PRIVACY EN DE CLOUD

Zorg dat de gegevens van je klanten en personeel veilig zijn

Meer en meer bedrijven maken gebruik van cloudopslag voor hun gegevens. Met name voor zelfstandig ondernemers en het mkb is cloudopslag aantrekkelijk want dure apparatuur is niet noodzakelijk en de technische aspecten wordt allemaal geregeld. Maar waar is deze cloud eigenlijk gestald en met welke privacywetten moet je rekening houden?

Tegenwoordig is het vaak heel praktisch om klant- en personeelsgegevens in de cloud te stallen waardoor je ze overzichtelijk bij elkaar hebt en/of makkelijk kunt verwerken. Er bestaan talloze clouddiensten waaruit je kan kiezen, zowel betaald als gratis. Denk aan Google Docs of Office365. De naam van die aanbieder weet je, maar weet je ook waar hij jouw gegevens verwerkt en hoe ze zijn beschermd? Een vraag waar je niet altijd bij stilstaat als je bijvoorbeeld Google Docs gebruikt. Toch is het in het huidige landschap van cyberinvallen en datalekken niet onverstandig bewust te zijn van waar de informatie en gegevens over jouw personeel en klanten worden opgeslagen en door wie. Want de cloud klinkt misschien als een ongrijpbare locatie, in werkelijkheid kunnen die gegevens ergens ter wereld op een server staan.

HET IS GELUKKIG NIET zo dat iedereen maar lukraak clouddiensten mag aanbieden. Er is een regelgeving waar je als aanbieder moet voldoen en die is binnen de Europese Unie centraal geregeld. Voor alle lidstaten geldt een wetgeving waar landen zich minimaal aan moeten houden. De lidstaten kunnen bovendien afzonderlijk meer privacyregels invoeren. Dat verklaart waarom gegevens in het ene land beter beschermd kunnen zijn dan in het andere land. Buiten Europa kennen afzonderlijke landen een eigen regelgeving. De wetgeving die in Nederland over privacy van persoonsgegevens gaat is de Wet Bescherming Persoonsgegevens (Wbp). In veel gevallen zal een provider echter ook rekening moeten houden met landelijk bepaalde wetgeving van landen binnen de EU en tevens daarbuiten, zoals de Verenigde Staten. Dit is waar Solcon de concurrentie een stap voor is, door haar serverruimtes voor de volle 100 procent binnen Nederlands grondgebied te houden.

Clouddiensten in drie soorten:
- Infrastructuurclouddiensten: iaas (infrastructure as a service)
- Platformclouddiensen: paas (platform as a service)
- Applicatieclouddiensten: saas (software as a service)

OM TE BEGRIJPEN HOE de wet omspringt met jouw gegevens die in verschillende landen worden gestald, is het handig om eerst het basisprincipe van de Wbp te doorgronden. De Wbp is van toepassing op geautomatiseerde verwerking van persoonsgegevens én legt een aantal algemene verplichtingen op. De Wet maakt onderscheid tussen drie partijen die van belang zijn bij de privacybescherming bij clouddiensten: de verantwoordelijke, de bewerker en de betrokkene.

‘Het maakt wel degelijk uit in welk land je gegevens laat verwerken’

Sluit je een Bewerkersovereenkomst, zorg dan dat deze drie punten niet missen:

1. Gegevensverwerking gebeurt alleen in opdracht van de verantwoordelijken. ‘Verantwoordelijken’ zijn die bedrijven en organisaties die gegevens uit handen geven aan partijen zoals hostingproviders, de zogenaamde ‘bewerkers’. ‘Bewerkers’ hebben toegang tot de gegevens die zij opslaan en be- en verwerken. Daarom geldt voor hun een geheimhoudingsplicht.

2. Beveilig gegevens adequaat. Een goede beveiliging van gegevens hebben verantwoordelijken voor een groot deel zelf in de hand. Bijvoorbeeld door encryptie te gebruiken voor bestanden.

3. Geeft het recht op controle aan verantwoordelijke en betrokkene. Verantwoordelijken en andere betrokkenen kunnen controleren of bewerkers omgaan met de gegevens zoals zij zeggen en beloven dat zij doen. Dit kan door een zogenaamde ‘third party mededeling’ of TPM, waarbij een externe partij vaststelt dat bewerkers doen wat zij beloven op het gebied van veiligheid voor gegevens. De ISO 27001-certificering die Solcon bezit, is geldt als een dergelijke TPM en verzekerd verantwoordelijken en betrokkenen er van dat er veilig met gegevens omgegaan wordt door Solcon.

NB: *Vooral het laatste punt komt niet altijd voor in een standaardcontract!*

DE VERANTWOORDELIJKE IS de aanbieder van de dienst. Voer jij het beheer over persoonsgegevens van je klanten en personeel, dan ben jij in veel gevallen de verantwoordelijke. Je klanten en personeel (de betrokkenen) verstrekken immers aan jou hun gegevens en geven toestemming voor verwerking daarvan. Jij kunt vervolgens de verwerking – bijvoorbeeld de opslag in de cloud - van de persoonsgegevens aan een ander overlaten. Dat is de bewerker. De bewerker is degene die de gegevens verwerkt. Er is dus een verschil tussen de verantwoordelijke en de bewerker: de laatstgenoemde bepaalt niet de doelen en middelen voor de verwerking van de gegevens, maar verwerkt deze slechts in opdracht van jou, de verantwoordelijke. De bewerker moet ook aan de regels voldoen. Die worden vastgelegd in een overeenkomst tussen de verantwoordelijke en de bewerker. Soms is het lastig om precies te zeggen wie nu welke rol vervult, maar op die complexiteit zullen we nu niet ingaan.

ISO 27001
Om veiligheid voor je data te garanderen heeft Solcon een ISO 27001-certificering behaald. Hiermee worden allerlei processen beschreven hoe het bedrijf die de certificering heeft behaald jouw data beveiligd. Kort houdt in dat je de garantie hebt dat je data bij Solcon veilig staat, aangezien je als bedrijf deze certificering niet zomaar krijgt. Het bedrijf moet aan strenge eisen voldoen wat privacy betreft.

HET KENMERK VAN cloud computing is dat het al snel landsgrenzen overstijgt. Dat maakt veel diensten bruikbaar, maar het zorgt er ook voor dat de bescherming van de gegevens een complexe aangelegenheid is. Want welke wet geldt nu als jij in Nederland bent gevestigd, maar de gegevens wel op een server in Amerika hebt staan? En wat als je ervoor kiest om de gegevens waar jij de verantwoordelijkheid over hebt tijdelijk even onder te brengen op een andere server in een misschien wel ander land?
Om te bepalen aan welke wet jij je als verantwoordelijke moet houden, kijkt de Wbp voornamelijk naar je vestigingsplaats. Het begrip vestiging ziet op het centrum van de economische activiteit van de onderneming. Ben je in Nederland gevestigd, dan gelden de Nederlandse regels. Het is in de regel dus alleen relevant waar de verantwoordelijke zijn hoofdactiviteiten heeft, de plek waar de gegevens later worden verwerkt doet er in beginsel niet toe bij bepaling van de juiste wetgeving.
Toch maakt het voor jou wel degelijk uit waar de gegevens waar jij de verantwoordelijkheid over hebt verwerkt. Niet elk land is immers even veilig en transparant. In Amerika bijvoorbeeld, gebruikt de National Security Agency PRISM, waarmee communicatie en gegevens nauwgezet gevolgd en ontrafeld kunnen worden. Dit programma richt zich op gebruikers buiten Amerika die gebruik maken van services die zich in Amerika bevinden, zoals de diensten van Microsoft en Google.

CASE

Wie is verantwoordelijk?

Bedrijf A is een groot bedrijf dat veel personeelsgegevens en klantgegevens in zijn systeem heeft. Om efficiënter te werk te gaan en meer overzicht te krijgen, schakelt het bedrijf een cloudaanbieder in die de personeels- en de klantenadministratie voor hem beheert. De cloudaanbieder is in Nederland gevestigd, maar bewaart de gegevens van zijn opdrachtgevers op een server in Amerika. In de eerste maanden van het jaar is het altijd erg druk bij de cloudaanbieder, vanwege de belastingaangifte die voor 1 april gedaan moeten worden. Omdat de aanbieder in die maanden niet genoeg ruimte in zijn cloud heeft, stalt hij doorgaans de klantenadministratie van bedrijf A op de server van een collega in Mexico.

Deze casus laat zien hoe complex het kan zijn om een juiste privacy van je persoonlijke gegevens te organiseren. Stel dat jij bedrijf A bent, dan worden de volgende juridische stappen gemaakt om jouw gegevens zo goed mogelijk te beschermen:

1. Allereerst is er een juridisch onderscheid tussen personeelsgegevens en klantgegevens. De privacywetgeving geldt alleen voor persoonsgegevens. Dat wil zeggen gegevens die te herleiden zijn tot een individu. Staan er persoonlijke gegevens van je klanten vermeld bij de klantgegevens? Dan is de Wbp wel van toepassing.
2. De verantwoordelijke is het bedrijf A. De cloudaanbieder is de bewerker. Bedrijf A zal zich er dus van moeten vergewissen dat de cloudaanbieder voor wat betreft de verwerking van de gegevens voldoende beveiligingsmaatregelen heeft genomen om de persoonsgegevens te beveiligen en dat bovendien wordt voldaan aan de andere eisen die de Wbo stelt. De verantwoordelijke, bedrijf A, zal dus met de cloudaanbieder een bewerkersovereekomst moeten sluiten.
   Vaak neemt een cloudaanbieder in zijn contract of algemene voorwaarden al op dat hij aan de regels voldoet, maar het is aan de verantwoordelijke om er zorg voor te dragen dat het inderdaad goed is afgesproken.
3. Als het zo is dat de Amerikaanse cloudaanbieder een Mexicaanse partner inschakelt, zal bedrijf A moeten controleren of Mexico op de witte lijst staat en bovendien moeten controleren of het Mexicaanse bedrijf zijn zaken op orde heeft. Want daar gaat het tenslotte om. Ieder bedrijf die de gegevens van bedrijf A verwerkt, moet voldoen aan de strenge Nederlandse privacyregels omdat de verantwoordelijke – bedrijf A – in Nederland is gevestigd. Als de cloudaanbieder in Amerika of het bedrijf in Mexico een fout begaat en de privacygevoelige gegevens op straat komen te liggen, kunnen de betrokkenen een klacht indienen bij het College Bescherming Persoonsgegevens of rechtstreeks aanspraak maken op een schadevergoeding. Er moet uiteraard wel sprake zijn van schade. En dat is niet altijd het geval.

Dit laatste punt laat nog eens zien hoe complex de privacyregelgeving over clouddiensten is. Bedrijf A weet vaak namelijk niet waar de provider de data neerzet. Hij heeft dus vaak geen weet van de Mexicaan terwijl op hem wel de plicht rust te onderzoeken wat er met zijn data gebeurt. Bedrijf A zal dus aan de provider informatie moeten vragen hierover.

Juist daarom stelt de Wbp dat je als verantwoordelijke niet zomaar in elk willekeurig land gegevens van anderen mag opslaan en verwerven. Om als provider zaken te kunnen doen met bedrijven uit landen buiten de EU, moet je zeker stellen dat deze landen en deze bedrijven een passend beschermingsniveau van persoonsgegevens hebben. Je bent dan ook verplicht om een zogenoemde 'Bewerkingsovereenkomst' met de bewerker te sluiten waarin deze bescherming staat vermeld. Binnen de EU vormt dit uiteraard geen probleem aangezien elke lidstaat zich aan minstens dezelfde richtlijnen moet houden. Wanneer je over de Europese grens zaken gaat doen, zul je kritischer moeten zijn.

De plichten van een verantwoordelijke
- Persoonsgegevens mogen alleen voor vooraf bepaalde en gerechtvaardigde doeleinden worden gebruikt.
- Er moet sprake zijn van een legitieme verwerkingsgrond.
- Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor de afgesproken doeleinden.
- De verantwoordelijke moet maatregelen treffen zodat de persoonsgegevens correct en nauwkeurig zijn.
- De verantwoordelijke heeft informatieplicht.
- De verantwoordelijke heeft een beveiligingsplicht.
- Voor bijzondere gegevens (ras, gezondheid, geloof) gelden strengere regels en mogen slechts onder zeer strikte voorwaarden worden verwerkt.

De rechten van betrokkenen:
- Recht op informatie: de verantwoordelijke moet desgewenst informeren over wat er met de gegevens gebeurt.
- Recht op inzage in persoonsgegevens en gebruik daarvan.
- Recht op aanpassing, aanvulling, verwijdering of afscherming.
- Recht op verzet: de betrokkene mag bezwaar maken tegen het gebruik van zijn gegevens door de verantwoordelijke.

Een handig hulpmiddel waartoe je je kunt wenden is de 'Witte lijst' waarop landen staan waarvan de EU heeft bepaald dat de privacybescherming voldoende is. Het is een nuttige lijst, maar uiteindelijk ben jij degene die zorg moet dragen dat de binnen- of buitenlandse bedrijven die de gegevens verwerken, zich aan de afgesproken privacyregels houden.

ZAKEN DOEN MET BEDRIJVEN IN DE VS
De Verenigde Staten staat niet meer op de Witte lijst sinds het als reactie op de aanslagen van 11 september 2001 de Patriot Act aannam. Deze wet verleent autoriteiten toegang tot persoonsgegevens die worden verstrekt door bedrijven die in de VS zijn gevestigd, waaronder Amerikaanse cloudleveranciers. Het is daarbij niet van belang of deze gegevens binnen of buiten de VS zijn opgeslagen. Om toch zaken te kunnen doen met bedrijven uit de VS, is de zogenoemde Safe Harbor-overeenkomst in het leven geroepen. Bedrijven die de principes van deze overeenkomst onderschrijven, hebben volgens de EU een voldoende beschermingsniveau om zaken mee te doen. Overigens is de Safe Harbor een omstreden overeenkomst. Er is vastgesteld dat er fraude wordt gepleegd met de certificaten waardoor bedrijven die niet aan de beschermingseisen van de overeenkomst voldoen, wel degelijk zaken doen met Europese verantwoordelijke partijen.

Privacy is bij cloud computing een zeer complexe aangelegenheid. Daarom zijn contracten waarin de relatie tussen verantwoordelijke, bewerker en betrokkenen zijn vastgelegd van groot belang. Een Bewerkingsovereenkomst is verplicht en ook bij export van gegevens kan een overeenkomst vereist zijn. Uiteindelijk is het voor alle partijen belangrijk dat het duidelijk is waar ieders verantwoordelijkheden en rechten liggen, vooral in het geval dat er onverhoopt een datalek ontstaat.

Met dank aan Mark Krul,
WiseMen Advocaten
www.wisemen.nl

Solcon: even voorstellen

Solcon is een Nederlands bedrijf op Nederlandse bodem, met twee eigen datacenters (in Dronten en in Apeldoorn). We leveren diverse hostingoplossingen zoals virtuele desktops waarbij wij het onderhoud en de veiligheid voor ons rekening nemen, terwijl jij maximale flexibiliteit met minimale downtime tot je beschikking hebt. Ook colocated hosting behoort tot de mogelijkheden, waarbij je jouw eigen server beheert, maar profiteert van de veiligheid die Solcon biedt. Wij garanderen dat jouw data op Nederlandse bodem staat en blijft, en dat deze hier ook veilig staat. Dit dankzij een ISO 27001-certificering, maar ook omdat we aangesloten zijn bij de DHPA, ofwel de Dutch Hosting Provider Association. Deze organisatie zorgt ervoor dat aangesloten organisaties zich op een bepaalde manier opstellen tegenover hun klanten en de data van hun klanten. Een uitgebreide 'Code of Conduct' kun je lezen op ***www.dhpa.nl***.
Wil je meer weten over Solcon, neem dan gerust contact met ons op via ***www.solcon.nl***.

CONTACT
Particulier: 088-0032222
Bereikbaar op werkdagen van 8.00u - 20.00u en op zaterdag van 9.00u - 17.30u

Zakelijk: 088-0032525
Bereikbaar op werkdagen van 8.00u - 20.00u en op zaterdag van 9.00u - 17.30u

Postadres:
Solcon
Postbus 127
8250 AC, Dronten

Bezoekadres:
Solcon
Het Spaarne 11
8253 PE, Dronten