scwitch

ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

LOGBOEK

GDPR

switch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

I Wat is de Algemene Verordening Gegevensbescherming (AVG of GDPR)?

II Wat moet mijn organisatie doen om in regel te zijn?

III Stappenplan: ontwikkeling van een intern databeleid

stap 1 bewustmaking
stap 2 inventaris
stap 3 audit en stappenplan
stap 4 register verwerkingsaciviteiten
stap 5 privacyverklaring
stap 6 aanstellen verantwoordelijke gegevensregistratie
stap 7 melding datalekken

IV Documenten

Bijlage 1	Inhoudstafel en checklist Logboek	
Bijlage 2	Inventaris	(online template)
Bijlage 3	inschatting gevolgen gegevensverlies	(excel)
Bijlage 4	gegevensverwerkingsanalyse	(interne audit, handleiding)
Bijlage 5	het register	(online template)
Bijlage 6	het register	(toelichting)
Bijlage 7	checklist privacyverklaring	(checklist)
Bijlage 8	aangifteformulier datalek	(template)
Bijlage 9	Begrippen	(doc)
Bijlage 10	Faq's	

GDPR

I Wat is GDPR?

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

De Algemene Verordening Gegevensbescherming (AVG, of GDPR: General Data Protection Regulation) is een geheel van Europese regels om de burger te beschermen rond gebruik van persoonsgegevens. De wet is een herziening van de 'Data Protection Directive', de Europese wetgeving uit 1995.

De GDPR is in werking sinds 24 mei 2016. Ze is van toepassing vanaf 25 mei 2018. Organisaties hebben dus de tijd tot die datum om zich in regel te stellen. Vanaf 25 mei 2018 moet je bij een controle of betwisting actief kunnen aantonen dat je volgens de nieuwe wetgeving handelt.

Elke organisatie, ook vzw's en feitelijke verenigingen die persoonsgegevens gebruiken, opslaan of verwerken, vallen onder de regelgeving en moeten zich in orde stellen. Zelfs als je organisatie geen enkel winstdoel nastreeft of geen enkele commerciële ingesteldheid heeft.

De regelgeving geldt voor zowel de commerciële als de niet-commerciële sector.

- De regelgeving is niet van toepassing als je gegevens uitsluitend gebruikt voor persoonlijk of huiselijk gebruik.
- De regelgeving is niet van toepassing als je de persoonsgegevens alleen maar afleest van een papieren drager en die drager nadien niet bijhoudt maar weggooit, vernietigt of teruggeeft aan de eigenaar.

De principes rond gegevensverwerking blijven dezelfde, maar de methodes worden aangepast, wegens technologische ontwikkelingen en globalisering.

De Verordening hamert vooral op:

- een grotere verantwoordingsplicht, dus meer transparantie over de verwerking, het beheer en de bewaring van persoonsgegevens
- nadruk op de rechten van de betrokkene
- bewijslast bij de verwerkingsverantwoordelijke en de verwerker.
- een sterker toezicht. De Privacycommissie wordt naast informatieorgaan ook waakhond en kan boetes opleggen.

De Verordening voorziet in een omkering van de bewijslast bij aansprakelijkheidskwesties.

Als een betrokkene schade heeft geleden (bv. doordat een derde onrechtmatig toegang heeft gehad tot de gegevens), is het aan de verwerker en/of de verwerkingsverantwoordelijke om aan te tonen dat zij de GDPR correct hebben nageleefd en dus niet verantwoordelijk zijn voor geleden schade. Als ze dat bewijs niet kunnen leveren, heeft de betrokkene recht op een schadevergoeding.
Tot nu moest de schadelijder het bewijs leveren van de overtreding die de schade had veroorzaakt. Onder de GDPR moet de verantwoordelijke het tegendeel bewijzen.

GDPR

Gevoelige gegevens

In de socioculturele sector worden persoonsgegevens verzameld en verwerkt die door de Verordening als 'gevoelige gegevens' beschouwd worden en om die reden extra bescherming vereisen: medische gegevens, politieke voorkeur, seksuele voorkeur, geloofsovertuiging, etnische afkomst, lidmaatschap van vakbonden, enz.

Gevoelige gegevens mogen alleen verwerkt worden met het oog op een beperkt aantal doeleinden (nooit op basis van een overeenkomst) en op strikte voorwaarden. Met uitzondering van de strafrechtelijke gegevens bepaalt de GDPR dat de gegevensverwerking toegelaten is voor vzw's, stichtingen of andere instanties zonder winstoogmerk op volgende voorwaarden:

- de organisatie is werkzaam op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied
- de verwerking gebeurt in het kader van die gerechtvaardigde activiteiten en met passende waarborgen
- de verwerking heeft alleen betrekking op leden of voormalige leden van de organisatie OF op personen die regelmatig contact met haar onderhouden in verband met haar doeleinden
- de persoonsgegevens worden niet zonder toestemming van betrokkene buiten die instantie doorgegeven

Ook de verwerking die noodzakelijk is voor archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt toegelaten door de GDPR.

Ons inziens zullen die doelstellingen doorgaans volstaan voor de socioculturele sector om de betreffende gegevens legitiem te mogen verwerken.

Daarnaast moeten uiteraard ook alle algemene beginselen voor rechtmatige verwerking nageleefd worden (transparantie en proportionaliteit) en moeten passende waarborgen aanwezig zijn voor de rechten van de betrokkenen en de beveiliging.

Specifiek voor werkgevers is bepaald dat zij gevoelige gegevens mogen verwerken wanneer dit noodzakelijk is met het oog op de uitvoering van verplichtingen en de uitvoering van specifieke rechten van de organisatie, als verantwoordelijke of van de betrokkene op het vlak van arbeidsrecht, socialezekerheids- en socialebeschermingsrecht. Op voorwaarde dat dit bij wet of cao is toegelaten.

Strafrechtelijke gegevens mogen alleen verwerkt worden onder toezicht van de overheid of als het toegelaten is bij wet en die wet ook in passende waarborgen voorziet voor de rechten en vrijheden van de betrokkenen.

Voor socioculturele organisaties die deze gegevens verwerken, zal het dus de vraag zijn of zij daartoe wettelijke machtiging hebben (op basis van een decreet bijvoorbeeld) en of er passende waarborgen zijn.

De Belgische wetgever en de sociale partners zullen de Verordening vermoedelijk nog aanvullen en verduidelijken (de Verordening is een minimum).
Ook zal veel nog moeten blijken uit de toepassing, de rechtspraak en bijsturing.

GDPR

II. Wat moet mijn organisatie doen om in regel te zijn?

De GDPR hecht veel belang aan legaliteit, proportionaliteit en transparantie met betrekking tot de verzameling en verwerking van persoonsgegevens en de rechten van de betrokkenen.

II.1. De legaliteitsvereiste

De GDPR bepaalt dat de verantwoordelijke, vooraleer hij de persoonsgegevens verwerkt, duidelijk het doel moet bepalen en aangeven waar hij de gegevens voor gebruikt.

Het is dus van belang dat je goed inventariseert en omschrijft voor welke doeleinden je bijvoorbeeld leden- en gebruikersgegevens gaat verzamelen en verwerken. Je mag de doeleinden tijdens het verwerkingsproces immers niet zonder meer veranderen of uitbreiden.

Bovendien bepaalt de GDPR welke doeleinden de verwerking van persoonsgegevens kunnen rechtvaardigen. De doeleinden die je als organisatie vooropstelt, moeten daar dus in passen.

De GDPR somt wettelijke doeleinden op die persoonsgegevensverwerking rechtvaardigen:

- contractuele basis (noodzakelijk voor uitvoering van overeenkomst, bv arbeidsovereenkomst)
- wettelijke verplichting (noodzakelijk voor uitvoering wettelijke plicht (bv opgelegd in decreet)
- algemeen belang of openbaar gezag (door de wet opgedragen, bv. aan de politie)
- vitaal belang (bv om dringende medische reden)
- gerechtvaardigd belang (activiteit is anders niet uitvoerbaar), enkel als dit zwaarder doorweegt dan het belang, de rechten en de redelijke privacyverwachtingen van de betrokkenen
- ondubbelzinnige toestemming (vrije, actieve en specifieke toestemming van betrokkenen)

II.2. De proportionaliteitstoets

Zorg ervoor dat elke beslissing en maatregel die je neemt de **proportionaliteitstoets** doorstaat. Stel je altijd de vraag of de verwerking of maatregel noodzakelijk is om de doelstelling die je vooropstelt te bereiken.

'Is het echt noodzakelijk in functie van onze doelstelling om:'

- deze gegevens te verzamelen en verder te verwerken? Zijn er misschien andere manieren?
- deze gegevens zo lang te bewaren?
- al deze personen toegang te geven tot de gegevens?
- deze gegevens aan een specifieke persoon te blijven koppelen, of kunnen we ze pseudonimiseren?

Het gerechtvaardigd belang en de ondubbelzinnige toestemming kan best enkel als toepassing worden gebruikt als de overige wettelijke doelstellingen niet van toepassing zijn.

voorbeeld: werkgevers moeten zich als dat kan baseren op een wettelijke of contractuele verplichting. Pas in laatste instantie en uitzonderlijk (zelfs dat is voor betwisting vatbaar) kunnen ze zich op toestemming (bv gebruik foto's) of gerechtvaardigd belang (bv controle e-mail) baseren.

GDPR

II.3. Transparantie

De betrokkenen (leden, werknemers, doelgroep, mensen die deelnemen aan de activiteiten, je vrijwilligers,...) moet duidelijk geïnformeerd worden in een heldere taal.

De transparantie- of informatieplicht geldt ongeacht de wettelijke doelstelling die je beoogt. Je organisatie moet dus altijd actief informeren over de verwerking van de persoonsgegevens en de rechten van de betrokkenen.

Dat moet proactief gebeuren. De verantwoordelijke mag dus niet wachten met het geven van de informatie totdat een betrokkene ernaar vraagt.

Heel eenvoudig komt het erop neer dat je een **privacyverklaring** moet hebben op de website, in het ledenblad, op het lidmaatschapsformulier, in het arbeidsreglement, in de infonota voor vrijwilligers,...

Deze zaken neem je op in je privacyverklaring

- WELKE gegevens worden verwerkt?
- WAAR krijgt of verzamelt je organisatie de gegevens?
- WAAROM worden de gegevens bewaard?
- WIE verwerkt in je organisatie gegevens?
- WIE krijgt de gegevens?
- WAT wordt precies HOE, WAAR en HOELANG bewaard?
- HOE worden gegevens beveiligd?
- HOE faciliteer je de uitoefening van de rechten van betrokkenen?

Technische & organisatorische maatregelen

De GDPR bepaalt ten slotte ook dat elke organisatie passende technische en organisatorische maatregelen moet treffen die garanties geven voor de beveiliging en de vertrouwelijkheid.

Met deze maatregelen moet je waarborgen kunnen geven dat je verwerkingsactiviteiten conform de GDPR en voldoende beveiligd verlopen.

Welke maatregelen passend zijn, beoordeel je in functie van het doel van de verwerkingsactiviteiten, potentiële kansen op verlies en de impact van de gevolgen hiervan . Dit kan dus verschillend zijn voor elke organisatie.

meer info over de diverse vormen van wettelijke basis:
www.scwitch/toolkit GDPR - PRIVACYVERWERKING
bijlage 4 analyse gegevensverwerking deel 4.1 legitimiteit

GDPR

Hoe omgaan met de rechten van de betrokkene

De GDPR besteedt veel aandacht aan de rechten van de betrokkenen.

Belangrijk is dat je de betrokkenen heel goed informeert over die rechten (bv via privacyverklaring) en hoe je organisatie de uitoefening van die rechten faciliteert.

Als verantwoordelijke voor de verwerking moet je organisatie regelingen treffen en eventueel mechanismen en/of procedures uitwerken die zorgen dat de betrokkenen hun rechten effectief en gemakkelijk kunnen uitoefenen.

De rechten van de betrokkenen, die je als organisatie moet faciliteren, zijn:

- recht op informatie
- recht op inzage en kopie
- recht op aanpassing (rectification)
- recht op bezwaar
- recht op vergetelheid (verwijderen van gegevens)
- recht op intrekken toestemming
- recht op overdraagbaarheid
- recht op weigering geautomatiseerde individuele besluitvorming, profilering
- recht op beperking van verwerking

Aan de hand van dit logboek kan je organisatie haar huidige privacybeleid in kaart brengen, aanpassingen plannen en zich in regel brengen met de nieuwe wetgeving.

De beste manier om te voldoen is :

- opmaak van een inventaris van je gegevensverwerking
- toesten aan de vereisten van de nieuwe wetgeving
- planning van noodzakelijke wijzigingen of aanvullingen
- een opstelling van een heldere privacyverklaring, raadpleegbaar op je website of een andere plaats als die geschikter is. bv op het papieren inschrijvingsformulier, infonota vrijwilligers,arbeidsreglement, policy enz.

Bij werknemers is de meest geschikte plaats het arbeidsreglement dat zij krijgen bij ondertekening van hun contract.

verwerking persoonsgegevens van -16 jarigen

De GDPR biedt speciale bescherming aan de persoonsgegevens van kinderen, in het bijzonder in de context van commerciële internetdiensten zoals sociale netwerken. Profilering is sowieso niet toegestaan.

Als je organisatie gegevens van kinderen onder de 16 jaar verzamelt, in het kader van een rechtstreeks aanbod van onlinediensten aan kinderen en als voor die verwerking toestemming nodig is, moet een ouder of voogd die toestemming geven.
Een kind kan immers zelf pas geldig toestemming geven vanaf de leeftijd van 16 jaar.

Er moet geen toestemming gevraagd worden, noch van het kind, noch van de ouder wanneer de verwerking niet op een toestemming moet gebaseerd worden, maar bijvoorbeeld mag omdat het noodzakelijk is voor de uitvoering van de wettelijke verplichtingen.
Je moet natuurlijk wel duidelijk informeren over de verwerking van de persoonsgegevens.

Daarnaast is er ook een uitzondering op de toestemming van de ouders of voogd van -16 jarigen voor preventieve of adviesdiensten voor kinderen.

Als verwerkingsverantwoordelijke moet je organisatie kunnen aantonen dat je voldoende en redelijke inspanningen levert om de gegeven toestemmingen van ouders of voogd te verifiëren.

Gebruik beeldmateriaal

‘De GDPR is van toepassing zodra er sprake is van een "verwerking” van "persoonsgegevens". De brede definitie van beide begrippen maakt het mogelijk om bijvoorbeeld foto’s of video-beelden van een concreet iemand onder de wet te laten vallen.

Vooraleer je een foto neemt van iemand, moet je zijn/haar toestemming vragen.

Wil je nadien deze foto’s publiceren op het internet of in een krant(je), dan moet je hiervoor nogmaals de toestemming vragen.

Vóór je beelden gebruikt, moet je altijd nagaan of sommige daarvan niet auteursrechtelijk beschermd zijn (het zogenaamde “copyright"). ‘

Er zijn enkele uitzonderingen, bijvoorbeeld:

Wanneer bepaalde personen toevallig op een foto of video staan, genomen op een publieke plaats (bv. een foto van een monument waar enkele personen toevallig mee op afgebeeld staan), gaat men er in principe van uit dat een toestemming voor het verdere gebruik van die foto of video niet vereist is.

Wanneer afbeeldingen van een menigte worden genomen, is er in principe ook geen toelating nodig (noch voor het nemen, noch voor het gebruik nadien), omdat ook hier de weergave van de persoon bijkomstig is.

meer info rond het gebruik van afbeeldingen vind je op de site van de Privacycommissie:

https://www.privacycommission.be/nl/recht-op-afbeelding

GDPR

Het scwitch Stappenplan

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

stap 1	bewustmaking
stap 2	inventaris
stap 3	audit en stappenplan
stap 4	gegevensverwerkingregister
stap 5	privacyverklaring
stap 6	aanstellen verantwoordelijke gegevensregistratie
stap 7	aanpak datalek

Elke organisatie moet haar persoonsgegevens in kaart brengen en zorgen dat dit conform de GDPR verordening verloopt.

In vele gevallen volstaat een screening, gevolgd door de nodige effectieve maatregelen en acties om je in orde te stellen met de GDPR.

Het scwitch stappenplan zet je op weg.

GDPR

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

stap 1 Bewustmaking

Elke organisatie die persoonsgegevens verwerkt, moet zich in regel stellen.

Een eerste belangrijke stap is de bewustmaking binnen de organisatie, zodat iedereen die persoonsgegevens verwerkt op de hoogte is en betrokken wordt bij de opmaak van de dataproctectieregels.

Informeer de sleutelfiguren in je organisatie (medewerkers die met gegevens werken, directie, bestuur, ...) over de noodzakelijke ontwikkeling van een interne dataprotectieregeling.

Houd in een logboek bij welke stappen je onderneemt, hoe je de sleutelfiguren informeert en welke stappen je verder zet.

Tip: Agendeer de aanpak van de bescherming van de persoonsdata op het eerstvolgende overleg met al je medewerkers en op de eerstvolgende raad van bestuur.

Vermeld duidelijk dat je organisatie een persoonsdataprotectieregeling ontwikkelt.

Overloop met je medewerkers en bestuurders wie welke persoonsgegevens verwerkt en gebruikt.

Zo heb je een zicht op de gegevensverwerkingsactiviteiten en kun je afspraken maken over wie meewerkt aan de opmaak van de beschermingsregels.

Houd de agenda en verslagen bij in het logboek.

In bijlage 1 vind je een algemene inhoudstabel en checklist voor je logboek

www.scwitch/toolkit GDPR - PRIVACYVERWERKING
bijlage 1: inhoud en checklist logboek

GDPR

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

Stap 2 Inventaris

Alvorens concrete stappen te zetten, kijk je best naar de huidige stand van zaken binnen je organisatie.

Breng in kaart welke persoonsgegevens verwerkt worden binnen de organisatie en hoever de verwerking gaat (verzamelen, bewaren, verspreiden, kopiëren, bewerken,...) om een overzicht te krijgen van de activiteiten die moeten getoetst worden aan de GDPR.

Kijk ook na waar die gegevens vandaan komen, wie er toegang toe heeft, welke partners of onderaannemers (bv overheid, andere VZW's, sociaal secretariaat, online marketing organisatie, data hosting bedrijf) die gegevens in handen krijgen, ... om op die manier tot een inschatting van veiligheidsrisico's te komen.

Lijst op:

- Welke gegevens worden er bewaard (naam, adres, leeftijd,...) ?
- Waar worden de gegevens bewaard ?
- Hoe lang worden ze bewaard ?
- Wie heeft er toegang toe?
- Worden de gegevens beschermd?
- (Hoe) worden gegevens intern uitgewisseld? (vb aanwezigheidslijst)
- (Hoe) worden gegevens extern uitgewisseld ?
- Waarvoor gebruiken jullie de gegevens? (direct mailing, nieuwsbrief, bevestigingen)

Welke persoonsgegevens verwerk je op dit ogenblik?

Waar komen ze vandaan?

Met wie deel je ze?

Gebruik gerust het scwitch excel-model voor de opmaak van een inventaris

www.scwitch/toolkit GDPR - PRIVACYVERWERKING
bijlage 2: inventaris

GDPR

stap 3 audit en stappenplan

Breid de inventaris uit met een audit zodat je zicht krijgt op de noodzakelijke maatregelen die je moet nemen om in regel te zijn.

Op basis van de inventaris bekijk je per gegevenscategorie of

- je een legitieme doelstelling hebt om deze te verwerken
- de verwerkingsactiviteiten in verhouding zijn tot die doelstelling (dus niet te verregaand zijn)
- je voldoende transparant bent over de verwerkingsactiviteiten
- je de rechten van de betrokkenen voldoende faciliteert.

Zet na deze screening de verwerking van persoonsgegevens stop die niet noodzakelijk zijn voor de verwerkingsdoelstelling.

Breng voor de persoonsgegevens die je blijft verwerken, de risico's in kaart op verlies, diefstal of ongeoorloofde toegang en de mogelijke gevolgen die elk daarvan zou kunnen hebben voor de betrokken personen.

Bekijk welke verbeterstappen je kan / moet zetten en lijst op wie welke maatregelen hoe gaat nemen binnen welke timing.

Op basis van de resultaten zijn waarschijnlijk aanpassingen nodig in lopende contracten, privacypolicies of -verklaringen, arbeidsreglementen, interne organisatiepolicies, verzekeringspolissen, inschrijvingsformulieren, vrijwilligersnota's, enz..

Misschien zijn er ook nieuwe afspraken of structurele technische of organisatorische aanpassingen nodig binnen je team (toegang tot data beperken, veiligheidsprocedures invoeren, policies voor gebruik van eigen pc of laptop, ...).

Verdeel de maatregelen onder in een

- een organisatorisch deel
- een technisch deel
- (eventueel) juridisch deel.

Streef ernaar om de geregistreerde gegevens transparant te beheren, beperk je daarbij tot de gegevens die noodzakelijk zijn voor de verwerkingsdoelstelling en houd ze niet langer bij dan nodig.

Koppel de audit aan een stappenplan over de aanpassingen die je zal doorvoeren.

Je kan de audit door een expert laten uitvoeren maar je kan gerust ook zelf een intern onderzoek doen en stappen uitwerken om je organisatie in regel te brengen.

Een audit helpt je om de verwerkingsactiviteiten van je organisatie te toetsen aan de vereisten van de GDPR en de noodzakelijke maatregelen in kaart te brengen.

Ga aan de slag met de de scwitch 'gegevensverwerkingsanalyse'
www.scwitch/toolkit GDPR - PRIVACYVERWERKING
Bijlage 4: analyse gegevensverwerking

GDPR

Overeenkomsten met partners

De GDPR verplicht de verantwoordelijke om met de organisaties of derden waaraan hij verwerkingsctiviteiten uitbesteedt (de verwerkers, bijvoorbeeld sociale secretariaten, verzekeraars, externe diensten voor preventie en bescherming op het werk,...) een contract te sluiten met daarin een minimum aantal verplichte afspraken en vermeldingen (artikel 28).

Je moet met de betrokkenen wiens persoonsgegevens je verwerkt, geen contract sluiten over de gegevensverwerking.

Wel moet je hun de verplichte informatie verstrekken over hoe je omgaat met hun gegevens (via de privacyverklaring) zodat je voldoet aan de transparantieverplichting.

De GDPR heeft ook een impact op de diensten en tools die je organisatie gebruikt.

Zowel contractpartners als softwaretools en onlineservices waar je mee werkt, moeten in de toekomst GDPR-compliant zijn, in een schriftelijk contract gegarandeerd.

Dat geldt overigens ook voor allerlei cloudoplossingen.

Sluit met alle betrokken partijen een verwerkersovereenkomst, met afspraken over de duur, beschrijving en doeleinden van de gegevensverwerking, de beveiligingsmaatregelen, enz.

Als verantwoordelijke moet je altijd nagaan of de verwerker die je aanstelt, passende waarborgen biedt. Dat geldt zowel binnen als buiten België.

De verordening voorziet ook in regels ingeval er zaken gebeuren met landen buiten de EU. De lijst van landen die een passend beschermingsniveau aanbieden, is te vinden op de website van de Europese Commissie. Vraag is wel of deze lijst nog relevant blijft aangezien deze gekoppeld is aan de vorige privacywet.

Controleer dus al je lopende overeenkomsten, zorg voor of informeer naar de nodige aanpassingen in de al bestaande contracten en zorg ervoor dat de dienstverlener waarmee je samenwerkt, aantoont dat hij conform de GDPR handelt.

lijst derde landen buiten de EU:
https://www.privacycommission.be/nl/doorgifte-buiten-de-eu-met-passende-bescherming

GDPR

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

stap 4 Register verwerkingsactiviteiten

De GDPR verplicht organisaties en hun verwerkers om in een elektronisch register al hun verwerkingsactiviteiten en hun kenmerken bij te houden.

Organisaties met minder dan 250 werknemers in dienst zijn in principe vrijgesteld van deze verplichting, tenzij de verwerking:

- een risico inhoudt voor de rechten en vrijheden van betrokkenen
- gevoelige gegevens betreft
- niet incidentieel is

In praktijk moet dus elke organisatie die persoonsgegevens verwerken van personeel, leden, vrijwilligers, deelnemers of andere personen een register bijhouden, ongeacht het aantal werknemers in dienst of de grootte van de organisatie.

Het register is een handige leidraad voor de verwerkers binnen je organisatie, maar is vooral bedoeld als instrument om bij controle te voldoen aan je verantwoordingsplicht als verwerkingsverantwoordelijke.

Het register komt in de plaats van de huidige aangifteplicht bij de privacycommissie.

In tegenstelling tot de inventaris en audit, is het register een document dat continu wordt bijgehouden en geactualiseerd door de verwerkingsverantwoordelijke en de verwerker.

Je kan je natuurlijk wel op de informatie uit de inventaris en audit baseren voor een verdere uitwerking in een register.

Het dataregister biedt een overzicht van de verwerking van gegevens, gekoppeld aan doeleinden per verwerkingsprocedure.

Het begrip 'gegevensverwerking' is heel breed.

Het gaat van het verzamelen, raadplegen, verspreiden, koppelen, registreren tot het vernietigen van gegevens.

De wetgever vraagt zo specifiek mogelijk te zijn in je doelomschrijving.
Vermijd daarom algemene beschrijvingen zoals: 'administratie van het personeel, de controle op de werkplaats, klantenbeheer, leveranciersbeheer, …

Gebruik gerust de scwitch tool dataregister als basis voor de opmaak van een register.
www.scwitch/toolkit GDPR - PRIVACYVERWERKING bijlage 5 register verwerkingsactiviteiten
Meer info over de inhoud en opmaak van het register vind je in bijlage 6.
www.scwitch/toolkit GDPR - PRIVACYVERWERKING bijlage 6 het register (toelichting)

De Privacycommissie werkte zelf ook een model voor register uit: zie
https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten

GDPR

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

stap 5 opmaak privacyverklaring

Als verwerkingsverantwoordelijke moet je organisatie de betrokkenen proactief informeren over de verwerking van persoonsgegevens en hun rechten.

Dit moet beknopt, transparant, in een duidelijke eenvoudige taal en in een begrijpelijke en gemakkelijk toegankelijke vorm.

Door de opmaak van een heldere en makkelijk raadpleegbare privacyverklaring voldoe je duidelijk aan deze verplichting.

Opgelet: je maakt de privacyverklaring op in functie van de categorie betrokkenen waar je je toe richt (leden, werknemers,...).

De inhoud en locatie waarop je de privacyverklaring meedeelt hangen dus ook af van deze categorie.

Je privacyverklaring zet je raadpleegbaar op de meest aangewezen plaats voor de betrokkenen van wie de persoonsgegevens verwerkt worden.

je website voor leden, algemene voorwaarden van het lidmaatschapsformulier, arbeidsreglementen, vrijwilligersnota,...

Werk o.a. volgende luiken uit in een heldere privacyverklaring

- welke informatie wordt verzameld
- wie verzamelt de informatie
- hoe wordt ze verzameld
- waarom wordt ze verzameld
- hoe wordt ze gebruikt
- met wie wordt de informatie gedeeld
- wat is het effect op het individu dat zijn toestemming geeft voor het gebruik van zijn persoonlijke gegevens (enkel wanneer sprake van geautomatiseerde besluitvorming, art 13, 14 GDPR)

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

stap 6 Aanstellen functionaris voor gegevensbescherming en privacy (Data Protection Officer, DPO)

De Data Protection Officer is een deskundige inzake gegevensbescherming die je organisatie bijstaat in het toezicht op de interne naleving van de GDPR.

De DPO geeft advies over nieuwe software, gebruik van database, etc…

De DPO is ook de contactpersoon met de overheid bij bv datalekken.

DE TAKEN VAN DE DPO

- Toezicht op de naleving van de GDPR en van het interne beleid daaromtrent in je organisatie .
- De organisatie en haar medewerkers informeren en adviseren omtrent hun verplichtingen om te voldoen aan de GDPR en andere gegevensbeschermingsregelgeving
- Monitoring van het al dan niet voldoen aan de regels van de GDPR
- Contactpunt voor en samenwerking met privacycommissie
- Brengt jaarlijks verslag uit van zijn/haar werkzaamheden en bevindingen aan de hoogste leidinggevende in de organisatie
- Kan door de betrokkene gecontacteerd worden over GDPR-aangelegenheden

In de GDPR wordt niet beschreven welke specificaties gelden voor een DPO.
Er wordt geen gewag gemaakt van een specifiek diploma of certificaat.

De DPO moet volgens de wet beschikken over “de nodige professionele kwaliteiten en deskundigheid op het gebied van wetgeving en de praktijk inzake gegevensbescherming”.

De taak van de DPO kan toegewezen worden aan een externe of een interne medewerker zolang de professionele taken van de medewerker compatibel zijn met deze van de DPO en dit niet leidt tot belangenconflicten.

De taak van DPO kan extern uitbesteed worden. Scwitch kan je helpen bij de zoektocht naar een DPO met kennis van de sector.

GDPR

Wanneer ben je verplicht een DPO (intern of extern) aan te duiden?

Je hebt een DPO nodig in volgende gevallen:

- Je organisatie is een overheidsinstantie of een overheidsorgaan
- Je organisatie is hoofdzakelijk belast met verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen (wegens aard, omvang en doeleinden)
- Je verwerkt op grote schaal bijzondere categorieën van gevoelige gegevens zoals ras, politieke voorkeur, religie, medische of strafrechtelijke gegevens

De verwerking ‘op grote schaal’ en ‘bijzondere categorieën’ geldt ons inziens enkel als je organisatie van bepaalde groepen heel regelmatig individuele voorkeuren gaat onderzoeken, profileren.

We nemen aan dat er in de socioculturele sector weinig organisaties onder bovenvermelde voorwaarden vallen en dus geen DPO moeten aanduiden. Tenzij er later nog nationale wetgeving komt die deze verplichting zal opleggen of de commissie of rechtspraak een ander standpunt inneemt.

Conclusie:

We nemen aan dat de meeste van de vzw’s in de socioculturele sector geen externe DPO hoeven aan te stellen en dat een register plus maatregelen en privacyverklaring volstaat.

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

GDPR LOGBOEK

stap 7 melding van datalekken

De GDPR voorziet in een meldplicht voor datalekken die de betrokkene(n) schade kunnen berokkenen (bv financieel verlies, schending geheimhoudingsplicht, identiteitsdiefstal).

Een datalek is trouwens niet enkel een hacking van je database.

Elk incident dat impact kan hebben op de veiligheid van je data (zoals diefstal van een laptop of verlies van een usb-stick) en waarschijnlijk enige vorm van schade kan veroorzaken aan de betrokkenen(n), moet binnen 72 uur gemeld worden aan de privacycommissie.

Bij een hoog risico voor zijn rechten en vrijheden moet dit ook aan de betrokkene zelf gemeld worden zodat deze de nodige voorzorgsmaatregelen kan nemen. (zie art 34 GDPR)

Organisaties die laattijdig lekken melden riskeren een geldboete.

Voorzie in gepaste procedures en afspraken in je organisatie om datalekken zo snel mogelijk op te sporen, te onderzoeken en tijdig te melden aan de privacycommissie.

Vaak is het de verwerker en de verantwoordelijke die de verantwoordelijkheid krijgen rond het melden van datalekken.

Maak gerust gebruik van het scwitch datalek aangifteformulier

www.scwitch/toolkit GDPR - PRIVACYVERWERKING
bijlage 8: datalek aangifteformulier

GDPR