De Algemene Verordening Gegevensbescherming (AVG)

Eén privacywetgeving voor de hele EU

Voor wie geldt de wet?

- Alle bedrijven, verenigingen en andere organisaties binnen de EU
- Alle bedrijven, verenigingen en andere organisaties buiten de EU die gegevens verwerken van EU burgers

Wat is verwerken?

- ‘elke bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;....’ (AVG art. 4, lid2)

Wat zijn persoonsgegevens

- Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. De informatie dient direct of indirect (door middel van herleiding) te kunnen leiden tot identificatie van een natuurlijk persoon.
- Zonder speciale bevoegdheden, is het verwerken van “bijzondere persoonsgegevens” als ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, lidmaatschap van een vakbond, genetische en biometrische gegevens, gezondheid, seksueel gedrag of seksuele gerichtheid, verboden

Waarvoor geldt de wet?

- Voor alle persoonsgegevens zoals: NAW-gegevens, bankrekeningnr., BSN-nummer en e-mailadres. Maar ook: IP-adres, haarkleur, medische gegevens, geloofsovertuiging

Wanneer mogen persoonsgegevens verwerkt worden?

- Toestemming van betrokken persoon
- Uitvoering van een overeenkomst
- Wettelijke verplichting
- Uitvoering taak algemeen belang of openbaar gezag
- Bescherming vitale belangen
- Behartiging gerechtvaardigde belangen

Kernbegrippen

- Privacy by Design; organisaties moeten bij het ontwerpen van producten en diensten ervoor zorgen dat de persoonsgegevens goed worden beschermd. Waaronder:

  1. Dataminimalisatie; niet meer gegevens verzamelen, bewaren of opslaan dan nodig.

  2. Autorisatie; alleen gegevens inzien die noodzakelijk zijn voor het uitvoeren van de functie
- Privacy by Default; alle technische- en organisatorische maatregelen die ervoor zorgen dat alléén die persoonsgegevens worden verwerkt die voor een specifiek doel noodzakelijk zijn

Rechten betrokkenen

- Het recht om persoonsgegevens over te dragen (dataportabiliteit)
- Het recht om ‘vergeten’ te worden
- Het recht om de persoonsgegevens die worden verwerkt in te zien
- Het recht om de persoonsgegevens die worden verwerkt te wijzigen
- Het recht om minder gegevens te laten verwerken
- Het recht op een menselijke interventie bij besluiten
- Het recht om bezwaar te maken tegen de gegevensverwerking
- Het recht te weten wat met persoonsgegevens wordt gedaan

Toestemming verlenen

- Kunnen aantonen dat toestemming geldig is verkregen
- Vaststellen en registreren wijze(n) van toestemming
- Bieden eenvoudige mogelijkheden om toestemming in te trekken

In kaart brengen privacyrisico’s

- Voor gegevensverwerkingen met een (hoog) privacyrisico geldt dat hiervoor een risico analyse moet worden uitgevoerd; een “data protection impact assessment” (DPIA)

Meldplicht datalekken

- Er is sprake van een datalek wanneer er ongeautoriseerd toegang is verkregen of kan worden verkregen tot persoonsgegevens
- Alle datalekken moeten worden gedocumenteerd
- Ernstige datalekken moeten binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens (AP)
- Ernstige datalekken moeten, afhankelijk van situatie, worden gemeld aan betrokkenen

Delen van Data

- Delen van persoonsgegevens mag alleen binnen de EU
- Delen van gegevens buiten de EU mag alleen onder strikte voorwaarden

Mogelijk gevolgen niet naleven

- Aansprakelijkheid stelling voor (vervolg)schade
- Forse boete opgelegd door de Autoriteit Persoonsgegevens (AP)
- Reputatieschade

woonCompagnie