HOGESCHOOL ROTTERDAM

Privacy en Security

Presentatie

mr. R. Grandia

11 mei 2012

overtref jeze

Agenda

Introductie

Wat is privacy?

De Wet Bescherming persoonsgegevens

Beveiliging persoonsgegevens

overtref jezelf

HOGESCHOOL ROTTERDAM

Introductie

Rechten Erasmus Universiteit (1998)

Advocaat

Specialisatie ICT-recht (ICT-contracten)

Extern docent HRO

Cases in afgelopen jaar

overtref jezelf

HOGESCHOOL ROTTERDAM

Wat is “privacy”?

Het recht om met rust gelaten te worden (Warren & Brandeis, “*The Right to Privacy*”, Harvard Law Review, 15 december 1890)

Grondrechten (hoofdstuk 1 van de Grondwet)

- **Recht op ruimtelijke privacy** (bijv. onschendbaarheid woning, art. 12 Grondwet)
- **Recht op relationele privacy** (brief- en telefoongeheim, art. 13 GW)
- **Recht op lichamelijke integriteit** (art. 11 GW)
- **Recht op informationele privacy** (algemene privacyrecht art. 10 GW)

Privacy

- Het recht op bescherming van persoonsgegevens is vastgelegd in (inter)nationale wetgeving.

- Voorbeelden:
  - Artikel 8 EVRM en 17 IVBPR
  - Artikel 27 lid 1 onder k en l WOR
  - Artikelen 10 en 11 Grondwet
  - Artikel 138a, 139b, 237d etc. Wetboek van Strafrecht
  - Artikel 7:611 en 7:660 Burgerlijk Wetboek
  - Artikel 5.3 onder c Arbeidsomstandigheden-regeling
  - Wet op de Medische Keuringen
  - etc.

Privacy is actueel onderwerp

- Dataverzamelingen (toegang, bewaren, koppelen)
- Burgerservicenummer (sofi-nummer nieuwe stijl)
- Cameratoezicht (sprekende camera's)
- Ov-chipkaart
- SUWI-keten (UWV, CWI, reintegratiebureau's, sociale diensten)
- EKD, EPD
- Zoekmachines (Google, Yahoo etc.)
- Biometrische controle (bijv. Bij voetbalstadions)
- RFID, GPS

Kunnen we nog 1 dag anoniem door het leven?

- Bellen/sms'en met mobiele telefoon
- Reizen met ov (camera's op stations, bruggen, vliegen)
- Autorijden, tanken
- Betalen (winkel met pin of geld uit automaat)
- Internetten/mailen
- Hyves, linkedin, plaxo, facebook

…en *willen* we dat ook? (de "Privacy Paradox" ?!)

Wet bescherming persoonsgegevens (Wbp)

- Europese Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens (Richtlijn nr. 95/46 EG)
- Wet Bescherming persoonsgevens (Wbp) ingevoerd in 2001
- technologie-neutrale wetgeving
- Evaluatie

Principes die ten grondslag liggen aan de Wet bescherming persoonsgegevens (Wbp)

- **Gerechtvaardigde grondslag** (goede reden)
- **Doelbinding** (niet voor ander doel)
- **Proportionaliteit en subsidiariteit** (evenredigheid resp. minst vergaande middel)
- **Transparantie** (beoordeling betrokkene)
- **Geheimhouding** (geen verdere verspreiding dan nodig)
- **Fair play** (verwerrking op behoorlijke en zorgvuldige wijze)
- **Rechten van betrokkene** (gelegenheid uitoefenen rechten)

Sleutelbegrippen Wet bescherming persoonsgegevens (Wbp)

- **persoonsgegeven**: elk gegeven betreffende een geidentificeerde of identificeerbare natuurlijke persoon (sub a)
- **betrokkene**: degene op wie een persoonsgegeven betrekking heeft (sub f)
- **toestemming**: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt (sub i)
- **verwerking**: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens...t/m…uitwissen of vernietigen van gegevens.(sub b)
- **Verantwoordelijke** (zie sub d)
- **Bewerker (**zie sub e)

overtref jezelf

HOGESCHOOL ROTTERDAM

Kernbepalingen Wet bescherming persoonsgegevens (Wbp)

- Gegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt (art. 6 Wbp)
- Gegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinde verzameld (art. 7 Wbp)
- Verwerkingsgrondslag (art. 8 wbp)
- Nevengebruik: in beginsel niet toegestaan, tenzij…
- Bewaren gegevens (art. 10 Wbp)
- “niet bovenmatig” (minimum=maximum, art. 11 Wbp)
- Bijzondere gegevens (zoals ras, etniciteit, godsdienst, gezondheid, strafrechtelijke gegevens, art. 16 Wbp)

Rechten van de betrokkene:

- Inzagerecht (art. 35 Wbp)
- Correctierecht (recht op verbetering, aanvulling en verwijdering, afscherming, art. 36 Wbp)
- Recht van verzet (art. 40, 41 Wbp)

Verplichtingen verwerker persoonsgegevens:

- Gegevens beveiligen tegen verlies, diefstal, onbevoegd gebruik of andere vormen van onrechtmatige verwerking (art. 13 Wbp)
- Informatie verstrekken aan betrokkene over identiteit en doeleinden verwerking (art. 33 en 34 Wbp)
- Voldoen aan meldingsplicht (art 27 Wbp, zie ook Vrijstellingsbesluit)

Beveiliging Persoonsgegevens

- Wet Bescherming Persoonsgegevens (WBP):

- **Artikel 2 WBP:**
  1.Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- Onder omstandigheden niet van toepassing op verwerking voor journalistieke, artistieke, literaire, persoonlijke doeleinden en staatsbelangen (politie/defensie)

overtref jezelf

HOGESCHOOL ROTTERDAM

Beveiliging Persoonsgegevens

- Wat is verwerking?

- **Artikel 1 WBP:**
  (…)
  b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder <u>in ieder geval</u> het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
  (…)

overtref jezelf

HOGESCHOOL ROTTERDAM

Beveiliging Persoonsgegevens

- De WBP verplicht tot behoorlijke en zorgvuldige verwerking van persoonsgegevens (art. 6 WBP).

- Voorts verplicht de WBP de verantwoordelijke (*de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt, art. 1 onder d*) maatregelen te nemen tot beveiliging van persoonsgegevens

Beveiliging Persoonsgegevens

Er zijn 3 aspecten bij beveiliging persoonsgegevens:

1. **Exclusiviteit**
   Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens.
2. **Integriteit**
   De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid en niets mag ten onrechte worden achtergehouden of zijn verdwenen.
3. **Continuïteit**
   De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmeringen beschikbaar zijn overeenkomstig de daarover gemaakte afspraken en de wettelijke voorschriften.

(*Van Blarkom&Borking)*

Beveiliging Persoonsgegevens

- **Art. 13 WBP**
  De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Technisch/organisatorisch

- **Technische maatregelen:** logische en fysieke maatregelen in en rondom de informatiesystemen (bijv. toegangscontroles, vastlegging van gebruik en back-up). Onder technische maatregelen worden tevens verstaan de voorzieningen die bekend staan onder de verzamelnaam Privacy-Enhancing Technologies (PET).
- **Organisatorische maatregelen:** maatregelen voor de inrichting van de organisatie en voor het verwerken van persoonsgegevens (zoals toekenning en deling van verantwoordelijkheden en bevoegdheden, instructies, trainingen en calamiteitenplannen).

(*Van Blarkom&Borking)*

Passende maatregelen

Of een maatregel passend is, hangt af van:

- Risicoklasse van de gegevens;
- Stand van de techniek;
- Kosten tenuitvoerlegging;
- Omstandigheden van het geval

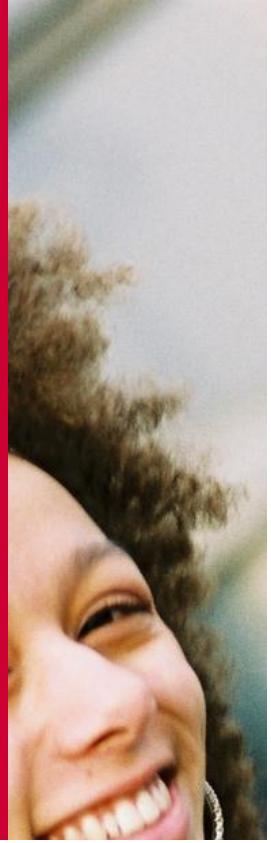
Dus: zwaardere eisen naarmate de gegevens een gevoeliger karakter hebben of worden verwerkt in een risicovolle context; en indien met naar verhouding geringe extra kosten meer beveiliging kan

worden bewerkstelligd zijn deze maatregelen eerder passend (marginale kosten beveiliging < marginale opbrengst)

Het risico

- Risico = P (kans op schade) x B (omvang schade)

- Risico is afhankelijk van:
  - Betekenis van de persoonsgegevens in het maatschappelijk verkeer (*bijv. gevoelige en/of zeer persoonlijke gegevens zoals godsdienst, gezondheid, politieke voorkeur etc.*);
  - Bewustzijn binnen een organisatie t.a.v. bescherming persoonsgegevens en privacy *(meer bekendheid met belang ervan zorgt voor effectievere bescherming);*
  - ICT-infrastructuur waarin de persoonsgegevens verwerkt worden *(zowel hardware als software)*.



Het risico

- Vier risico-categorieën:
  - risicoklasse 0 (publiek niveau);
  - risicoklasse I (basisniveau);
  - risicoklasse II (verhoogd risico);
  - risicoklasse III (hoog risico).

Aard van de persoonsgegevens:		Persoonsgegevens	Bijzondere persoonsgegevens	Financieel en / of economische persoonsgegevens
Hoeveelheid persoonsgegevens (aard en omvang)	*Aard van de verwerking*		Conform artikel 16 WBP	
Weinig persoonsgegevens	Lage complexiteit van verwerking	**Risicoklasse 0**	**Risicoklasse II**	**Risicoklasse II**
Veel persoonsgegevens	Hoge complexiteit van verwerking	**Risicoklasse I**	**Risicoklasse III**	

Beveiliging in de praktijk

- Risicoklasse 0:
  Geen bijzondere maatregelen nodig, want het betreft publiek toegankelijke gegevens.

- Hogere risicoklassen vereisen strengere maatregelen: cumulatie van eisen.

Beveiliging in de praktijk

- Bij risicoklassen I t/m III: letten op
  1. Beveiligingsbeleid en –plan;
  2. Administratieve organisatie;
  3. Beveiligingsbewustzijn en overige aan personeel te stellen eisen;
  4. Inrichting van de werkplek;
  5. Beheer en classificatie ICT-infrastructuur;
  6. Toegangsbeheer en –controle;
  7. Netwerken en externe verbindingen;
  8. Gebruik van software van derden;
  9. Bulkverwerking van persoonsgegevens;
  10. Bewaring/vernietiging persoonsgegevens;
  11. Calamiteitenplan;
  12. Uitbesteding verwerking persoonsgegevens.

overtref jezelf

HOGESCHOOL ROTTERDAM

Toezicht en sancties

- Toezicht op naleving door CBP
  (College Bescherming Persoonsgegevens)

- **Art. 51 WBP**
  1. Er is een College (…) dat tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. (…)

- **Art. 60 WBP**
  1. Het College kan ambtshalve of op verzoek van een belanghebbende, een onderzoek instellen naar de wijze waarop ten aanzien van gegevens-verwerking toepassing wordt gegeven aan het bepaalde bij of krachtens de wet.

Toezicht en sancties

- Sancties bij niet-naleving, op te leggen door CBP
  - Onderzoek instellen (art. 60 Wbp)
  - Toepassen bestuursdwang (art. 65 Wbp) (bijvoorbeeld beslag leggen op computers)
  - Bestuurlijke boete (art. 66 Wbp)
  - Strafrechtelijke sancties (art. 75 Wbp)

- Rechtsbescherming:
  - Betrokkene kan mogelijk optreden tegen verantwoordelijke bijvoorbeeld bij bestuursrechter of bij civiele rechter (schadevergoeding)