legaltree

Auteur:
mr. J.J. Braat
M +31 633 97 09 55

Europese privacywet mogelijk nóg strenger

In Brussel ligt momenteel een wetsvoorstel voor een Europa-brede privacywet. De eerste aanzet voor het voorstel (uit januari 2012) scherpt de bestaande privacy-regels aan. Hoewel de basis-regels niet zo veel zullen veranderen, komt er wel een aantal verplichtingen bij. Het gaat dan met name om interne maatregelen die verantwoordelijken zullen moeten nemen om te zorgen voor betere "privacy compliance". Daarnaast staan er in het voorstel ook hoge boetes op bepaalde overtredingen, tot wel € 1.000.000 of 2% van de wereldwijde omzet. Op 21 oktober 2013 heeft het Europees Parlement er nog een schepje bovenop gedaan en het wetsvoorstel nog verder aangescherpt. Het Parlement heeft een groot aantal wijzigingen op de bestaande concepttekst voorgesteld. In dit stuk worden een aantal van de belangrijkste wijzigingsvoorstellen op een rij gezet.

Boetes tot € 100.000.000 (€ 100 miljoen)

Het parlement wil dat de boetes op overtreding van verplichtingen die in de Europese privacywet staan, nog veel hoger worden. Eerst was het voorstel om maximale boetes voor drie verschillende categorieën overtredingen in te voeren: de eerste was tot € 250.000 of 0,5% van de wereldwijde omzet, de tweede tot € 500.000 of 1% van de wereldwijde omzet en de derde tot € 1.000.0000 of 2% van de wereldwijde omzet. Het Parlement wil de maximale hoogte van een boete nu stellen op € 100.0000.000 (dus 100 miljoen euro). De categorieën verdwijnen dan en de boetes kunnen worden opgelegd voor iedere verplichting die wordt overtreden.

In het oorspronkelijke voorstel stond dat de boetes alleen konden worden opgelegd in geval van opzettelijke of nalatige overtreding van de privacy-regels. Het Parlement wil deze voorwaarde schrappen maar introduceert een lijst met omstandigheden aan de hand waarvan de toezichthouder (in Nederland het College Bescherming Persoonsgegevens) zou moeten beoordelen hoe hoog de boete is die moet worden opgelegd. Voorbeelden van deze omstandigheden zijn de ernst van de overtreding, of er opzettelijk of nalatig is gehandeld, of er sprake was van bijzondere persoonsgegevens en de schade die zich heeft voorgedaan.

De door het Parlement voorgestelde opzet is niet gunstig voor de rechtszekerheid van partijen die zich aan de privacywet moeten houden. Waar in het wetsvoorstel duidelijk was aangegeven welke boete zou gelden voor het overtreden van welke verplichting, zou er met het voorstel van het parlement een "black box" ontstaan over de hoogte van de boete. In potentie heeft iedere verplichting daarmee een sanctie van 100 miljoen euro. Het geeft de toezichthouders erg weinig concrete handvatten mee over hoe ze op een duidelijke manier moeten handhaven. Dit werkt nadelig voor goede privacy compliance.

Standaard privacy verklaring

Het Parlement wil een soort standaard privacy verklaring introduceren die door alle verantwoordelijken zouden moeten worden gehanteerd. Op die verklaring moet de verantwoordelijke organisatie met een groen vinkje of een rood kruis aangeven of het op de daar genoemde punten "compliant" is.

De volgende punten moeten in deze standaard statement komen te staan:

- Er worden niet meer gegevens verzameld dan noodzakelijk voor het doel waarvoor ze worden verzameld (data minimalisatie)
- De gegevens worden alleen gebruikt in overeenstemming met het doel waarvoor ze zijn verzameld
- De gegevens worden niet langer bewaard dan noodzakelijk
- De gegevens worden niet doorgegeven aan commerciële derde partijen
- De gegevens worden niet verkocht of verhuurd
- De gegevens worden niet in onversleutelde vorm opgeslagen.

De eerste drie punten zijn hoe dan ook verplicht, zowel onder huidige als toekomstige wetgeving. De kans is dus zeer klein, zo niet non-existent dat een verantwoordelijke daar "niet aan voldaan" in zou vullen. Als hij dat wel zou doen dan zou hij zich immers blootstellen aan een boete. De in de laatste drie punten genoemde handelingen zijn op grond van de privacywet overigens niet verboden respectievelijk verplicht.

De gedachte achter het invoeren van een deze standaard privacy verklaring is wellicht dat een ieder in één oogopslag kan zien of de verantwoordelijke zich aan een aantal van de essentiële privacy-regels houdt. Deze standaard verklaring vervangt overigens niet de informatieplicht. Onder het wetsvoorstel zullen verantwoordelijken de betrokkenen veel uitgebreider moeten informeren dan onder het huidige recht het geval is. Concreet betekent dit dat de huidige privacy statements veel uitgebreider zouden moeten worden, en dat die privacy statements naast de hiervoor genoemde standaard verklaring aan de betrokkene moet worden getoond.

Privacy risk analyses en PIA uitvoeren

Het Parlement wil een verplichte "risk analysis" invoeren voor ieder voorgenomen gebruik van persoonsgegevens die waarschijnlijk specifieke risico's met zich meebrengt. Het gaat dan bijvoorbeeld om het gebruik van persoonsgegevens van meer dan 5000 mensen, het gebruik van bijzondere persoonsgegevens, profiling, het monitoren van openbare ruimten op grote schaal of als de persoonsgegevens ter beschikking worden gesteld aan een groot aantal mensen. De risk analysis moet na 1 jaar worden herzien óf zodra de scope of het doel van de gegevensverwerking verandert.

Tijdens de risk analysis moet onder meer worden vastgesteld of een "privacy impact assessment" (PIA) nodig is voor de specifieke gegevensverwerking. In de PIA gaat men dieper in op de privacy-risico's en hoe ze moeten worden geadresseerd. De PIA moet iedere twee jaar worden herzien tijdens een "compliance review" waarin wordt nagegaan of de persoonsgegevens nog worden gebruikt overeenkomstig de aanbevelingen van de PIA.

Informeren over het doorgeven van gegevens aan autoriteiten.

Waarschijnlijk in reactie op de PRISM onthullingen wil het Parlement een bepaling introduceren die we wel de "NSA bepaling" kunnen noemen. Die bepaling houdt in dat iedere verantwoordelijke organisatie die een verzoek krijgt van een rechter of overheidsorgaan uit een derde, niet-EU land om inzage te geven in persoonsgegevens, dit verzoek moet melden bij de privacy toezichthouder. De toezichthouder onderzoekt dan of doorgifte is toegestaan en laat de uitkomst van het onderzoek weten aan de verzoekende autoriteit. Als de toezichthouder toestemming geeft moet de verantwoordelijke organisatie vervolgens aan de betrokkenen om wie het gaat doorgeven dat het verzoek is gedaan, dat de toezichthouder toestemming heeft gegeven om de gegevens door te geven en ook of de verantwoordelijke al eerder in de afgelopen 12 maanden persoonsgegevens heeft doorgegeven aan een overheidsinstantie.

Het de betrokkene laten weten of de verantwoordelijke al eerder in de afgelopen 12 maanden persoonsgegevens heeft doorgegeven aan een overheidsinstantie wil het Parlement ook introduceren bij de algemene informatieplicht. Dat houdt in dat de verantwoordelijke ook in de privacy statement zal moeten opnemen of de persoonsgegevens gedurende de afgelopen 12 maanden aan een overheidsinstantie zijn doorgegeven.

Overigens geldt dat niet alleen voor overheidsinstanties in derde landen, het gaat ook om overheidsinstanties in eigen land of andere landen binnen de EU.

legaltree

Uitwisseling binnen concern makkelijker maken

Voorgesteld wordt om uitwisseling van persoonsgegevens in een concern binnen de EU makkelijker te maken. Als het nodig is om dat te doen voor gerechtvaardigde interne administratieve doeleinden, en gezorgd wordt voor een voldoende beschermingsniveau middels interne afspraken, dan mogen de gegevens binnen de EU tussen groepsmaatschappijen worden uitgewisseld.

Security Policy invoeren

Toe te juichen is verder dat het Parlement probeert de verantwoordelijke organisaties meer houvast te geven op het gebied van beveiliging. Dit willen ze doen door een aantal minimumeisen op te nemen voor beveiligingsprocedures en voor de inhoud van het beveiligingsbeleid ("security policy").

De beveiligingsprocedures moeten in ieder geval:

- Er voor zorgen dat de persoonsgegevens alleen maar door bevoegd personeel toegankelijk zijn voor juridisch toegestane doeleinden;
- Zorgen voor bescherming van de opgeslagen of doorgegeven persoonsgegevens tegen ongeautoriseerde vernietiging, wijziging of toegang;
- Zorgen voor het invoeren van een beveiligingsbeleid voor het gebruik van de persoonsgegevens.

Het beveiligingsbeleid moet in ieder geval de volgende punten adresseren:

- De mogelijkheid om de integriteit van de persoonsgegevens te valideren;
- De mogelijkheid om de vertrouwelijkheid, integriteit, beschikbaarheid en weerstand van de systemen en diensten waarmee de persoonsgegevens worden verwerkt te valideren;
- De mogelijkheid om de beschikbaarheid en toegankelijkheid van de persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch beveiligingsincident;
- Als er bijzondere persoonsgegevens worden verwerkt moeten extra beveiligingsmaatregelen worden ingevoerd om te zorgen voor bewustheid van de betrokken risico´s en de mogelijkheid om preventieve, correctieve en mitigerende maatregelen te nemen bij beveiligingsincidenten;
- Een procedure voor het op regelmatige basis testen, beoordelen en evalueren van de effectiviteit van de beveiligingsprocedures en plannen van aanpak om te zorgen voor continue effectiviteit daarvan.

Ook zal in de privacy statement algemene informatie moeten worden opgenomen over de getroffen beveiligingsmaatregelen.

Datalekken niet binnen 24 uur melden maar "zonder vertraging"

In het oorspronkelijke voorstel stond dat een datalek binnen 24 uur zou moeten worden gemeld aan de toezichthouder. Het Parlement wil deze strikte termijn laten varen en in plaats daarvan opnemen dat een datalek "zonder onnodige vertraging" moet worden gemeld. Enerzijds geeft dit verantwoordelijke organisaties meer tijd om een datalek uitvoeriger te onderzoeken, anderzijds zorgt het voor onzekerheid over wat dan een tijdige melding is. Desalniettemin zullen security experts er niet rouwig om zijn als er geen strikte in uren uitgedrukte termijn meer zou worden gehanteerd.

Verder stelt het Parlement voor dat de toezichthouders een register bijhouden van soorten datalekken die zijn gemeld. Dit zal met name bedoeld zijn om de markt daarover te informeren zodat waar nodig het beveiligingsbeleid kan worden aangepast.

Instellen Functionaris voor de Gegevensbescherming

Waar het wetsvoorstel oorspronkelijk inhield dat verantwoordelijken een Functionaris voor de Gegevensbescherming ("FG") moeten instellen (o.a.) als zij meer dan 250 werknemers hadden, stelt het Parlement voor om een FG verplicht te stellen wanneer een verantwoordelijke van meer dan 5000 personen persoonsgegevens verwerkt. Ook stelt het Parlement voor om dit verplicht te stellen wanneer de kernactivitei-

ten van de verantwoordelijke bestaan uit het op grote schaal in systemen verwerken van bijzondere persoonsgegevens, locatiegegevens, werknemersgegevens of gegevens van kinderen. Dit zou betekenen dat partijen zoals ziekenhuizen (o.a. medische persoonsgegevens zijn bijzondere persoonsgegevens), TomTom (die op grote schaal locatiegegevens verwerkt) maar ook bedrijven met veel werknemers en elektronische personeelssystemen verplicht zouden worden een FG in te stellen.

Certificering door CBP

Verder stelt het Parlement voor om verantwoordelijken de mogelijkheid te geven om de toezichthouder te vragen te worden gecertificeerd op "privacy compliance" en zo een "European Data Protection Seal" te ontvangen. In Nederland zou dat moeten worden aangevraagd bij het CBP, deze zou daarvoor een redelijke administratie fee mogen vragen.

Enkele overige voorstellen

Dan nog een aantal andere noemenswaardige wijzigingsvoorstellen kort op een rij:

- **Reactietermijn.** De termijn waarbinnen de verantwoordelijke organisatie moet reageren op verzoeken van de betrokkenen, zou worden verlengd van 1 maand naar 40 dagen.
- **Correctie.** Wanneer de verantwoordelijke op verzoek van de betrokkene persoonsgegevens corrigeert, zou de verantwoordelijke dit ook aan derde partijen aan wie de gegevens zijn doorgegeven moeten laten weten.
- **Inzage via remote access.** Als het feitelijk mogelijk is, mag de verantwoordelijke aan een betrokkene inzage geven door remote access te geven zodat de betrokkene direct bij zijn gegevens kan. Dit kan bijvoorbeeld bij web applicaties waarin persoonsgegevens staan.
- **Toestemming.** Als het gebruik van persoonsgegevens wordt gebaseerd op toestemming en de betrokkene wil zijn toestemming intrekken, dan zou de verantwoordelijke moeten laten weten of de betrokkene daardoor geen gebruik meer zal kunnen maken van de door de verantwoordelijke aangeboden diensten.
- **Privacy compliance in jaarverslag.** In het jaarverslag van bedrijven zou moeten worden opgenomen welke maatregelen de verantwoordelijke heeft genomen om te zorgen voor "privacy compliance".
- **Privacy by design bij aanbestedingen.** Bij aanbestedingen zou "privacy by design" een eis moeten worden wanneer persoonsgegevens worden verwerkt door de inschrijver.
- **Profilen.** Het "profilen" van mensen aan de hand van hun persoonsgegevens, als dat uitsluitend op basis van bijzondere persoonsgegevens gebeurt, zou verboden worden.

Volgende stap

De Europese Commissie en het Europees Parlement hebben nu hun zegje gedaan over de nieuwe privacywet. Nu moeten zij met de regeringsleiders onderhandelen over de tekst van de wet. De druk wordt steeds groter, omdat het de bedoeling is om voor de volgende Europese parlementsverkiezingen in mei 2014 tot overeenstemming te komen. Het ziet er alleen naar uit dat de partijen nog ver uit elkaar liggen dus het zal er om spannen.

U kunt zich aanmelden voor de Legaltree Privacy Update door een mail te sturen naar bieneke.braat@legaltree.nl.

Privacy begrippen

“Verantwoordelijke”: dit is de organisatie die verantwoordelijk is voor het gebruik van persoonsgegevens. Het gaat dan meestal om een bedrijf, een non-profit instelling of een overheidsinstantie.

“Betrokkene”: dit is de persoon wiens persoonsgegevens worden gebruikt.

“Verwerken”: dit zijn vrijwel alle handelingen met persoonsgegevens zoals het bekijken, kopiëren, opslaan, doorsturen, afschermen of verwijderen.

“Datalek”: een incident waarbij persoonsgegevens vernietigd worden of ter beschikking komen van een onbevoegde derde partij.

Auteur van deze Legaltree Update, Bieneke Braat is advocaat sinds 2001 en specialist op het gebied van IT-recht, privacy, softwarebescherming en contractenrecht. In 2009 rondde zij met succes de Grotius specialisatieopleiding Informaticarecht af. Bieneke heeft ruime ervaring met het opstellen, beoordelen en uitonderhandelen van (IT-)contracten en algemene voorwaarden, privacyvraagstukken, bescherming van software, ecommerce eisen voor websites en onrechtmatige uitingen op het internet. Op regelmatige basis publiceert Bieneke en geeft zij lezingen over onderwerpen op het gebied van IT-recht en privacy. Bieneke staat zowel kleine als (middel) grotere ondernemingen bij.

mr. J.J. Braat
Rapenburg 83
2311 GK Leiden
T +31 70 215 92 21
F +31 70 215 92 23
M +31 633 97 09 55
bieneke.braat@legaltree.nl

Quality is personal

Onder het motto ‘Quality is Personal’ heeft Legaltree een geheel eigen visie en wijze van werken ontwikkeld. Daarbij staat de aandacht voor - en het ontspannen contact met - u als inspirerende cliënt centraal. .