EOR platform 18 maart

Bescherming persoonsgegevens

Mr. Lars van Westerlaak, Sprengers Advocaten

Presentatie

Wet bescherming Persoonsgegevens is gebaseerd op Europese Richtlijn, vandaar dat alle landen in de EU/EER een vergelijkbaar beschermingsniveau hebben en dus ook gegevens mogen uitwisselen (Wet bescherming persoonsgegevens art. 76 en 77).

Buiten de deze landen mogen data niet worden verstrekt. Er zijn wel mogelijkheden hiervoor:

- Mogelijkheid om data te versleutelen
- Contractueel dichttimmeren aan wie de gegevens mogen worden verstrekt
    - Maar dit zal i.g.v. bv corrupte landen of VS (i.v.m. de Patriot Act, denk aan de NSA bijv.) geen garantie bieden

Autoriteit Persoonsgegevens kan ambtshalve (op eigen initiatief) onderzoek verrichten. Er kunnen (hoge!) boetes worden uitgedeeld.

(E)OR kan melding doen bij de Autoriteit, die bekijkt vervolgens zelf wat ze er mee doen.

Stel dat alle werknemers tekenen voor vrijwillige overdracht naar niet EU/EER: dan is dat nog steeds in strijd met de wet.

Na uitspraak van het Europese Hof van Justitie over *Safe Harbor:* Geen juridische basis meer voor gegevensuitwisseling met de VS. Een oplossing is te vinden in Binding Corporate Rules. Er is intussen wel een opvolger voor Safe Harbor in de maak: Privcay Shield.

Er is ook een EU model contract: te gebruiken bij een aantal landen.

Wereldwijde database: soms zijn er tegenstrijdige regels in de wetten van de verschillende landen. In Indonesië moet bijvoorbeeld de godsdienst van de werknemer worden vermeld, terwijl dat in Nederland verboden is. De wet zal overal moeten worden gevolgd, desnoods moet men een technische oplossing bedenken of toch verschillende databases bijhouden.

Manus Bolders, lid Select Committee EOR Sabic

Bij Sabic werd een aantal jaren geleden de HR administratie wereldwijd op één systeem gezet en opgeslagen in verschillende *hubs.*

De zeven Europese landen die de EOR vormden hebben aan de EOR het mandaat gegeven om te onderhandelen. Na twee jaar onderhandelen sloot de EOR een verdrag met management. De Duitse OR speelde prominente rol in onderhandelingen – hier was men het meest gevoelig voor dit thema en bovendien heeft de Duitse OR ook verstrekkende rechten bij maatregelen die de bescherming van

persoonsgegevens betreffen. De EOR heeft samen met de Duitse OR (die op zijn beurt gebruik maakte van de hulp van een expert) alle datavelden bekeken en alleen een beperkte lijst van datavelden toegelaten om uitgewisseld te worden. Zo heeft de EOR niet toegestaan dat zaken als religie en vakbondslidmaatschap het land verlaten. Ook is er vastgesteld welke functiegroepen tot welke data toegang hebben. Hiernaast is overeengekomen dat Sabic data encryptie gaat gebruiken. Eén jaar na implementatie mag EOR door een externe auditor het hele systeem laten doorlichten, wat nog niet gebeurd is Nadat het verdrag tussen EOR en Sabic was gesloten, hebben de OR's in alle landen het verdrag geratificeerd, wat inhield dat ze de inhoud van het verdrag integraal overnamen bij de medezeggenschapsprocedure op lokaal niveau (voor zover van toepassing). Dit scheelde Sabic uiteindelijk zes keer onderhandelen. Met name voor die landen waar geen instemmingsrecht voor de OR geldt of een zwakkere bescherming persoonsgegevens, was het verdrag van de EOR een extra bescherming.

Bij BAM is op een dergelijke manier door de EOR een modelcontract ontwikkeld dat in de landen door de OR's gebruikt kon worden.

Mr. Udo Oelen, hoofd van afdeling Toezicht Private Sector van de Autoriteit Persoonsgegevens

Verwerken persoonsgegevens binnen de arbeidsrelatie is een belangrijk thema, daar gaat veel mis. Bijvoorbeeld verkeerd gebruik van camera's bij het werk of meetgegevens over de gezondheid van werknemers.

Exporteren van gegevens buiten EU/EER mag alleen als hetzelfde beschermingsniveau gegarandeerd wordt.

- EU: Adequatheidsbeschikking kan worden afgegeven voor bepaalde landen, bijvoorbeeld Argentinië en Israël hebben dit. Tot voor kort was ook de VS afgedekt met Safe Harbor.
- Modelcontract: Standaardcontracten die tussen organisaties kunnen worden gebruikt. Zolang ze integraal worden gebruikt, is er geen toestemming vereist. Bij wijzigingen in de tekst moet Ministerie van Justitie toestemming verlenen.
- Binding Corporate Rules.

Een mogelijkheid is ook dat er individuele toestemming wordt verleend voor het exporteren van data, maar in een arbeidsrelatie mag dat doorgaans niet. Wij veronderstellen een dergelijke afspraak tussen werkgever en werknemer niet als vrije toestemming, tenzij de werknemer er duidelijk voordeel bij heeft.

Corrupt land: als alles goed is geregeld en er zijn goede controles ingebouwd, dan is datatransfer toelaatbaar. We kunnen dus niet bij voorbaat zeggen: we hebben geen vertrouwen in bijvoorbeeld India.

CV's van werknemers die aan internationale klanten worden gestuurd: daar kan de werkgever een gerechtvaardigd belang bij hebben, maar dit moet worden afgewogen tegen privacybelang van de werknemer. Dit zal iedere keer opnieuw moeten worden afgewogen en kan niet zo maar automatisch. De vraag die altijd moet worden gesteld is: kun je niet hetzelfde doel bereiken met minder ingrijpende middelen (subsidiariteitsbeginsel)?

Op foto's zit een strenger regime, net zoals op politieke en seksuele voorkeur.

Hoe werkt de controle? De organisatie die verantwoordelijk is voor gegevens en die de gegevens door een andere organisatie laat bewerken, moet met de andere partij afspraken maken over de controle. Die afspraken zijn vormvrij, hetgeen betekent dat aan de betrokken partijen wordt overgelaten op welke manier ze worden gemaakt. Maak je slechte afspraken en gaat het fout, dan ben je als verantwoordelijke partij hiervoor aansprakelijk. De Autoriteit doet dit soort toetsingen niet.

Ook bij softwarepakketten: op basis van de wet kan de werknemer ((E)OR) eisen dat er een variant gekozen wordt waar de gegevens worden versleuteld (ook als dat duurder is).

Binding Corporate Rules: als die in één Europees land zijn afgesloten, gelden deze voor heel Europa. Is er dan nog een verschil voor welk land men kiest (zou je een land met een sterke privacy standaard moeten kiezen, bijvoorbeeld Duitsland in plaats van Engeland)? Niet persé. De Europese richtlijn is overal geïmplementeerd, dit geeft een gemeenschappelijke basis, hoewel er wel verschillen zijn tussen de landen. Maar binnenkort komt de Europese verordening er aan die de richtlijn gaat vervangen. De verordening heeft rechtstreekse werking en hoeft niet eerst in nationale wetgeving worden omgezet. Vanaf dan zijn er geen verschillen meer. Bovendien kan een bedrijf niet zo maar een land voor de vestiging van de Binding Corporate Rules kiezen, de vestigingsplaats van het hoofdkantoor is bepalend. En: niet alleen de toezichthouder van dat land kijkt mee, maar ook nog toezichthouders uit twee andere landen. En alle toezichthouders in Europa moeten uiteindelijk de afspraken goedkeuren (meestal vertrouwen ze daarbij op de drie toetsende landen en toetsen ze niet zelf nog eens).

De Autoriteit treedt in eerste plaats als handhaver en toezichthouder op maar doet ook aan voorlichting. Ze zijn in principe geen adviseur, tenzij er nieuwe wetgeving in de maak is of er nieuwe ontwikkelingen zijn die om een advies vragen. De Autoriteit werkt op basis van risicoanalyse. Signalen komen binnen via de frontoffice, tips via de website en het netwerk. Bij mogelijke overtreding van de wet die mogelijk veel mensen treffen of die binnen jaarlijkse thema's passen ("oranje signalen"), volgt onderzoek. Bij rode signalen - duidelijke overtreding van de wet – volgt altijd een onderzoek. De Autoriteit stuurt ook brieven uit om bedrijven ergens op te wijzen (bijvoorbeeld: "u kopieert paspoorten, dat mag niet").

Bij mogelijke overtredingen gebeurt het volgende: onderzoek, voorlopige bevindingen, definitieve bevindingen, boete, eventueel last onder dwangsom. Onderzoeksresultaten worden gepubliceerd. Het feit dat de Autoriteit nu boetes uit kan delen, maakt wel dat werkgevers het thema serieuzer nemen. Als het onderzoek eenmaal loopt, is het moeilijk te stoppen. Een (E)OR kan wel contact opnemen en met ons overleggen, wij helpen hem dan op weg met de juiste in formatie.

Hebben werkgevers er iets aan als er een wereldwijd personeelsdatasysteem is en de server in Nederland staat? Dit helpt wel wat. Als partijen buiten Europa aan de gegevens kunnen komen, kan dat alleen na het maken van afspraken.

Systemen moeten worden gebouwd volgens de juiste principes. De medezeggenschap speelt daarbij een rol. Achteraf corrigeren is bovendien erg ingewikkeld.

In Duitsland hebben alle deelstaten een eigen toezichthouder voor de private sector.