

Europese Privacy verordening: hoe zit het precies?

13-11-2014 00:00

Door Bas Le Large

[Bosselaar & Strengers Advocaten](#)

Op 12 maart 2014 heeft het Europees Parlement met een grote meerderheid van stemmen het voorstel van de Europese Commissie tot introductie van een Algemene Verordening Gegevensbescherming aangenomen die naar alle waarschijnlijkheid in 2016 in werking zal treden. De verordening heeft directe werking, wat betekent dat de lidstaten deze niet eerst hoeven te implementeren. De verordening wordt daarmee direct van kracht in alle lidstaten, waardoor in heel Europa dezelfde privacywetgeving zal gelden.

Dat retailers die over de grens actief zijn, of deze ambitie hebben, niet langer geconfronteerd zullen worden met verschillende privacywetgeving is een groot voordeel. Dit scheelt immers een hoop uitzoekwerk en zal naar alle waarschijnlijkheid leiden tot meer grensoverschrijdende activiteit.

In de aanloop naar de verordening zullen veel retailers wel hun bedrijf goed onder de loep moeten nemen om ervoor te zorgen dat aan de nieuwe wetgeving wordt voldaan. Hoewel de invoering van de verordening nog ver weg lijkt, brengt de verordening namelijk grote veranderingen met zich mee. Daarom moeten retailers er nu al voor zorgen dat privacy compliance de komende tijd hoog op de agenda staat.

De belangrijkste wijzigingen op een rij

In de verordening staan de rechten van betrokkenen centraal. Voordat de retailer tot het verwerken van persoonsgegevens mag overgaan, moet in veel gevallen eerst expliciet toestemming van de betrokkene te worden verkregen. Onder persoonsgegevens vallen – kort gezegd - alle gegevens die je kunt herleiden tot een natuurlijk persoon.

Het begrip 'persoonsgegevens' wordt met de introductie van de verordening heel breed; ook IP-adressen, cookiedata en geodata valt straks onder dit begrip. Het verwerken van persoonsgegevens betreft elke handeling met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, bewaren, opvragen en verspreiden. Door deze brede definitie zullen straks veel retailers die nu nog geen persoonsgegevens verwerken in de zin van de privacywetgeving straks wel onder de privacywetgeving vallen.

Betrokkenen krijgen met de introductie van de verordening bovendien het recht om hun persoonsgegevens te laten verwijderen. Dit 'recht om vergeten te worden' stond recentelijk centraal in een spraakmakende zaak tegen Google. In deze uitspraak nam het Europese Hof van Justitie alvast een voorschot op de inwerkingtreding van de verordening, door te oordelen dat Google op verzoek van betrokkenen tot verwijdering van zoekresultaten moet overgaan.

Daarbij stelt de verordening strengere eisen aan de informatievoorziening naar de betrokkenen toe en aan de beveiliging van persoonsgegevens. Om aan alle vereisten van de verordening te kunnen voldoen zullen veel retailers dan ook de inrichting van hun systemen en de wijze waarop zij persoonsgegevens verwerken moeten aanpassen.

De verandering die misschien wel het meest in het oog springt is de sanctiemogelijkheid bij overtreding van de bepalingen uit de verordening. Na introductie van de verordening kan een overtreding leiden tot een maximale boete van honderd miljoen euro of vijf procent van de wereldwijde jaaromzet. Dit is een groot verschil met de huidige situatie waarin het College Bescherming Persoonsgegevens 'slechts' een boete van ten hoogste 4.500 euro kan opleggen.

De verwachting is dat de verordening uiterlijk in 2016 in werking zal treden. Dit lijkt ver weg, maar vooruitlopend op de Verordening is de Tweede Kamer nu al bezig met het aanscherpen van de huidige wetgeving. Zo wordt op korte termijn een Wet meldplicht datalekken ingevoerd, waarmee de in de Verordening opgenomen regels ten aanzien van het melden van datalekken vervroegd in werking zal treden. Het is daarom voor retailers van groot belang om zich nu alvast voor te bereiden op wat komen gaat.

Door het stellen van de onderstaande vijf vragen bereidt u zich als retailer alvast voor op wat komen gaat.

1. Welke persoonsgegevens worden binnen het retailbedrijf verwerkt?

Om in kaart te brengen hoe uw bedrijf ervoor staat met haar privacy compliance dient allereerst duidelijk te worden of, en zo ja, persoonsgegevens worden verwerkt binnen het retailbedrijf. Onder persoonsgegevens vallen – kort gezegd - alle gegevens die u kunt herleiden tot een natuurlijk persoon. Het verwerken daarvan is elke handeling met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, bewaren, opvragen en verspreiden daarvan. Het hebben van een klantenbestand valt hier dus al onder. Is voor het verwerken van deze gegevens aantoonbaar toestemming verleend door de betrokkene? Sommige verwerkingen zullen niet langer worden toegestaan indien hiervoor geen expliciete toestemming is verkregen, en het is aan het retailbedrijf deze toestemming te bewijzen. Breng daarom in kaart welke persoonsgegevens binnen het bedrijf worden verwerkt.

2. Worden persoonsgegevens onnodig lang bewaard?

Zodra duidelijk is welke persoonsgegevens binnen het retailbedrijf worden verwerkt, dient de vraag te worden gesteld of, en zo ja voor welke duur, deze persoonsgegevens worden bewaard. Voor welke doeleinden worden deze gegevens bewaard? Zitten er misschien gegevens tussen die niet bewaard hoeven worden? Gegevens die niet (langer) worden bewaard voor een duidelijk omschreven doel, kunnen met het oog op privacy-compliance beter worden verwijderd.

3. Wie is verantwoordelijk voor privacy compliance?

Met de introductie van de verordening dient elk retailbedrijf dat in een periode van twaalf maanden persoonsgegevens verwerkt van meer dan vijfduizend personen een zogenaamde 'functionaris voor de gegevensbescherming' aan te stellen. Dit kan een werknemer zijn, of een persoon van buitenaf die voor minimaal twee jaar op basis van een overeenkomst deze taak vervult.

Deze functionaris moet onder meer toezien op de uitvoering en toepassing van het privacybeleid en op de uitvoering en toepassing van verschillende bepalingen van de verordening, zoals het zoveel mogelijk beperken van gegevensverwerkingen, het beveiligen van gegevens en het voldoen aan bijvoorbeeld een verzoek tot verwijdering van een betrokkene.

Hoewel de grens van vijfduizend personen hoog lijkt, zullen ook de kleinere retailbedrijven al snel een klantenbestand hebben waarin gedurende twaalf maanden gegevens worden verwerkt van vijfduizend personen of meer, waarmee ook zij dus verplicht zijn een functionaris aan te stellen. Maar ook voor retailbedrijven die hier niet onder vallen is het aan te raden iemand aan te wijzen die het naleven van de privacy wetgeving coördineert. Wijs daarom nu alvast iemand aan die verantwoordelijk wordt gemaakt voor privacy compliance en die de nieuwe ontwikkelingen op de voet volgt.

4. Is het privacybeleid nog up-to-date?

Op dit moment is een privacybeleid, hoewel nuttig, niet verplicht. Dit wordt anders na inwerkingtreding van de verordening. De verordening verplicht alle bedrijven, groot en klein, om een transparant privacybeleid te voeren dat bovendien voor betrokkenen toegankelijk is. Dus stel een privacybeleid op en maak deze voor iedereen makkelijk toegankelijk. Zorg daarbij dat uit het beleid in ieder geval duidelijk wordt welke gegevens worden

verwerkt, voor welke doeleinden dit gebeurd en op welke wijze betrokkenen hiertegen bezwaar kunnen maken.

5. Hoe zit het met de systeembeveiliging?

Vooruitlopend op de meldplicht voor datalekken die is opgenomen in de Verordening buigt de Tweede Kamer zich momenteel over een eerdere invoering van een meldplicht voor datalekken. Op grond van het wetsvoorstel moet een bedrijf een datalek zo snel mogelijk, maar uiterlijk binnen 24 uur, melden aan het College Bescherming Persoonsgegevens en in sommige gevallen ook aan de betrokkene wiens gegevens door het datalek in gevaar zijn gekomen. Op het niet (tijdig) melden staat een boete van maximaal 450 duizend euro.

Neem dus de systeembeveiliging onder de loep en verbeter deze waar mogelijk. Stel daarnaast een noodplan op voor het geval een datalek plaatsvindt, zodat iedereen binnen het retailbedrijf weet hoe hij bij een datalek moet reageren, welke stappen moeten worden ondernomen en wie verantwoordelijk is voor de uitvoering hiervan.

Na beantwoording van deze vragen heeft u alvast een eerste belangrijke stap gezet in de aanloop naar de Verordening. Mocht u naar aanleiding van dit artikel vragen hebben, neem dan vrijblijvend contact op met het brancheteam Retail van Bosselaar & Strengers Advocaten.