# Hotelsector meer en meer onderhevig aan cybercrime

## Het belang van goed risicomanagement en AVG-compliancy

Hotels worden steeds afhankelijker van geautomatiseerde en gedigitaliseerde systemen. Om de beleving van de gasten te optimaliseren, is digitalisering een veelal gekozen methode. Potentiële gasten oriënteren zich veelal online, waar zij een reservering plaatsen en betalen. Online profilering is voor hotels dan ook steeds belangrijker geworden. Het vindbaar zijn tussen alle concurrenten en 24-7 online bereikbaarheid voor reserveringen: de noodzaak van een goed werkende IT-omgeving is van levensbelang voor de continuïteit van een hotel.

Als u dit goed heeft geregeld, vergroot u de kans op goede reviews. En deze profilering kan van doorslaggevend belang zijn om een potentiële gast te doen verleiden om een reservering te maken. Maar naast de vele voordelen van de digitalisering is het goed om ook eens stil te staan bij de nadelen.

> ‘Hotels moeten per 25 mei voldoen aan de AVG. Daarbij draait het niet alleen om de kans op boetes, maar juist ook om het beste willen voor je klant. AVG-compliancy is ook goed ondernemersschap.’

## Malware en hacks: financiële en reputatieschade

Een ‘mooi’ voorbeeld is de hack bij Seehotel Jaegerwirt (Oostenrijk). Door een ‘lock down’ was het voor de 180 gasten van het hotel en de medewerkers onmogelijk om de kamer nog te betreden. De hackers dwongen het hotel een som van EUR 1.500 in bitcoins te betalen. Financieel en qua reputatie een klap, en de continuïteit van het hotel kwam hierdoor zwaar onder druk te staan.

Ook het Hilton hotel publiceerde einde 2015 het bericht getroffen te zijn door malware. Bij deze vorm van cybercrime verstoort men computersystemen om gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. In het geval van Hilton waren de gegevens van de betaalpassen het doelwit.

Beide voorbeelden geven aan dat ook hotels voorbereid dienen te zijn op cybercrime.
Per 25 mei 2018 maakt de sector zich op voor de aankomende **Algemene Verordening Gegevensbescherming (AVG)**.

## De AVG komt er aan: 11 risicomanagementhandvatten

Door volledig compliant te zijn aan deze Europese privacywetgeving, verkleint u ook de kans op cybercrime. In grote lijnen zijn de grootste veranderingen t.o.v. de huidige privacywetgeving: versterking en uitbreiding van privacyrechten, meer verantwoordelijkheden bij het hotel zelf, aan kunnen tonen dat het hotel voldoet aan de AVG, betere samenwerking toezichthouders en hogere boetes.

Hierbij treft u elf handvatten, gezien vanuit risicomanagement, om u goed te kunnen voorbereiden op de Algemene Verordening Persoonsgegevens.

### 1. Het belang van de AVG

Hotels die falen in het naleven van de AVG riskeren boetes die kunnen oplopen tot 20 miljoen euro of 4 procent van de jaarlijkse wereldwijde omzet. Daarnaast loopt u risico op reputatieschade. Voldoen aan de AVG draait echter niet alleen om compliance, maar vooral om het verhogen van de bescherming van persoonsgegevens. Een proactieve aanpak zorgt er voor dat u aan de meest essentiële eisen voldoet.

>>

Empower Results®

**2. De AVG gaat over (persoons)gegevens**
Onder persoonsgegevens wordt alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon verstaan. De informatie dient direct of indirect (door middel van herleiding) te kunnen leiden tot identificatie van een natuurlijk persoon. Voor de hand liggende persoonsgegevens zijn iemands naam, adres, woonplaats, BSN-nummer en (e-mail)adres. Minder voor de hand liggende persoonsgegevens zijn kentekengegevens en IP-adressen.

**3. Samenwerken met andere afdelingen**
Zorg er in de eerste plaats voor dat de privacy- en gegevensbescherming binnen uw hotel is verankerd op het hoogste niveau. Daarnaast wil geen enkele afdeling de AVG volledig op zijn bordje krijgen. Het voldoen aan de AVG vergt nauwe samenwerking tussen de afdelingen.

**4. Zelf verantwoordelijk voor implementatie**
De wet maakt geen melding van technologieën of specifieke processen die uw hotel moet gebruiken om de bescherming van persoonsgegevens te leveren. Elk hotel moet haar eigen plan opstellen om ervoor te zorgen dat er aan de AVG wordt voldaan. Aon's consultants merken in de praktijk dat veel hotels weten dat ze iets moeten doen, maar niet goed kunnen inschatten welke acties wanneer, hoe en door wie genomen moeten worden. Neem daarom, indien nodig, contact op met Aon om ervoor te zorgen dat de implementatie goed verloopt.

**5. Voer een impactanalyse uit**
Voer een impactanalyse uit om uw privacyrisico's te identificeren. Hieruit volgen de stappen die u moet nemen om middels passende technische en organisatorische maatregelen te voldoen aan de AVG. Dit wordt ook wel een data privacy impact analyse genoemd (DPIA).

**6. Nieuwe grondslagen, transparantie en inzagerechten**
Uw hotel moet niet alleen bewijzen dat zij toestemming heeft verkregen om gegevens van een persoon op te slaan en te gebruiken, maar ook elektronische kopieën van privérecords op aanvraag aan kunnen bieden aan degenen die informatie over zichzelf willen inzien. Daarnaast moet u kijken naar de grondslagen waarop u de persoonsgegevens tot op heden heeft verwerkt en nagaan of deze onder de AVG moeten veranderen.

**7. Bewaartermijn persoonsgegevens**
Er is een bewaartermijn voor de opgeslagen persoonsgegevens. Gegevens mogen niet langer bewaard worden dan noodzakelijk. Naast het inregelen van een proces en het technisch realiseren van een (automatische) verwijderfunctie, is het afstemmen met de afdeling Legal over de bewaartermijnen noodzakelijk.

**8. Overdraagbaarheid, inzage, correctie en vergeetrecht**
Er dienen procedures te zijn voor overdraagbaarheid van persoonsgegevens, inzage in gegevens, gegevenscorrectie en de mogelijkheid om vergeten te worden. Zodra een persoon verzoekt om een van deze activiteiten, moet er direct geleverd kunnen worden.

**9. Zorg voor een goed privacybeleid**
Veel van de te nemen maatregelen gaan over het aanpassen van systemen, processen en juridische afspraken met gasten en leveranciers. Hoe er invulling wordt gegeven aan het privacybeleid wordt voor een groot deel bepaald door hoe medewerkers er mee omgaan. Geef hier daarom continu aandacht aan en zorg dat u daadwerkelijk kunt nakomen wat in het beleid aan stakeholders wordt beloofd.

**10. Train uw personeel**
Binnen veel hotels zijn medewerkers niet op de hoogte van wat een datalek is en/of weten niet bij wie ze dit moeten melden. Training is daarom essentieel. Als u uw privacybeleid moet wijzigen, doe het nu en zorg ervoor dat uw medewerkers hun individuele verantwoordelijkheid begrijpen. Door te voldoen aan het beleid beschermen ze hun eigen persoonsgegevens (en is het netwerk veiliger), die van relaties alsook alle data van het hotel.

**11. Stel, indien nodig, een Functionaris Gegevensbescherming aan**
Een Functionaris Gegevensbescherming (FG) moet deskundige kennis hebben van wetgeving inzake gegevensbescherming en is verantwoordelijk voor de naleving van de AVG. Een bestaande medewerker kan dienen als de FG, op voorwaarde dat hij de vereiste expertise heeft en de rol niet in strijd is met een andere rol die hij in het hotel heeft.

## Wij helpen u graag succesvol te ondernemen

Indien u graag meer informatie wilt hebben, neem dan contact op met:

**Perry Steenvoorden**
06 523 378 96
perry.steenvoorden@aon.nl

**Myriam Smit**
06 526 578 38
myriam.smit@aon.nl

**aon.nl/cyber**



Empower Results®