DECLERCQ
Advocaten · Notarissen

Whitepaper Europese Privacy Verordening

Welke veranderingen staan ons te wachten?

Op 25 januari 2012 deed de Europese Commissie een voorstel voor een nieuwe Europese Privacy Verordening. Het is nu aan de Europese Raad en het Europees Parlement om tot overeenstemming te komen over een definitieve tekst van het wetsvoorstel. Er zullen zeker nog veranderingen doorgevoerd worden in de Verordening, maar op hoofdlijnen bestaat er duidelijkheid. Hieronder een kort overzicht van de belangrijkste veranderingen in het privacyrecht.

Waarom een nieuwe Privacy Verordening?

De huidige Privacyrichtlijn stamt uit 1995. Sindsdien is veel veranderd op het gebied van gegevensbescherming. 20 jaar aan technologische ontwikkelingen hebben het mogelijk gemaakt meer informatie te halen uit dezelfde gegevens en hebben de volumes vergaarde en verwerkte gegevens sterk vergroot. Deze gegevens worden ook voor commerciële doeleinden gebruikt. Bovendien is een lappendeken aan gegevensbeschermingsregels ontstaan en zijn de markt en de samenwerkingsverbanden gemondialiseerd. Gegevens worden doorgegeven naar alle delen van de wereld. Niet altijd is even duidelijk waar de gegevens zich precies bevinden, wie verantwoordelijk is voor deze gegevens en welk recht van toepassing is.

Het is voor individuen ("betrokkenen") daardoor steeds moeilijker om hun rechten op gegevensbescherming uit te oefenen. Ook bedrijven moeten weten aan welke vereisten zij moeten voldoen voordat zij persoonsgegevens gaan verwerken. Er is gekozen voor een Verordening in plaats van een Richtlijn. Dit betekent dat de Verordening geldt voor alle lidstaten zonder dat deze wordt omgezet in nationale wetgeving.

Meer gegevens worden 'persoonsgegevens'

Meer gegevens zullen worden gekwalificeerd als 'persoonsgegevens' dan nu het geval is. Denk hierbij aan locatie-data en online-identifiers zoals IP-adressen en identificatiecookies voor zover deze (in combinatie met andere gegevens) de betrokkene identificeerbaar maken.

Verwerkers buiten de EU

De Verordening zal gelden voor alle bedrijven die persoonsgegevens verwerken van Europese burgers. Dit betekent dat ook verwerkers gevestigd buiten Europa gebonden worden aan de Europese gegevensbeschermingsregels. Dit is een belangrijke wijziging, aangezien steeds meer persoonsgegevens worden verwerkt in zogenaamde derde landen, zoals de VS en India.

Toestemming

De Verordening beoogt toestemming van de betrokkene voor de verwerking van zijn persoonsgegevens de belangrijkste verwerkingsgrondslag te maken. De huidige Privacyrichtlijn vereist 'expliciete toestemming', waarvan het verkrijgen inefficiënt kan zijn door de vele vereisten die hieraan zijn gekoppeld. Het Europees Parlement stelt dat ook technische normen die uitdrukking geven aan uitdrukkelijke wensen van een betrokkene mogen worden aangemerkt als een geldige manier van verlening van toestemming. Hierbij kan worden gedacht aan toestemming door middel van browserinstellingen, waarvan gedurende het cookiedebat is gesuggereerd dat hiermee toestemming kan worden gegeven. Dit biedt ruimte voor een verdere ontwikkeling van de toestemming in de digitale omgeving. Omdat betrokkenen geneigd kunnen zijn hun toestemming te geven onder druk van de verantwoordelijke is in de Verordening opgenomen dat de toestemming niet als verwerkingsgrondslag

kan dienen wanneer een aanzienlijke onevenwichtigheid bestaat tussen de positie van de betrokkene en die van de verantwoordelijke. Hoe dit in de praktijk ingevuld zal worden is echter nog onduidelijk.

Pseudonimisering

De Verordening beoogt pseudonimisering van gegevens aan te moedigen. Het begrip 'pseudonieme gegevens' wordt geïntroduceerd, wat wordt uitgelegd als: "persoonsgegevens die niet aan een specifieke betrokkene kunnen worden gekoppeld zonder dat aanvullende gegevens worden gebruikt, zo lang als dergelijke aanvullende informatie apart wordt bewaard en op voorwaarde dat technische en organisatorische maatregelen worden genomen om niet-koppeling te waarborgen". Hiervan is bijvoorbeeld sprake wanneer de identificerende gegevens zijn vervangen door nummers en maatregelen zijn getroffen om te voorkomen dat deze nummer worden gekoppeld aan de identificerende gegevens. Pseudonomisering door verantwoordelijken en verwerkers wordt aangemoedigd door de verwerking van gepseudonimiseerde gegevens vrij te stellen van een aantal verplichtingen uit de Verordening.

Het recht om vergeten te worden

Het recht om vergeten te worden staat niet in de Privacyrichtlijn, maar bestaat sinds het arrest Google Spanje / Mario Costeja González van 13 mei 2014. In dit arrest werd bepaald dat burgers het recht hebben om privacygevoelige informatie te laten verwijderen uit online zoekmachines wanneer deze informatie gedateerd, irrelevant of ongepast is. Wanneer sprake is van 'gedateerde, irrelevante of ongepaste privacygevoelige informatie' dan wordt het belang bij verwijdering afgewogen tegen (bijvoorbeeld) het algemene belang bij beschikbaarheid van informatie. Hierop stranden op dit moment veel verwijderingsverzoeken.

In de Verordening wordt de bewijslast ten aanzien van het recht om te worden vergeten echter omgedraaid. Wanneer de betrokkene een beroep doet op het recht om te worden vergeten, dan is het aan de verantwoordelijke om te bewijzen dat de gegevens onder een uitzondering vallen. Voorbeelden van uitzonderingen zijn dat het bewaren van de gegevens nodig is voor de uitoefening van het recht op vrijheid van meningsuiting of voor het voldoen aan een wettelijke verplichting.

Daarnaast is het recht om vergeten te worden in de Verordening veel breder dan het nu is. In de verordening geldt het recht om vergeten te worden voor alle verantwoordelijken die gegevens openbaar maken, waar het recht nu slechts van toepassing is op zoekmachines. Daarnaast moet onder het huidige recht de zoekmachine slechts de link uit haar systeem verwijderen, terwijl de Verordening stelt dat de verantwoordelijke derden die de gegevens verwerken verzoekt iedere koppeling naar, reproductie van of kopie van de gegevens te wissen.

One-stop-shop

In de Privacy Verordening zijn maatregelen opgenomen om de administratieve druk te verlichten voor verwerkers gevestigd in meerdere lidstaten. Om dit te bereiken wordt de 'one-stop-shop' ingevoerd. Dit houdt in dat de toezichthoudende autoriteit van het land waar de belangrijkste vestiging van de verwerker is gevestigd, ook toezicht houdt op de verwerkingen van deze verwerker in andere lidstaten. Hierdoor hebben bedrijven die gegevens verwerken in meerdere lidstaten één aanspreekpunt, hetgeen de administratieve druk moet verlichten.

Concrete verplichtingen voor bedrijven

Privacy Officer

Om de controle op de naleving van de Privacyverordening te vergroten is de Privacy Officer in het leven geroepen. De Privacy Officer moet zijn geregistreerd bij de nationale privacy autoriteit en ziet onafhankelijk van de onderneming toe op de naleving van de Privacy-verordening. Een organisatie moet een Privacy Officer moeten aanstellen indien:

i) de verwerking van persoonsgegevens wordt uitgevoerd door een overheidsinstantie of –orgaan; of
ii) de verwerking van persoonsgegevens wordt uitgevoerd door een onderneming met minimaal 250 werknemers; of
iii) de verantwoordelijke of verwerker hoofdzakelijk is belast met verwerkingen die

vanwege hun aard, omvang en/of doel regelmatige en stelselmatige observatie vereisen.

Het Europees Parlement meent dat de verplichting tot het aanstellen van een Privacy Officer slechts afhankelijk moet zijn van de relevantie van de gegevensverwerking, en niet van de hoeveelheid werknemers van een onderneming. Voor de relevantie van de gegevensverwerking is van belang welke categorie persoonsgegevens worden verwerkt, welke verwerkingsactiviteit plaatsvindt en het aantal betrokkenen waarvan de gegevens verwerkt worden.

Privacy Impact Assessment

De Verordening verplicht organisaties een Privacy Impact Assessment (PIA) te doen wanneer zij een verwerking doen die gezien hun aard, reikwijdte of doeleinde bijzondere risico's inhouden voor de rechten en vrijheden van de betrokkene. Dit is een vrij vaag begrip, maar de Verordening geeft enkele voorbeelden waarbij sprake zal zijn van bijzondere risico's:

i) profiling om iemands economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag te analyseren of te voorspellen waarop maatregelen zijn gebaseerd die deze persoon in aanzienlijke mate treffen;
ii) verwerking van bijzondere persoonsgegevens, bijvoorbeeld gegevens over seksuele leven, gezondheid, ras of etnische afkomst;
iii) de bewaking van openbaar toegankelijke ruimten, met name wanneer videobewaking wordt gebruikt;
iv) verwerking van grote verzamelingen persoonsgegevens over kinderen of over genetische of biometrische gegevens.

De PIA moet ten minste een algemene beschrijving van de beoogde verwerking(en) bevatten en een beoordeling van risico's voor de rechten en vrijheden van betrokkenen, de maatregelen die worden beoogd om de risico's te beperken en de waarborgen, beveiligingsmaatregelen en mechanismen die de bescherming van persoonsgegevens verzekeren en aantonen dat aan de Verordening is voldaan.

Privacy by design en by default

Privacy by design en by default verbiedt de verantwoordelijke meer gegevens te verzamelen dan strikt noodzakelijk voor het doeleinde van de verwerking en hier al in een vroeg stadium rekening mee te houden. Dit betekent dat, voor zover technisch mogelijk zonder exorbitante uitvoeringskosten, bij de ontwikkeling of aanschaf van een IT-systeem, maatregelen moeten worden genomen om de hoeveelheid verwerkte gegevens tot een minimum te beperken en te voorzien in automatische verwijdering van de gegevens wanneer deze niet meer noodzakelijk zijn. Daarnaast moet worden voorkomen dat de verzamelde gegevens niet aan een onbeperkt aantal personen toegankelijk wordt gemaakt, oftewel, het IT-systeem moet voorzien in de mogelijkheid om het gedeelte waarin de persoonsgegevens toegankelijk zijn, slechts toegankelijk te maken voor de personen die deze toegang nodig hebben.

De Verordening voorziet in de mogelijkheid van nadere invulling door middel van technische normen door de Europese Commissie. In ieder geval is duidelijk dat organisaties kritischer moeten bekijken of zij de gegevens die zij verzamelen kunnen verantwoorden en het opslaan van persoonsgegevens op een centrale server zal in veel gevallen niet meer toegestaan zijn zonder dat hierbij toegangsrestricties worden opgelegd.

Doorgifte naar derde landen

De regels voor doorgifte van persoonsgegevens naar derde landen worden versimpeld. Voor doorgifte naar derde landen op basis van de door de Europese Commissie goedgekeurde modelbepalingen is geen voorafgaande toestemming van de toezichthouder meer vereist. In Nederland is deze toestemming overigens ook op dit moment niet vereist; in enkele Europese landen ligt dit echter anders. Daarnaast hoeft voortaan slechts één toezichthouder de binding corporate rules goed te keuren, waar dat er nu nog drie zijn.

Wanneer geen sprake is van een passend beschermingsniveau, binding corporate rules of modelbepalingen, biedt de Verordening de mogelijkheid tot doorgifte wanneer deze noodzakelijk is

voor de gerechtvaardigde belangen van de verantwoordelijke of verwerker, mits de doorgifte niet als frequent of massaal kan worden beschouwd en er indien nodig passende garanties worden geboden.

Daarnaast is het interessant dat in de Verordening 'doorgifte van persoonsgegeven naar derde landen of internationale organisaties' als één onderwerp behandelt. Het is vooralsnog onduidelijk wat onder 'internationale organisaties' moet worden verstaan. Een brede uitleg van dit begrip zou het mogelijk maken dat de Europese Commissie oordeelt dat bepaalde bedrijven een passend beschermingsniveau hanteren.

Meldplicht datalekken

In de Verordening wordt de verplichting opgenomen om datalekken te melden aan de Autoriteit en, indien het de privacy van de betrokkene aantast, aan de betrokkene. Vooruitlopend op de Verordening zal de meldplicht datalekken in Nederland al op 1 januari 2016 van kracht worden.

Er is sprake van een datalek wanneer persoonsgegevens toegankelijk zijn (geweest) voor derden, zijn vernietigd, gewijzigd of vrijgekomen buiten de bedoeling van de verantwoordelijke om. Onder de huidige wetgeving is sprake van een datalek wanneer er een inbreuk is op de beveiliging in de zin van artikel 13 Wbp. Welke datalekken precies onder de verplichting van de Verordening zullen vallen is nog onduidelijk, het Europees Parlement wil dat vrijwel alle datalekken worden gemeld, daar waar de Europese Commissie wil dat enkel datalekken worden gemeld die (ernstige) gevolgen hebben voor de privacy van de betrokkene. De Verordening stelt dat datalekken binnen 'bekwame tijd' moeten worden gemeld bij de Autoriteit en, indien nodig, bij de betrokkene. Naar verwachting zal aan het begrip 'bekwame tijd' later een meer concrete invulling worden gegeven.

Documentatieplicht in plaats van meldplicht

Een belangrijke wijziging is het vervallen van de meldplicht. Onder de Privacyrichtlijn moeten verwerkingen van persoonsgegevens worden gemeld bij het CBP, tenzij de specifieke verwerking is vrijgesteld. De meldplicht vervalt in de Verordening en wordt vervangen door een documentatieplicht. De verantwoordelijke moet documenten bewaren waarin (onder andere) is opgenomen wat de doeleinden voor de verwerking zijn, van welke categorieën betrokkenen welke categorieën gegevens worden verwerkt en met wie deze gegevens worden gedeeld. Op verzoek van de toezichthoudende autoriteit worden deze gegevens aan haar ter beschikking gesteld.

Dit brengt meer verantwoordelijkheid met zich mee voor bedrijven die persoonsgegevens verwerken. Waar nu nog iedere verwerking vooraf wordt getoetst door het CBP, komt deze verantwoordelijkheid volledig bij de verantwoordelijke voor de verwerking te liggen.

Tot slot

In hoofdlijnen zijn de wijzigingen die de Verordening met zich mee zal brengen bekend. Het is dus zaak dat organisaties zich gaan voorbereiden op de komende veranderingen. Compliance met de Verordening is immers niet optioneel: toezichthouders hebben de bevoegdheid boetes op te leggen van maximaal € 1.000.000 of 2% van de wereldwijde jaaromzet. Bovendien kunnen de bestuurders van organisaties die zich niet aan de Verordening houden, hoofdelijk aansprakelijk worden gesteld.

De privacy-specialisten van De Clercq helpen u graag met het compliance-traject en houden u tussentijds op de hoogte van de mogelijke wijzigingen die nog in de tekst van de Verordening zullen worden doorgevoerd.

Leiden/Den Haag, augustus 2015

Natascha van Duuren (n.vanduuren@declercq.com)
Willem Balfoort (w.balfoort@declercq.com)
Marijn Storm (m.storm@declercq.com)