Bijlage 4: Analyse gegevensverwerking (interne audit)

Inhoudstafel

1. Kader

Deze analyse van de verwerkingen van persoonsgegevens bij organisatie … (naam) bevat de algemene context, informatie over de verwerkingen, conclusies en concrete maatregelen die genomen worden om de verwerking van de persoonsgegevens uit te voeren conform de GDPR.

1. 1. context organisatie
Omschrijf de organisatie, haar activiteiten en andere informatie, relevant in het kader van de analyse van verwerking van persoonsgegevens, bv. decretale erkenning, link met de overheid, samenwerkingsverbanden.

1.2. context verwerking
Algemene omschrijving van de verwerking van gegevens binnen de organisatie …… (naam).

Voorbeelden:
- *De organisatie registreert persoonsgegevens van haar gewone leden voor het bijhouden van het wettelijk verplichte ledenregister (VZW-wet) en van haar gewone en toegetreden leden zodat ze die op de hoogte kan houden over de interne werking en activiteiten.*
- *De organisatie registreert persoonsgegevens voor de organisatie van activiteiten en registratie van betalingen.*
- *De organisatie registreert persoonsgegevens van leden, gebruikers, medewerkers van partnerorganisaties, enz., voor het mailverkeer via nieuwsbrieven en rechtstreekse mailing.*
- *De organisatie registreert persoonsgegevens van haar werknemers, vrijwilligers en freelancers om haar wettelijke en/of contractuele verplichtingen in het kader van hun samenwerking te kunnen naleven.*

2. Actoren

2.1. betrokken actoren
Oplijsting van alle betrokken actoren die in contact komen met de organisatie (stakeholders, overheid, administratie, directie,…)

2.2. betrokken personen die binnen de organisatie gegevens verwerken
Oplijsting van de personen binnen de organisatie die persoonsgegevens verwerken, de aard van verwerking en (contractuele) afspraken met hen omtrent de gegevensverwerking.

2.3. betrokken externe verwerkers
Oplijsting externe verwerkers die namens en voor rekening van de organisatie persoonsgegevens verwerken (sociale secretariaten, externe diensten, verzekeraars enz.)

3. Beschrijving verwerkingsactiviteiten

Weergave van de verwerkingsactiviteiten binnen de organisatie. Van bij de ontvangst, het verzamelen of de input van de gegevens tot uiteindelijke vernietiging, archivering of het doorsturen van gegevens. Dat kan een oplijsting zijn, een infographic, …

zie bijlage 5

4. Toetsing verwerking persoonsgegevens

4.1. legitimiteit

Omschrijf duidelijk en specifiek de doeleinden op van de verwerkingsactiviteiten. Ga goed na of het verwerken van (bepaalde) persoonsgegevens noodzakelijk is voor de doeleinden. Ga na of deze doelstellingen voldoende legitiem zijn volgens de GDPR. Dat is het geval wanneer je de verwerkingsactiviteit als volgt kunt verantwoorden.

mogelijke wettelijke basis	
wettelijke verplichting	De verwerking is noodzakelijk voor de uitvoering van een wettelijke plicht Dus ook wat subsidiërende of lokale overheid oplegt op basis van decreet. *Bv. lijst van vrijwilligers bijhouden, verwerking van persoonsgegevens voor loonsverwerking (Dimona, loonberekening, enz.), neerlegging/publicatie van gegevens bestuurders (VZW-wet)*
contractuele basis (noodzakelijk voor uitvoering van overeenkomst)	Als je met iemand een overeenkomst hebt gesloten, mag je diens persoonsgegevens verwerken voor zover dat noodzakelijk is om de overeenkomst uit te kunnen voeren. *Bv. arbeidsovereenkomst: bankrekeningnummer , naam, aantal kinderen ten laste, burgerlijke stand, geboortedatum, rijksregisternummer van de werknemer om het loon te kunnen laten berekenen en storten …* *Bv. lidmaatschapsovereenkomst: naam en e-mailadres voor het versturen van een nieuwsbrief waarin de activiteiten worden aangekondigd.*
vitaal belang	uit dringende medische noodzaak *Bv. als bij bewusteloos slachtoffer van (arbeids)ongeval gezocht wordt naar medische gegevens m.o.o. zijn verzorging (bloedgroep bv.)*
gerechtvaardigd belang	Als je de activiteit niet behoorlijk kunt uitoefenen zonder het verwerken van persoonsgegevens, dan heb je een gerechtvaardigd belang, tenzij de belangen, grondrechten of individuele vrijheden van de betrokkene zwaarder doorwegen. *Bv. controle op internet- en mailgebruik van werknemers kan een gerechtvaardigd belang zijn in het licht van fraudevoorkoming in de relatie werknemer-werkgever die hier als een relevante en passende verhouding wordt aangezien.*
algemeen belang of openbaar gezag	Met een publiekrechtelijke taak wordt bedoeld een taak die bij of krachtens de wet is opgedragen. *Bv. de politie die gegevens opvraagt met referentie naar een onderzoek, op voorwaarde dat ze **gemachtigd** is door het Openbaar Ministerie*
ondubbelzinnige toestemming	De verwerking is gebaseerd op vrije, actieve en specifieke toestemming van de betrokkenen. Je mag gegevens op grond van de ondubbelzinnige toestemming van de betrokkene verwerken, mits je expliciet de toestemming hebt gekregen van de betrokkenen voor een bepaalde verwerking van bepaalde gegevens, de toestemming uit vrije wil is geuit, je de betrokkene hebt geïnformeerd over de gang van zaken rond de verwerking en er geen twijfel is over de inhoud en reikwijdte van de toestemming.

4.2 proportionaliteit

Ga voor elk persoonsgegeven na of je ze daadwerkelijk nodig hebt én of elke verwerkingsactiviteit die jullie erop uitvoeren, ook noodzakelijk is voor het bereiken van het (de) vooropgestelde doeleinde(n). Ga na of er alternatieven zijn.

4.2.a. gegevensverwerking
Hoe wordt getracht de gegevens zo juist mogelijk te verkrijgen en juist te houden? (koppelingen met andere gegevensbronnen, periodieke pop-ups voor de gebruiker, etc.)

Hebben we de gegevens echt nodig om onze doelstelling te bereiken? Moeten we de gegevens echt bewaren en verder verwerken om onze doelstelling te bereiken of kan dit op een andere manier? Is elke verwerkingsactiviteit noodzakelijk of kunnen we deze beperken? Kunnen we de gegevens op een bepaald ogenblik bijvoorbeeld pseudonimiseren?

4.2.b Opslagbeperking
Is het nodig om de gegevens te bewaren? Wat is de bewaringstermijn van de gegevens, en waarom juist die bewaringstermijn, kan deze korter? Als we gegevens wissen, zijn ze dan daadwerkelijk ook 'weg' of kunnen we ze nog altijd raadplegen op een of andere manier?

4.3. beveiliging en vertrouwelijkheid
Welke technische en organisatorische maatregelen treffen we om de beveiliging, de vertrouwelijkheid, integriteit en van de gegevens te waarborgen zodat o.a. ongeoorloofde toegang en gebruik, onopzettelijk verlies, vernietiging, beschadiging of kwaliteitsverlies voorkomen worden?

Bv. - toegang tot de gegevens beperken tot de personen die de gegevens moeten verwerken, met paswoorden die maandelijks wijzigen
- een policy voor werknemers met gebruiksregels die gecontroleerd en gesanctioneerd worden
- overeenkomsten met crm-operatoren, cloudsystemen dat hun aanbod GDPR-compliant is.

De beveiliging bevat o.m. (waar passend):

- pseudonimisering en versleuteling van persoonsgegevens
- het vermogen om permanent de vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van de verwerkingssystemen en diensten te garanderen
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en toegang tot persoonsgegevens tijdig te herstellen
- een procedure voor het op gezette tijden testen, beoordelen en evalueren van de doeltreffendheid van de maatregelen

4.4. transparantie
Benoem per gegevenscategorie (bv. leden, werknemers, vrijwilligers, …) de door de GDPR verplicht te bezorgen informatie (cf. 5. toetsing rechten van betrokkenen), de wijze waarop zij geïnformeerd worden en welke informatie ze precies krijgen.

Bv. leden worden geïnformeerd via een privacyverklaring in het ledenblad, op de website,…; werknemers via een verklaring in het arbeidsreglement; vrijwilligers via een verklaring in de vrijwilligersnota, ….
en geef aan welke informatie daarbij gegeven wordt.

5. Toetsing rechten van de betrokkene

Hoe worden de volgende rechten van betrokkenen gefaciliteerd (regelingen, procedures, mechanismen) en worden de betrokkenen daar voldoende duidelijk en transparant over geïnformeerd?

- het recht op informatie
- het recht op toegang, inzage en kopie
- het recht op aanpassing (*rectification*) van onjuiste of onvolledige gegevens
- het recht van bezwaar
- het recht om vergeten te worden (verwijdering van gegevens)
- het recht op beperking van de verwerking tot welbepaalde doeleinden
- het recht van intrekking van toestemming
- het recht op overdraagbaarheid aan een andere verantwoordelijkheid
- het recht van weigering
- het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming, zoals profilering
- het recht van klacht bij de privacycommissie

Opgelet: als je een rechtmatig doel hebt voor de verwerking van gegevens, proportioneel en transparant werkt, moet je niet nog eens de toestemming van de betrokkene vragen. Zij kunnen uiteraard wel hun rechten uitoefenen die ze krijgen krachtens de GDPR.

6. Conclusies en maatregelen

6.1. Stap 1 Oplijsten verwerkingsactiviteiten en toetsingen

Voeg de oplijsting van de diverse verwerkingsactiviteiten samen met de toetsingen op basis van legitimiteit, proportionaliteit, beveiliging, en vertrouwelijkheid en transparantie.

Maak een oplijsting per gegevenscategorie (bv. werknemers, leden enz.)

gegevenscategorie	diverse manieren van gegevens verwerking	wettelijke basis	noodzaak verwerking gegevens	bewaartermijn	betrouwbaarheid en integriteit	toetsing transparantie
leden	**verzamelen voor ledenbeheer**					
	raadplegen					
	verspreiden					
	koppelen					
	registreren voor deelname en betaling activiteiten					
werknemers	**verzamelen voor loonadministratie**					
	…					
vrijwilligers						
…						

Toets ook de mogelijke impact op de personen wier gegevens verwerkt worden aan de de rechten van de betrokkenen (hoofdstuk 5), de gevoeligheden van gegevens en de mogelijke gevolgen van een datalek.

gegevens-categorie	diverse manieren van gegevens-verwerking	toetsing rechten betrokkene	toetsing gevoeligheid gegevens	toetsing gevolg datalak
leden	**verzamelen voor ledenbeheer**			
	raadplegen			
	verspreiden			
	koppelen			
	registreren voor deelname en betaling activiteiten			
werknemers	**…**			
vrijwilligers				
…				

6.2. Stap 2 Conformiteit GDPR en leemtes bepalen

Lijst per verwerkingsactiviteit op basis van de oplijsting in stap 1 de zaken op die niet conform de GPDR zijn. Bekijk of er leemtes zijn rond bescherming, verlies of diefstal van de diverse manieren van gegevensverwerking.

6.3. Stap 3 Maatregelen treffen

Bepaal de maatregelen (plus timing en verantwoordelijken) die je moet treffen om de risico's op te lossen en de gegevensverwerking te conformeren aan de GDPR.

De aard van de maatregelen bepaal je rekening houdend met de technische mogelijkheden, uitvoeringskosten, aard, omvang, context en doel van de verwerking. Je bekijkt de grootte van je maatregelen en inspanningen ook in verhouding met de waarschijnlijkheid en ernst van de uiteenlopende risico's voor rechten en vrijheden.

gegevens-categorie	diverse manieren van gegevens-verwerking	niet conform GDPR en leemte	genomen maatregel	timing	verantwoordelijke
leden	**verzamelen voor ledenbeheer**	geen duidelijk omschreven doeleinde	doeleinde bepalen		
	doorgeven aan derden	ontbreken van goedkeuring	goedkeuring vragen met aanvinkknop		
	raadplegen				
	verspreiden				
	koppelen				
werknemers					
vrijwilligers					
…	**registreren voor deelname en betaling activiteiten**				
	…				

6.4. Stap 4 Opvolging

Volg de timing goed op, evalueer geregeld de stand van zaken en bekijk op basis van het register of er nieuwe leemtes ontstaan. Agendeer jaarlijks de opvolging van GDPR op de raad van bestuur en/of teamvergadering.