GDPR & NIS2

websites en digitale communicatie

paddle.be

Overzicht

Achtergrond en doel

Wat is GDPR ?

- **GDPR** (General Data Protection Regulation) of **AVG** (Algemene verordening Gegevensbescherming) = **Europese privacywet** van kracht sinds 25 mei 2018
- **Doel**: bescherming van de privacy en persoongegevens van natuurlijke personen
- Geldt voor **alle organisaties die persoongegevens verwerken**

Verwerken wij persoongegevens ?

- Voorbeelden **persoonsgegevens** = e-mail, IP-adres, geslacht, medische info, foto's van medewerkers
- Wat is **verwerken** ?
  - Verzamelen
  - Vastleggen/opslaan en ordenen
  - Bijwerken of wijzigen
  - Opvragen en raadplegen
  - Doorsturen naar derden of beschikbaar stellen

Mag je zomaar persoongegevens verwerken ?

- Er moet een **geldige reden** zijn voor de verwerking, 6 mogelijkheden/grondslagen:
  - **Toestemming**: de betrokkene heeft toestemming gegeven voor de verwerking
    vb: invullen formulier, inschrijven nieuwsbrief
  - **Overeenkomst:** de verwerking is noodzakelijk voor de uitvoering van een overeenkomst
    vb: verwerken gegevens van medewerkers
  - **Wettelijke verplichting:** de verwerking is nodig om aan een wettelijke plicht te voldoen
    vb: werkgever is verplicht om de gegevens van de werknemer mee te delen aan de bevoegde instellingen van de sociale zekerheid
  - **Vitale belangen:** bescherming van het leven van een persoon
    vb: verwerken van persoongegevens bij een ramp door de medische diensten
  - **Taak van algemeen belang of openbaar gezag**
    vb overheid mag zonder expliciete toestemming financiele gegevens verwerken voor bv belastingsaangifte
  - **Gerechtvaardigd belang:** legitiem belang van een organisatie, mits dit niet zwaarder weegt dan de belangen van de betrokkene
    vb toegangsbeveiliging van gebouwen

Rechten van de betrokkenen

- **Recht op inzage**
  - Recht om de persoonsgegevens die over je verwerkt worden te bekijken/raadplegen
- **Recht op correctie**
  - Recht om wijzigingen en aanvullingen aan te brengen in de persoonsgegevens die een organisatie over je verwerkt
- **Recht op verwijdering(vergeetrecht)**
  - Recht om je persoonsgegevens te laten verwijderen
- **Recht op dataportabiliteit**
  - Recht hebt om je persoonsgegevens over te dragen aan een andere organisatie.

GDPR in de praktijk

Persoonsgegevens verzamelen via websites

- Via **webformulieren**
  -> Zorg voor een duidelijk doel en eventueel extra toestemming
- **Externe toepassingen** zoals afspraak maken
  -> beveiligde verbinding bij de externe platformen
- **Analaytics/statistieken** website
  -> toestemming via cookiebanner voor het tracken voor analytische doeleinden
- Publicatie van **foto's/video's/contactgegevens** medewerkers
  -> toestemming bij het plaatsen van foto's waar mensen herkenbaar zijn
- **Nieuwsbrieven/mailinglijsten**
  -> dubbele opt-in, duidelijke afmeldlink

Verantwoordelijkheden webadmins

- Verzamel enkel **noodzakelijke persoonsgegevens**
- **Verwijder** regelmatig **oude gegevens**
  - Manueel oude inzendingen bij formulieren verwijderen
  - Automatische verwijderdatum voor inzendingen instellen bij formulieren
- **Privacyverklaring up-to-date & volledig**
  - Duidelijke vermelding contactgegevens
  - Welke gegevens verzamelen en waarom? + Bewaartermijnen
  - Worden gegevens doorgestuurd naar derden?
  - Vemelding rechten van betrokkenen
- **Cookieverklaring & cookiebanner**
- **Verwerkingsovereenkomst** met leveranciers

NIS2 & cyberveiligheid

Wat is NIS2

- **NIS2** (Network and information Security) **= 2de Europese richtlijn voor cyberbeveiliging**
- **Doel:** verhogen van cybersecurity bij kiritieke infrastructuren en organisaties
- Geldt voor **alle organisaties die essentiële diensten leveren**

Kernpunten NIS2

- Beleid rond **risicobeheer en beveiligingsmaatregelen** opstellen
  - Toegangsbeheer, back-ups, encryptie/versleuteling, software-updates,..
  - Zowel technisch als organisatorische maatregelen
- **Bestuurlijke verantwoordelijkheid**
  - De directie/bestuur is rechtstreeks verantwoordelijk voor naleving
- **Incidentenrapportage** binnen 24 uur
  - Melding maken van incidenten aan bevoegde instanties zoals CCB
- **Leveranciers en cloud-diensten betrekken**
  - Samenwerking op verschillende niveau's
  - Ook toeleverenciers en IT-dientverleners moeten voldoen aan NIS2-eisen
- **Toezicht en sacties**
  - Nationale autoriteiten krijgen meer toezichts- en sanctiebevoegdheden

Samenwerking met Paddle

Websites in het Paddle CMS

Veiligheid is geen aparte module, maar **een integraal onderdeel** van ons platform

- **Beveiligd CMS**
- **Veilige hosting**
- **Patch-beleid**
- **Bestandsbeveiliging**

Extra mogelijkheden

- **Veiliger inloggen**
  - Streng wachtwoordbeleid
  - MFA
  - Inloggen met active directory
- **Extra bescherming voor je webformulieren**
  - ReCaptcha tegen spam
  - Virruscanner op uploads (CLAM-AV)
  - Bestandsnamen automatisch opschonen
- **Technische beveiligingsheaders**
  - Strikte ‘transport security’-headers
  - Content Security Policy (CSP)
- **E-mail authenticatie**
  - DMARC & DKIM

Checklist GDPR & NIS2

Checklist GDPR

1. Transparantie & informatieplicht

- ❑ Privacyverklaring aanwezig, duidelijk en gemakkelijk vindbaar
- ❑ Privacyverklaring legt uit: welke gegevens worden verzameld, waarom, hoe lang bewaard, met wie gedeeld
- ❑ Contactgegevens van de DPO (Data Protection Officer) vermeld

2. Toestemming en cookies

- ❑ Cookiebanner aanwezig die expliciet toestemming vraagt (geen vooraf aangevinkte vakjes)
- ❑ Mogelijkheid om cookies te weigeren zonder verlies van basisfunctionaliteit
- ❑ Cookiebeleid beschrijft welke cookies gebruikt worden en hun doel

3. Formulieren en gegevensverzameling

- ❑ Alleen de strikt noodzakelijke gegevens worden gevraagd (bv. geen geboortedatum als dat niet nodig is)
- ❑ Toestemming expliciet vragen bij gevoelige gegevens (bv. gezondheid, rijksregisternummer)

4. Beveiliging van persoonsgegevens

- ❑ Verzamelde gegevens worden veilig bewaard, zodat onbevoegder er niet bijkunnen
- ❑ Wachtwoorden van gebruikers worden veilig opgeslagen: zelfs beheerders kunnen ze niet lezen

5. Rechten van betrokkenen

- ❑ Bezoekers kunnen eenvoudig hun rechten uitoefenen: inzage, correctie, verwijdering
- ❑ Duidelijk contactpunt (formulier of e-mailadres) voor GDPR-verzoeken
- ❑ Proces om binnen 30 dagen te reageren op verzoeken

paddle.be

Checklist GDPR

6. Datalekken en incidenten

- ❑ Er bestaat een plan voor wat te doen bij een datalek (bv. als gegevens van bezoekers op straat belanden)
- ❑ Ernstige datalekken kunnen binnen 72 uur gemeld worden aan de toezichthouder
- ❑ Er wordt bijgehouden welke incidenten er zijn geweest

7. Externe partijen en verwerkers

- ❑ Duidelijke verwerkersovereenkomsten met externe partners en IT-leveranciers
- ❑ Externe tools (bv. Matomo analytics, sociale media plugins) worden getoetst op GDPR-conformiteit
- ❑ Data blijft waar mogelijk binnen de EU/EER

8. Bewaartermijnen en dataminimalisatie

- ❑ Persoonsgegevens worden niet langer bewaard dan nodig.
- ❑ Automatische verwijdering ingesteld (bv bij webformulieren)
- ❑ Regelmatige review van gegevens die via de website verzameld worden.

Checklist NIS2

1. Veilig beheer van de website

- ❑ De website draait op actuele software en krijgt regelmatig updates.
- ❑ Er wordt gebruikgemaakt van een beveiligde verbinding (https).
- ❑ Beheerders hebben sterke wachtwoorden en extra beveiliging (MFA/active directory).

2. Bescherming tegen aanvallen

- ❑ De website is beschermd tegen hackpogingen en spam.
- ❑ Er is een plan om de website online te houden bij grote aanvallen (zoals DDoS).

3. Incidenten snel aanpakken

- ❑ Er is een duidelijk proces: wie doet wat bij een cyberincident.
- ❑ Incidenten worden binnen 24 uur gemeld aan de bevoegde instanties.
- ❑ Medewerkers weten hoe ze een mogelijk probleem moeten melden.

4. Back-ups en herstel

- ❑ Er worden regelmatig back-ups gemaakt van de website en gegevens.
- ❑ Er is een noodplan voor als de website tijdelijk uitvalt.

5. Samenwerking met leveranciers

- ❑ Er zijn duidelijke contracten en verwerkingsovereenkomsten met externe partijen.
- ❑ Leveranciers voldoen aan de NIS2-veiligheidsregels.

6. Bestuurlijke verantwoordelijkheid

- ❑ Het bestuur/directie is op de hoogte van hun verantwoordelijkheid bij NIS2.
- ❑ Er is iemand aangeduid als contactpersoon voor cyberveiligheid.
- ❑ Jaarlijks wordt de beveiliging van de website geëvalueerd en besproken.

7. Bewustwording en opleiding

- ❑ Medewerkers die toegang hebben tot de website krijgen intern opleiding rond cyberveiligheid.
- ❑ Er worden regelmatig oefeningen of simulaties gedaan (bv. phishingtests).
- ❑ Cyberveiligheid is een vast agendapunt bij beleidsvergaderingen.

paddle.be