Executive Brief

Cloud, naleving van regelgeving en waarom HR-transformatie goed is voor uw HCM-strategie

Gesponsord door: ADP

Duncan Brown Alexandros Stratis

30-11-2016

SAMENVATTING

HR-managers hebben te maken met allerlei verouderde methoden voor het vastleggen en verwerken van personeelsgegevens. Daarbij kunnen er ook grote verschillen bestaan tussen het hoofdkantoor en de dochterondernemingen, onder meer veroorzaakt door een combinatie van verschillende softwaretoepassingen, uitbesteding aan externe bureaus en het gebruik van verschillende datacenters. Daarnaast is er sprake van toenemende druk van beveiligingsvoorschriften vanwege het wijdverbreide gebruik van clouddiensten. Veel HR-managers bevinden zich daarom in een lastige positie.

Om deze zaken grondig aan te pakken, maar ook vanwege de noodzaak om zichtbaar strategischer te opereren, zetten Chief HR Officers (CHRO's) in op HR-transformatieprojecten en investeringen in HR-technologie. De keuze voor een HR-technologieleverancier die gegevensbeveiliging en naleving van regelgeving als best practice in zijn diensten en oplossingen heeft meegenomen, is een van de sleutelvoorwaarden om hiermee het beoogde rendement te behalen.

Oplossingen voor Human Capital Management (HCM) ondergaan momenteel een snelle transformatie die de samenstelling en het beheer van personeelsgegevens opnieuw vormgeeft. De drijvende factor hierbij is de evaluatie van prestaties op basis van projecten, samenwerking en resultaten, de algehele betrokkenheid bij medewerkers en hoe ze hun loopbaan en toekomst kunnen plannen. De HR-afdeling, van oudsher voornamelijk gericht op het bewaren van personeelsgegevens, het aanbieden van opleidingen en het verwerken van HR-transacties, evolueert nu tot een strategische partner voor de groei van de organisatie.

HCM ondergaat een snelle transformatie die het beheer van het personeelsbestand opnieuw vormgeeft

Een essentieel onderdeel van deze HCM-transformatie is de toename van automatisering en het gebruik van clouddiensten waardoor veel handmatige processen snel vervangen zullen worden. De overstap naar cloudoplossingen zorgt waarschijnlijk voor een groter aantal gebruikers en geeft ook het voordeel van de efficiëntie en flexibiliteit van cloudarchitecturen.

De veiligheid van personeelsgegevens blijft echter wel een punt van zorg voor veel organisaties. Gevoelige informatie toevertrouwen aan derden is altijd een grote stap, maar om de personeelsgegevens onder te brengen in de cloud, op een onbekende locatie die wordt beschermd door vage veiligheidsgaranties, dat vinden de meeste HR-managers ontoereikend. Hoe kunnen werkgevers er zeker van zijn dat hun personeelsgegevens écht veilig zijn?

De situatie staat op het punt nog veel serieuzer te worden, zowel wat betreft verplichtingen als gevolgen. Met ingang van 25 mei 2018 wordt de Algemene verordening gegevensbescherming (AVG) van kracht, waarmee de eisen inzake veiligheid en andere verwerkingsactiviteiten van

persoonsgegevens die aan risico's blootstaan, nog worden verhoogd. Belangrijk is dat de AVG een verordening is, geen richtlijn, hetgeen betekent dat deze geldt voor alle 28 lidstaten en dus niet in nationale wetgeving hoeft te worden omgezet.

Door de AVG vinden bedrijven het moeilijk om veranderingen in de regelgeving te begrijpen en erop te reageren. De kosten en risico's van het niet naleven van deze verordening en alle bijbehorende regelgeving kunnen aanzienlijk zijn.

Cloud - indien goed uitgevoerd - kan de risico's van niet-naleving van de AVG en lokale arbeidswetgeving verkleinen. IDC gelooft dat veel bedrijven kiezen voor het uitbesteden van HR-gegevensverwerking om zo hun risico's en nalevingsverplichtingen te *reduceren*. Maar een HR-technologieleverancier moet beschikken over een sterk actieplan, retentieplannen voor data, robuuste beveiligingsplatforms en programma's voor het migreren van data. Dit allemaal onder toezicht van een gegevensbeveiligingsinstantie (DPO).

Cloud - indien goed uitgevoerd - kan de risico's van niet-naleving van de AVG en lokale arbeidswetgeving verkleinen.

In deze white paper wordt de impact van de AVG beschreven en wordt getoond hoe een cloud-implementatie de naleving van wet- en regelgeving kan bevorderen in plaats van belemmeren en tegelijk uw digitale HCM-strategie kan verbeteren.

DE VERANDERENDE REGELGEVING ROND HR-GEGEVENS

De AVG is de grootste verandering op het gebied van wetgeving inzake gegevensbescherming van de afgelopen drie decennia. Deze verordening actualiseert de bestaande wetgeving die dateert uit een tijd toen nog niemand van Facebook, LinkedIn of de cloud had gehoord. De AVG bundelt de wetgeving inzake gegevensbescherming van alle 28 EU-lidstaten en is daarmee van grote invloed in heel Europa.

De AVG is de grootste verandering op het gebied van wetgeving inzake gegevensbescherming van de afgelopen drie decennia.

De bestaande richtlijn inzake gegevensbescherming werd in 1995 overeengekomen en is niet geschikt voor het beschermen van persoonsgegevens in een wereld waar we te pas en te onpas online persoonlijke informatie opslaan en uitwisselen. De richtlijn werd bovendien door elke afzonderlijke lidstaat uitgevoerd volgens haar eigen zakelijke gebruiken en cultuur, waardoor er binnen de Unie verschillen in beschermingspraktijken voor gegevens zijn ontstaan. De AVG is daarom een belangrijke stap voorwaarts in de homogenisering en modernisering van de wetgeving inzake de bescherming van persoonsgegevens in Europa.

De definitie van persoonsgegevens is behoorlijk breed: het beslaat alle informatie waarmee een persoon - direct of indirect - kan worden geïdentificeerd. Dit omvat de voor de hand liggende informatie zoals naam of identificatienummer, maar ook locatiegegevens of IP-adres en eveneens biometrische en genetische informatie. Ook belangrijk is dat onder persoonsgegevens zowel de gegevens van een werknemer als die van de cliënten of klanten van een bedrijf worden verstaan.

De belangrijkste implicatie van de AVG met betrekking tot HR-gegevens is misschien vanzelfsprekend, maar desondanks wel de moeite waard om te noemen. Personeelsgegevens worden volgens de AVG dezelfde rechten toegekend als klantgegevens. Dit betekent dat de verplichtingen van de onderneming om zijn HR-gegevens te beschermen nog serieuzer worden, dat de rechten van werknemers om hun gegevens in te zien, te actualiseren en te verwijderen worden gehandhaafd en dat de gevolgen van inbreuk op deze rechten ernstig zijn (zoals we zullen zien).

Personeelsgegevens worden krachtens de AVG dezelfde rechten toegekend als klantgegevens.

HR-afdelingen hebben echter niet alleen te maken met de regelgeving rondom de AVG en gegevensprivacy; het aantal regels en nationale (landspecifieke) voorschriften waaraan organisaties moeten blijven voldoen, is een uitdaging op zich. Er zijn vijf verschillende gebieden waar HR ervoor moet zorgen dat het blijft voldoen aan alle richtlijnen en wet- en regelgeving: uitkeringen en verzekeringen, werving en selectie, arbeidsveiligheid en gevaren, salarisadministratie en de dienstverbandcyclus van werknemers.

Steeds meer organisaties vragen hun HR-afdelingen proactief op te treden en zich met allerlei 'mensenrisico's' met betrekking tot de vijf bovenstaande gebieden bezig te houden. De uitdaging is echter ingewikkelder voor organisaties die in verschillende rechtsgebieden opereren en die dochter- of moederbedrijven op verschillende locaties hebben. Het is hier van belang om te begrijpen dat de naleving binnen HR moet worden gezien als een afgeronde risicomanagementfunctie die ook gunstig uitpakt voor het menselijk kapitaal.

Daarnaast helpt het om de rol van HR omhoog te tillen van een verzameling dossiers met minimale strategische functie tot een belangrijke strategische partner die de aan risico's verbonden kosten voor de organisatie kan verminderen en die tegelijkertijd de productiviteit en betrokkenheid van werknemers verhoogt.

Voorbeelden van nalevingsvereisten voor HR-afdelingen die constante bewaking en beheer van hun parameters vereisen, kunnen uiteenlopen van salarisadministratie en fiscale premies (het PAYE-systeem in het Verenigd Koninkrijk versus "impôt sur le revenu" in Frankrijk, enz.), training (introductie, fraudedetectie, enz.) en professionele ontwikkeling (monitoring van Credits van beroepsontwikkeling/CPDs of andere cijfers die door beroepsorganisaties en boards worden gebruikt om lidmaatschap te verzekeren) of due diligence in de werving en selectie en het ontslagproces.

BELANGRIJKSTE KENMERKEN VAN DE AVG

Zoals al eerder is aangegeven, is de definitie van 'persoonsgegevens' die in de AVG wordt gehanteerd heel breed. Vanuit HR-perspectief is alle informatie die betrekking heeft op een werknemer beschermd, en zijn er zelfs enkele categorieën gegevens die niet mogen worden verzameld. Hieronder vallen de zogenaamde 'bijzondere gegevenscategorieën', vaak ook wel gevoelige gegevens genoemd. Het gaat dan onder meer om genetische gegevens, biometrische gegevens en gezondheidsgegevens alsook seksuele voorkeur of geaardheid. Er is echter een belangrijk voorbehoud met betrekking tot dit verbod: de verwerking van gegevens ten behoeve van preventieve of arbeidsgeneeskunde of voor de beoordeling van de arbeidscapaciteit van een werknemer (AVG artikel 9).

De AVG introduceert in sommige gevallen ook een gemeenschappelijke verantwoordelijkheid en aansprakelijkheid tussen gegevensbeheerders (in het kader van HR-gegevens meestal de werkgever) en verwerkers (derden die gegevens namens de werkgever verwerken). Dit is belangrijk voor iedere werkgever die zijn HR-gegevensverwerking uitbesteedt of overweegt dit te doen.

Wat betreft beveiligingseisen is de AVG opzettelijk vaag. Van de 99 artikelen in de definitieve tekst van de AVG heeft er slechts één (artikel 32) specifiek betrekking op veiligheid en dit artikel is weinig

gedetailleerd. De hoofdlijn van de verordening is dat organisaties dienen uit te gaan van 'de nieuwste' technologie, evenals kosten, risico en de bedrijfscontext. Organisaties moeten beslissen wat dit voor hun organisatie betekent en dat is geen eenvoudige taak. Het artikel moedigt tevens versleuteling (hoewel geen verplichting) en pseudonimisering aan (ongeveer gelijkwaardig aan het gebruik van tokens).

Beveiliging is echter een fundamenteel onderdeel van de beginselen inzake de verwerking van persoonsgegevens (artikel 5). De AVG stelt met name verplicht dat gegevens worden verwerkt op een wijze die "zorgt voor adequate beveiliging van de persoonsgegevens". Dus hoewel de AVG onduidelijk is over de te nemen beveiligingsmaatregelen, is de verordening ondubbelzinnig over het belang van veiligheid.

Vanuit HCM-perspectief wijst de AVG CHRO's op een aantal belangrijke technologische beslissingen. Hoewel niet verplicht, zullen veel CHRO's concluderen dat versleuteling van alle personeelsgegevens wenselijk is, zowel ‘in rust’ als in doorvoer en in back-up ervan. De AVG verplicht het bijhouden van gegevensbestanden en de mogelijkheid om controles uit te kunnen voeren, zowel in het kader van naleving als voor forensische doeleinden.

De AVG is onduidelijk over de te nemen beveiligingsmaat regelen, maar expliciet over het belang van veiligheid.

AVG: meer dan beveiliging

Een algemene misvatting is dat de AVG hoofdzakelijk een gegevensbeveiligingsrichtlijn is. Hoewel de beveiliging van gegevens, zoals gezegd, een belangrijk aspect van de AVG is, is het een vergissing om te denken dat beveiliging de fundamentele technologie is waar het om draait. Er zijn andere vereisten met betrekking tot uiteenlopende technologieën op andere gebieden dan beveiliging.

Zo geeft bijvoorbeeld de vereiste van overdraagbaarheid van gegevens (artikel 20) individuen het recht om hun persoonsgegevens bij de beheerder op te vragen, waar mogelijk in een voor een machine leesbare vorm, wanneer de verwerking is gebaseerd op toestemming van de betrokkene of op een contract. Met het recht op verwijdering (vaak aangeduid als het recht om te worden vergeten, artikel 17) kan een persoon een beheerder vragen om zijn of haar persoonsgegevens te verwijderen (onder specifieke omstandigheden en met diverse uitzonderingen). En de regels voor toestemming - met name het verzamelen van ouderlijke toestemming over gegevens van kinderen (artikel 8) - zijn veel strenger geworden.

Een van de belangrijkste aandachtspunten van de AVG, zoals wordt geïllustreerd door de zeven artikelen over het onderwerp, is gegevensoverdracht (artikel 44 t/m 50). Gegevensoverdracht omvat ook de verplaatsing van gegevens naar een zogenaamd extern land. Een extern land is een land dat geen lid is van de EU. Het gaat erom dat gegevensbeheerders voor voldoende bescherming van de gegevens moeten zorgen, ook wanneer deze naar buiten het eigen rechtsgebied worden overgebracht. De EU heeft twee mechanismen om deze bedreiging het hoofd te bieden: de beheersing van gegevensoverdrachten naar buiten de EU en een extra-territorialiteitsclausule waarmee het bereik van de AVG wordt uitgebreid voor alle gegevens betreffende een persoon in de EU (ongeacht de locatie van die gegevens, zie artikel 3).

Gegevensoverdrachten zijn belangrijk in het kader van HR-gegevens waarbij werkgevers gebruikmaken van clouddiensten of HR-uitbestedingspartners. Het is een wettelijke verplichting voor werkgevers om te weten waar hun HR-gegevens zich fysiek bevinden, en in het bijzonder of dat buiten de EU is. Het is volstrekt legaal om gegevens naar buiten de EU te exporteren, maar dit moet dan wel gebeuren in het kader van een van de diverse mechanismen van regulerend toezicht. Deze omvatten:

- Overdrachten op basis van adequaatheid: de EU houdt een lijst bij van landen met wetgeving inzake gegevensbescherming die als adequaat (of equivalent) wordt

beschouwd voor de AVG. Er staan slechts 12 landen op deze lijst en (voor velen belangrijk) de VS hoort daar niet bij.

- Bindende bedrijfsregels (BCR's): dit is een officiële verbintenis door een gegevensverwerker om een gegevensbeschermingsprogramma te implementeren met een hoog niveau van bescherming dat aan de vereisten van de AVG voldoet en dat door de gegevensbeschermingsinstanties van de EU is goedgekeurd. Dit is geen geringe onderneming en toont een blijvende en juridisch bindende verbintenis aan de Europese privacyregels.
- Standaardmodelclausules die per contract worden toegevoegd.
- Toestemming van de betrokkenen om hun gegevens naar buiten de EU over te brengen.
- Naleving van een goedgekeurde gedragscode of certificering. Beide structuren worden in de AVG vastgelegd, maar zijn nog niet ten uitvoer gebracht.

Het andere belangrijke mechanisme voor het realiseren van wettige gegevensoverdrachten geldt in gevallen waar een specifieke overeenkomst bestaat tussen de EU en het externe land. Deze aanpak wordt doorgaans gebruikt wanneer er geen adequaatheidsbesluit werd verleend. Het beste voorbeeld van deze situatie is het 'Privacy Shield', een bilaterale overeenkomst tussen de VS en de EU waarmee gegevensoverdrachten naar verwerkers die aan de voorwaarden van de overeenkomst voldoen, worden toegestaan. Het Privacy Shield zal echter waarschijnlijk in gerechtshoven worden getest, net zoals zijn voorganger Safe Harbor. IDC denkt dat bedrijven met het hoofdkantoor in de VS die willen aantonen dat ze zich langdurig aan de AVG-beginselen houden, de BCR-route zouden moeten volgen.

Een actuele illustratie van de gegevensoverdrachtspraktijk is natuurlijk de Brexit. Voor zover het wetgeving inzake gegevensbescherming betreft, is de Brexit grotendeels irrelevant. Dit komt door de gegevensoverdrachtsregels in de AVG: als een Brits bedrijf wil zakendoen met een EU-partner of persoonsgegevens uit de EU wil verwerken, zal dat bedrijf zich aan de gegevensoverdrachtsregels in de AVG moeten houden. Gezien de omvang van de zakelijke relatie tussen het Verenigd Koninkrijk en de EU vandaag de dag, is het waarschijnlijk dat het Verenigd Koninkrijk bij het verlaten van de EU een AVG-achtige wet zal aannemen (en het ICO heeft dit standpunt al aangegeven).

Voor zover het wetgeving inzake gegevensbescherming betreft, is de Brexit grotendeels irrelevant.

Sancties voor niet-naleving

In de pers is veel aandacht gegeven aan de "doeltreffende, proportionele en afschrikwekkende" administratieve boetes die door de toezichthouders kunnen worden opgelegd. Er is met name veel aandacht gegeven aan de maximale boetes van tot 4% van de totale wereldwijde jaaromzet of € 20 miljoen, indien laatstgenoemd bedrag hoger uitvalt. Het is opmerkelijk dat dit niveau van boetes alleen van toepassing is op overtredingen die betrekking hebben op de beginselen van de AVG (artikel 5), fundamentele rechten van betrokkenen zoals toestemming en verwijdering, en schendingen met betrekking tot gegevensoverdracht. Voor datalekken zelf die bijvoorbeeld voortkomen uit slechte beveiliging geldt een lagere boete van maximaal 2% van de totale wereldwijde jaaromzet of € 10 miljoen. Werkgevers maken zich wellicht meer zorgen over verplichte inbreukmeldingen. Gegevensbeheerders zijn verplicht om hun toezichthoudende instantie op de hoogte te stellen bij een inbreuk op persoonsgegevens die resulteert in een "risico voor de rechten en vrijheden van personen" (artikel 33). In een dergelijk geval moet de gegevensbeheerder dit tevens aan de betrokken personen zelf melden (artikel 34). Dit kan vervolgens leiden tot negatieve publiciteit met daaruit voortvloeiend merk- en reputatieschade.

In het uiterste geval heeft een toezichthoudende instantie de bevoegdheid tot opschorting van de gegevensverwerking (artikel 58). Dit kan in feite een bevel betekenen om zakelijke activiteiten of

de uitvoering van een personeelsadmistratiecyclus te staken als de betreffende gegevensverwerking noodzakelijk is voor een kernbedrijfsproces.

Gezien deze sancties is het niet verwonderlijk dat de AVG de aandacht heeft van de directies bij bedrijven in de EU (en daarbuiten, door extra-territorialiteit). Het is echter belangrijk om te weten dat er sancties (zoals boetes) kunnen worden opgelegd bij gebrek aan medewerking. Er ligt een sterke nadruk in de AVG op het zorgen voor de aanwezigheid van bewijsmateriaal, waaronder het aanleggen en bijhouden van een administratie van gegevensverwerking. Controleerbaarheid is essentieel en de mogelijkheid om naleving aan te tonen (verantwoording) is een fundamenteel principe van de AVG.

ARGUMENTEN VOOR CLOUD: WAAROM CLOUD HR-ACTIVITEITEN HELPT EN NIET BELEMMERT

In essentie zijn clouddiensten een vorm van uitbesteding. Zoals bij elke uitbestedingsactiviteit moet een due diligence-onderzoek worden uitgevoerd naar de leverancier of aanbieder van diensten. HR-oplossingen die in de cloud worden aangeboden moeten dus grondig worden gecontroleerd.

Cloud is anders vanwege de veelheid van verwerkingsvoorzieningen die het met zich meebrengt. Bedrijven moeten praktische due diligence toepassen door verschillende vragen te stellen over het niveau van beveiliging en de gegevensbeschermingsprocessen en door analyse van auditrapporten, inclusief rapporten van onafhankelijke derden die eventueel door de cloudaanbieder beschikbaar worden gesteld. Zo is bijvoorbeeld inzicht in de fysieke beveiliging van het datacentrum waar persoonsgegevens worden gehost essentieel. Een geloofwaardige leverancier zal minstens even goede veiligheidsvoorzieningen hebben als de grootste onderneming, en vermoedelijk aanzienlijk beter dan het gemiddelde bedrijf met werknemers in dienst. Dit omvat waarschijnlijk certificering volgens ISO 27001 en (steeds meer) 27018, dat zich richt op persoonsgegevens in publieke clouds.

Er is geen juridische of technische belemmering voor het opslaan van HR-gegevens in de cloud.

Er is dus geen juridische of technische belemmering voor het opslaan van HR-gegevens in de cloud. Sommige bedrijven kiezen voor een configuratie met een datacenter in de EU, inclusief bewezen fysieke en logische beveiligingscertificeringen. Verder zou de toegang tot die EU-gegevens alleen binnen de EU mogelijk moeten zijn: toegang van buiten de EU zou neerkomen op een overdracht van gegevens (door gegevens in doorvoer) en de doeltreffendheid van EU-datacenters verminderen.

De meeste cloudoplossingen vereisen in meer of mindere mate gegevensoverdrachten buiten de EU. Leveranciers hebben oplossingen ontwikkeld om de persoonlijke gegevens te beschermen, waaronder modelcontractclausules. Maar bindende bedrijfsregels lijken de meest robuuste vorm van juridische zekerheid met betrekking tot gegevensoverdracht te worden.

Bindende bedrijfsregels lijken de meest robuuste vorm van juridische zekerheid met betrekking tot gegevensoverdracht te worden.

Veel bedrijven kiezen voor het uitbesteden van HR-gegevensverwerking ter verlaging van hun risico's en nalevingsverplichtingen. Werkgevers kunnen

niet alle risico wegnemen, maar kiezen voor een geloofwaardige provider is een stap in de goede richting.

TECHNOLOGIELEVERANCIERS EN HUN ROL IN HR-TRANSFORMATIE EN NALEVING

Er wordt vaak gezegd dat bedrijven wel hun verwerking kunnen uitbesteden, maar nooit hun verantwoordelijkheid. Wat betreft de AVG geldt dat nog steeds, maar de verbreding in aansprakelijkheid naar verwerking betekent dat ten minste een deel van de verantwoordelijkheid voor de naleving nu ook komt te liggen bij een externe gegevensverwerkingsprovider.

Natuurlijk blijft de beheerder verantwoordelijk voor de fundamentele beginselen van de AVG (artikel 5) en dient deze de naleving daarvan te kunnen aantonen. Maar de eerste vereiste voor een gegevensverwerker is dat deze in staat is om technische en organisatorische maatregelen door te voeren zoals overeengekomen met de beheerder. Ook gelden voor de gegevensverwerker dezelfde sancties voor niet-naleving. Dit roept de vraag op: hoe kan een beheerder vaststellen of een verwerker in staat is om aan deze vereiste te voldoen?

Nu 25 mei 2018 dichterbij komt, moeten werkgevers de AVG niet negeren, noch de aanzienlijke veranderingen die deze brengt.

Gedragscodes en certificeringen zijn onder de AVG wettelijk verplicht, maar tot op heden bestaat geen van beide mechanismen in de praktijk. Dus verwerkers kunnen werkgeversorganisaties door andere aanvullende middelen van hun kwaliteiten overtuigen, zoals de ISO-certificeringen 27001 (informatiebeveiligingsbeheer), 27018 (bescherming van persoonsgegevens in publieke clouds) of 29100 (privacyframework), onafhankelijke auditrapporten en BCR's voor verwerkers die de langdurige wil van hun organisatie om de beginselen van de AVG na te leven willen aantonen. BCR's worden door gegevensbeschermingsinstanties in de EU beschouwd als de gouden standaard voor gegevensbescherming.

HRO-aanbieders staan voor de uitdaging om rendement te maken door op schaal voor meerdere werkgevers maar met kennis van lokale arbeidswetten en praktijken te opereren. Dus ze moeten internationaal zijn in hun bedrijfsvoering, maar lokaal in de uitvoering: IDC denkt dat weinig HRO-providers deze combinatie van mogelijkheden kunnen leveren.

Een belangrijk aspect voor de HR-professional is het feit dat moderne bedrijven meer van de HR-afdeling zien, willen en verwachten.

Een belangrijk aspect voor de HR-professional is het feit dat moderne bedrijven meer van de HR-afdeling zien, willen en verwachten. De HR-systemen uit het verleden zijn dossiersystemen met beperkte toegevoegde waarde voor de organisatie, die uitsluitend gericht waren op het beheer van de eenvoudigste zaken rond het dienstverband van de werknemers.

Na verloop van tijd, met de verandering in de mogelijkheden, regelgeving en bovenal in de rol die men HR toedicht, streeft de HR-professional ernaar strategischer, inzichtelijker en waardevoller te zijn voor de hele organisatie. Vanuit deze invalshoek kan naleving niet worden onderschat; integendeel, beheer van het nalevingsaspect wordt vanuit het oogpunt van HR een belangrijke risicobeperkende factor voor het bedrijf, het biedt de mogelijkheid om kosten te verlagen en beschermt tegen rechtszaken, ondanks de toegenomen complexiteit en de omvang van de rol van de HR-afdeling.

BELANGRIJKSTE AANBEVELINGEN

Negeer de AVG niet

Nu 25 mei 2018 dichterbij komt, is het belangrijk dat de werkgevers de AVG en de aanzienlijke veranderingen die deze brengt, niet negeren. De juridische en technische achtergrond van de AVG is enorm en de meeste organisaties zullen moeite hebben om de verordening volledig te hebben

doorgevoerd op het moment dat deze van kracht wordt. Als werkgevers nog niet begonnen zijn met het onderzoeken van het effect van de AVG, moeten ze dat nu onmiddellijk gaan doen.

De AVG is een kans

Het is gemakkelijk om de AVG, met haar vele wijzigingen, als een grote hindernis en een afleiding van de normale bedrijfsactiviteiten te zien. IDC is er echter van overtuigd dat de AVG aanzienlijke kansen voor de werkgevers biedt. Het creëert een duidelijke en gelijkmatige regelgeving voor de overdracht van gegevens die een basis vormt voor cloud-HRO-diensten. Met de juiste maatregelen ten aanzien van veiligheid van een provider kunnen bedrijven veilig en legaal gebruikmaken van cloud-HRO als onderdeel van hun HCM-strategie.

Naleving is een partnerschap

In augustus 2016 voltooide IDC zijn *Human Capital Management Survey* in West-Europa, waarop meer dan 250 reacties kwamen van HR-managers. In dit onderzoek werden de kwesties van gegevensprivacy en wijzigingen in de wetgeving (waaronder AVG) door één op de drie respondenten als een belangrijk aandachtspunt gezien, terwijl slechts 23% enigszins bezorgd tot helemaal niet bezorgd bleek te zijn. De meerderheid van de respondenten (76%) ziet gegevensprivacy en naleving van wetgeving nog wel als een factor die invloed heeft op de aankoopbeslissing voor een HCM-oplossing.

Het is van cruciaal belang voor leveranciers om HR van de benodigde hulpmiddelen en inzichten te voorzien. Klanten moeten ervan verzekerd zijn dat HCM-oplossingen aan alle wet- en regelgeving voldoen en goed beveiligd zijn, want dan kunnen ze zich gaan richten op belangrijke langetermijndoelstellingen, zoals de omvorming van een back-officefunctie naar een gewaardeerde partner van de directie.

Over IDC

International Data Corporation (IDC) is de voornaamste wereldwijde leverancier van marktinformatie, adviesdiensten en evenementen voor de informatietechnologie-, telecommunicatie- en consumententechnologiebranche. IDC ondersteunt ICT-deskundigen, leidinggevenden en investeerders bij beslissingen op basis van de harde feiten over de aankoop van technologie en de strategie van bedrijven. Er zijn ruim 1.100 IDC-analisten werkzaam in 110 landen die op mondiale, regionale en lokale schaal advies geven over technologie, mogelijkheden en trends. Al 50 jaar voorziet IDC zijn klanten van strategisch advies ten behoeve van hun belangrijkste zakelijke doelstellingen. IDC is een dochteronderneming van IDG, 's werelds grootste media-, onderzoeks- en evenementenbedrijf op het gebied van technologie.

IDC U.K.

IDC UK
5th Floor, Ealing Cross
85 Uxbridge Road
Londen
W5 5TH, Verenigd Koninkrijk
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Auteursrechten en beperkingen