

Privacybeleid en wet & regelgeving

- Uitleg
- Opdracht

Uitleg

Inleiding privacywetgeving Privacywetgeving is ontworpen om de rechten van individuen te beschermen en organisaties verantwoordelijk te houden voor de verwerking van persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG of GDPR) is sinds 2018 van kracht in de EU en geldt voor alle organisaties die in Europa actief zijn of Europese burgers bedienen.

- **Persoonsgegevens:** Alles wat een persoon direct of indirect identificeert, zoals naam, e-mailadres, locatiegegevens.
- **Verwerkingsverantwoordelijke (controller):** Organisatie die doelen en middelen van verwerking bepaalt.
- **Verwerker (processor):** Partij die persoonsgegevens verwerkt namens de controller.

Belangrijkste AVG-principes

- **Rechtmatigheid, behoorlijkheid en transparantie:** Verwerk data op een wettelijke manier en wees duidelijk naar betrokkenen.
- **Doelbinding (purpose limitation):** Verwerk alleen voor expliciete en legitieme doelen.
- **Dataminimalisatie:** Verzamel alleen wat echt nodig is.
- **Juistheid (accuracy):** Houd data actueel en correct.
- **Opslagbeperking:** Bewaar data niet langer dan nodig.
- **Integriteit en vertrouwelijkheid:** Bescherm data tegen ongeoorloofde toegang.
- **Verantwoording (accountability):** Documenteer maatregelen en toon naleving aan.

Rechten van betrokkenen

Gebruikers hebben verschillende rechten onder de AVG:

- **Recht op informatie:** Duidelijke privacyverklaring en inzage.
- **Recht van inzage:** Recht om te zien welke data is opgeslagen.
- **Recht op correctie:** Onjuiste gegevens laten aanpassen.
- **Recht op wissing ('recht om vergeten te worden'):** Data laten verwijderen.
- **Recht op dataportabiliteit:** Ontvangen van eigen data in machineleesbaar formaat.
- **Recht van bezwaar:** Verzet tegen bepaalde verwerkingen, zoals direct marketing.

Privacybeleid opstellen

Een privacybeleid (privacyverklaring) bevat:

- **Doeleinden:** Waarom je data verwerkt.
- **Basis voor verwerking:** Toestemming of gerechtvaardigd belang.

- **Categorieën persoonsgegevens:** Welke data je verzamelt.
- **Bewaartermijnen:** Hoelang je data bewaart.
- **Rechten van gebruikers:** Hoe zij hun rechten kunnen uitoefenen.
- **Datalekprocedure:** Hoe je omgaat met en meldt datalekken.

Data Protection Impact Assessment (DPIA)

Een DPIA is een risicobeoordeling voor verwerkingen die waarschijnlijk een hoog privacyrisico hebben, zoals grootschalige monitoring of verwerking van gevoelige data.

Stappen in een DPIA:

1. **Beschrijving van de verwerking:** Proces en doelen.
2. **Beoordeling noodzaak en proportionaliteit:** Waarom is de verwerking nodig?
3. **Risicoanalyse:** Identificeer privacyrisico's voor betrokkenen.
4. **Maatregelen en mitigatie:** Beschrijf technische en organisatorische maatregelen.
5. **Consultatie:** Raadpleeg belanghebbenden of autoriteit.
6. **Documentatie en goedkeuring:** Leg vast en laat het interne reviewproces doorlopen.

Praktijkvoorbeeld

Een gezondheidsapp die hartslaggegevens verzamelt:

1. **Persoonsgegevens:** Naam, leeftijd, hartslagmetingen.
2. **Doel:** Monitoren van fitnessdoelen.
3. **Rechte grondslag:** Toestemming van de gebruiker.
4. **DPIA:** Risico's bij misbruik van gezondheidsdata -> maatregelen zoals sterke encryptie en pseudonimisering.

Opdracht

1. **Concept privacyverklaring:** Schrijf een privacyverklaring (minimaal 400 woorden) voor een fictieve app die locatiegegevens gebruikt om lokale aanbiedingen te tonen. Beschrijf doelen, rechtsgrondslag, bewaartermijnen en rechten van gebruikers.
2. **DPIA-rapport:** Maak een DPIA (minimaal 500 woorden) voor deze app:
 - Beschrijving van de verwerking en doeleinden.
 - Identificeer ten minste vijf privacyrisico's voor betrokkenen.
 - Formuleer per risico passende technische of organisatorische maatregelen.
 - Beschrijf het proces van toestemming en hoe gebruikersrechten worden gegarandeerd.
3. **Reflectie (200 woorden):**
 - Bespreek uitdagingen bij het formuleren van transparante tekst voor gebruikers.
 - Reflecteer op de balans tussen functionaliteit en privacybescherming.