aangereikt, het volgende beeld:

---

<sup>1</sup> In het juridisch jargon heeft dit geval ' de uitzondering voorzien in art. 9, 2<sup>e</sup> lid, h) en art. 9, 3<sup>e</sup> lid. Omwille van efficiëntie gebruiken we deze verwijzing ook in het Register en in onderstaande voorbeelden.

## Voorbeeld

1. Patiëntenbeheer
  - Noodzakelijk voor de uitvoering van een overeenkomst
  - In sommige gevallen kan de wetgever ook verplichten om bepaalde gegevens te verwerken; dan is er sprake van een wettelijke verplichting
  - Bijzondere categorieën van gegevens:
    - Ofwel: algemeen belang ( verwerkingen in de gezondheidszorg) in combinatie met art. 9, 2<sup>e</sup> lid, h) en art. 9, 3<sup>e</sup> lid GDPR.
    - Ofwel: toestemming
2. Leveranciersbeheer
  - Noodzakelijk voor de uitvoering van een overeenkomst
3. Boekhouding
  - Noodzakelijk voor de uitvoering van een overeenkomst
  - wettelijke verplichting
4. Communicatie/Public Relations
  - Gerechtvaardigd belang (vrijheid van ondernemen)
5. Personeelsadministratie
  - Noodzakelijk voor de uitvoering van de arbeidsovereenkomst
  - wettelijke verplichting ( alles wat te maken heeft met uitbetaling van loon en gegevens die doorgegeven moeten worden aan RSZ en FOD Financiën)
  - Gerechtvaardigd belang (als u bijvoorbeeld controle voert op de online communicatiemiddelen van uw personeel
6. Camerabewaking
  - Gerechtvaardigd belang (controle op veiligheid)

Op die manier kan het dus zijn dat voor één doeleinde, meerdere juridische gronden worden aangegeven. Als we dus onder het doeleinde 'patiëntenadministratie' meerdere juridische grondslagen omschrijven, wil dat zeggen dat de grondslag 'uitvoering van een overeenkomst' de algemene grondslag is voor dat doeleinde, maar dat specifiek voor de gevoelige gegevens, de grondslag 'algemeen belang' of 'toestemming' wordt ingeroepen.

Strikt genomen hoeft u dus geen toestemming te vragen aan de patiënt, toch niet voor de initiële verwerkingen ( voor bepaalde afgeleide verwerkingen, zoals doorgifte van gegevens, zal u wel toestemming nodig hebben, zie verder), tenzij u niet gebonden bent door het beroepsgeheim. Let op: de huidige regeling waarbij het elektronisch delen van gezondheidsgegevens via systemen die onderling verbonden zijn enkel kan op basis van een geïnformeerde toestemming van de betrokkene, blijft onverkort bestaan!

Het staat u evenwel vrij om toch voor bepaalde doeleinden toestemming te vragen, bijvoorbeeld omdat u vindt dat dat uw patiënten een veiliger gevoel geeft. Maar puur vanuit de GDPR gezien is dat dus niet nodig. Als u echter toch toestemming zou vragen, moet u wel zeker zijn dat die toestemming correct wordt gevraagd.

## 5<sup>e</sup> Vraag: vraagt u op een correcte manier toestemming?

Volgens de GDPR moet toestemming *vrij, specifiek, geïnformeerd* en *ondubbelzinnig* zijn. Toestemming moet ook steeds een duidelijk *bevestigende handeling* zijn.

**Ga na of u de volgende principes hanteert als u om toestemming vraagt:**

- ✓ Ik voorzie bij de toestemming een vrijwillige keuze; waarbij de betrokkene uitdrukkelijk kan instemmen (*dit is een zogenaamde 'opt-in'*);
- ✓ Ik licht de betrokkene duidelijk in voor wat en voor welke doeleinden toestemming wordt gegeven (*cf. recht op informatie*);
- ✓ Ik leid geen toestemming af uit een stilzwijgen, een vooraf aangevinkt vakje of uit een niet-handelen;
- ✓ Ik voorzie de mogelijkheid dat de betrokkene ten allen tijde zijn toestemming kan intrekken. Het intrekken van de toestemming is even eenvoudig als het geven van de toestemming, bv. duidelijk weergeven van uitschrijfmogelijkheden.

Belangrijk is ook dat de toestemming steeds *controleerbaar* moet zijn. Dat wil zeggen dat u moet kunnen aantonen wie, wanneer en hoe er toestemming werd gegeven. U registreert dit best in een document.

## OPGELET: Kinderen

Kinderen vormen een bijzondere categorie van personen. De GDPR legt ten aanzien van kinderen dan ook een aantal specifieke regels op:

- De grondslag 'gerechtvaardigd belang', zal ten aanzien van kinderen in principe niet kunnen worden gebruikt; voor de verwerking van hun gegevens vraagt u best ook toestemming aan de ouders;
- Ten aanzien van kinderen moet informatie op een extra eenvoudige manier worden voorzien;
- De Wet Patiëntenrechten bepaalt dat de rechten met betrekking tot persoonsgegevens van minderjarige patiënten door de ouders worden uitgeoefend. Enkel wanneer de minderjarige patiënt 'tot een redelijke beoordeling van zijn belangen in staat kan worden geacht, mag de minderjarige patiënt de rechten met betrekking tot zijn gegevens zelfstandig uitoefenen.
- Ten aanzien van 'diensten van de informatiemaatschappij' (online dienstverlening zoals online psychologische bijstand), is steeds toestemming vereist van de ouders als het kind jonger is dan 16 jaar (die leeftijd zal in België hoogstwaarschijnlijk verlaagd worden tot 13 jaar).

## 6<sup>e</sup> Vraag: hoe lang bewaart u de gegevens die u verzamelt?

Persoonsgegevens mogen niet eeuwig bewaard worden. Helaas voorziet de GDPR geen wettelijke bewaartermijnen, maar moet u die zelf bepalen. Het gaat evenmin op om voor al uw gegevens één bewaartermijn te voorzien.

U zal dus zelf moeten bepalen hoe lang het volgens u gerechtvaardigd is om een bepaald gegevens bij te houden. Enkele richtlijnen daarbij:

## Bewaartermijnen

- **Bewaring gedurende de verwerking**

Het spreekt voor zich dat u de betrokken persoonsgegevens kan bijhouden zolang u ze nodig heeft voor de verwerking(en) binnen het doeleinde dat u had aangegeven.

Bijvoorbeeld: Zolang iemand patiënt is van u, kan u de gegevens in het kader van patiëntenzorg, - registratie en - beheer bewaren.

- **Bewaring na de verwerking**

Soms bent u wettelijk verplicht om gegevens ook daarna nog te bewaren. Zo geldt er een wettelijke bewaartermijn van 7 jaar nadat een factuur werd uitgereikt, en een wettelijke bewaartermijn van 5 jaar voor personeelsgegevens. Voor artsen geldt bijvoorbeeld een bewaartermijn van 30 jaar voor medische dossiers.

Maar ook los van een wettelijke verplichting kan u er baat bij hebben bepaalde gegevens langer te bewaren. Voor verbintenissen uit overeenkomsten kan u bijvoorbeeld (in de meeste gevallen) tot 10 jaar na datum worden aangesproken ( de verjaringstermijn voor eventuele rechtsvorderingen door uw medecontractant). U kan dan ook perfect verantwoordelijk dat u persoonsgegevens die noodzakelijk zijn voor de uitvoering van de overeenkomst, kan bewaren gedurende die verjaringstermijn.

- **Archiveringstermijn**

Na deze termijnen begint de eigenlijke archiveringstermijn. De GDPR bepaalt dat in dat geval gegevens enkel geanonimiseerd mogen worden bewaard. Bovendien wordt aan elke betrokkene het recht toegekend om de wissing van deze gegevens te vragen zodra ze gearchiveerd worden in deze betekenis.

Die termijnen moeten ook ter kennis worden gebracht van de betrokkenen, in de informatie die hen moet worden verstrekt. Is het niet mogelijk om de bewaringstermijn zelf mee te delen, moeten minstens de criteria worden aangegeven die worden gebruikt om die termijn te bepalen. In een aantal privacyverklaringen ziet men nu al de boodschap verschijnen ‘*Wij bewaren uw persoonsgegevens niet langer dan noodzakelijk voor de beoogde doeleinden van de verwerking*’. Toch doet u er best aan om, waar mogelijk, de bewaartermijn toch concreter te omschrijven, bijvoorbeeld: “*Na het einde van de patiëntrelatie bewaren wij uw gegevens nog 30 jaar bijgehouden worden ( aangezien dit de gangbare bewaartermijn is voor medische dossiers).*”

## TO DO

Het is mogelijk om in een toepassing of programma een termijn op te nemen na verloop van dewelke de gegevens zonder meer worden gewist. Dit vereist vooral dat er voor elk gegeven een duidelijke aanvangstermijn wordt bepaald. Dit moet op een goede manier worden aangepakt omdat het wissen van gegevens die nog nodig of vereist zijn, kan worden aangemerkt als een gegevenslek.

Alternatief kan zijn om periodiek na te gaan of bepaalde gegevens nog wel vereist zijn en ze, indien nodig of aangewezen, te wissen.



Daarnaast moet u een afweging maken om ervoor te zorgen dat de bewaartermijn zoveel mogelijk wordt beperkt (tot wat noodzakelijk is):

- ✓ Zo is het best mogelijk dat om een vordering van een betrokkene te weerleggen, er slechts een beperkt aantal gegevens moeten worden bewaard. In dat geval is in beginsel de bewaring van de andere gegevens niet langer vereist. Dat neemt niet weg dat het in vele gevallen niet evident zal zijn om deze gegevens “uit elkaar te halen”.  
In zo’n geval moet het mogelijk zijn om *alle* gegevens gedurende de verjaringstermijn te bewaren, maar dan hanteert u best een passief beheer. Dit houdt in dat de toegang tot die andere gegevens heel beperkt moet worden en blijven.
- ✓ Hou er ook rekening mee dat de bewaartermijn voor ‘gevoelige gegevens’ hogere eisen stellen, waardoor u er bijvoorbeeld best aan doet de bewaring van dergelijke gegevens bijvoorbeeld extra te beveiligen, bijvoorbeeld door deze gegevens zeker niet op papier te bewaren, maar in een afzonderlijk bestand, indien mogelijk zelfs een afzonderlijke IT-oplossing die gebruik maakt van encryptie, en bijvoorbeeld slechts voor één persoon toegankelijk is.

### 7<sup>e</sup> Vraag: geeft u gegevens door aan derde partijen?

Indien u gegevens doorgeeft aan een derde partij, dan noemt met die derde partij een ‘ontvanger’ van uw gegevens. Intuïtief zal u misschien aangeven dat u geen gegevens doorgeeft aan dergelijke ontvangers, maar hou er rekening mee dat de term ‘ontvangers’ veel ruimer is dan u misschien zou denken. Het gaat niet alleen over bijvoorbeeld de overdracht van een patiëntendossier.

Binnen de groep ‘ontvangers’ zit immers ook de groep ‘verwerkers’. In Stap 1 hebben we gezien dat de verwerker iedere instantie is die gegevens voor u verwerkt. Sociale secretariaten, boekhouders, boekhoudpakketten, mailingsoftware, ... zijn allemaal ‘verwerkers’, en dus ook ‘ontvangers’. Het gaat in al die gevallen om derde partijen die gegevens van u verkrijgen.

#### TO DO

Breng in kaart aan wie u gegevens doorgeeft. Maak gebruik van algemene categorieën, zoals:

- Medewerkers
- Commerciële partners
- Overheid
- Verwerkers
- ....

Heeft u al deze vragen geanalyseerd en beantwoord? Dan bent u klaar om naar stap 3 te gaan.

# Checklist

- Ik heb nagekeken welke gegevens binnen elk doeleinde correct zijn en proportioneel, de overige gegevens heb ik verwijderd.
- Ik heb voor alle gegevens die ik verwerk een geldige juridische grondslag bepaald.
- Indien ik toestemming moet vragen, heb ik nagekeken of ik die toestemming op een correcte manier vraag.
- Ik heb voor alle gegevens een passende bewaartermijn vastgelegd.
- Ik heb in kaart gebracht aan wie ik persoonsgegevens doorgeef.