Executive Brief

So unterstützen Sie im Zeitalter von Cloud und Compliance Ihre HCM-Strategie

Gesponsert von: ADP

Duncan Brown Alexandros Stratis
November 2016

EXECUTIVE SUMMARY

Personalverantwortliche erleben derzeit, dass ihre bisherigen Methoden bei der Handhabung und Verarbeitung von Personaldaten in Frage stehen. Diese Methoden und Prozesse können sich zwischen Zentrale und Niederlassung stark unterscheiden. Gründe dafür sind etwa die unterschiedliche Nutzung von Software, das Outsourcing an Dritte oder verteilte Rechenzentren. Auch der verbreitete Einsatz von Cloud-Technologien erhöht den Druck auf die bestehenden Sicherheitsregeln.

Deshalb und um ihre strategische Bedeutung fürs Kerngeschäft zu erhöhen, initiieren Personalverantwortliche HR (Human Relations)-Transformationsprojekte und investieren in HR-Technologien. Erfolgsentscheidend ist dabei unter anderem, dass der ausgewählte Technologieanbieter lückenlosen, dauerhaften Datenschutz und praktisch bewährte Compliance-Prozesse in seine Dienste und Softwareangebote integriert hat.

HCM (Human Capital Management) verändert sich rapide und damit das gesamte Personalmanagement. Die wichtigsten Treiber sind hier die Bewertung der Mitarbeiter nach Projekterfolg, Kooperationsfähigkeit und Ergebnissen sowie das gesamte Engagement für die Mitarbeiter und ihre individuellen Aufstiegs- und Karriereplanung. Der Personalbereich, historisch für die Aufbewahrung der Personalakten, Organisation der Weiterbildung und Verarbeitung von HR-Transaktionen zuständig, wird so zu einem strategischen Partner bei der Weiterentwicklung der Organisation.

Die rasante Transformation von HCM verändert das gesamte Personal-management drastisch.

Ein Schlüsselthema der HCM-Transformation ist der schnelle Ersatz proprietärer Lösungen und händischer Prozesse durch vorgefertigte Lösungen und Public-Cloud-Services. Der Einsatz von Cloud-Lösungen bietet Anwendern mehr Funktionen sowie die Effizienz und Flexibilität von Cloud-Architekturen.

Doch es bestehen noch immer Sicherheitsbedenken. Es ist immer ein großer Schritt, Dritten sensitive Informationen anzuvertrauen. Personaldaten einfach in die Cloud zu stellen, wo sie an einem unbekannten Ort mit vagen Sicherheitsversprechen gespeichert werden, reicht den meisten Personalverantwortlichen nicht aus. Wann also kann sich das Unternehmen darauf verlassen, dass die Daten der Mitarbeiter sicher verwahrt sind?

Dafür sind weitaus striktere Regeln als bisher nötig – hinsichtlich der Pflichten und der Folgen von Pflichtverletzungen. Ab 25. Mai 2018 gilt in Europa die Europäische Datenschutzverordnung (GDPR, Generals Data Protection Regulation). Sie steigert die Anforderungen an Sicherheitsmaßnahmen und andere Prozesse im Zusammenhang mit der risikobehafteten Verarbeitung persönlicher Daten. Die GDPR ist keine Direktive, sondern eine Verordnung, mithin direkt anwendbares Recht. Sie gilt gleichermaßen in allen 28 Mitgliedsstatten und muss nicht eigens in lokale Gesetze umgesetzt werden.

Viele Unternehmen halten es für schwierig, alle regulatorischen Anforderungen der GDPR fristgerecht umzusetzen. Doch die Kosten fehlender Compliance und die Risiken sind beträchtlich.

Die Cloud kann, richtig eingesetzt, das Risiko fehlender Compliance mit der GDPR und dem lokalen Arbeitsrecht verringern. IDC nimmt an, dass viele Unternehmen die Verarbeitung von Personaldaten auslagern werden, gerade um ihr Risiko und Compliance-Verpflichtungen zu verringern. Allerdings braucht ein HR-Outsourcingprovider (HRO) einen wirkungsvollen Aktionsplan, Datenflussdiagramme, eine durchgeplante Datenhaltung, robuste Sicherheitsplattformen und Datentransferprogramme, all dies unter Aufsicht eines Datenschutzbüros (DPO, Data Protection Office).

Die Cloud kann, richtig eingesetzt, die Risiken mangelhafter Compliance mit der GDPR und dem lokalen Arbeitsrecht verringern.

Dieser Text beschreibt die Rolle der GDPR und zeigt, wie Cloud eine regelkonforme digitale HCM-Strategie vereinfachen kann, statt sie zu behindern.

DIE REGULIERUNGSUMGEBUNG FÜR DATEN ÄNDERT SICH

Die GDPR ist die größte Veränderung des Datenschutzrechts der vergangenen 30 Jahre. Sie erneuert das bestehende Datenschutzrecht aus den Zeiten vor Facebook, LinkedIn und der Cloud und vereinheitlicht es in allen 28 Mitgliedsländern.

Die GDPR ist die größte Veränderung des Datenschutzrechts der vergangenen 30 Jahre.

Die bestehende Datenschutzrichtlinie wurde 1995 verabschiedet und reicht nicht, um die persönlichen Daten von Einzelnen in einer Welt zu schützen, in der ständig persönliche Daten online gespeichert und ausgetauscht werden. Die Richtlinie wurde zudem in jedem Mitgliedsland entsprechend den dortigen Geschäftsusancen umgesetzt. Das führte zu länderspezifisch unterschiedlichen Datenschutz-Regimes in der Europäischen Union. Die GDPR ist deswegen ein wesentlicher Schritt in Richtung Vereinheitlichung und Modernisierung des europäischen Datenschutzrechts.

Die Definition persönlicher Daten ist sehr breit angelegt: Sie erfasst alle Informationen, mit deren Hilfe es möglich ist, potentiell oder tatsächlich – direkt oder indirekt – ein Individuum zu identifizieren. Dazu gehören offensichtliche Merkmale wie der Name oder Identifikationsnummern, aber auch Geolokationsdaten oder IP-Adressen, biometrische oder genetische Informationen. Wichtig ist: Personal- und Kundendaten sind betroffen.

Zwar ist der Einfluss der GDPR auf HR-Daten vielleicht offensichtlich, er soll aber hier trotzdem besonders hervorgehoben werden: Mitarbeiterdaten unterliegen laut GDPR dem gleichen Recht wie Kundendaten. Für Unternehmen bedeutet das mehr Pflichten zum Schutz ihrer Mitarbeiterdaten, zudem wurde das Recht der Mitarbeiter auf Datenzugriff, -aktualisierung und -löschung verstärkt, und es hat gravierende Folgen, wenn ein Unternehmen die Regeln nicht einhält (siehe weiter unten).

Mitarbeiterdaten unterliegen laut GDPR demselben Recht wie Kundendaten.

HR-Abteilungen müssen aber nicht nur die GDPR- und Datenschutz-Regeln einhalten – dazu kommt eine Fülle anderer Regeln und länderspezifischer Regulierungen, was eine große Herausforderung ist. Auf fünf Themengebieten müssen HR-Abteilungen besonders auf Compliance achten: Versicherungen und Sonderleistungen, Einstellung, Arbeitssicherheit und Arbeitsschutz, Lohnbuchhaltung und die gesamte Mitarbeiterentwicklung von der Einstellung bis zum Verlassen des Betriebes (Employee-Life-Cycle-Management).

Organisationen fordern von ihren Personalabteilungen diesbezüglich immer öfter proaktives Handeln und eine bewusste Handhabung aller “personenbezogenen Risiken”. Das fällt

Organisationen schwerer, die in mehreren Rechtsordnungen gleichzeitig präsent sind, beispielsweise, weil sich Hauptfirmensitz und Niederlassungen in unterschiedlichen Ländern befinden. Wichtig ist: Compliance sollte innerhalb des Personalmanagements als ergänzende Risikomanagementfunktion verstanden werden, die auch das Management des Humankapitals positiv beeinflusst.

Zudem erhöhen Compliance-Aufgaben die Bedeutung des Personalbereichs: Bisher war er lediglich zuständig für die passive Verwaltung der Personaldaten, eine Aufgabe mit minimaler strategischer Bedeutung. Nun verwandelt er sich in einen strategischen Schlüsselpartner, der die Risikokosten des Unternehmen verringert und gleichzeitig Produktivität und Engagement der Mitarbeiter erhöht.

Es gibt viele und vielfältige Compliance-Anforderungen an HR-Bereiche, die eine ständige Überwachung und Management ihrer Parameter erfordern: Lohnbuchhaltung und Steuererklärungen (PAYE-System in Großbritannien, „impôt sur le revenu“ in Frankreich, etc), Training (Einarbeitung, Betrugsdetektion etc.), berufliche Weiterentwicklung (Überwachung der Credits of Personal Developments/CDPs oder anderer Metriken, die von professionellen Organisationen und Vorständen angewendet werden, um die Mitgliedschaft zu erhalten) oder die angemessene Überprüfung von Kandidaten vor der Anstellung und bei Beendigung des Arbeitsverhältnisses.

DIE WICHTIGSTEN INHALTE DER GDPR

Wie oben diskutiert, verwendet die GDPR eine sehr umfassende Definition persönlicher Daten. Aus HR-Sicht ist jede Information geschützt, die sich auf einen individuellen Mitarbeiter bezieht, und einige Informationstypen dürfen gar nicht gesammelt werden. Das betrifft „spezielle Datenkategorien“, die auch als sensitive Daten bezeichnet werden. Dazu gehören genetische, biometrische und Gesundheitsdaten sowie Daten zu sexuellen Präferenzen oder der sexuellen Orientierung. Allerdings gibt es zu diesem Verbot eine wichtige Ausnahme: die Verarbeitung von Informationen zum Zweck der Vorbeugung, des betrieblichen Gesundheitswesens oder der Beurteilung der Arbeitsfähigkeit eines Mitarbeiters (GDPR Artikel 9).

Die GDPR führt auch in einigen Fällen eine gemeinsame Verantwortung und Haftung von Datenverantwortlichen (bei HR-Daten meist der Arbeitgeber) und Datenverarbeitern (Dritte, die Daten für den Arbeitgeber verarbeiten) ein. Das ist wichtig für alle Arbeitgeber, deren HR-Datenverarbeitung bereits ausgelagert ist oder ausgelagert werden soll.

Hinsichtlich der Sicherheitsanforderungen ist die GDPR absichtlich vage formuliert. Von den 99 Artikeln im finalen Text der GDPR befasst sich nur ein sehr detailarm formulierter (Artikel 32) explizit mit der Herstellung von Sicherheit. Die Regulierung zielt vor allem darauf ab, dass Organisationen „State-of-the-art“-Technologie einsetzen und zudem die Kosten, Risiken und den geschäftlichen Kontext berücksichtigen sollen. Daher müssen Organisationen im Vorfeld entscheiden, was State-of-the-art für die jeweilige Organisation bedeutet: eine schwierige Aufgabe. Der Artikel rät auch nachdrücklich zu Verschlüsselung (obwohl sie nicht vorgeschrieben wird) und Pseudonymisierung (im Allgemeinen gleichbedeutend mit der Verwendung von Tokens).

Die GDPR ist ungenau hinsichtlich der Sicherheits-maßnahmen, aber eindeutig hinsichtlich der Bedeutung von Sicherheit.

Allerdings ist zu bedenken, dass Sicherheit ein grundlegendes Prinzip bei der Verarbeitung persönlicher Daten ist (Artikel 5). Insbesondere verlangt die GDPR, dass Daten so verarbeitet werden, dass „eine angemessene Sicherheit der persönlichen Daten sichergestellt ist“. Obwohl also die GDPR unpräzise hinsichtlich der Maßnahmen ist, die

ergriffen werden sollen, um Sicherheit herzustellen – hinsichtlich der herausragenden Bedeutung von Sicherheit ist die Verordnung eindeutig.

Aus HCM-Perspektive markiert die GDPR einige technologische Schlüsselentscheidungen, die der CHRO (Company Human Relations Officer) treffen muss. So werden wohl die meisten CHROs sich für Verschlüsselung aller gespeicherten, transferierten oder gesicherten Mitarbeiterdaten aussprechen, obwohl sie nicht vorgeschrieben ist. Die GDPR verlangt die Protokollierung der Datenverarbeitung und die Möglichkeit, Audits zu forensischen und Compliance-Zwecken zu erleichtern.

GDPR: Mehr als Sicherheit

Ein häufiges Missverständnis ist, dass es in der GDPR im Grunde vor allem um die Datensicherheit geht. Zwar ist Datensicherheit, wie oben beschrieben, ein wichtiger Teil der GDPR, es ist aber falsch, anzunehmen, dass Sicherheit das grundlegende technologische Thema der Verordnung ist. Die Verordnung stellt auch andere Anforderungen, die andere Sicherheitstechnologien verlangen.

Ein Beispiel ist die Datenportabilität (Artikel 20). Danach haben Individuen das Recht, ihre persönlichen Daten vom Datenverantwortlichen möglichst in maschinenlesbarem Format zu verlangen, sobald die betreffende Person der Verarbeitung zugestimmt oder einen entsprechenden Vertrag geschlossen hat. Nach dem Recht auf Löschung (bekannter als „Recht auf Vergessen“, Artikel 17) kann jede Person von einem Datenverantwortlichen verlangen, dass er persönliche Daten löscht (unter spezifischen Umständen und mit einigen Ausnahmen). Besonders verschärft wurden die Einwilligungsregeln für die Erfassung von Daten über Jugendliche unter 16 Jahren – hier ist nun grundsätzlich das elterliche Einverständnis erforderlich (Artikel 8).

Eines der wichtigsten Themen der GDPR – allein sieben Artikel befassen sich damit – sind Datentransfers (Artikel 44 bis 50).Dazu gehört auch der Transport von Daten in sogenannte Drittländer. Ein Drittland ist eines, das nicht zur EU gehört. Die Verordnung will sicherstellen, dass Datenverantwortliche Daten angemessen schützen, auch wenn sie in Bereiche transferiert werden, in denen die EU-Rechtsordnung nicht mehr gilt. Die EU hat zwei Mechanismen, um diese Bedrohung abzuwehren: Die Kontrolle von Datentransfers außerhalb der EU und eine Exterritorialitätsklausel, die die Geltung der GDPR auf alle Daten ausdehnt, die eine Person in der EU betreffen (ohne Berücksichtigung des Ortes, an dem sich die Daten befinden, siehe Artikel 3).

Datentransfers können bei HR-Daten vorkommen, wenn Arbeitgeber einen Cloud-Service oder HR-Outsourcing-Provider nutzen. Sie müssen in diesem Fall jederzeit wissen, wo ihre HR-Daten sich physisch befinden und insbesondere, ob sie an einem Ort außerhalb der EU sind. Es ist vollkommen legal, Daten aus der EU zu exportieren. Allerdings erfordert das eine von mehreren möglichen Formen der Rechtsaufsicht. Zu ihnen gehören:

- Transfers auf Basis rechtlicher Angemessenheit: Die EU pflegt eine Liste von Ländern, deren Datenschutzbestimmung als angemessen (oder gleichwertig) mit der GDPR gelten. Derzeit stehen nur 12 Länder auf dieser Liste und (das ist für viele wichtig) die USA gehören nicht dazu.
- Bindende Unternehmensregeln (Binding Corporate Rules, BCRs): Sie bestehen in einer offiziellen Verpflichtung durch einen Datenverarbeiter, Datenschutzprogramme zu implementieren, die ein hohes Datenschutzniveau in Übereinstimmung mit der GDPR garantieren und die von der EU-Datenschutzbehörde genehmigt wurden. Das ist nicht trivial und bedeutet eine dauerhafte, rechtlich bindende Verpflichtung auf die Datenschutzprinzipien der EU.
- Standardklauseln, die in jeden einzelnen Vertrag integriert werden.

- Die Zustimmung der betroffenen Person zum Transport ihrer Daten aus der EU.
- Die Einhaltung definierter Verhaltensregeln (Codes of Conduct) oder das Absolvieren einer entsprechenden Zertifizierung. Beide Strukturen sind in der GDPR vorgesehen, müssen aber noch implementiert werden.

Der zweite wichtige Mechanismus, der rechtskonforme Datentransfers erlaubt, kann genutzt werden, wenn eine spezifische Vereinbarung zwischen der EU und dem Drittland besteht. Diese Herangehensweise empfiehlt sich, wenn die rechtliche Angemessenheit nicht garantiert ist. Das beste Beispiel dafür ist Privacy Shield, eine bilaterale Vereinbarung zwischen den USA und der EU, die Datentransfers zu Datenverarbeitern entsprechend der Vereinbarung erlaubt. Allerdings ist damit zu rechnen, dass Privacy Shield wie Safe Harbour gerichtlich überprüft wird. IDC rät Firmen mit dem Hauptsitz in den USA, die langfristig GDPR-konform arbeiten wollen, zu BCRs.

Ein aktuelles Beispiel für dieses Datentransfer-Regime ist der geplante Austritt Großbritanniens aus der EU (Brexit). In Bezug auf das Datenschutzrecht ist der Brexit wegen der Datentransferregeln der GDPR weitgehend irrelevant. Britische Unternehmen, die mit einem EU-Partner Handel treiben oder persönliche Daten aus der EU verarbeiten wollen, müssen die Datentransferregeln der GDPR einhalten. Angesichts des großen Umfangs der aktuellen Handelsaktivitäten zwischen Großbritannien und der EU ist es wahrscheinlich, dass Großbritannien beim Verlassen der EU GDPR-ähnliche Bestimmungen erlassen wird (die britische Datenschutzbehörde hat bereits diesen Standpunkt artikuliert).

In Bezug auf das Datenschutzrecht ist der Brexit nahezu irrelevant.

Sanktionen bei Nichteinhaltung von Regeln

Viel Aufmerksamkeit wurde bisher den “effektiven, angemessenen und abschreckenden” Bußgeldern gewidmet, die die Regulierungsbehörden verhängen können. Dies gilt besonders für die Obergrenzen, die bei 4 % des weltweiten Gesamtumsatzes oder 20 Millionen Euro liegen, wobei jeweils die höhere Summe gilt. Wichtig ist zunächst, dass Bußgelder in dieser Höhe nur dann verhängt werden dürfen, wenn es sich um Verstöße gegen die Grundprinzipien der GDPR (Artikel 5), fundamentale Rechte der Betroffenen wie Einwilligung und Löschung sowie Rechtsverletzungen beim Datentransfer handelt. Bei Datenverlusten, die zum Beispiel aus Sicherheitsschwachstellen resultieren, gilt eine niedrigere Höchstgrenze von maximal 2 Prozent des weltweiten Umsatzes oder 10 Millionen Euro. Arbeitgeber sind möglicherweise besorgt über Pflichtmeldungen bei Sicherheitsverletzungen persönlicher Daten. Datenverantwortliche müssen ihre Aufsichtsbehörde bei solchen Vorkommnissen benachrichtigen, sofern sie zu einem „Risiko für die Rechte und Freiheiten von Individuen“ (Artikel 33) führen. Dann müssen sie das Ereignis auch den Betroffenen selbst mitteilen (Artikel 34). Das kann zu negativer Publizität führen, die anschließend Marke und Reputation beschädigt.

Als äußerste Maßnahme kann eine Aufsichtsbehörde die weitere Datenverarbeitung aussetzen (Artikel 58). Im Endeffekt kann das bedeuten, dass der Handel oder die Lohnauszahlung unterbrochen werden müssen, wenn der betroffene Datenverarbeitungsvorgang einen Kerngeschäftsprozess unterstützt.

Es überrascht angesichts dieser Sanktionen nicht, dass die GDPR auch in den Vorstandsetagen der in der EU ansässigen Unternehmen Aufmerksamkeit erregt (und wegen der Exterritorialitätsregeln darüber hinaus). Allerdings werden wohl Sanktionen (wie Bußgelder) vor allem dann verhängt werden, wenn die Betroffenen sich nicht bemühen, Rechtskonformität herzustellen. Die GDPR legt viel Wert auf nachweisbare Compliance-Bemühungen. Dazu gehören die Dokumentation der Datenverarbeitungsprozesse und deren Aufbewahrung. Lückenlose Dokumentation und Auditierbarkeit sind kritisch. Jederzeit Compliance im Sinn von Verantwortlichkeit demonstrieren zu können, ist ein fundamentaler Grundsatz der GDPR.

WARUM DIE CLOUD HR-PROZESSE UNTERSTÜTZT UND NICHT BEHINDERT

Im Grunde sind Cloud-Services eine Form der Auslagerung. Wie immer beim Outsourcing muss der Dienstleister im Vorfeld sorgfältig geprüft werden. Das gilt auch für Vereinbarungen hinsichtlich Cloud-basierender HR-Prozesse.

Es gibt kein rechtliches oder technisches Hindernis für die Speicherung von HR-Daten in der Cloud.

Cloud-Verarbeitung unterscheidet sich von vielen anderen Prozessen allerdings wegen der Vielfalt der involvierten Datenverarbeitungseinrichtungen. Unternehmen müssen sie praktisch überprüfen, indem sie gezielt Fragen zum Sicherheitsniveau und implementierten Datenschutzprozessen stellen und die entsprechenden Auditberichte prüfen. Dazu gehören auch Berichte von Dritten, die der Cloud-Provider möglicherweise zur Verfügung stellt. So ist es kritisch, die physische Sicherheit des Rechenzentrums, das die persönlichen Daten speichert, zu verstehen und bewerten zu können. Das Sicherheitsniveau eines glaubwürdigen Anbieters sollte mindestens so gut sein wie das von Großunternehmen, und sehr wahrscheinlich besser als das durchschnittlicher Arbeitgeber. Dazu gehören meist auch Zertifizierungen nach ISO 27001 und (zunehmend) nach ISO 27018. Letztgenannte Norm befasst sich mit persönlichen Daten in Public Clouds.

Es gibt also keine rechtlichen oder technischen Faktoren, die die Speicherung von HR-Daten in der Cloud verbieten. Manche Unternehmen werden ein Rechenzentrum in der EU vorziehen, einschließlich dessen zertifizierter physischer und logischer Sicherheit. Dann sollte auch der Zugriff auf EU-Daten nur aus der EU möglich sein: Zugriff von außerhalb der EU würde einen Datentransfer (durch die Daten im Transit) bedeuten und so die Effizienz EU-basierter Rechenzentren vermindern.

Bindende Unternehmens-regeln erweisen sich derzeit als wirksamste rechtliche Maßnahme bei Datentransfers aus der EU.

Die meisten loud-basierenden Lösungen erfordern allerdings in größerem oder kleinerem Umfang Datentransfers über die EU-Grenzen hinaus. Anbieter haben Lösungen entwickelt, um die persönlichen Daten dabei zu schützen. Dazu gehören auch formalisierte Vertragsklauseln. Aber bindende Unternehmensregeln erweisen sich derzeit als wirksamste rechtliche Maßnahme bei Datentransfers aus der EU.

Viele Unternehmen werden zukünftig die Auslagerung der HR-Datenverarbeitung wählen, um ihre diesbezüglichen Risiken und Compliance-Verpflichtungen zu verringern. Arbeitgeber können ihr Risiko so zwar nicht vollständig beseitigen, aber die Auswahl eines glaubwürdigen Providers ist eine angemessene Maßnahme.

DIE ROLLE DER TECHNOLOGIEANBIETER BEI HR-TRANSFORMATION UND COMPLIANCE

Oft heißt es, Unternehmen könnten zwar die Verarbeitung, niemals aber ihre Verantwortung für persönliche Daten auslagern. Was die GDPR angeht, ist das noch immer richtig, allerdings bedeutet die Ausdehnung der rechtlichen Verantwortung auf die Datenverarbeiter, dass wenigstens etwas Verantwortung für die Regelkonformität sich auf einen externen Datenverarbeitungs-Provider verlagert.

Um es klar zu sagen: Der Datenverantwortliche bleibt verantwortlich für die Einhaltung der Kernprinzipien der GDPR (Artikel 5) und muss sie nachweisen. Ein Datenverarbeiter muss in der Lage sein, technische und organisatorische Maßnahmen zu implementieren, die mit einem Datenverantwortlichen vereinbart werden. Er unterliegt bei Nichteinhaltung auch denselben Sanktionen. Das führt zu der Frage: Wie kann ein Datenverantwortlicher feststellen, ob ein Datenverarbeiter diese Anforderung erfüllt?

Codes of Conduct und Zertifizierungen sind unter der GDPR geltendes Recht, aber bis heute gibt es beides praktisch nicht. Deshalb müssen Datenverarbeiter die Arbeitgeber mit anderen Mitteln von ihrer Glaubwürdigkeit überzeugen, beispielsweise mit Zertifizierungen nach ISO 27001 (Informationssicherheitsmanagement), 27018 (Schutz persönlicher Daten in Public Clouds) oder 29100 (Privacy-Framework), unabhängigen Auditierungen und BCRs für Datenverarbeiter, die sich langfristig und organisatorisch auf die Einhaltung der Prinzipien der GDPR verpflichten wollen. BCRs sind für die EU-Datenschutzbehörden der Goldstandard beim Datenschutz.

Da der 25. Mai 2018 unaufhörlich näher rückt, dürfen Arbeitgeber die GDPR und die mit ihr verbundenen grundlegenden Änderungen nicht ignorieren.

HRO-Provider sehen sich der Herausforderung gegenüber, gleichzeitig ihr Geschäft so zu skalieren, dass sie mehrere Arbeitgeber effizient unterstützen können und die nötigen Kenntnisse von lokalem Arbeitsrecht und lokalen Usancen besitzen. Sie müssen Betriebsprozesse internationalisieren, aber gleichzeitig lokal implementieren: IDC geht davon aus, dass nur wenige HRO-Provider in der Lage sind, beide Aspekte unter einen Hut zu bringen.

Ein bedeutender Aspekt für HR-Profis sind die steigenden Anforderungen, die das Kerngeschäft an den Personalbereich stellt. Die HR-Systeme der Vergangenheit zeichneten vor allem Daten auf und speicherten sie. Sie hatten nur geringen zusätzlichen strategischen Wert für die Organisation und befassten sich nur mit dem Management der einfachsten Aspekte rund um die Betriebszugehörigkeit der Mitarbeiter.

Ein bedeutender Aspekt für HR-Profis sind die steigenden Anforderungen, die das Kerngeschäft an den Personalbereich stellt.

Mit der Zeit und veränderten Fähigkeiten, Regeln und vor allem der neuen Rolle, die von der HR erwartet wird, wollen HR-Spezialisten ihre strategische Bedeutung erhöhen, tiefere Einblicke gewinnen und wertvoller für die gesamte Organisation werden. Aus diesem Blickwinkel kann man Compliance kaum überschätzen; im Gegenteil: Den Compliance-Aspekt aus der HR-Perspektive zu managen, ist ein Schlüsselfaktor zur Verringerung von Geschäftsrisiken. Es kann Kosten senken und Rechtsstreitigkeiten verhindern, gleichzeitig wird die Rolle des Personalbereichs komplexer und weitreichender.

EMPFEHLUNGEN

Befassen Sie sich mit der GDPR

Da der 25. Mai 2018 unaufhörlich näher rückt, dürfen Arbeitgeber die GDPR und die durch sie verursachten grundlegenden Änderungen nicht ignorieren. Die GDPR stellt die meisten Organisationen vor große rechtliche und technische Herausforderungen – viele werden damit kämpfen, sie voll umfänglich bis zum ersten Geltungstag zu implementieren. Arbeitgeber, die sich noch nicht mit den Auswirkungen der GDPR befasst haben, sollten unverzüglich damit beginnen.

Sehen Sie die GDPR als Chance

Es ist einfach, die GDPR und die vielen Veränderungen, die sie hervorruft, als großes Hindernis und Ablenkung von den üblichen Geschäftsaktivitäten zu betrachten. Tatsächlich glaubt IDC, dass die GDPR Arbeitgebern ausgezeichnete Chancen bietet. Sie schafft eine klare und geregelte Regulierungsumgebung für die Datentransfers, die Cloud-basierenden HRO-Diensten zugrunde liegt. Mit angemessenen Sicherheitszusicherungen des Providers können Unternehmen cloud-basierte HRO unter dem GDPR-Regime sicher und rechtskonform als Teil ihrer HCM-Strategie einsetzen.

Compliance bedeutet Partnerschaft

Im August 2016 schloss IDC seine Studie zum *Human Capital Management* in Westeuropa ab. Mehr als 250 Entscheidungsträger aus dem Personalmanagement und Manager wurden befragt. In unserer Befragung zeigten sich der Datenschutz und Veränderungen in der Gesetzgebung (GDPR) als wichtigste Themen für einen von drei Teilnehmern. Nur 23 % der Befragten sahen sich lediglich leicht oder gar nicht betroffen. Die Mehrheit der Antwortenden (76 %) sieht Datenschutz und Compliance (zur GDPR und anderen Gesetzen) noch immer als kaufentscheidenden Faktor bei der Auswahl einer HCM-Lösung.

Anbieter müssen dem HR-Bereich die erforderlichen Werkzeuge und Erkenntnisse zusammen mit der Zusicherung bieten, dass die Lösungen in ihrem Portfolio sowohl regelkonform als auch sicher sind. Nur dann unterstützen sie HR-Abteilungen dabei, ihre langfristigen Ziele besser zu erreichen, insbesondere die Transformation von einer Back-Office-Funktion zu einem wichtigen Partner des Vorstands.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions