

Wat de nieuwe privacywetgeving betekent voor etailers

07-01-2016 12:26

Een nieuw jaar betekent ook: nieuwe privacywetgeving. In 2015 hebben etailers al het nodige zien veranderen op het gebied van bescherming van klantgegevens, per 1 januari 2016 zijn er weer wat nieuwe wijzigingen van kracht. De belangrijkste veranderingen voor webwinkels op een rijtje.

Meldplicht datalekken

Misschien wel de meest omstreden verandering, is de plicht om datalekken en andere veiligheidsincidenten te melden, de zogeheten 'meldplicht datalekken'. Zowel werkgeversorganisatie VNO-NCW, MKB-Nederland als brancheorganisatie Thuiswinkel.org noemen de invoering van de meldplicht 'ondoordacht'. Zo is er volgens Thuiswinkel.org nog helemaal niet onderzocht of zo'n meldplicht wel echt leidt tot minder problemen als gevolg van beveiligingsincidenten. Bovendien zullen de lasten voor webwinkels alleen maar groter worden, denkt de brancheorganisatie. Zo zijn er nog tal van vragen en onduidelijkheden: welke lekken moeten nou wel en niet gemeld worden? En bij wie moet dat gebeuren? Alleen bij toezichthouder Autoriteit Persoonsgegevens (het voormalige CBP) of ook aan de klanten van wie gegevens gelekt zijn? En wat gebeurt er als etailers een lek niet melden?

Allereerst: de Autoriteit Persoonsgegevens spreekt van een datalek als er een beveiligingsincident optreedt waarbij persoonsgegevens verloren gaan. Als een etailer vaststelt dat er een datalek is, moet hij zelf inschatten of hij het moet melden en bij wie. Als het gaat om gegevens van 'gevoelige aard', dan moet het lek gemeld worden bij de toezichthouder. Inloggegevens en financiële informatie, maar ook gegevens over bijvoorbeeld levensovertuiging zijn voorbeelden die daar onder vallen. Als de kans groot is dat de gelekte informatie direct nadelige gevolgen heeft voor de shopper, moet dit ook bij hem gemeld worden. Dit is bijvoorbeeld het geval als de gelekte informatie reputatieschade of identiteitsfraude tot gevolg kan hebben.

Wat te doen?

Webwinkels werken veel samen met derden, zoals hostingdiensten en datacenters. Die partijen verzorgen vaak de bewerking van persoonsgegevens, maar de etailer zelf blijft daarvoor wettelijk verantwoordelijk. Daarom raadt adviesbureau Webwinkelrecht aan de overeenkomsten die webshops met derden hebben aan te passen naar aanleiding van de wetswijziging. Daarin moeten duidelijke afspraken staan hoe webwinkel en partner elkaar ondersteunen in geval van een lek.

Voor etailers met een grotere organisatie is er nog een belangrijk artikel toegevoegd aan de Wet bescherming persoonsgegevens. Klantgegevens moeten sinds 1 januari niet meer alleen technisch beschermd worden tegen toegang van derden. Ook binnen een bedrijf mag de informatie alleen toegankelijk zijn voor de afdelingen en medewerkers voor wie die bedoeld is. Onzorgvuldig omgaan met informatie binnen een bedrijf, kan tot hogere boetes leiden.

Boetes

Verder wordt het boetebeleid aangescherpt. Webwinkels die zich voorheen niet aan de privacyregels hielden, kwamen daar tot en met 31 december vaak nog vrij ongeschonden vanaf. Het College Bescherming Persoonsgegevens (CBP) had weinig boetebevoegdheid. Sinds 1 januari heeft het CBP de naam veranderd in Autoriteit Persoonsgegevens, en die gaat een stuk sneller boetes uitdelen. Voor vrijwel iedere overtreding van de wet kan de Autoriteit boetes opleggen, die kunnen oplopen tot 820 duizend euro. Voor grote webwinkels, waarvoor dat geen passend boetebedrag is, kan dat zelfs oplopen tot tien procent van de jaaromzet. Vaak zal de toezichthouder eerst een waarschuwing geven, maar bij ernstige gevallen kan direct een boete worden gegeven.

Dat de kans op een datalek bij webshops reëel is, bleek wel uit een onderzoek van het CBP uit 2014. Daaruit kwam naar voren dat 86 procent van de Nederlandse webwinkels geen versleutelde verbinding heeft om het onderscheppen van persoons- en inloggegevens te voorkomen. Brancheorganisatie Thuiswinkel.org stelt zogeheten SSL-beveiliging sinds vorig jaar verplicht voor zijn leden, maar daarbij gaat het om slechts zo'n veertienhonderd, vooral grotere etailers. In totaal zijn er in Nederland naar schatting zo'n vijftigduizend tot 75 duizend webwinkels.

Uit een [infographic](#) die eerder op RetailWatching verscheen, bleek al dat een datalek meer schade oplevert dan alleen door boetes.