Mr. F.C. van der Jagt[1]

Privacytoezichthouder krijgt tanden: hoge privacyboetes en meldplicht datalekken op komst

Bb 2015/55

Eind mei heeft de Eerste Kamer het wetsvoorstel[2] *waarmee hoge boetes bij niet-naleving van de Wet bescherming persoonsgegevens worden geïntroduceerd, aangenomen. Ook zijn bedrijven binnenkort verplicht om datalekken aan de privacytoezichthouder te melden en in bepaalde gevallen ook aan de personen van wie gegevens gelekt zijn. Niet-naleving van de privacywetgeving kan leiden tot een bestuurlijke boete van maximaal € 810.000,- of – indien de toezichthouder daar aanleiding toe ziet – zelfs tot 10% van de jaaromzet van de onderneming. Daarnaast krijgt het College bescherming persoonsgegevens na inwerkingtreding van het wetsvoorstel een nieuwe naam en zal voortaan de Autoriteit persoonsgegevens heten.*

1. Achtergrond

Door de toegenomen digitalisering en de opkomst van social media worden steeds meer persoonsgegevens verwerkt. De bescherming van deze gegevens staat echter bij veel organisaties nog niet bovenaan de prioriteitenlijst. Privacycompliance verdient desalniettemin de aandacht, omdat nieuwe strengere regels op komst zijn. Daarnaast kan, door het voeren van een adequaat privacybeleid, reputatieschade worden voorkomen. Steeds vaker verschijnen immers berichten in de media over privacygevoelige informatie die publiek toegankelijk is geworden door een hack of een lek in de beveiliging.

Door de invoering van de nieuwe wetgeving worden hogere privacyboetes en een specifieke meldplicht voor datalekken geïntroduceerd. Door de uitbreiding van de boetebevoegdheid wordt uitvoering gegeven aan het regeerakkoord van 2012, waarin dit expliciet was opgenomen. Het beboeten van het niet-naleven van de privacywetgeving, waaronder de meldplicht datalekken, versterkt het toezicht op en de handhaving van de naleving van de Wet bescherming persoonsgegevens. Hierbij verschuift de focus van herstelsancties, zoals de last onder dwangsom die momenteel vaak door het College bescherming persoonsgegevens (hierna: CBP) wordt opgelegd, naar sanctionering via bestuurlijke beboeting.

Met de meldplicht datalekken beoogt de regering niet alleen de beperking van de gevolgen van datalekken voor de betrokkenen, maar ook de versterking van het niveau van beveiliging van persoonsgegevens. Uit de beveiligingsincidenten kan lering worden getrokken, waardoor deze in de toekomst voorkomen kunnen worden. Het vertrouwen van burgers in de digitale verwerking van hun persoonsgegevens zal hierdoor worden vergroot.

2. Meldplicht datalekken en verplicht intern overzicht

Door de nieuwe wetgeving worden bedrijven verplicht om bij de toezichthouder melding te maken van iedere inbreuk op de beveiliging van persoonsgegevens *"die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens"* (art. 34a lid 1 Wbp nieuw). Ook indien versleutelde gegevens worden gelekt, dient een melding bij het CBP plaats te vinden. De achtergrond daarbij is dat versleutelde gegevens juist vaak extra gevoelige gegevens zijn, zoals creditcard- en bankgegevens. Het CBP zal jaarlijks een overzicht van het aantal datalekken publiceren. Bedrijven moeten bovendien zelf een intern overzicht gaan bijhouden van deze inbreuken.

Daarnaast moeten de personen van wie de persoonsgegevens zijn gelekt, hiervan op de hoogte worden gebracht indien *"de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer"* (art. 34a lid 2 Wbp nieuw). De algemene meldplicht zal niet of slechts deels van toepassing zijn op bedrijven die op grond van specifieke wetgeving al een meldplicht kennen. Hierbij kan gedacht worden aan telecomproviders en financiële ondernemingen.

3. Boetes

Het CBP kan door de aanpassing van de Wbp hoge boetes gaan opleggen voor de overtreding van een groot aantal algemene verplichtingen (zie aangepast art. 66 Wbp).

Op dit moment is deze bevoegdheid beperkt tot een aantal specifieke administratieve bepalingen, zoals het aanmelden van een gegevensverwerking bij het CBP. Daarnaast is de hoogte van de mogelijk op te leggen boete laag (€ 4500,-) en wordt deze in de praktijk niet opgelegd. Vaak kiest het CBP ervoor om een last onder dwangsom op te leggen, waarmee het bedrijven dwingt om alsnog privacycompliant te handelen. In 2011 legde het CBP bijvoorbeeld aan verschillende vervoersbedrijven een last onder dwangsom op, omdat zij reisgegevens van studenten te lang en ongeanonimiseerd bewaarden. Hierdoor was het mogelijk om het reisgedrag van studenten te volgen. De bedrijven werden via de last gedwongen om de gegevens te vernietigen en kortere bewaartermijnen in te voeren. Ook Google kreeg meerdere malen met een last onder dwangsom te maken. Zo werd aan Google in 2011 een last onder dwangsom van € 1 miljoen voor het ongeoorloofd verzamelen van gegevens door Google's Street View-auto's opgelegd. Sinds december 2014

1 Friederike van der Jagt is privacyrechtadvocaat bij Stibbe. Deze bijdrage is gebaseerd op eerdere blogberichten van haar hand op www.stibbeblog.nl. Dit artikel werd door de auteur geschreven en aangeleverd met de bedoeling het te laten verschijnen in nr. 15 van Bedrijfsjuridische berichten. Door omstandigheden werd het artikel later geplaatst.

2 *Kamerstukken I* 2014/15, 33662, A.

hangt Google een last onder dwangsom van maximaal € 15 miljoen boven het hoofd, omdat Google volgens het CBP gegevens van internetgebruikers combineert om hen persoonlijke advertenties te kunnen tonen, zonder de gebruikers hierover adequaat te informeren.
Waarom dan toch boetes, als de last onder dwangsom ook tot privacycompliancy kan leiden? Hiervoor zijn verschillende redenen aanwezig. Allereerst heeft het CBP te maken met een beperkte onderzoekscapaciteit. Daarom richt het zich met name op structurele en ernstige overtredingen die veel mensen treffen en waarbij door de inzet van handhavingsmiddelen een verschil kan worden gemaakt. Daarbij stelt het CBP elk jaar een agenda op met thema's waarop het zich zal focussen. Van een last onder dwangsom gaat weinig afschrikkende werking uit, zeker nu steeds een herstelmogelijkheid wordt geboden. Tel daarbij op dat geen hoge boetes kunnen worden opgelegd en het is duidelijk dat de kans, dat bij een commerciële afweging de privacybelangen het onderspit delven, vergroot wordt. Juist nu het verwerken van persoonsgegevens een steeds belangrijker onderdeel vormt van de dienstverlening van bedrijven, acht de overheid het van belang dat aan de bescherming van deze gegevens meer belang wordt gehecht.
Het wetsvoorstel breidt de boetebevoegdheid van het CBP dan ook uit tot de handhaving van een groot aantal algemene verplichtingen van de Wbp, zoals de verplichting om persoonsgegevens adequaat te beveiligen, de informatieplicht en de naleving van het verbod op de verwerking van bijzondere persoonsgegevens. Er worden boetecategorieën ingevoerd die variëren van € 20.250,-, voor relatief lichte overtredingen, tot maximaal € 810.000,- voor opzettelijke en herhaaldelijke overtredingen, die grote maatschappelijke gevolgen kunnen hebben. Voor wat betreft de hoogte van de boetes wordt aangesloten bij de boetecategorieën zoals neergelegd in art. 23 Wetboek van Strafrecht.
Voor rechtspersonen wordt de hoogte van de boete geflexibiliseerd: dit betekent dat indien de hoogste boetecategorie van € 810.000,- niet tot een passende bestraffing leidt, het CBP een boete tot maximaal 10% van de jaaromzet van de rechtspersoon mag opleggen. Opmerkelijk (en voor de praktijk prettig) is dat de boete voor het niet aanmelden van een gegevensverwerking bij het CBP, die tot nu toe als een van de weinige bepalingen van de Wbp wel beboetbaar was, zal komen te vervallen.
Van belang is om op te merken dat het CBP eveneens bevoegd blijft om bestuursdwang toe te passen of een last onder dwangsom op te leggen (zie art. 65 Wbp).

4. Bindende aanwijzing

Boetes mogen pas worden opgelegd nadat het CBP een bindende aanwijzing aan de onderneming heeft gegeven. Deze verplichting vloeit voort uit het advies van de Raad van State,[3] die van mening is dat gelet op de 'vage' normen van de Wbp, het ongewenst is dat zonder voorafgaande waarschuwing een boete wordt opgelegd. Het CBP kon zich echter in dit deel van de wet niet vinden: het voelt zich 'tandeloos' en meent dat het hierdoor niet snel en effectief zal kunnen optreden. De vrees bestaat dat bedrijven en organisaties zich hierdoor niet geroepen zullen voelen om de wet na te leven. Deze vrees is niet geheel gegrond: in gevallen waarin sprake is van opzet of ernstig verwijtbare nalatigheid, blijft een bindende aanwijzing achterwege en kan het CBP direct een boete opleggen. Bij ernstige nalatigheid moet worden gedacht aan grof, aanzienlijk onzorgvuldig, onachtzaam dan wel onoordeelkundig handelen. Daarbij geldt dat indien eenzelfde soort overtreding meerdere malen heeft plaatsgevonden, sneller sprake zal zijn van nalatigheid. Voor het aantonen van opzet is het niet nodig dat een overtreding willens en wetens wordt begaan. Aansluiting dient te worden gezocht bij de situatie die in het strafrecht als *voorwaardelijk opzet* wordt aangemerkt. Dat betekent dat ook bij die gevallen waarin een overtreder redelijkerwijs wist of had moeten weten dat zijn handelen of nalaten tot ernstige nadelige gevolgen voor de privacy van de betrokkenen kon leiden en deze gevolgen zich verwezenlijken, direct een boete kan worden opgelegd.
Bij het geven van een bindende aanwijzing kan een termijn worden opgelegd waarin de overtreder de aanwijzing moet opvolgen. De overtreder kan tegen dit besluit bestuursrechtelijke rechtsmiddelen aanwenden, zoals het indienen van een bezwaarschrift. Het indienen daarvan heeft echter geen schorsende werking. Wel kan de overtreder de voorzieningenrechter vragen om op grond van art. 8:81 Awb de aanwijzing te schorsen of om een andere voorziening te treffen.

5. Richtsnoeren

Vanwege het grote aantal open normen in de Wbp moeten bedrijven weten wat er van hen verwacht wordt. Overeenkomstig het *lex certa*-beginsel is het van belang dat de eisen waaraan een bedrijf moet voldoen en de gevolgen die voortvloeien uit niet-naleving, voldoende duidelijk, voorzienbaar en kenbaar zijn. Wanneer is bijvoorbeeld, in het licht van een datalek, sprake van *'een aanzienlijke kans'* op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens? Hoe moet het verplichte interne register eruit komen te zien? En welke informatie moet precies worden verschaft aan het CBP bij een datalek? Deze zaken zullen nader worden uitgewerkt in specifieke richtsnoeren van het CBP. Deze duidelijkheid is ook nodig, omdat anders de kans bestaat dat bij de uitvoering van de meldplicht datalekken een bedrijf, om boetes te voorkomen, zekerheidshalve alle datalekken meldt aan zowel het CBP als de personen van wie de gegevens zijn gelekt. Het risico is dat dan 'meldingsmoeheid' optreedt. Een vergelijking kan worden gemaakt met de cookie-banners die veelal op websites verplicht zijn. Veel websitegebruikers geven zonder de informatie te lezen toestemming voor het plaatsen van cookies. Hierdoor wordt het doel van de regels – het vergroten van de privacybescherming van de websitegebruikers – eerder ondermijnd

3 Advies W03.13.0464/II, Raad van State d.d. 19 februari 2014, *Stcrt.* 2014, nr. 34523.

dan behaald. Het is derhalve van belang dat de richtsnoeren klaar zijn op het moment van de inwerkingtreding van de wet. Daarom treedt de wet niet direct in werking, maar naar verwachting op 1 januari 2016.

6. Verhouding met voorstel voor Europese Privacyverordening

Op Europees niveau wordt momenteel gewerkt aan een herziening van de uit 1995 daterende Europese Privacyrichtlijn. In 2012 presenteerde de Europese Commissie daartoe een voorstel voor een Europese Privacyverordening.[4] In tegenstelling tot de huidige Privacyrichtlijn, heeft de Privacyverordening rechtstreekse werking. Dit betekent dat de Privacyverordening niet hoeft te worden omgezet in nationale wetgeving, maar rechtstreeks aan bedrijven verplichtingen oplegt. Het voorstel introduceert, naast een meldplicht in geval van datalekken, ook hoge boetes – maximaal € 1 miljoen of 2% van de wereldwijde omzet van een onderneming – in geval van niet-naleving van de privacywetgeving. Het Europees Parlement heeft meer dan 4.000 amendementen op het Commissievoorstel ingediend en de boetes opgeschroefd tot € 100 miljoen respectievelijk 5% van de wereldwijze omzet van een onderneming.[5] Inmiddels heeft de Raad van Ministers ook zijn standpunt bepaald: de Raad sluit aan bij de boetes zoals voorgesteld door de Europese Commissie.[6] De komende maanden zal op Europees niveau overleg plaatsvinden om tot een akkoord te komen. Indien de Europese Privacyverordening wordt aangenomen, start een implementatieperiode van twee jaar. Gedurende die periode moet de Nederlandse wetgeving aan de nieuwe Verordening worden aangepast. Nu de Verordening rechtstreekse werking heeft, betekent dit dat de Wet bescherming persoonsgegevens, en dus ook de daarin opgenomen boetes en de meldplicht datalekken, zal worden ingetrokken.

7. Nieuwe naam voor het CBP: Autoriteit persoonsgegevens

Het CBP krijgt een nieuwe naam en zal in de toekomst als 'Autoriteit persoonsgegevens' door het leven gaan. Dit is gedaan om aan te sluiten bij de terminologie van de nieuwe Europese Privacyverordening en om de bestaande verwarring met het Centraal Planbureau (CPB) uit de wereld te helpen.

8. Tot slot: tijd voor actie

Voor bedrijven is het belangrijk om te bezien hoe het staat met de privacycompliance en privacy awareness binnen hun organisatie. In kaart moet worden gebracht welke persoonsgegevens voor welke doeleinden verwerkt worden en of deze gegevens goed beveiligd zijn. Ook is het aan te raden om te inventariseren wie er intern betrokken kunnen en moeten zijn om een datalek tegen te gaan. Want ook indien de Nederlandse wetgeving op den duur wordt ingetrokken, zal vanuit de nieuwe Europese Privacyverordening een meldplicht datalekken gelden. Het is verstandig om afspraken te maken over het bijhouden van het verplichte interne overzicht van datalekken en het daadwerkelijk verrichten van de meldingen bij de toezichthouder. Van belang is dat eenieder op de werkvloer zich bewust is van de basisprincipes van de privacyregels en hier ook naar handelt. Met de nieuwe boetes op komst, is dit dan ook het moment om privacycompliance-trainingen of informatiebijeenkomsten te (laten) geven over dit belangrijke onderwerp.

4 Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), 25 januari 2012, COM(2012)11 final.

5 Wetgevingsresolutie van het Europees Parlement van 12 maart 2014 over het voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

6 Raad van de Europese Unie, Nota voorbereiding algemene oriëntatie, d.d. 11 juni 2015, Interinstitutioneel dossier 2012/0011 (COD), 9565/15.