ALLES OVERZIEN EN DAN EEN PUNT MAKEN

Dataprivacy

- Wet bescherming persoonsgegevens (Wbp)
  - (wet) meldplicht datalekken
- Safe Harbor Ø
- Binding Corporate Rules

Wbp

- Neerslag EU-regelgeving (rl. 95/46/EG), in hele EU
- De titel van de wet zegt het al..
- “elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon”
- elke handeling of elk geheel van handelingen m.b.t. een persoonsgegeven is in beginsel een inbreuk op de privacy

Wbp

- Persoonsgegevens mogen slechts worden verwerkt op een wijze die met het doel verenigbaar is (het voeren van personeelsbeleid)

Wbp

- Persoonsgegevens mogen niet langer worden bewaard dan met het oog op het doel van de verwerking noodzakelijk is

Wbp

- Inzage- en correctierecht voor degenen wiens persoonsgegevens worden verwerkt

- Inbreuk kan toelaatbaar zijn, criteria:

- noodzakelijkheidsbeginsel

- proportionaliteitsbeginsel

- subsidiariteitsbeginsel

noodzakelijkheidsbeginsel

- dient de inbreuk makende handeling een legitiem doel en vormt zij een geschikt middel om dat doel te bereiken

proportionaliteitsbeginsel

- staat de inbreuk in het concrete geval in redelijke verhouding tot het belang bij het bereiken van het beoogde doel?

subsidiariteitsbeginsel

- Is er in het concrete geval geen minder ingrijpend middel voorhanden om hetzelfde doel te bereiken?

Een praktijkvoorbeeld

- Invoering (nieuw) personeelinformatiesysteem
- Daarin alle personeelsgegevens als: NAW, functioneren, opleiding, ontwikkeling vastgelegd

Praktijkvoorbeeld: stappen

- Betreft vastlegging persoonsgegevens, dus toetsen aan de privacywetgeving
- Kan a.d.h.v. vragenschema Autoriteit Persoonsgegevens (oud: Cbp)
- WOR: dubbel instemmingsplichtig (vorm)
- Noodzaak, belang, rechtvaardiging, subsidiair (inhoud)

Praktijkvoorbeeld

- Aandachtspunten OR ook:
- Of en hoe is gewaarborgd dat aan alle eisen is voldaan?
- Ontvangst risico-analyse
- Is nieuwe systeem niet minder veilig dan het oude? Of ingrijpender dan?

Internationaal

- Wbp, artt. 76 en 77: persoonsgegevens mogen slechts naar een land buiten de EU/ EER worden doorgegeven als dat land een passend beschermingsniveau waarborgt

USA

- Amerikaanse moeder
- Server in de USA (cloudcomputing)
- Veel serviceproviders zijn Amerikaans

Internationaal

1. Buiten de EU/ EER is doorgifte dus in strijd met de wet, tenzij dat land passend beschermingsniveau waarborgt

2. Daarop bestond een uitzondering: USA

- Omdat de USA niet zo’n passend beschermingsniveau waarborgt, hadden de EU en de USA een overeenkomst (Safe Harbor Framework)

- Doel was doorgifte van persoonsgegevens vergemakkelijken zonder afbreuk te doen aan bescherming van persoonsgegevens

- Uitgangspunt daarbij was een vorm van zelfcertificering waarbij ondernemingen verklaren een aantal regels op het gebied van de persoonsbescherming na te zullen leven

- AP (Cbp) vond dat altijd al onvoldoende waarborg: de verklaring garandeert immers niet. Aanvullend bewijs vragen was nodig

Maximilian Schrems

- Hof van Justitie EU 6 oktober 2015, C-362/14

- Oostenrijkse student tegen de Data Protection Commissioner inzake facebook in Ierland en doorgifte van persoonsgegevens naar de USA

Hof van Justitie

- *Beschikking 2000/520/EG van de Europese Commissie van 26 juli 2000 (overeenkomstig Richtlijn 95/46/EG betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de VS zijn gepubliceerd) ongeldig*

Hof van Justitie (III)

- AG en Hof zelf oordelen dat Safe Harbor Framework geen passend niveau van bescherming biedt.

- Juridische grondslag voor gegevensuitwisseling met USA dus i.b. komen te vervallen

Oplossing?

- Binnen internationale concerns:
- Binding Corporate Rules (BCR)
- In BCR legt een organisatie de waarborgen vast voor de bescherming van persoonsgegevens bij doorgifte naar landen zonder passend beschermingsniveau. BCR moeten in overeenstemming zijn met de Europese privacyrichtlijn. De Europese privacytoezichthouders moeten de BCR goedkeuren.

BCR (II)

- Ziet alleen op doorgifte persoonsgegevens binnen internationale organisaties, tussen de verschillende vestigingen
- Feitelijk een (bindende) interne gedragscode
- Goedkeuring privacytoezichthouder nodig

Wet meldplicht datalekken

- Opgenomen in de Wbp per 1 januari 2016

- “Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens”

- Verwijst naar 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”

- Meldplicht in art. 34a Wbp
- Beleidsregels voor de toepassing van art. 34a op www.autoriteitpersoonsgegevens.nl

- Verlies usb-stick?

- Hack/verlies pleitnotitie?

Nieuwe regelgeving in het verschiet

- Vanuit de EU volgt vervanging Wbp door “Algemene Dataverordening”
- Harmonisatie wetgeving binnen EU en inhaalslag ontwikkeling ICT

Fitnessarmbandje van de baas mag niet, je slaappatroon is privé

Privacy

Een bedrijf mag het gedrag van werknemers niet volgen via een fitnessarmband. Ook niet als zij ermee instemmen.

Door onze medewerker **Joost Pijpker**

AMSTERDAM. Werkgevers mogen niet via fitnessarmbandjes volgen hoeveel hun personeel beweegt of slaapt, zelfs als werknemers vrijwillig aan zo'n experiment meewerken. Tot die conclusie komt de Autoriteit Persoonsgegevens (AP) na het onderzoeken van twee bedrijven. Beide werkgevers zijn daarom gestopt met het verzamelen van de gezondheidsgegevens, aldus de waakhond.

De bedrijven hadden werknemers een fitnessarmband cadeau gedaan en kregen zo inzicht in hun beweeg- en slaappatroon. Dat is in strijd met de Wet bescherming persoonsgegevens (Wbp). Het gaat om gevoelige gegevens en daarvoor gelden „strenge wettelijke eisen", meldt de AP.

Dat het personeel de keuze kreeg om de gegevens te delen, verandert volgens het voormalige College bescherming persoonsgegevens weinig, legt een woordvoerder uit: „Je moet je helemaal vrij kunnen voelen om ja of nee te zeggen. En in een arbeidsrelatie is een werknemer financieel afhankelijk van zijn werkgever. Dan ben je dus niet helemaal vrij."

Een van de bedrijven waar de Autoriteit Persoonsgegevens zich op richtte, is vastgoedadviseur Colliers, waarover NRC vorige maand schreef. Het concern vond 35 van de 45 werknemers op een afdeling bereid om een jaar lang hartslag, stressniveau en het aantal gezette stappen per dag te meten. Deelname is vrijwillig en het personeel kan elk moment stoppen.

Directeur Harold Coenders van Colliers kan de uitspraak van de toezichthouders „wel begrijpen", maar, zegt hij: „Waarom mag een bedrijf als Ajax wel de fitheid van zijn spelers bijhouden en mogen wij dat niet?"

Zijn bedrijf heeft een oplossing die volgens hem wél mag: de gegevens van de polsbandjes versturen naar een coach buiten de organisatie. „Die kan ons dan een beeld geven van het welzijn op een afdeling en ook aan de bel trekken wanneer het met een van de werknemers minder gaat."

- www.sprengers.nl
- l.vanwesterlaak@sprengers.nl
- 030- 252 09 00


SPRENGERS
ADVOCATEN
www.sprengersadvocaten.nl