

GDPR

online GDPR sessie

Emmanuel Steyaert (T&C Blue Horizon) GDPR-expert

Luk Tas (switch) projectmanager / GDPR

Stefan Ost (NXT-PRO) expert digitale leeroplossingen



GDPR

General Data Protection Regulation
Algemene Verordening Gegevensbescherming

bescherming en verwerking persoonsgegevens

verwerking: verzamelen, raadplegen, verspreiden, koppelen, registreren, vernietigen van gegevens.

persoonsgegevens: gegevens over een natuurlijke persoon.

Naam, adres, leeftijd, geslacht, lichamelijke kenmerken, psychische kenmerken, financiële situatie, kenmerken gezin, geaardheid, vrijetijdsbesteding, lidmaatschap van vakbond of politieke partijen, gerechtelijke gegevens, opleiding, beroep, beeldopname, geluidsopname,...

betrokkene = de persoon wiens gegevens je verwerkt (lid, deelnemer,...)

moet mijn organisatie zich ook in regel stellen met GDPR ?

JA

- GDPR geldt voor alle organisaties ook vzw's en feitelijke verenigingen die persoonsgegevens verwerken (ledenbestanden, deelnemersbestanden, nieuwsbrieven, mailings, gsm nummers bijhouden,...)
- Accountability principe: elke organisatie is verantwoordelijk en moet verantwoording afleggen
- Voornaamste acties : documenteren / informeren / beveiligen

principe GDPR

je mag geen persoonsgegevens verwerken

tenzij

wettelijke grond = 'uitzonderingen' waardoor je wel gegevens mag verwerken

- **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)

stappenplan

- stap 1 bewustmaking
- stap 2 inventaris
- stap 3 analyse en maatregelen
- stap 4 gegevensverwerkingregister
- stap 5 duidelijk informeren: privacyverklaring
- stap 6 procedures rechten betrokkenen
- stap 7 aanpak datalek

stap 1: bewustmaking

raad van bestuur team

Informeer de medewerkers in je organisatie die met gegevens werken over:

- de noodzakelijke voorwaarden (legaliteit / proportionaliteit / transparantie)
- stappen om je organisatie in regel te brengen
- beveiliging van persoonsgegevens

belangrijk om **iedereen** die persoonsgegevens verwerkt te informeren en te betrekken

—> agenderen en verslagen bijhouden

stap 2: opmaak inventaris

- Welke gegevens bewaart je organisatie (naam, adres, leeftijd,...) ?
- Waar bewaart je organisatie de gegevens ?
- Hoe lang worden ze bewaard ?
- Wie heeft er toegang toe?
- Worden de gegevens beschermd?
- Waarvoor gebruiken jullie de gegevens?(direct mailing, nieuwsbrief, bevestigingen deelname,...)

stap 3 analyse

Op basis van de inventaris bekijk je of

- je de leden, deelnemers, partners **duidelijk informeert** (privacyverklaring)
- je een wettelijke **grond** hebt om gegevens te verwerken
- je **niet te veel gegevens** opvraagt en deze niet te lang bewaart
- leden, deelnemers, de mogelijkheid hebben om hun gegevens in te zien, te corrigeren, te laten verwijderen,...

stap 3 analyse

- Lijst op hoe je papieren documenten, gegevens in bestanden of (online) beeldmateriaal **technisch** (vb paswoorden, foto's enkel in beveiligde omgeving) **en organisatorisch** (vb medische fiches in gesloten kistje) **beveiligt**.
- Ga voor de gegevens die je verwerkt na of er risico is op verlies, diefstal of ongeoorloofde toegang.
- Bekijk welke verbeterstappen je kan / moet zetten. Lijst op wie welke maatregelen hoe gaat nemen binnen welke timing

interessante site:

www.safeonweb.be

stap 4 opmaak register

verplicht document!

- overzicht van de verwerking van gegevens, gekoppeld aan de doeleinden (vb ledenregistratie, registratie van activiteiten en deelnemers,...)
- verplicht instrument om bij controle te voldoen aan je verantwoordingsplicht als verwerkingsverantwoordelijke
- wordt continu geactualiseerd en aangevuld. (In tegenstelling tot de inventaris en analyse)
- de informatie uit de inventaris en analyse zijn goede basis voor een verdere uitwerking in een register
- online template scwitch als basis

Stap 5 duidelijk informeren: privacyverklaring

verplicht document!

De betrokkenen (leden, werknemers, doelgroep, deelnemers, je vrijwilligers,...) moeten **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. Je doet dit best via een **privacyverklaring**.

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

Opgelet: Het is een verklaring, mededeling van de organisatie naar het lid, deelnemer,.../
De betrokkenen moet de verklaring **niet goedkeuren**.

stap 5 duidelijk informeren: privacyverklaring

Je organisatie moet de betrokkenen **proactief informeren** over de verwerking van persoonsgegevens en hun rechten.

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

op de meest aangewezen plaats voor de betrokkenen van wie de persoonsgegevens verwerkt worden.

stap 5 duidelijk informeren: privacyverklaring

Werk o.a. volgende zaken uit in een heldere 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 zorg je voor je de uitoefening van de rechten van betrokkenen?

Stap 6 procedures rechten betrokkenen

De voornaamste rechten van de betrokkenen voor lokale organisaties:

- recht op **inzage en kopie**
- recht op **aanpassing** (rectification)
- recht op **vergetelheid** (verwijderen van gegevens)
- recht op **intrekken** toestemming (bij toestemming als rechtsgrond)

stap 7 datalek

Meldplicht voor datalekken die de betrokkene(n) schade kunnen berokkenen (bv financieel verlies, schending geheimhoudingsplicht, identiteitsdiefstal).

Elk incident dat impact kan hebben op de veiligheid van je gegevens (zoals diefstal van een laptop of verlies van een usb-stick) en 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.

Bij probleem: contacteer scwitch

www.scwitch.be
zakelijk organisatiemanagement

gratis GDPR logboek, templates: do it yourself —>toolbox
actieve groepssessies met expert
1op1 begeleiding door expert



nieuwsbrief

combinatie GDPR en e-commerce (mail & sms)

hoofdregel: **actieve toestemming** vragen

maar:

- uitzondering voor 'klanten' 'promo gelijkaardige producten'
 - leden // overeenkomst, gerechtvaardigd belang

foto's & filmpjes

‘gerichte beelden’

- close up
- toestemming nodig om foto te nemen
- toestemming nodig om foto te publiceren, gebruiken

‘niet gerichte beelden’

- sfeerbeelden
- geen toestemming nodig om foto te nemen
- geen toestemming nodig om foto te publiceren, gebruiken
- best opnemen in privacyverklaring dat je organisatie sfeerbeelden neemt en gebruikt van activiteiten