De GDPR in 10 stappen

Stap 4- Vul uw gegevens aan in het Verwerkingsregister

De GDPR in 10 Stappen

Stap 4 – Vul uw gegevens aan in het Verwerkingsregister

Inleiding

In de vorige 3 stappen heeft u een overzicht gemaakt van alle gegevens die u verwerkt, en van de manier waarop u die verwerkt. Die stappen waren echter niet alleen nodig om na te gaan of u persoonsgegevens op een correcte manier verwerkt, ze waren ook nodig om te kunnen voldoen aan een nieuwe verplichting die de GDPR oplegt: het bijhouden van een 'Register van Verwerkingsactiviteiten'.

Wat is het Register?

Het Register is een puur intern document, dat documenteert op welke manier u persoonsgegevens verwerkt. Het moet dus niet openbaar gemaakt worden, maar bij een eventuele controle moet u het wel kunnen voorleggen. Daarnaast is het Register ook een handig hulpmiddel wanneer iemand vraagt welke gegevens u juist over hem verwerkt, of vraagt om geschrapt te worden uit uw bestanden.

Hoe moet zo'n Register er uit zien?

Het staat u volledig vrij om zelf te bepalen op welke manier u het Register opmaakt. U moet er alleen rekening mee houden dat de volgende elementen steeds in het Register moeten opgenomen worden:

Verplichte vermeldingen

- Uw naam en contactgegevens
- De doeleinden van de verwerking
- Eventueel: [de verwerkingsactiviteiten]
- [De juridische basis]
- Een beschrijving van de categorieën van betrokkenen
- Een beschrijving van de categorieën van persoonsgegevens
- De categorieën van ontvangers (personen aan wie gegevens worden doorgegeven)
- Eventuele doorgiften aan derde landen
- De bewaartermijn van de gegevens
- De technische en organisatorische beveiligingsmaatregelen

U zal merken dat u de meeste zaken die in het Register moeten komen, al in kaart heeft gebracht in de vorige stappen:

- In Stap 1 heeft u een overzicht gemaakt van de doeleinden van de verwerking, de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In Stap 2 heeft u een overzicht gemaakt van de categorieën van ontvangers, de juridische basis waarop u gegevens verwerkt en heeft u een bewaartermijn bepaald voor uw gegevens;
- In Stap 3 heeft u de technische en organisatorische beveiligingsmaatregelen in kaart gebracht, en bent u nagegaan of u gegevens doorgeeft aan derde landen.

Op zich kan u dus volstaan om de informatie die u in de vorige drie stappen heeft vergaard, in een Register in te schrijven. U kan echter ook gebruik maken van het Model dat UNIZO ter beschikking stelt.

Hoe vult u dit UNIZO Model Register in?

Tabblad 'Algemene Info'

Dit tabblad bevat drie kolommen: 'verwerkingsverantwoordelijke', 'verwerker' en ' functionaris voor gegevensbescherming'.

U kan zoals gezegd gegevens verwerken als 'verwerkingsverantwoordelijke' of als 'verwerker'. Als u optreedt als 'verwerker' voor iemand anders, moet u daar een afzonderlijk register voor bijhouden. U maakt dan één register voor uw activiteiten als verwerkingsverantwoordelijke, en één voor uw activiteiten als verwerker.

Treedt u niet op als verwerker voor iemand anders, dan vult u enkel de kolom 'verwerkingsverantwoordelijke' in, en laat u de kolom 'verwerker' achterwege.

De kolom 'functionaris voor gegevensbescherming' is enkel nodig wanneer u zo'n functionaris moet aanstellen (zie verder, stap 9). Voor u zal dat in beginsel niet nodig zijn; u kan deze kolom in dat geval weglaten.

'Register'

In het Register zelf vindt u per doeleinde een tabblad. In elk tabblad zijn de elementen voorzien die volgens de GDPR zouden moeten opgenomen worden in het Register:

1. [Verwerkingsactiviteit)
2. [Rechtsgrond]
3. Categorieën betrokkenen
4. Categorieën gegevens
5. Bewaringstermijn
6. Technische en organisatorische beveiligingsmaatregelen
7. Categorieën ontvangers
8. Doorgiften

Toelichting bij de diverse rubrieken

1. Verwerkingsactiviteit

Volgens de GDPR is het niet verplicht deze rubriek te voorzien. We voorzien de rubriek hier echter toch, omdat het soms handig kan zijn om binnen een bepaald doeleinde wat meer in detail te omschrijven welke activiteiten juist plaatsvinden binnen dat doeleinde. Het kan immers zijn dat u verschillende rechtsgronden gebruikt binnen een bepaald doeleinde, of gegevens van verschillende soorten betrokkenen die gekoppeld zijn aan de activiteit.

<u>Bijvoorbeeld:</u>

- Binnen het doeleinde ‘personeelsadministratie’ zijn er bijvoorbeeld (minstens) de volgende ‘verwerkingsactiviteiten’, die elk een eigen juridische grondslag hebben:
    - Evaluatie / opleiding en Vorming
    - Uitbetaling van lonen
    - Controle van online communicatiemiddelen
    - Sollicitantenbeheer
    - …
- Binnen het doeleinde ‘Patiëntenzorg’, kunnen er in principe ook verschillende activiteiten zijn:
    - Registratie van patiënten bij hun bezoek
    - Aanleggen van een patiëntendossier
    - Behandeling van patiënten (diagnose, preventie, remediëring, …)
    - …

Door te werken met verschillende verwerkingsactiviteiten binnen een doeleinde, kan u dus in uw Register iets meer in detail gaan.

2. Rechtsgrond

In deze rubriek voegt u voor elke categorie van gegevens de juridische grondslag toe die u in Stap 2 bepaald heeft.

3. Categorieën betrokkenen

In deze rubriek voegt u het overzicht toe dat u in Stap 1 heeft gemaakt van de personen van en over wie er persoonsgegevens worden verwerkt (de ‘betrokkenen’). Zoals gezegd volstaat het te werken met algemene categorieën. Bij ‘Klantenbeheer’ zal dat dus gewoon ‘klanten’ zijn. Bij ‘leveranciersbeheer’ waarschijnlijk gewoon ‘leveranciers’.

Bij een aantal andere doeleinden kan het zijn dat u meerdere categorieën moet invullen. Bijvoorbeeld:

- Het doeleinde ‘personeelsadministratie’ zal niet enkel gegevens van werknemers bevatten, maar bijvoorbeeld ook van sollicitanten of gepensioneerde werknemers.
- Het doeleinde ‘boekhouding’ zal zowel gegevens van ‘patiënten’ als van ‘leveranciers’ bevatten.

4. Categorieën gegevens

In deze rubriek voegt u het overzicht toe dat u in Stap 1 heeft gemaakt van de soorten persoonsgegevens die u binnen elk doeleinde verwerkt. Ook hier volstaat het te werken met algemene categorieën.

5. Bewaringstermijn

In deze rubriek voegt u voor elke categorie van gegevens de bewaartermijn toe die u in Stap 2 bepaald heeft. Zoals gezegd moet u minstens de criteria aangeven die worden gebruikt om die termijn te bepalen. Indien mogelijk, bepaalt u de concrete bewaartermijn.

Tip:

- Voor gegevens die nodig zijn om een overeenkomst uit te voeren, zal in de regel een bewaartermijn van 10 jaar na het einde van de overeenkomst gerechtvaardigd kunnen worden (= contractuele verjaringstermijn); dit is dan ook de bewaartermijn die u voorziet in het doeleinde 'leveranciersbeheer'. Kijk dit wel na voor uw situatie: kent de u de juiste verjaringstermijn niet, neem dan geen risico en zeg 'einde overeenkomst + contractuele verjaringstermijn';
- Gegevens in verband met personeel moeten in elk geval minstens 5 jaar na het einde van de arbeidsrelatie bewaard worden, maar vraag aan uw sociaal secretariaat welke bewaartermijnen in uw geval kunnen gelden;
- Documenten die bewaard worden binnen het doeleinde 'boekhouding', moeten op basis van een wettelijke verplichting 7 jaar bewaard worden;
- Documenten uit het patiëntendossier moeten 30 jaar bewaard worden.

6. Technische en organisatorische beveiligingsmaatregelen

In deze rubriek voegt u het overzicht van beveiligingsmaatregelen toe dat u in Stap 3 heeft gemaakt. Indien u binnen een doeleinde (of verwerkingsactiviteit) gevoelige gegevens verwerkt, doet u er best aan te omschrijven welke extra beveiligingsmaatregelen u juist neemt in dat verband.

7. Categorieën ontvangers

In deze rubriek voegt u het overzicht toe dat u in Stap 2 heeft gemaakt van de derde partijen aan wie u gegevens doorgeeft (inclusief de 'verwerkers') die u binnen elk doeleinde verwerkt. Ook hier volstaat het te werken met algemene categorieën, en bent u dus niet verplicht elke verwerker afzonderlijk te vernoemen. In praktijk wil dat zeggen dat u meestal enkel 'verwerkers' moet vermelden (in sommige gevallen ook 'overheid').

8. Doorgiften

In deze rubriek voegt u voor elke categorie van gegevens toe of u de gegevens doorgeeft aan derde landen (zie stap 3):

Geeft u inderdaad gegevens door aan een derde land (bijvoorbeeld omdat u werkt met een softwarepakket waarvan de servers in zo'n derde land staan), dan schrijft u in de subrubriek 'aard van de doorgifte' één van de volgende mogelijkheden:

- Enkel landen die door de EU goedgekeurd zijn https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Enkel ondernemingen die voorkomen op de Privacy Shield List
- Andere (in dit geval moet u een omschrijving toevoegen van de passende waarborgen die werden voorzien)

Voorbeelden

Het is helaas onmogelijk om u een vooraf ingevuld register te bezorgen, omdat het register noodzakelijk moet worden opgemaakt op basis van uw specifieke situatie. Omdat we weten dat het invullen van een

register geen evidentie is, geven we u hieronder 3 voorbeelden van ingevulde doeleinden. Hou er rekening mee dat u dit niet gewoon mag copy-pasten, u moet altijd nagaan wat u in uw specifieke situatie doet!

Patiëntenzorg

VERWERKINGSACTIVITEIT 1: BEHANDELING VAN PATIËNTEN

CATEGORIEËN VAN BETROKKENEN

- Patiënten

CATEGORIEËN VAN PERSOONSGEGEVENS – VERWERKING OP GROND VAN ALGEMEEN BELANG

- Persoonlijke identificatiegegevens (naam, adres, telefoon, mail)
- Rijksregisternummer/identificatienummer van de sociale zekerheid
- Financiële identificatiegegevens (bankrekeningnummer)
- Beroepsactiviteit (werkgever, titel, …)
- Persoonlijke bijzonderheden (leeftijd, geslacht, geboortedatum, geboorteplaats, burgerlijke staat, nationaliteit, …)
- Samenstelling van het gezin (naam van de partner, aantal, kinderen, …)
- Vrijetijdsbesteding en interesses (hobby's, sport, andere interesses)
- Beeldopnamen
- Leefgewoonten
- …

BIJZONDERE CATEGORIEËN VAN PERSOONSGEGEVENS – VERWERKING OP GROND VAN ALGEMEEN BELANG EN ARTIKEL 9, 2E LID, H) EN ARTIKEL 9, 3E LID ALGEMENE VERORDENING GEGEVENSBESCHERMING

- Gezondheidsgegevens
- Genetische gegevens
- Raciale en etnische gegevens
- …

BEWAARTERMIJN

- Einde patiëntenrelatie + 30 jaar

ONTVANGERS

- Verwerkers
- Overheid

DERDE LAND?

- Neen
- Enkel landen die door de EU goedgekeurd zijn https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Enkel ondernemingen die voorkomen op de Privacy Shield List + 10 jaar (contractuele aansprakelijkheid)

[SCHRAPPEN WAT NIET PAST]

BEVEILIGING

- Zie algemene beveiligingsuiteenzetting (bijlage)

- Extra beveiligingsmaatregelen voor gevoelige gegevens: …

Personeelsadministratie

VERWERKING 1 : LOONADMINISTRATIE

CATEGORIEËN VAN BETROKKENEN

- Werknemers
- Gepensioneerden
- Familieleden

CATEGORIEËN VAN PERSOONSGEGEVENS

- Persoonlijke identificatiegegevens (naam, adres, telefoon, mail, nummer identiteitskaart)
- Financiële identificatiegegevens (bankrekeningnummer)
- Financiële transacties (betalingen die de persoon heeft gedaan of nog moet doen)
- Beroepsactiviteit (werkgever, titel, …)
- Persoonlijke bijzonderheden (leeftijd, geslacht, geboortedatum, geboorteplaats, burgerlijke staat, nationaliteit, …)
- Samenstelling van het gezin (naam van de partner, aantal, kinderen, …)
- Opleiding en vorming
- GEVOELIGE GEGEVENS:
  - Gegevens van minderjarigen (naam, geslacht, geboortedatum, kinderbijslag, ten laste, bijkomende info)
  - Invaliditeit
  - Gezondheidsgegevens (ziektebriefjes)
  - Rijksregisternummer/identificatienummer van de sociale zekerheid

RECHTSGROND

- wettelijke verplichting
- verwerking van bijzondere categorieën van gegevens: artikel 9, 2e lid, b) Algemene Verordening Gegevensbescherming

CATEGORIEËN VAN ONTVANGERS

- Overheidsdiensten
- Verwerkers

DERDE LAND?

- Neen
- Enkel landen die door de EU goedgekeurd zijn https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Enkel ondernemingen die voorkomen op de Privacy Shield List + 10 jaar (contractuele aansprakelijkheid)

[SCHRAPPEN WAT NIET PAST]

BEWAARTERMIJN

- Vanaf het einde van de arbeidsovereenkomst loopt een termijn gelijk aan de wettelijke bewaartermijn of de verjaringstermijn die relevant is voor eventuele rechtsvorderingen.

BEVEILIGING

- Zie algemene beveiligingsuiteenzetting (bijlage)
- Extra beveiligingsmaatregelen voor gevoelige gegevens: …

Boekhouding

CATEGORIEËN VAN BETROKKENEN

- Leveranciers
- Patiënten

CATEGORIEËN VAN PERSOONSGEGEVENS

- Persoonlijke identificatiegegevens (naam, adres, telefoon, mail, nummer identiteitskaart)
- Financiële identificatiegegevens (bankrekeningnummer)
- Financiële transacties (betalingen die de persoon heeft gedaan of nog moet doen)
- Beroepsactiviteit (werkgever, titel, …)
- Ondernemingsnummer van leveranciers
- …

RECHTSGROND

- wettelijke verplichting

CATEGORIEËN VAN ONTVANGERS

- Overheidsdiensten
- Verwerkers

DERDE LAND?

- Neen
- Enkel landen die door de EU goedgekeurd zijn https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Enkel ondernemingen die voorkomen op de Privacy Shield List + 10 jaar (contractuele aansprakelijkheid)

[SCHRAPPEN WAT NIET PAST]

BEWAARTERMIJN

- Einde overeenkomst + 7 jaar (bewaartermijn facturen)

BEVEILIGING

- Zie algemene beveiligingsuiteenzetting (bijlage)