De GDPR / AVG

WAT IS HET EN WAT MOET IK ER MEE?

PrivacyTrends.nl
Privacy Trends. Tips. Tools & Trivia

De GDPR / AVG

- Vooraf
- Historie
- Definities en Begrippen
- De GDPR:
  - Demonstrate Compliancy
  - Transparantie
  - Information Security
  - Besturing
- Tot slot..

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia

Vooraf:

- Ik doe zelf niet aan security, want ik heb niets te verbergen (eens/oneens)
- Wie communiceert uitsluitend versleuteld (PGP mail, Encrypted telefoon, Signal,..)?
- Wie zorgt bewust dat datahandelaren buiten de deur blijven (Focum, Experian, Google, Facebook, et cetera)?
- Wie gebruikt "zakelijk" algemene cloudvoorzieningen als I Cloud, Google drive of Onedrive
- Wie kan bewijzen dat de organisatie voldoet aan de AVG?

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia

“Nieuwe” privacybedreigingen:

PrivacyTrends.nl
Privacy Trends. Tips. Tools & Trivia

Historie:

“Mensenrechten zijn er om mensen te beschermen tegen de macht van de staat.

Het gaat bijvoorbeeld om vrijheid van meningsuiting of dat de overheid niet zomaar geweld tegen burgers kan gebruiken, maar ook recht op onderwijs is van belang bij mensenrechten.

Het is de afspraak deze rechten voor iedereen te garanderen, ongeacht ras, kleur, geslacht, taal, godsdienst, afkomst, welstand of enige andere status.”

(Bron: oneMen.org, verdere uitleg: mensenrechten.nl)

PrivacyTrends.nl
Privacy Trends. Tips. Tools & Trivia

Historie:

Zo ontstond de basis voor de Europese Privacywetgeving:

Universele Verklaring voor de Rechten van de Mens (1948, VN)

Artikel 8 Europese verklaring van de rechten van de Mens (1950, Raad van Europa)

Artikel 8 - Recht op eerbiediging van privéleven, familie- en gezinsleven

1.Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2.Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

PrivacyTrends.nl
Privacy Trends. Tips. Tools & Trivia

Historie:

Één manier van werken binnen de Europese Gemeenschap:

- van privacy-richtlijnen (directives) naar verordeningen (regulations);
- handhaving door (o.a.) de Autoriteiten Peroonsgegevens (AP's)

Er zijn meerdere wetten die de privacy raken, zoals:

Wet Justitiële en Strafvorderlijke Gegevens (Wjsg); Artikel 7:457 BW (medisch beroepsgeheim); Hfdst 11,13 en art 18.13 van de Telecomwet; Gemeentewet 151c (cameratoezicht); Algemene Wet inzake Rijksbelastingen (AWR); Art. 7 Wet Geneeskundige Behandelings Overeenkomst (WGBO); Art. 272&273 Wetboek van Strafrecht; Richtlijn 2002/58/EG (ePrivacy Directive)

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia

Definities en Begrippen:

- Privacy is het grondrecht op bescherming van persoonsgegevens, inclusief vertrouwelijke communicatie*

- Een persoonsgegeven (PI) is ELK gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon.

(*Definitie overeenkomstig de missie van de Autoriteit Persoonsgegevens, zie ook www.Privacytrends.nl)

PrivacyTrends.nl
Privacy Trends. Tips. Tools & Trivia

Definities en Begrippen:

- Een Verwerking is zo ongeveer alles wat je met data kunt doen: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens
- Uitgangspunt bij de wetgeving: PI mag je NIET verwerken…
- ….tenzij het wel mag (verwerkingsgrondslagen)

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia

Definities en Begrippen:

- Verwerkingsgrondslagen:
  - Toestemming (ondubbelzinnig, geinformeerd, vrijwillig),
  - Vitaal belang (levensreddend)
  - Wettelijke verplichting
  - Noodzakelijk voor een overeenkomst
  - Algemeen belang
  - Gerechtvaardigd belang

- Verwerken van bijzondere persoonsgegevens (ras, godsdienst/overtuiging, lidmaatschap vakbond, gezondheid, politieke voorkeur, seksuele leven, strafrechtelijk verleden)? Alleen als het in de wet staat!

PrivacyTrends.nl
Privacy Trends. Tips. Tools & Trivia

Definities en Begrippen:

- Drie rollen:
  - Betrokkene,
  - Verwerkingsverantwoordelijke,
  - Verwerker

- Subsidiariteit, Proportionaliteit en Doelbinding blijven gelden

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia

GDPR / AVG:

- Geldt voor iedere organisatie, ook non-profit, die een vestiging heeft binnen de Europese Gemeenschap, of goederen/diensten aanbiedt aan ingezetenen van de Europese Gemeenschap

- Boete's:
  - niet nakomen van je verplichtingen (10 miljoen euro) / 2% WWO of
  - bij het overtreden van de uitgangspunten (20 miljoen euro) / 4% WWO

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia

GDPR: Demonstrate compliancy

- ACTIEF Bewijzen dat je voldoet aan de wetgeving

- Aantonen:
  - Overzicht verwerkte PI, verwerkingen, logging (toegang)
  - Toestemming betrokkene (of andere verwerkingsgrondslag)
  - Doelbinding
  - Gegevensbescherming, bewaartermijn
  - Dataminimalisatie
  - Privacy by default, Privacy by design

- Ketenverantwoordelijkheid (bewerkingsovereenkomsten): audits!

PrivacyTrends.nl
Privacy Trends. Tips. Tools & Trivia

GDPR: Transparantie

- Informatieplicht
  - ACTIEF aan betrokkenen melden dat u gegevens verwerkt, welke, met welk doel, hoe lang u ze bewaart, de rechten van betrokkene, wie toegang had
  - Inzagerecht (gratis!)
  - Rectificatie en recht om vergeten te worden
  - Profiling alleen als het geen rechtsgevolgen heeft, en de betrokkene niet treft
- Dataportabiliteit
- Meldplicht datalekken

PrivacyTrends.nl
Privacy Trends. Tips. Tools & Trivia

GDPR: Information security

- Organisatorisch en technisch

- Naar de stand der kennis en techniek
  - PET's: versleuteling, anonimiseren, pseudonimiseren
  - CIA (Confidentiality, Integrity, Availability)
  - Fysiek!
  - Awareness
  - Auditen!

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia

GDPR: Besturing

- Privacybeleid (in- en extern)
- Privacymanagementproces
- Audits (DPIA's)
- FG/DPO (naast overheid ook verplicht voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken!)

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia

GDPR: tot slot

- Het goede nieuws: 2 jaar overgangstermijn
- Het slechte nieuws: die ging in op 25 mei 2016

- Export van gegevens?

- Tip: heeft u nog geen actie ondernomen? Doe het NU!

PrivacyTrends.nl
Privacy Trends, Tips, Tools & Trivia