Informatieveiligheid bekeken vanuit juridisch perspectief

Inforum | Brussel | 5 juni 2014

Johan Vandendriessche

Advocaat (crosslaw)

| www.crosslaw.be |

| j.vandendriessche@crosslaw.be |

Informatieveiligheid: algemeen

- Informatieveiligheid
  - Beschikbaar en integriteit van informatie
  - Exclusiviteit, confidentialiteit en bescherming van informatie
- Wet- en regeling i.v.m. informatieveiligheid
  - Geen geconsolideerde wetgeving
  - Algemene zorgvuldigheidsnorm (art. 1382-83 B.W.)
    - (Onrechtstreekse) plicht tot naleving van de wet
    - (Onrechtstreekse) wettelijke plicht tot informatiebeveiliging?

Informatieveiligheid: algemeen

- Uitgebreide contractuele regeling
  - Beschikbaarheid en integriteit
    - SLAs
    - IT policies
  - Exclusiviteit, confidentialiteit en bescherming
    - NDAs
    - ICT & IP-overeenkomsten
    - IT policies

Verwerking van persoonsgegevens

- Beperkingen m.b.t. de verwerking van persoonsgegevens
  - Persoonsgegeven: "*elke informatie m.b.t. een geïndentificeerde of identificeerbare natuurlijke persoon […]*"
    - Ruime interpretatie
    - Niet noodzakelijk privacygevoelig
  - Verwerking: elke manipulatie
- Doeleinde: opleggen strikte verantwoordelijkheid
  - Verantwoordelijke voor de verwerking
  - Verwerker ("dienstverlener")

Verwerking van persoonsgegevens

- Beveiligingsplicht
  - Algemene verplichting
  - Bijzondere verplichtingen
  - Verplichtingen i.v.m. de aanstelling van verwerkers
- Lijst van referentiemaatregelen
  - Beschrijving van 10 veiligheidsmaatregelen
  - Geïnspireerd door ISO 27000 norm
  - Informatief doeleinde
    - Geen minimumlijst

Verwerking van persoonsgegevens

- Algemene verplichting om veiligheidsmaatregelen te implementeren
  - Technische maatregelen
    - Gebruikersbeheer en logging
    - Veiligheidstools (antivirus, firewall, …)
    - Brandmaatregelen
  - Organisatorische maatregelen
    - Dataclassificatie
    - Policies t.a.v. werknemers
  - Maatregelen zijn inwisselbaar

Verwerking van persoonsgegevens

- Bieden van bescherming tegen elke vorm van niet-toegelaten verwerking
- Passend veiligheidsniveau
  - Beschikbare technologie en de kosten
  - Aard van de persoonsgegevens en de potentiële risico's
- Passend ≠ absoluut
  - Een loutere niet-toegelaten verwerking is niet noodzakelijk een tekortkoming

Verwerking van persoonsgegevens

- Verplichting inzake datakwaliteit
- ‘Need to know’ toegangsbeperkingen
  - M.b.t. personen
  - M.b.t. de persoonsgegevens
- Informatieplicht
  - Werknemers die persoonsgegevens verwerking
  - Strikter indien de persoonsgegevens tot de bijzondere categorieën behoren (beperkte training)
- Beperking van de functionaliteiten van de software gebruikt voor verwerkingen

Verwerking van persoonsgegevens

- Verwerkingen worden dikwijls uitbesteed
- Veiligheidsmaatregelen m.b.t. verwerkers
  - Keuze van verwerker (betrouwbaarheid)
  - Opleggen van veiligheidsmaatregelen
  - Vastleggen van de aansprakelijkheid
    - Strikte aansprakelijkheid
    - Verantwoordelijke voor de verwerking blijft initieel aanspreekpunt
  - Beperking van de opdracht van de verwerker
  - Verwerkingsovereenkomst

Verwerking van persoonsgegevens

- Verwerking van persoonsgegevens en beveiliging
  - Controle van werknemers
    - Cameratoezicht (CAO nr. 68)
    - Elektronische communicatie (CAO nr. 81)
  - Bewakingscamera's
  - Klokkenluidersregelingen
  - Zwarte lijsten
  - Toegangscontrole / identiteitscontrole
  - Biometrische gegevens
  - Achtergrondcontrole
  - Archivering

Verwerking van persoonsgegevens

- Meldingsplicht bij veiligheidsincidenten
  - Nog niet algemeen van toepassing
  - Communicatiesector
- Data Protection Officer
  - Nog niet (algemeen) van toepassing
- Impact op bewijs bij schending
  - Onwettig of onwettig verkregen bewijs
  - Evolutie naar soepelere toepassing onder de zgn. ‘Antigoon’-leer

Sancties?

- Verenigd Koninkrijk
  - Boete van ong. 2,3 M£ door FSA wegens verlies van back-up tapes
    - Geen bewijs van misbruik van informatie, maar duidelijke afwezigheid van effectieve maatregelen om de risico's te beheersen
  - Regelmatige controles en boetes door ICO
- Frankrijk
  - Regelmatige controles en boetes door CNIL
- Duitsland
  - Boete van 1,1 MEUR wegens onrechtmatige controle van communicatie

Toekomst?

- ‘Privacyverordening’
  - Eengemaakt EU-instrument
- Bijkomende verplichtingen
  - DPO voor grote ondernemingen / privacygevoelige ondernemingen
  - Privacy by design
  - Privacy by default
  - Dataoverdraagbaarheid
  - Meldingsplicht voor incidenten
  - Impactanalyse inzake privacy
  - Boetes

Cybercrime

- Misdrijven die een bedreiging vormen voor de confidentialiteit, de integriteit en de beschikbaarheid van IT-systemen
  - (Interne of externe) Hacking
  - Computersabotage
  - Computerfraude
    - Computerfraude (monetair effect)
    - Valsheid in informatica (juridisch effect)
- Onderzoeksmaatregelen
  - Netwerkzoeking
  - Databeslag
  - Medewerkingsplicht van IT-experten

Bedankt voor uw aandacht!
Vragen?