JZ/MC/257942

Notitie implementatie Europese Privacy Verordening
Waar hebben we het over?

Inleiding

De concept Europese Privacy Verordening (EPV) wordt op dit moment behandeld door het Europees Parlement. Na goedkeuring door het Europese Parlement treedt de EPV direct in werking in alle lidstaten van de EU. De lidstaten krijgen een periode van 2 jaar om de EPV te implementeren. Op dit moment wordt nog gediscussieerd over details, maar de grote lijnen zijn wel duidelijk.

In de EPV zijn de regels voor de verwerking van persoonsgegevens op veel punten aangescherpt. Op het niet voldoen aan de verplichtingen en/of de overtreding van de regels zijn hoge boetes (tot M€ 100 of 5% van de jaarlijkse wereldwijde omzet) gesteld. Niets doen is derhalve geen optie. Vanwege het materiële belang van de boetes zal de accountant een 'in control statement' verlangen, voor wat betreft de beheersing van privacy risico's.

De EPV gaat expliciet uit van verantwoordelijkheden op het hoogste niveau van de organisatie. Het CvB kan aansprakelijk gesteld worden voor de naleving van de EPV.

Rechten van betrokkenen

Betrokkenen hebben met betrekking tot de verwerking van persoonsgegevens de volgende rechten:
- Het recht op toegang tot hun gegevens (artikel 14 EPV),
- Het recht op rectificatie (artikel 14 EPV),
- Het recht om vergeten te worden (artikel 17 EPV),
- Het recht om gegevens te laten wissen (artikel 5d EPV),
- Het recht van gegevensoverdraagbaarheid (artikel 18 EPV),
- Het recht op bezwaar (artikel 19 EPV).

Gevolgen voor de EUR

Om de rechten van betrokkenen te beschermen, verplicht de EPV organisatorische maatregelen te treffen, die ook personele en technische consequenties hebben.
De EUR is o.m. verplicht om:
- Intern privacy beleid vast te stellen,
- Modellen voor het afhandelen van incidenten op te stellen,
- Procedures en mechanismen op te stellen waardoor betrokkenen hun rechten kunnen uitoefenen (elektronisch indienen van verzoeken, termijn waarbinnen verzoeken moeten worden beantwoord, een weigering van een verzoek dient deugdelijk gemotiveerd te worden),
- Een Functionaris Gegevensbescherming aan te wijzen (profiel opstellen),
- Een overzicht van alle informatiesystemen met persoonsgegevens binnen de EUR op te stellen,
- Privacy te integreren als vast onderwerp binnen de bedrijfsvoering en de werking ervan jaarlijks controleren,
- De privacy deskundigheid van medewerkers die met persoonsgegevens omgaan te bevorderen,
- Privacy-by-Design op te nemen in het informatiemanagement, de architectuur en programma's van eisen,
- Voor de huidige systemen dienen passende technische en organisatorische maatregelen en procedures te worden getroffen (Privacy-by Default),
- Risico analyses uit te voeren,
- Privacy Impact Assessments uit te voeren bij majeure wijzigingen in de informatiehuishouding (nieuwe systemen maar ook majeure releases).

Verplichtingen uit de EPV kort uitgewerkt

1. Privacy beleid (artikel 11 en 22 EPV)
   De EUR is verplicht om privacy beleid vast te stellen, te hanteren en te handhaven. Het privacy beleid moet transparant en toegankelijk zijn. De informatie en mededelingen dienen duidelijk te zijn en in eenvoudige op betrokkene aangepaste taal te worden vertrekt. Het is van belang dat aantoonbaar is in het privacy beleid dat aan de eisen die voortkomen uit de EPV worden voldaan.

   (*) Onder profilering wordt verstaan het geautomatiseerd verwerken van persoonsgegevens met als doel aspecten van de persoonlijkheid van betrokkene te evalueren of om zijn beroepsprestaties, economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid en gedrag te analyseren of te voorspellen.

Onder privacy beleid valt de verplichting om:

- Documentatie over alle verwerkingen die hebben plaatsgevonden te bewaren (artikel 28 EPV).
- Passende technische en organisatorische maatregelen te nemen ter beveiliging van persoonsgegevens (artikel 30 EPV),
- In bepaalde gevallen een privacy-effect-beoordeling, ook wel Privacy Impact Assessment genoemd (PIA) uit te voeren. Een PIA moet worden uitgevoerd wanneer verwerkingen gezien aard, reikwijdte of doeleinden bijzondere risico's inhouden voor de rechten en vrijheden van betrokkenen. Dat is met name het geval wanneer profilering (*) plaatsvindt, bij de videobewaking van openbaar toegankelijke ruimtes en dergelijke (artikel 33 EPV),
- Een Functionaris Gegevensbescherming aan te wijzen,
- Te voldoen aan de eisen inzake voorafgaande toestemming of voorafgaande raadpleging CBP.

2. Plicht om verwerking van persoonsgegevens te beperken (artikel 5, sub c EPV)
   Persoonsgegevens mogen alleen worden verwerkt als de doeleinden niet kunnen worden bereikt door verwerking van andere (bijvoorbeeld geanonimiseerde) gegevens.
3. Privacy-by-Design en Privacy-by-Default (artikel 23 EPV)
   Het CvB is bij de aanschaf en het laten ontwikkelen van software, de inrichting van databases en de inrichting van een IT-systeem verplicht maatregelen te nemen om te zorgen dat de hoeveelheid verwerkte gegevens en de bewaartermijn daarvan zijn afgestemd op het doel waarvoor zij worden verzameld en dat de gegevens niet aan een onbeperkt aantal personen ter beschikking worden gesteld. De maatregelen moeten voldoen aan de stand van de techniek van het moment.
   - Privacy-by-Design betekent dat al in de voorfase van een ICT project wordt gekeken naar technische en organisatorische maatregelen die de privacybescherming verhogen, door bijvoorbeeld gebruik te maken van Privacy Enhancing Technology (PET). De privacywet wordt in het systeem ingebouwd. Het omvat een aan de bouw van systemen, diensten en netwerken voorafgaande Privacy Impact Analyse (PIA) en een management cyclus waar privacybescherming een vast onderdeel van is.
     Het gaat om het ontwerpen van informatiesystemen, die de privacy van mensen beschermen: door gegevensminimalisatie; door transparantie over het gebruik van hun gegevens; door afscherming van de identiteit van het individu; door het gebruik van kleefbeleid (sticky policies); door het volgen van persoonsgegevens nadat deze zijn verzameld (data tracking); door gebruik van privacy bewustmakende icons en door privacy ontologie waardoor de privacy rechtsregels in systemen zijn in te bouwen. Wat betreft datatracking: het blijkt technisch mogelijk om het gegevensspoor van de bezoeker van een website door die bezoeker te laten opvragen. Dit gegevensspoor of datatrack geeft de condities aan de bezoeker van Internet weer, waaronder de opslag en verwerking van zijn gegevens hebben plaatsgevonden. De datatrack verschaft niet alleen transparantie voor gebruikers, maar stelt hen ook in staat aan het CvB later te vragen of zij werkelijk de gegevens zoals beloofd is, heeftbehandeld. Een privacy ontologie bevat een hiërarchische datastructuur met alle relevante entiteiten en hun onderlinge relaties en regels binnen het privacy domein. Op die manier kan privacywetgeving in een algemeen conceptueel model worden vertaald, waardoor de wetgeving in informatiesystemen kan worden ingebouwd.
   - Privacy-by-Default lijkt op het Privacy-by-Design principe en betekent dat door middel van systeeminstellingen maximale privacy van een betrokkene wordt gewaarborgd en voor zover mogelijk door het systeem wordt afgedwongen. Vereist is dat het CvB technische en organisatorische maatregelen treft die dit realiseren. Het kader hierbij is: 'met inachtneming van de stand van de techniek en de uitvoeringskosten'. Hierbij kan worden gesteld dat datgene dat technisch afdwingbaar is ook technisch geïmplementeerd dient te worden.

   Wanneer het ontwerp van een systeem privacy inbreuken mogelijk maakt, is het CvB aansprakelijk en niet de ontwerper of bouwer van het systeem. Ook kan het CvB een boete opgelegd krijgen en niet de ontwerper of bouwer. Dit betekent dat de EUR zal opdrachtgever duidelijke afspraken moet maken met de ontwerper of bouwer van een systeem dat deze in voorkomende gevallen de eventuele schadevergoeding of boete kan verhalen op de ontwerper of bouwer.
4. Informatieplicht (artikel 14 EPV)
   De informatie die moet worden verstrekt aan betrokkene over de verwerking van zijn persoonsgegevens is gedetailleerd in de EPV beschreven. Aan betrokkene moet duidelijke informatie worden verstrekt over zijn rechten (zoals het recht op inzage, op correctie en

(*) Onder profilering wordt verstaan het geautomatiseerd verwerken van persoonsgegevens met als doel aspecten van de persoonlijkheid van betrokkene te evalueren of om zijn beroepsprestaties, economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid en gedrag te analyseren of te voorspellen.

verwijdering van persoonsgegevens). Ook moet specifiek worden vermeld of profilering (*) wordt toegepast en of de intentie bestaat gegevens door te geven naar derde landen.

5. Recht om vergeten te worden (artikel 17 EPV)
   Betrokkene heeft het recht op volledige verwijdering van zijn persoonsgegevens indien hij zijn toestemming intrekt en er geen andere legitieme redenen zijn om de data te bewaren. Persoonsgegevens moeten worden gewist en verdere verspreiding moet achterwege blijven, wanneer:
   - betrokkene zijn toestemming intrekt,
   - betrokkene bezwaar maakt tegen verwerking
   - de verwerking niet voldoet aan de EPV, waarna de EUR uit eigen beweging de gegevens moet wissen.

   Wanneer de gegevens op verzoek van betrokkene worden verwijderd en ze zijn door of met toestemming van het CvB openbaargemaakt of doorgegeven aan derden, dan moeten alle redelijke maatregelen genomen worden om derden die de gegevens verwerken van de intrekking van de toestemming door betrokkene op de hoogte te stellen.
   Het recht op vrijheid van meningsuiting is uitgezonderd van de verplichting de gegevens te verwijderen (media zijn hierdoor in het algemeen gevrijwaard van de verplichting gegevens over personen op hun verzoek te verwijderen). Ook uitgezonderd van het recht om vergeten te worden zijn persoonsgegevens die verwerkt worden (artikel 17, lid 3 EPV):
   - om redenen van algemeen belang op het gebied van de volksgezondheid,
   - voor historische, statische of wetenschappelijke doeleinden.
   - gegevens ten behoeve van bewijsvoering.
6. Functionaris Gegevensverwerking (artikel 35, 36, 37 EPV)
   Een Functionaris Gegevensbescherming moet worden aangewezen. Deze functionaris geniet ontslagbescherming. Hij moet onder meer toezien op de uitvoering en toepassing van het privacy beleid, het beperken van gegevensverwerking door toepassing van Privacy-by-Design en Privacy-by- Default, het beveiligen van gegevens, het toezien op de uitvoering van de PIA en het voldoen aan een verzoek van betrokkenen om informatie in het kader van de EPV. Ook bij datalekken speelt de functionaris een belangrijke rol door toe te zien op het naleven van de meldplicht, de datalekken te documenteren, te melden en de inbreuken in verband met persoonsgegevens mee te delen in overeenstemming met artikelen 31 en 32 EPV.
7. Verplichtingen van de verwerker van persoonsgegevens (artikel 26 EPV)
   De verwerker (degene die voor het CvB de gegevens verwerkt en **niet** in hiërarchische relatie staat tot het CvB) krijgt verplichtingen (zoals het nemen van adequate beveiligingsmaatregelen, het handelen binnen de instructies van het CvB, het opleggen van geheimhoudingsplicht aan zijn personeel). Bij overtreding van die verplichtingen kan de verwerker gestraft worden met dezelfde hoge boetes als het CvB. De contracten met diegenen die voor de EUR Persoonsgegevens verwerken (salarisbetaling) moeten worden gecontroleerd of ze voldoen aan de EPV en eventueel uitgebreid worden zodat EPV wordt nageleefd.
8. Meldplicht datalekken (artikel 30, 31 en 32 EPV)
   Onder datalek wordt verstaan (artikel 4, sub 9 EPV) een inbreuk op de beveiliging met tot gevolg: vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens hetzij per ongeluk hetzij onrechtmatig.
   Uitgangspunt is dat ieder datalek, zo spoedig mogelijk en in beginsel niet later dan 24 uur nadat ervan kennis is genomen, moet worden gemeld aan het CBP. Een melding die later wordt gedaan moet gemotiveerd worden. Ook betrokkenen moeten geïnformeerd worden wanneer negatieve gevolgen voor de bescherming van de persoonsgegevens of de privacy van de betrokkenen waarschijnlijk zijn.

Enkele meer juridisch technische aspecten

1. Rechtsgrondslag
   De verwerking van persoonsgegevens dient een rechtmatige grondslag te hebben.
   Betrokkene dient uitdrukkelijk toestemming te geven voor het verwerken van zijn gegevens (artikel 4, lid 1 EPV) en het CvB moet dit kunnen aantonen (artikel 7, lid 1 EPV). Dat kan door een verklaring of een ondubbelzinnige handeling. Het hanteren van een opt-out is niet langer een rechtmatige grondslag voor de verwerking van persoonsgegevens.

(*) Onder profilering wordt verstaan het geautomatiseerd verwerken van persoonsgegevens met als doel aspecten van de persoonlijkheid van betrokkene te evalueren of om zijn beroepsprestaties, economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid en gedrag te analyseren of te voorspellen.

Onevenwichtigheid

Toestemming biedt geen rechtmatige grondslag voor verwerking van persoonsgegevens wanneer een aanzienlijke onevenwichtigheid bestaat tussen de positie van betrokkene en de positie van het CvB voor de verwerking (artikel 7, lid 4 EPV). Daarmee staat vast dat toestemming niet kan worden gebruikt in arbeidsverhoudingen, gezien de ongelijkheid in de positie van werknemer en werkgever (overweging 34). Het belang van werkgever om de persoonsgegevens te mogen verwerken, weegt zwaarder dan de bescherming van de privacy van betrokkene (artikel 6, lid 1 sub f EPV). Vaak bestaat er een andere gerechtvaardigde grondslag voor de verwerking dan toestemming, zoals de nakoming van een wettelijke plicht zoals aangifte loonheffing (overweging 36) of de uitvoering van een overeenkomst.

Voor wat betreft de verwerking van persoonsgegevens van studenten bestaat een gelijke onevenwichtigheid in de positie tussen de student en de EUR. Net als bij personeel biedt toestemming geen rechtmatige grondslag voor verwerking, maar is verwerking noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de EUR (artikel 6, lid 1 f EPV). Hier bestaat ook een andere grondslag voor de verwerking dan de toestemming, zoals de nakoming van een wettelijke plicht (overweging 36). Toestemming dient niet te worden gevraagd.

Profilering (*)

Onder profilering (*) wordt verstaan het geautomatiseerd verwerken van persoonsgegevens met als doel aspecten van de persoonlijkheid van betrokkene te evalueren of om zijn beroepsprestaties, economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid en gedrag te analyseren of te voorspellen.

In artikel 20 EPV wordt het verzamelen en verder verwerken van persoonsgegevens ten behoeve van profilering(*) en daarop gebaseerde marketing beperkt. Iedere betrokkene heeft het recht om niet op basis van profilering (*) aan een maatregel onderworpen te worden, waaraan voor hem rechtspositionele maatregelen zijn verbonden of die hem in aanmerkelijke mate treft en die louter wordt genomen op grond van geautomatiseerde verwerking.

Onder deze beperking valt ook het verwerken van persoonsgegevens ten behoeve van beoordelingsgesprekken en andere HR-doelen. De rechtsgrondslag hiervoor zal moeten liggen in de uitvoering van de arbeidsbetrekking (nagaan waar scheidslijn ligt!!).

Een persoon mag alleen aan een maatregel, die op basis van profilering (*) tot stand komt, worden onderworpen wanneer de verwerking:

- Wordt uitgevoerd in het kader van het sluiten of uitvoeren van een overeenkomst
- Uitdrukkelijk is toegestaan op grond van EU-wetgeving of nationale wetgeving
- Plaatsvindt op grond van toestemming van betrokkene.

Voor wat betreft de verwerking van persoonsgegevens van studenten bestaat een gelijke onevenwichtigheid in de positie tussen student en de EUR. Net als bij personeel biedt toestemming geen rechtmatige grondslag voor verwerking maar vindt verwerking noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de EUR. Toestemming dient niet te worden gevraagd.

2. Samenwerkingsverbanden

   Partners van samenwerkingsverbanden die voor een gezamenlijke verwerking van persoonsgegevens verantwoordelijkheid dragen moeten door middel van een onderlinge regeling vastleggen hoe de respectieve verantwoordelijkheden worden vastgelegd voor de nakoming van de verplichtingen uit de EPV, met name met betrekking tot de procedures en mechanismen voor de uitoefening van de rechten van betrokkenen.

3. Reikwijdte van de EPV (artikel 44 EPV)

   De EPV is ook van toepassing wanneer persoonsgegevens van iemand die in de EU woont worden bewerkt buiten de EU, wanneer de verwerking plaatsvindt in het kader van een transactie of om een gebruikersprofiel te kunnen maken (profilering).

(*) Onder profilering wordt verstaan het geautomatiseerd verwerken van persoonsgegevens met als doel aspecten van de persoonlijkheid van betrokkene te evalueren of om zijn beroepsprestaties, economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid en gedrag te analyseren of te voorspellen.