WEBSITES & GDPR …

25 mei 2018 nadert …

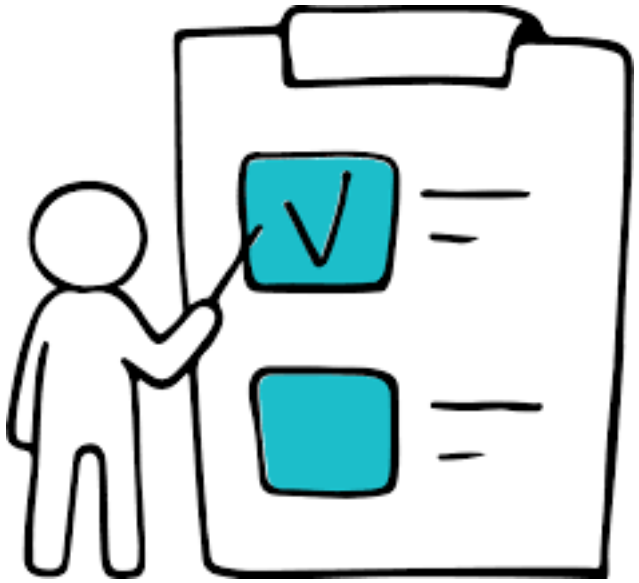
GDPR IN HET KORT

GDPR IN HET KORT

- Legitimiteit & transparantie
  De persoon van wie de gegevens verwerkt worden, is hiervan op de hoogte, heeft hiervoor toestemming gegeven en kent zijn rechten.
- Doelbeperking
  Persoonsgegevens mogen uitsluitend voor gewettigde doeleinden verzameld en gebruikt worden.
- Gegevensbeperking
  Alleen de gegevens die nodig zijn om het beoogde doel te bereiken, mogen worden verzameld.
- Accuraatheid
  Persoonsgegevens moeten correct zijn en blijven.
- Bewaarbeperking
  De persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.
- Inzage-, correctie- en verwijderrecht & dataportabiliteit
  Persoonsgegevens moeten in te zien, aanpasbaar, verwijderbaar en te verplaatsen zijn.
- Beveiliging
  Persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.
- Verantwoording
  De verantwoordelijke moet kunnen aantonen aan deze regels te voldoen. In sommige gevallen moet een *data protection officer* (DPO) worden aangesteld.

DE PRAKTIJK | MAAK EEN PLAN

- Met je ‘GDPR compliance plan’ toon je aan de autoriteit en je klanten hoe je voldoet aan de GDPR
- Zet het op je website
- Kort en bondig



DE PRAKTIJK | STAP 1

- Inventariseer van wie je gegevens opslaat en met welk doel je dit doet

DE PRAKTIJK | STAP 2

- Welke systemen gebruik je? Bepaal voor elk systeem het doel van de data en waar deze is opgeslagen.

Systemen zijn:

- Je website
- Je CRM Systeem
- Je Extern nieuwsbrief systeem (Cloud)
- …

DE PRAKTIJK | STAP 3A

- Welke informatie sla je op?
  Dit is het lastigste en het meest tijdrovend deel.
- Tip: maak een tabel met de kopjes Wat, Hoe, Waar en Waarom

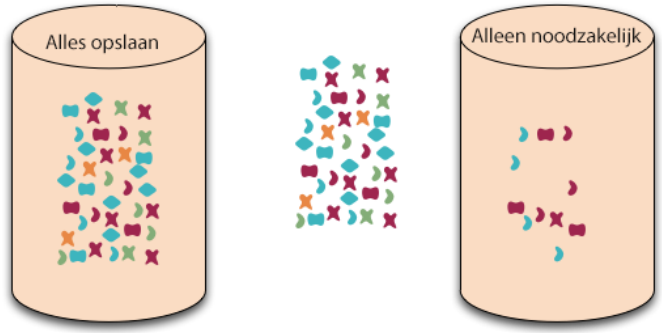
Wat (sla ik op)?	Hoe (is het verkregen)?	Waar (sla ik het op)?	Waarom (sla ik het op)?
Volledige naam	Ingevoerd door klant bij aanmelding via website	Database website CRM Systeem Ticketsysteem	
Email adres	Ingevoerd door klant bij aanmelding via website	Database website Nieuwsbriefsysteem Ticketsysteem	Marketing en communicatie waar de klant dit gebruik heeft toegestaan
Land	Bepaald door IP-adresresolutie op het moment dat de klant zich aanmeldt voor een abonnement	Database website	Gebruikt voor het bepalen van de btw en het bijhouden van financiële gegevens om naleving aan te tonen

DE PRAKTIJK | STAP 3B

Pas op de plaats!

- Door het maken van de tabel weet je nu precies welke je gegevens je opslaat en met welke reden. Als je merkt dat je gegevens verzamelt die je niet nodig hebt, stop dan met het verzamelen van deze gegevens!
- **Voorbeeld**: Je vraagt de geboortedatum in een aanmelding voor een subscriptie om te controleren of iemand ouder is dan 18 jaar.
- Volgens de GDPR-regels zijn er geen argumenten om de geboortedatum verder bij te houden zodra de subscriptie is goedgekeurd. Als alternatief kun je dan een eenvoudig selectievakje maken met een “ik ben ouder dan 18” optie.

Aan het einde van deze stap moet je weten welke gegevens je opslaat en waarom.



DE PRAKTIJK | STAP 4

Hoe verkrijg je toestemming?

- Je weet nu wat je opslaat en waarom. Nu moet worden vastgelegd hoe je toestemming hebt gekregen om dit te doen. Bijvoorbeeld via een invulformulier:

q ALGEMENE TOESTEMMING: ik stem ermee in dat u informatie over mij bewaart met het doel mij diensten te verlenen waarvoor ik betaal en die virtuele koppelprogrammeurs moeten verzamelen en houden om te voldoen aan alle wettelijke of reglementaire vereisten. Ik stem ermee in dat u per e-mail en telefoon met mij communiceert over eventuele problemen die kunnen voortvloeien uit de voortdurende veiligheid en het beheer van mijn account. (Verplicht - klanten moeten deze optie accepteren)

q ADVIESCOMMUNICATIE: ik stem ermee in dat u mij e-mails stuurt nadat ik een abonnement of een downloadbare cursus heb gekocht, met advies over het gebruik van de service. Dit kan een melding zijn van nieuwe cursussen die ik kan openen als gevolg van mijn aankoop zonder extra kosten.

q MARKETINGCOMMUNICATIE: Ik stem ermee in dat u mij e-mails stuurt met advies over nieuws en algemene marketing van [naam bedrijf]. Uw gegevens worden niet doorgegeven aan derden.

DE PRAKTIJK | STAP 5

Verzoek tot inzage

- Schrijf een kort document waarin je aangeeft hoe je omgaat met verzoeken tot het recht op inzage (wanneer een gebruiker vraagt om een kopie van alles wat over hem haar is opgeslagen).

- Je moet binnen één maand reageren op een klant die vraagt om een kopie van alles wat je over hem of haar bewaart. Over het algemeen kun je dit niet in rekening brengen.

DE PRAKTIJK | STAP 6

Recht om te worden vergeten

- Klanten kunnen je vragen om de gegevens die je over hen hebt te verwijderen.
- Er kunnen bepaalde gegevens zijn die je moet bewaren (bijvoorbeeld financiële gegevens om aan te tonen dat je het juiste bedrag aan belasting hebt betaald)
- Sommige gegevens kunnen we niet verwijderen omdat deze de integriteit van een of meer systemen zouden kunnen schaden, anonimiseer dan i.p.v. verwijderen - de naam van de klant veranderen in "Verwijderd Verwijderd" en zijn adres in "Verwijderde weg 1" bijvoorbeeld.

DE PRAKTIJK | KLAAR?

Met dit document heb je elk gegevenselement dat je bezit inzichtelijk gemaakt en aangegeven:

- dat je een geldige reden hebt om de gegevens te verzamelen
- dat je een geldige reden hebt voor doorlopende opslag van de gegevens
- dat je weet waar de gegevens zijn opgeslagen
- dat je open en eerlijk aan de klanten hebt uitgelegd welke gegevens je hebt en waarom / hoe je deze gebruikt
- dat je toestemming hebt verkregen van de klant om de gegevens die je hebt op te slaan en te gebruiken zoals je dat doet

DE PRAKTIJK

- Er zijn nog andere dingen om over na te denken (zoals wat er gebeurt als een gebruiker je vertelt dat er iets is veranderd - je moet dan alle relevante gegevensitems binnen 1 maand bijwerken)
- Natuurlijk de beveiliging rond je systemen (sterke wachtwoorden, enz.). Zie https://gdpr.insitevision.nl/stappenplan
- Privacyverklaring https://veiliginternetten.nl/privacyverklaring/
  Moet in Jip en Janneke taal /voor iedereen te begrijpen zijn
- Toestemming moet expliciet gegeven worden
- Toestemming moet ook eenvoudig weer ingetrokken kunnen worden

Bron: https://brian.teeman.net/joomla/gdpr-data-protection-and-you