Cloud & AVG

PvIB Thema avond 18 april 2019

Terugkoppeling Case Klant en leveranciers kant

PvIB Platform voor InformatieBeveiliging

Inleiding

Deze presentatie geeft een overzicht van de door de aanwezigen op de thema avond Cloud en AVG van 18 april 2019 genoteerde antwoorden op de vragen rondom risico's en verantwoordelijkheden wanneer je als klant je (persoonsgegevens) data bij een externe Cloud Servicer Provider (CSP) in de Cloud laat hosten.

De beide Cases worden nog eens herhaald, waarna de antwoorden op de vragen zoals die door de aanwezigen zijn genoteerd worden getoond.

Hier en daar is een kleine tekstuele aanpassing voor de leesbaarheid gedaan.

Verwachtingsmanagement:

Er worden in deze presentatie uitsluitend door de aanwezigen gegeven antwoorden getoond.

Deze presentatie is uitsluitend bedoeld om de aanwezigen te laten zien wat er uit de groepen is gekomen en misschien als reminder te dienen, wanneer de lezer zelf in een outsourcingtraject betrokken is.

Deze presentatie geeft geen weergave van de mening van het PvIB. Daarvoor zou diepgaander onderzoek nodig zijn.

PvIB Platform voor InformatieBeveiliging

De case: Klantkant

U bent werkzaam in een groot bedrijf in de retailsector, genaamd ‘PrivComp’.

Retail is de verzamelnaam voor bedrijven die goederen en diensten direct aan consumenten verkopen. Retail wordt vaak detailhandel genoemd.

PrivComp is gespecialiseerd in het inkopen en verkopen van tweedehands kleding in Europa. PrivComp heeft een 500tal medewerkers in dienst en een 40tal franchiseondernemers. PrivComp heeft 80 eigen vestigingen in Europa.

PrivComp heeft tot op heden altijd, vanuit het eerste begin, haar automatisering zelf gedaan. Ze draaien inmiddels een groot server park in Nederland. De volledige KA-omgeving, de boekhouding en ERP systemen worden intern gehost.

De omslag in denken kwam een paar jaar geleden toen PrivComp een klantenkaart introduceerde èn gebruik ging maken van een externe partij die pinbetalingen regelt.

Na uitgebreid onderzoek is besloten de stap naar de Cloud te gaan maken. PrivComp wil zich namelijk focussen op zijn core-business, het inkopen en verkopen van tweedehands kleding. U maakt zich echter wel zorgen over de enorme hoeveelheid klantdata die u heeft en voor zowel inkoop- als marketing doeleinden gebruikt. Naast die doelen bevat uw klantendatabase ook veel persoonsinformatie zoals onder andere NAW-gegevens, emailadressen, wachtwoorden voor de klantenportal en bankgegevens.

Aan u als groep is de vraag om duidelijk te krijgen welke risico’s u als klant van de Cloud Service Provider (CSP) denkt te lopen als het gaat om het compliant zijn en blijven aan de GDPR/AVG.

De vragen die u met uw groep zult beantwoorden zijn:

- Hoe regelt u het bedrijfsrisico in dat de klant loopt bij het outsourcen van de genoemde informatie?
- Hoe zijn de verantwoordelijkheden belegd?
- Welke eisen stelt u aan de klant?
- Welke wet- en regelgeving denkt u dat er op U als CSP van toepassing is?
- Aan welke wet- en regelgeving moet de klant voldoen?
- Hoe waarborgt u als CSP dat u aan de eisen van de wetgeving én aan de eisen van de klant voldoet?
- Laat u audits toe én onder welke voorwaarden?
- Welk soort verklaringen kunnen een klant audit vervangen?

PvIB Platform voor InformatieBeveiliging

Is het een risico om te gaan outsourcen?

- In eerste instantie is outsourcen geen risico mits er goede afspraken worden gemaakt en audits mogelijk zijn om te controleren of de CSP zijn afspraken na komt
- Er is een risico, maar niet per sé groter dan wanneer u het in eigen beheer doet
- Ja, er is altijd een risico, uw persoonsgegevens gaan in de Cloud
- Er ontstaat een nieuwe relatie, die van verantwoordelijke en verwerker
- Ja, door een gebrek aan regie en kennis van (grote) outsourcingsprojecten en juridische kennis bij de outsourcende partij
- Men denkt soms dat men de (eind)verantwoordelijkheid ook kan outsourcen
- Persoonsgegevens worden gecompromitteerd

Risico dat je loopt als je je data in de Cloud gaat zetten? 1/3

- Beschikbaarheid van de Cloud service
- Onduidelijkheid over verantwoordelijkheden
- Niet (kunnen) voldoen aan de AVG/GDPR
- Niet aan kunnen tonen dat je aan de AVG/GDPR voldoet
- Waar wordt de data opgeslagen?
- Ongeautoriseerde toegang door medewerkers CSP
- Hoe voorkom je onrechtmatige verwerkingen?
- Misbruik van data

Risico dat je loopt als je je data in de Cloud gaat zetten? 2/3

- Lekken van klant gegevens door een hack
- CSP meldt lekken te laat
- Lekken van klant gegevens door een interne medewerker Cloud Service Provider (CSP)
- Lekken van gegevens zonder dat je dat weet (CSP stelt je niet op de hoogte), Hierdoor ben je niet in staat op tijd de juiste acties te ondernemen
- Eigenaarschap van de backups gemaakt door de CSP
- Welk recht is van toepassing?
- Server / data locatie (binnen de EER?)
- Behoud van soevereiniteit op de data (Wie heeft er toegang tot de data)
- Faillissement van de CSP

Risico dat je loopt als je je data in de Cloud gaat zetten? 3/3

- Bedreiging van de data integriteit, Continuïteit van de klant in gevaar
- Onrechtmatige verwerkingen door CSP
- Mogelijke subverwerkers "onder" de CSP waarvan je niet op de hoogte bent, maar die wel jouw data verwerken
- Hoe lang blijft de data bestaan na beëindiging van het contract?
- Aansprakelijkheid niet goed belegd
- Verwerkersovereenkomst
- Screening onbekende CSP medewerkers

Hoe zijn de verantwoordelijkheden belegd? 1/2

- De klant is verwerkingsverantwoordelijke voor de gegevens en moet dus aan de AVG/GDPR voldoen
- De klant moet er voor zorgen dat alle verwerkingen vastgelegd zijn en in de verwerkersovereenkomst opgenomen zijn
- specifiek t.a.v. verwerkingen
- Gegevenscategorieën vastleggen
- Assurance / Toezicht vastleggen
- CSP is de externe verwerker
- Franchise ondernemers zijn verwerkingsverantwoordelijke van de klantgegevens

Hoe zijn de verantwoordelijkheden belegd? 2/2

- Vastleggen in het Service level Agreement (SLA)
- Hoe goedkoper de CSP hoe meer je zelf moet doen. Het maakt een groot verschil of je "bare metal, een Virtual Private Cloud of een full managed Cloud "koopt"
- In contract opnemen
- Procesbeschrijvingen waarin de verantwoordelijkheden goed beschreven zijn

Welke eisen stelt u aan de CSP? 1/2

- De CSP moet voldoende maatregelen nemen om de data te beschermen
- Voldoen aan het informatiebeveiligingsbeleid van de klant
- Borging kwaliteitseisen (BIV/CIA)
- Subverwerkers zijn een verantwoordelijkheid van de verwerkeer (CSP) en zijn gehouden aan het contract dat de klant met de CSP heeft afgesloten
- Data centers in de EU
- Recht om te auditen
- Audit rapportages
- Certificering ISO 27001
- SOC 3 rapportages
- (Third party) Assurance verklaring
- ISAE 3000

PvIB Platform voor InformatieBeveiliging

Welke eisen stelt u aan de CSP? 2/2

- Binnen de EER data opslaan en versleutelen
- Melden van data lekken conform overeengekomen procedure en termijnen
- Aansprakelijkheid en reactie op inbreuken
- Escalatie procedure
- Encryptie data
- Exit strategie vastgesteld in contract / Ondersteuning bij migratie bij beëindiging contract
- Vastleggen vernietigingstermijnen
- Escrow overeenkomst
- Screening personeel
- Backup beleid
- Recovery tests

PvIB Platform voor InformatieBeveiliging

Welke wet- en regelgeving is van toepassing op u en uw Cloud provider?

- AGV / GDPR, Uitvoeren DPIA's
- Burgerlijk Wetboek / Aansprakelijkheidsregeling
- Ondernemingsrecht
- Belastingwetgeving
- Archiefwet
- Comptabiliteitswet
- Buitenlandse wetgeving?
- Indien het om een vitale sector gaat: Wbni
- Sectorspecifieke wetgeving zoals Gaswet, Elektriciteitswet en bijbehorende NEN-Normen, Bankenwetgeving, Havenwet, luchtvaartwet etc.
- Privacy shield

De case: Cloud Service Provider

Cloud Service Provider (CSP) kant:

U werkt bij een grote CSP, genaamd Cloud & Co.. Cloud & Co. is gespecialiseerd in het leveren van computing power en netwerk én internet connectiviteit aan diverse organisaties, van groot tot klein. Cloud & Co. heeft inmiddels een 100.000tal klanten.

Een grote Nederlandse retail keten, PrivComp genaamd, is voornemens om de stap naar de cloud te maken. PrivComp heeft tot op heden altijd, vanuit het eerste begin, haar automatisering zelf gedaan. Ze draaien inmiddels een groot server park in Nederland. De volledige KA-omgeving, de boekhouding en ERP systemen worden intern gehost.

De omslag in denken kwam een paar jaar geleden toen PrivComp een klantenkaart introduceerde èn gebruik ging maken van een externe partij die pinbetalingen regelt.

Het besluit is binnen PrivCorp op directie niveau gemaakt om de IT te gaan outsourcen. PrivComp wil zich namelijk focussen op zijn core-business, het inkopen en verkopen van tweedehands kleding. U wordt benaderd als een van de mogelijke partijen waar de hosting ondergebracht kan worden. PrivComp maakt zich echter wel zorgen over de enorme hoeveelheid klantdata die men heeft en voor zowel inkoop- als marketing doeleinden gebruikt. Naast die doelen bevat hun klantendatabase ook veel persoonsinformatie zoals onder andere NAW-gegevens, emailadressen, wachtwoorden voor de klantenportal en bankgegevens.

De vragen die u met uw groep zult beantwoorden zijn:

Is het een risico voor u om te outsourcen?

Wat zijn de risico's?

Hoe zijn de verantwoordelijkheden belegd?

Welke eisen stelt u aan de CSP?

Hoe waarborgt u dat die CSP aan die eisen voldoet?

Welke wet- en regelgeving denkt u dat er op U en op de CSP van toepassing is?

Hoe regelt u het bedrijfsrisico in dat de klant loopt bij het outsourcen van de genoemde informatie?

- De klant is zelf verantwoordelijk voor de security. Vastleggen in het contract
  - (afhankelijk van het type CSP)
- De klant bepaalt de security eisen, de CSP implementeert die. (afhankelijk van het type CSP)

Hoe zijn de verantwoordelijkheden belegd?

- De CSP is verantwoordelijk voor de security infrastructuur

Welke eisen stelt u aan de klant?

- De CSP is verantwoordelijk voor de security incident meldingen, de klant moet ze ook melden als ze eerder bij hen bekend zijn
- Inrichten Identity & Acces management

Aan welke wet- en regelgeving moet de klant voldoen?

- Gelijk aan de wet- en regelgeving genoemd in slide 12 , aangevuld met sectorale wet- en regelgeving zoals PCI/DSS voor de bankensector en de NTA 8120 voor de energiesector

Hoe waarborgt u als CSP dat u aan de eisen van de wetgeving én aan de eisen van de klant voldoet?

- Inrichten ISMS, risico management
- Afspraken met de klant

Laat u audits toe én onder welke voorwaarden?

- Geen audits direct door klanten*
- Wel jaarlijkse audit door onafhankelijke partij

* Dit hangt wel sterk af van het type CSP. CSP’s met duizenden (grote) klanten kunnen het zich veroorloven 365 dagen per jaar meerdere audit teams over de vloer te hebben

Welk soort verklaringen kunnen een klant audit vervangen?

- SOC 2 rapporten,
- ISAE 3402 rapportages
- Third party statements
- Audit rapportages door onafhankelijke audit organisaties (Denk aan PWC, EY, DNV-GL, BSI etc.)

Tot ziens op de PvIB Thema avond - Vulnerability management

14 mei 2019 van der Valk Hotel Utrecht

PvIB Platform voor InformatieBeveiliging