

Verslag internetconsultatie wetsvoorstel meldplicht datalekken (wijziging Wet bescherming persoonsgegevens)

Het conceptwetsvoorstel heeft van 20 december 2011 tot en met 29 februari 2012 open gestaan voor reacties. De geconsulteerde versie bevatte naast de meldplicht voor datalekken tevens een regeling voor een verruiming van het gebruik van camerabeelden gemaakt met particuliere beveiligingscamera's van burgers en bedrijven ten behoeve van de opsporing van strafbare feiten. Dit onderdeel van het wetsvoorstel is naar aanleiding van het advies van de Raad van State afgesplitst en zal op termijn in een afzonderlijk wetsvoorstel worden ondergebracht.

De reacties die zijn binnengekomen concentreren zich vooral op de omschrijving van de voorgestelde meldplicht. De respondenten wijzen erop dat onduidelijkheid in de omschrijving kan leiden tot onnodige meldingen. Dit, omdat verantwoordelijken niet het risico op een boete willen lopen. De regering heeft, in de memorie van toelichting, de meldplicht verduidelijkt. In par. 3.2.2 van de memorie van toelichting is het beslismodel voor artikel 34a, eerste en tweede lid, van de Wet bescherming persoonsgegevens (Wbp) verder uitgewerkt. De organisatie die verantwoordelijk is voor de verwerking van persoonsgegevens zal bij inbreuken op de beveiliging van die gegevens aan de hand van de specifieke omstandigheden van het geval met behulp van dit beslismodel kunnen beoordelen of een melding aan de toezichthouder en in voorkomend geval ook aan de betrokkenen moet worden gedaan.

Enkele respondenten vrezen dat de in artikel 34a, eerste en tweede lid, gehanteerde maatstaf "onverwijld" de verantwoordelijke te weinig tijd laat voor een goede beoordeling. In de toelichting is opgemerkt dat deze maatstaf de voorkeur heeft boven een gefixeerde tijdslimiet, en dat deze de verantwoordelijke enige gelegenheid geeft om onderzoek te doen naar de inbreuk, te overwegen welke maatregelen hij aanbeveelt en de manier waarop hij communiceert met Cbp en betrokkenen. De maatstaf "onverwijld" wordt gehandhaafd om de aansluiting bij de meldplicht van artikel 11.3a Telecommunicatiewet te handhaven, waarmee een Europese richtlijn is geïmplementeerd (artikel 4 richtlijn 2002/58).

Er moet melding worden gemaakt van een "inbreuk op de beveiligingsmaatregelen, bedoeld in artikel 13". Als er geen maatregelen, bedoeld in artikel 13, zijn genomen, geldt de meldingsplicht dan niet? Het treffen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking is een –bestaande– wettelijke verplichting. Omdat de beveiligingsmaatregelen niet altijd afdoende zijn, wordt een meldplicht voor datalekken voorgesteld, om de bewustwording te vergroten en de nadelige gevolgen van een datalek zoveel mogelijk te minimaliseren. Indien een verantwoordelijke wordt geconfronteerd met een datalek zal hij zich niet snel verweren door te stellen dat hij het datalek niet hoeft te melden omdat hij in het geheel geen beveiligingsmaatregelen heeft getroffen. Daarmee beschadigt hij zijn eigen reputatie en maakt hij zich kwetsbaar voor schadeclaims.

Enkele respondenten vragen naar de samenhang met bestaande en aangekondigde meldplichten. In par. 2.4 van de memorie van toelichting is een beschouwing opgenomen over de verhouding van de meldplicht datalekken tot andere meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector.