

Bijlage 6: Het Register (toelichting)

I. Wat is het register

Het register is een actief document waarin de verwerkingsverantwoordelijke en de verwerker de verwerkingsactiviteiten bijhouden die onder hun verantwoordelijkheid worden uitgevoerd.

Voortdurende bijwerking

Het register is een levend instrument dat evolueert naarmate de activiteiten van de organisatie, overheid of instantie zich verder ontwikkelen. De gegevens worden niet geschrapt, maar worden door de verwerkingsverantwoordelijke en de verwerker constant aangevuld zodat er een duidelijke historiek is van de uitvoering van de verwerkingsactiviteiten

Voor kleine organisaties met minder dan 250 werknemers die gewoonlijk (niet incidenteel) persoonsgegevens verwerken, kan het register beperkt zijn tot de niet-incidentele verwerkingen. De incidentele verwerkingen moeten niet in het register opgenomen worden, tenzij het verwerkingen zijn die een risico vormen voor de rechten en vrijheden van de betrokkenen of het verwerkingen zijn van gevoelige gegevens.

II. Vorm

Een elektronisch Register

Dit register moet minstens elektronisch bijgehouden worden. Eventueel ook op papier.

Flexibiliteit qua model

Gelet op de waaier aan situaties bestaat er geen vast, officieel model voor het register.

Voorbeeldmodellen

De privacycommissie werkte zelf een voorbeeld van register uit dat je organisatie als vertrekpunt voor de opmaak van een register op maat kan gebruiken.

- <https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten>
- scwitch maakte een ontwerp van register waar je mee aan de slag kunt. (bijlage 5 register)

Deze modellen zijn geen officiële documenten. Je mag gerust een ander register gebruiken dat je een volledig overzicht biedt van de verrichte persoonsgegevensverwerkingen, met alle verplichte vermeldingen (zie verder) .

Het register wordt best opgesteld in het Nederlands (en/of het Frans). Als het in een andere taal is opgesteld, kan de privacycommissie immers een vertaling eisen waarvan de organisatie de vertaalkosten moet dragen.

III. WIE moet dit register bijhouden?

De verplichting berust tegelijk op:

- de verwerkingsverantwoordelijke, voor de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden
- de verwerker (bv. het sociaal secretariaat), voor de verwerkingsactiviteiten die hij voor rekening van de verantwoordelijke verricht

IV. WIE mag het register raadplegen?

Het register is in de eerste plaats een intern instrument als hulp voor de verwerkingsverantwoordelijke en verwerker om zich in regel te brengen met de GDPR.

Het register is ook bedoeld als informatiebron voor de privacycommissie die als toezichthoudende overheid controles kan uitvoeren op de naleving van de GDPR. Je moet het register kunnen voorleggen en ter beschikking stellen wanneer de commissie erom verzoekt.

Dit register is NIET bestemd voor het publiek of voor de betrokkenen van wie je organisatie de persoonsgegevens verwerkt.

Het kan echter zowel van nut zijn voor de verwerkingsverantwoordelijke als voor de functionaris voor gegevensbescherming wanneer zij bevraagd worden door betrokken personen in het kader van de uitoefening van hun rechten.

V. WAT moet er in het register staan?

Op 25 mei 2018 treedt de GDPR in werking en moet er een register bestaan met informatie over alle verwerkingsactiviteiten die op dat ogenblik plaatsvinden, al sinds lange tijd of pas recent opgestart. Nadien moet het register telkens aangevuld worden als er verwerkingsactiviteiten bijkomen of aangepast worden.

De volgende gegevens moet je in het register opnemen:

- 1. Wie verwerkt?**
- 2. Waarom (doeleinden) worden de welbepaalde gegevens verwerkt?**
- 3. Wat wordt verwerkt?**
- 4. Waar worden de gegevens gelokaliseerd en doorgegeven?**
- 5. Hoe lang worden de gegevens bewaard?**
- 6. Hoe worden de gegevens beveiligd?**

1. WIE verwerkt?

Vermeld de naam en de contactgegevens van de verwerkingsverantwoordelijke, en in voorkomend geval van de verwerker, de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming.

De verwerkingsverantwoordelijke is 'een natuurlijke persoon of rechtspersoon, een overheidsinstelling, een dienst of een orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'.

In de meeste gevallen is de organisatie de verwerkingsverantwoordelijke.

De verwerker is een externe onderaannemer die persoonsgegevens voor een organisatie verwerken. *Bv. het sociaal secretariaat, de cloudserviceprovider voor de opslag van gegevens...*

Een organisatie is soms verwerkingsverantwoordelijke en verwerker.

Soms kan eenzelfde entiteit tegelijk de rol spelen van verwerkingsverantwoordelijke en verwerker.

Wanneer zowel de rol van verwerkingsverantwoordelijke als verwerker wordt gespeeld, voorzie je in het Register best in twee aparte luiken. Een voor de verwerkingen verricht als verantwoordelijke voor de verwerking, en een andere voor de verwerkingen verricht als verwerker.

Alle personen die binnen je organisatie gegevens verwerken, werken best samen voor de opmaak van dit register aangezien zij alle bijzondere informatie over de verwerkingen kunnen verstrekken. Op die manier is ook iedereen betrokken en op de hoogte van het privacybeleid binnen je organisatie.

2. WAAROM worden gegevens verwerkt? De verwerkingsdoeleinden

Het begrip verwerking is heel breed. Het gaat van het verzamelen, raadplegen, verspreiden, kopiëren, registreren tot het vernietigen van gegevens. Per verwerking bepaal je het doeleinde.

Enkele mogelijke algemene doeleinden: personeelsadministratie, vrijwilligersadministratie, controle op de werkplaats, beheer welzijn op het werk, administratie nieuwsbrief, klantenbeheer, leveranciersbeheer, etc.

De verwerkingsverantwoordelijke let erop dat de verwerkingsdoeleinden met de nodige precisie worden omschreven. De GDPR beveelt aan dat de algemene omschrijving van het doeleinde wordt aangevuld met een gedetailleerde beschrijving.

Bv. administratie van personeel, vrijwilligers en tussenpersonen:

Selectie en aanwerving of aanstelling van personeel en tussenpersonen (freelancers, vrijwilligers, makelaars, ...). Administratie van de lonen, kostenvergoedingen, voordelen enz.. Toepassing van de sociale en fiscale wetgeving. Toepassing van de vrijwilligerswet. Toepassing van decretale verplichtingen.

3. WAT verwerken we?

Een beschrijving van categorieën van betrokkenen plus de categorieën van verwerkte persoonsgegevens ten opzichte van elk doeleinde.

De **betrokkenen** zijn de geïdentificeerde of identificeerbare natuurlijke personen van wie de gegevens worden verwerkt. Het gaat om leden, werknemers, klanten, leveranciers, externe dienstverstrekkers, enz.

Per categorie van betrokkenen lijst je de **persoonsgegevens** op die verwerkt worden: naam, adres, rijksregisternummer, e-mailadres, financiële gegevens (bv. bankrekeningnummer), gegevens betreffende studies, loopbaan, foto's, beeld of geluidsopnames, enz.

Maak een duidelijke vermelding in het register als je persoonsgegevens van minderjarigen verwerkt. Toets je verwerking aan specifieke regels die daarvoor gelden.

Identificeer duidelijk welke van de verwerkte gegevens gevoelige gegevens zijn, aangezien er ook daarvoor specifieke regels van toepassing zijn.

De inhoud van aangiftes die je organisatie misschien in het verleden heeft ingediend bij de privacycommissie, kan ook gebruikt worden als input voor het register.

Let wel: bepaalde verwerkingen moesten niet aangegeven worden zoals verwerkingen inzake personeelsbeheer. Er is dus nood aan aanvulling en voortdurende bijwerking.

zie ook:

https://www.privacycommission.be/sites/privacycommission/files/documents/aanbeveling_06_2017_0.pdf

4. WAAR worden de gegevens gelokaliseerd, doorgegeven?

Lijst voor elk geïdentificeerd doeleinde dat je vooropstelt, de categorieën 'ontvangers' op aan wie de gegevens werden verstrekt of zullen worden verstrekt. Doe dit ook voor de 'ontvangers' in landen die geen lid zijn van de Europese Unie of internationale organisaties en verwijst in voorkomend geval naar de documenten inzake passende waarborgen.

Het begrip 'ontvangers' wordt als volgt gedefinieerd: de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt.

5. HOE LANG worden de gegevens bewaard?

De gegevens mogen niet langer worden bewaard dan noodzakelijk voor de doeleinden waarvoor ze worden gebruikt.

Geef, zo mogelijk, de vooropgestelde termijnen weer waarbinnen de verschillende categorieën van gegevens moeten worden gewist.

De bewaartermijn is niet noodzakelijk een kwantitatieve beoordeling (een termijn in dagen, maanden, jaren). De bewaartermijn kan ook betrekking hebben op parameters zoals de tijd die nodig is om het doeleinde te verwezenlijken, de uitdoving van een verjaringstermijn, een wettelijke archiveringstermijn na beëindiging van de verwerking.

6. HOE worden de gegevens beveiligd?

Artikel 32.1 van de GDPR vereist van de verwerkingsverantwoordelijke en de verwerker dat zij alles in het werk stellen om de gepaste technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.

Maak daarom een opsplitsing tussen de technische, organisatorische en (zo mogelijk) juridische beveiligingsmaatregelen.

Bekijk de referentiemaatregelen inzake beveiliging op:

https://www.privacycommission.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens_0.pdf

VI. Mag het Register bijkomende informatie bevatten?

Het is aan iedere verwerkingsverantwoordelijke en verwerker om, in functie van de maatregelen die nodig zijn om zich in regel te stellen met de GDPR, te bepalen welke bijkomende informatie-elementen zij nuttig vinden om toe te voegen in het register.

Deze elementen moeten ook verstrekt worden aan de privacycommissie wanneer die daarom verzoekt. De privacycommissie kan in het kader van de uitoefening van haar opdrachten toegang vragen tot alle informatie.