Audit Committee News
Ausgabe 64 / Q1 2019 / Risk Management & Compliance

Der Compliance Stand von Unternehmen mit der DS-GVO – wo liegen die Risiken?

Der 25. Mai 2018 war ein prägendes Datum für den Datenschutz sowohl in Europa als auch weltweit. Die Datenschutz-Grundverordnung der Europäischen Union (DS-GVO, auf Englisch GDPR) fand nach zweijähriger Übergangsfrist ihre Gültigkeit. Als eine der weitreichendsten Neuerungen in der jüngeren Geschichte des Datenschutzes stellt die DS-GVO verschärfte Anforderungen an Unternehmen in- und ausserhalb der Europäischen Union. Welche Implikationen die DS-GVO für Schweizer Firmen hat, was der Stand der Umsetzung ist, wo die Schwierigkeiten lagen und wo heute noch die grossen Herausforderungen zu sehen sind, wird im Folgenden erläutert.

Anwendbarkeit der DS-GVO

Grosse Beachtung erfuhr die DS-GVO vor allem aufgrund ihrer weiten Anwendbarkeit. So müssen einerseits Unternehmen mit Niederlassung in der EU, welche personenbezogene Daten verarbeiten, die DS-GVO einhalten, andererseits jedoch auch Unternehmen ausserhalb der EU. Die letzteren fallen nur dann unter die DS-GVO, wenn sie im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen an Personen in der EU oder dem Beobachten des Verhaltens von Personen in der EU personenbezogene Daten verarbeiten. Dieser exterritoriale Effekt der DS-GVO hat auch für Schweizer Unternehmen konkrete Folgen. So muss beispielsweise ein Schweizer Uhrenunternehmen, welches seine Waren auf dem EU Markt vertreibt und in diesem Zusammenhang personenbezogene Daten von Personen in der EU verarbeitet, gleichermassen die DS-GVO einhalten wie ein deutscher Spielwarenhändler, welcher lediglich in Deutschland seine Produkte verkauft.

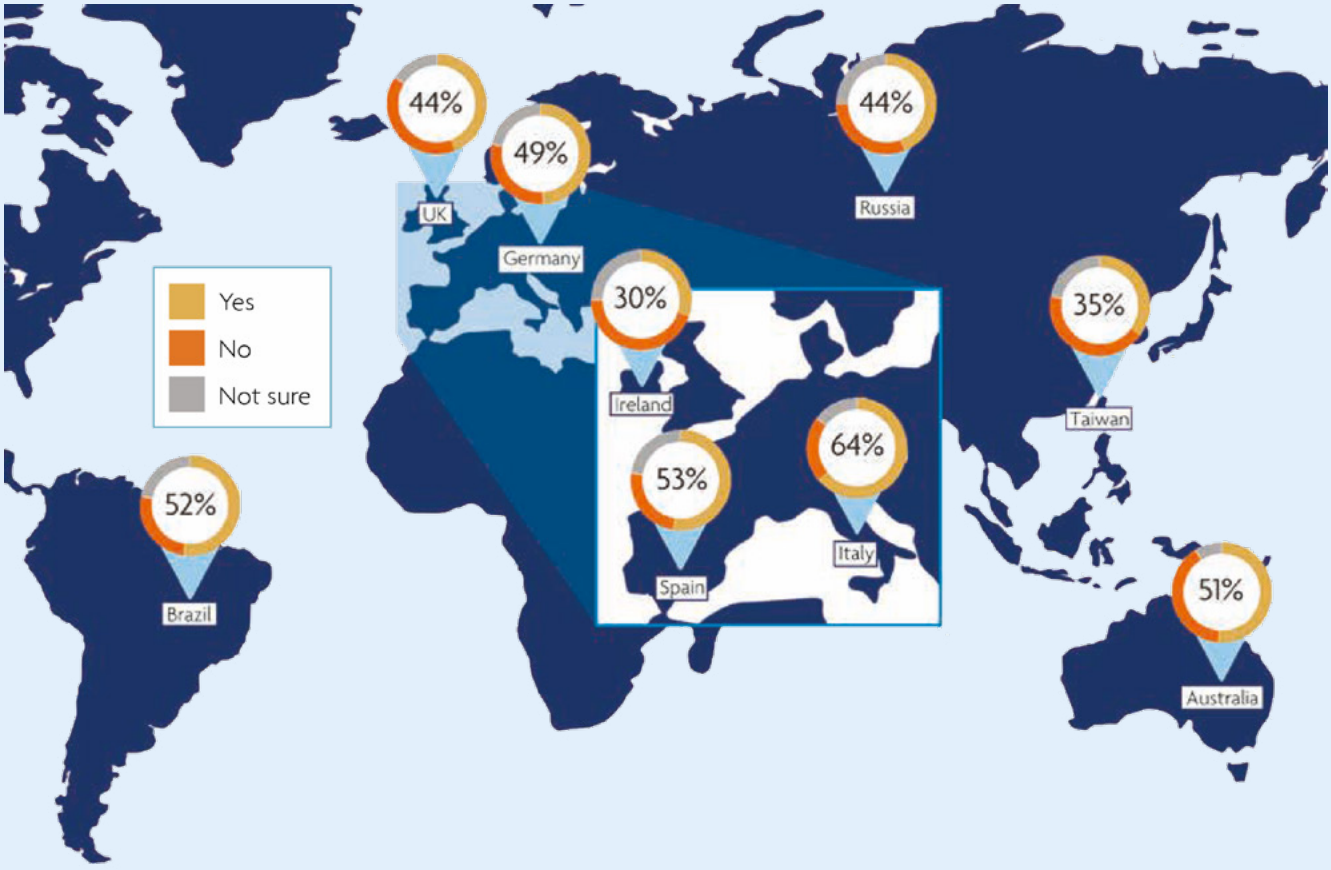
Wie sehen sich Schweizer Firmen betroffen?

Vor diesem Hintergrund und der hohen internationalen Verflechtung von Schweizer Unternehmen ist die Einhaltung der DS-GVO durch zahlreiche Schweizer ein Must. Darüber, wie viele Unternehmen in der Schweiz tatsächlich von der DS-GVO betroffen sind, gehen die Meinungen jedoch weit auseinander. Laut einer Studie der ZHAW sehen sich nicht viele der (vor allem aus dem KMU-Bereich) befragten Unternehmen von der DS-GVO betroffen. Berater und Anwälte dagegen erachten die DS-GVO auf das Gros der Schweizer Unternehmen als anwendbar.[1]

Anforderungen der DS-GVO

Die DS-GVO hat viele datenschutzrechtliche Neuerungen gebracht und ein breit angelegtes Umsetzungskonzept von

1 Ebert, Nico; Widmer, Michael; 2018. Datenschutz in Schweizer Unternehmen 2018 : eine Studie des Instituts für Wirtschaftsinformatik und des Zentrums für Sozialrecht. Winterthur: ZHAW Zürcher Hochschule für Angewandte Wissenschaften. Abgerufen unter: https://doi.org/10.21256/zhaw-4001, S. 3 f.



Selbsteinschätzung von Unternehmen weltweit zu ihrer DS-GVO Compliance.

Quelle: KPMG AG, The Legal 500 Series, The GC's Guide to GDPR: From schock and denial to acceptance and hope. Abgerufen unter: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/07/gdpr-july-2018.pdf, S. 7.

Unternehmen erfordert. Die drohenden Bussen von bis zu 20 Millionen Euro oder 4% des weltweit erzielten Umsatzes haben die Unternehmen zusätzlich unter Druck gesetzt, noch vor dem 25. Mai 2018 DS-GVO konform zu sein. Vor diesem Hintergrund haben Unternehmen einen risikobasierten Ansatz verfolgt und bei der Umsetzung diejenigen Elemente priorisiert, welche bei Nicht-Konformität die grössten finanziellen bzw. rufschädigenden Folgen nach sich ziehen würden. Als priorisierte Handlungsfelder gelten:

- Aufstellung einer Privacy Organisation, allenfalls inkl. Ernennung eines Datenschutzbeauftragten
- Einführung von Key Prozessen:
  - Notifikationsprozess für Datenschutzverletzungen
  - Prozess für Datenschutz-Folgenabschätzungen
  - Prozess zur Beantwortung von Anfragen durch Datensubjekte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch)
- Aufsetzen und Führen eines Verarbeitungsverzeichnisses
- Management von Einwilligungen und Datenschutz-Erklärungen
- Aktualisierung von bestehenden und Abschluss neuer DS-GVO konformer Verträge (z.B. bei Outsourcing Partnerschaften)
- Gewährleistung von geeigneten Schutzmassnahmen bei Datenübermittlungen ins Ausland
- Privacy by Design und Default
- Einsatz von technischen Massnahmen zum Schutz personenbezogener Daten.

Konkrete Umsetzung der DS-GVO Anforderungen

Die einzelnen Handlungsfelder wurden von den Unternehmen unterschiedlich schnell angegangen. So beanspruchte die Anpassung der Einwilligungstexte und Datenschutz-Erklärungen wenig Zeit, die Einführung der neuen Key Prozesse dagegen viel mehr, vor allem in schwach strukturierten und wenig organisierten Unternehmen. Verhältnismässig lange Zeit wurde für die Anpassung der bestehenden oder den Abschluss neuer Verträge benötigt – dies vor dem Hintergrund, dass viele Organisationen Outsourcing Partnerschaften im zweistelligen Bereich führen und vertragliche Anpassungen allgemein viel Zeit beanspruchen. Die Anpassung von Verträgen dauert teils bis heute noch an. Ebenso lange hat die Anpassung des Schutzniveaus der IT Security gebraucht und führte teilweise zum Aufsetzen separater IT Projekte.

Umsetzung der DS-GVO durch Schweizer Organisationen

Die Umsetzung der Anforderungen der DS-GVO wurde innerhalb von Schweizer Unternehmen sehr unterschiedlich thematisiert, budgetiert und durchgeführt. Wie weit die Umsetzung der DS-GVO Voraussetzungen fortgeschritten ist, hängt dabei grösstenteils von der Grösse, dem Regulierungsgrad und der internationalen Verflechtung der jeweiligen Organisation ab. So haben Unternehmen, welche europa- und weltweit agieren sowie mit Personen aus der Union in Berührung stehen früh angefangen, sich mit dem Thema der DS-GVO auseinanderzusetzen und entsprechende Budgets für Gap-Assessments und Implementierungsprojekte zu bestimmen. Auch regulierte Branchen (Finanzdienstleister, Pharma etc.) sind bereits lange an der Umsetzung und waren um den 25. Mai grösstenteils DS-GVO konform. Nichtregulierte Branchen haben eher später mit der Umsetzung der neuen Anforderungen begonnen und sind teilweise heute noch mittendrin. Weit fortgeschritten sind zudem auch grössere Organisationen, welche nebst dem benötigten Budget auch die entsprechenden Ressourcen zur Verfügung stellen konnten.

Am wenigsten fortgeschritten in der Schweiz sind KMUs. Sie haben zudem verhältnismässig spät angefangen, sich dem Thema Datenschutz und den neuen Anforderungen zu widmen. Eine Studie der ZHAW, welche 265 Deutschschweizer Unternehmen zu ihrem Datenschutz befragt hat, bestätigt dieses Bild. Die für den Datenschutz eingesetzten Ressourcen seien beschränkt und auch das Bewusstsein innerhalb der Organisationen mangels entsprechender Schulungen eher limitiert.[2] Dieselbe Studie hat ausserdem die Herausforderungen bei der Umsetzung festgehalten. So seien der Detailierungsgrad der Umsetzung, die rechtliche Konformität der Datenverarbeitungen und die Festlegung der erforderlichen Massnahmen von den befragten Unternehmen als besonders schwierig empfunden worden.[3] Unsere Erfahrungen im Consulting in verschiedenen Gap-Assessments und Implementierungsprojekten deckt sich mit dieser Einschätzung.

Dass Organisationen weltweit grosse Herausforderungen bei der Umsetzung der DS-GVO haben, hat auch eine Umfrage der KPMG unterstrichen. Nach Befragung von weltweit 448 Organisationen wurde festgehalten, dass die beschränkten Ressourcen, die Verantwortlichkeiten innerhalb des Unternehmens (wer ist für den Datenschutz zuständig), das Verständnis der DS-GVO selbst sowie das Verständnis der IT- und Datenlandschaft als grosse Herausforderungen angesehen werden.[4]

Schweizer Datenschutzrecht

Das Schweizer Datenschutzrecht (konkret das Datenschutzgesetz) befindet sich zurzeit noch immer in Revision. Vom Bundesamt für Justiz wird hervorgehoben, dass durch die Revision der Datenschutz gestärkt und gleichzeitig den Anforderungen der DS-GVO angenähert werden solle.[5] Die Annäherung an die europäischen Entwicklungen ist notwendig, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung in die Schweiz auch künftig möglich bleibt.

2 Ebert / Widmer (2018), S. 3 f.
3 Ebert / Widmer (2018), S. 17 f.
4 KPMG AG, The Legal 500 Series, The GC's Guide to GDPR: From schock and denial to acceptance and hope. Abgerufen unter: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/07/gdpr-july-2018.pdf, S. 4 f.
5 https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutz-staerkung.html, abgerufen am 21. November 2018.

Gemäss dem aktuellen Stand soll die Revision des Datenschutzgesetzes (DSG) gestaffelt durchgeführt werden. So soll in einem ersten Schritt eine Anpassung an das europäische Recht, konkret an die Schengen-Verträge erfolgen, im zweiten Schritt die weitere Revision durchgeführt werden. Eine ganzheitlich revidierte Fassung des DSG vor 2020 ist nicht zu erwarten.

Inhaltlich wird das Schweizer DSG aller Wahrscheinlichkeit nach in vielen Bereichen der DS-GVO gleichen:

- Identische Begriffsbestimmungen (z.B. Definition zu besonders schützenswerten Personendaten, Profiling, Verantwortlichem, Auftragsverarbeiter etc.)
- Grundprinzipien (z.B. rechtmässige Verarbeitung von Daten, Erfordernis Daten richtig und aktuell zu halten, Zweckbindung bei der Verarbeitung etc.)
- Privacy by Design und Default
- Ernennung eines Datenschutzberaters
- Verzeichnis der Bearbeitungstätigkeiten
- Gewährleistung von geeigneten Schutzmassnahmen bei Datenübermittlungen ins Ausland
- Rechte der Datensubjekte
- Datenschutz-Folgeabschätzung
- Notifikationsprozess bei Datenschutzverletzungen
- Abschluss von DSG konformen Verträgen bei Auslagerung von Datenverarbeitung an Dritte.

Im Gegensatz zur DS-GVO enthält der derzeitige Entwurf der DSG (E-DSG) zwei Teile, wobei der erste auf private Personen, der zweite auf Bundesorgane anwendbar ist. Zudem sieht das E-DSG ein Auskunftsrecht für Daten von verstorbenen Personen vor, was in der DS-GVO nicht vorgesehen ist.

Wie auch die DS-GVO sieht das E-DSG die Möglichkeit vor, bei Verstössen Bussen auszusprechen. Dabei werden insbesondere Verletzungen von Informations-, Auskunfts- und Mitwirkungspflichten, Verstösse gegen rechtmässige Bekanntgabe von Daten ins Ausland, nichtkonforme Auslagerung von Datenverarbeitungen an Drittparteien sowie Verstösse gegen Datensicherheitsstandards mit hohen Bussen geahndet. Anders als in der DS-GVO – und zugleich häufig kritisiert – bietet die E-DSG die Möglichkeit, Bussen gegen natürliche Personen auszusprechen, insbesondere Leitungspersonen in einem Unternehmen.

Nächste Schritte

Auch im kommenden Jahr wird die konforme Umsetzung der DS-GVO ein Thema bei Unternehmen in der Schweiz bleiben. Der Fokus wird darauf liegen, bereits eingeführte Massnahmen zu verbessern, Prozesse zu optimieren, IT Security Massahmen auszubauen, Vertragsverhältnisse weiter und vollständig anzupassen sowie Schulungen intern weiterzuführen. Unternehmen, welche bereits weit mit der Umsetzung fortgeschritten sind, werden zudem interne Audits durchführen sowie Zertifizierungen anstreben, um ihre die Konformität mit der DS-GVO gegen aussen zu kommunizieren. Unsere Dienstleistungen sind diesen Bedürfnissen angepasst – wir werden auch weiterhin Unterstützung bei der Umsetzung der DS-GVO anbieten, darunter «DPO as a service» (Unterstützung der internen Datenschutzbeauftragten) sowie Zertifizierungen gemäss DS-GVO.

Zusammenfassung

Die DS-GVO hat aufgrund ihres weiten Anwendungsbereichs auch grossen Einfluss auf Schweizer Unternehmen. Die Nichtkonformität bringt nebst hohen finanziellen Risiken auch grosse Reputationsrisiken mit sich. Der Stand der Compliance mit der DS-GVO ist in der Schweizer Unternehmenslandschaft höchst unterschiedlich. Regulierte Bereiche (Finanzdienstleister, Pharma etc.) haben bereits sehr viele Anforderungen der DS-GVO erfüllt, KMUs dagegen haben sehr wenig unternommen, um mit der DS-GVO konform zu sein. Bei der Umsetzung der DS-GVO sollten Unternehmen sich primär auf die Einführung der Schlüsselprozesse konzentrieren (Notifikationsprozess für Datenschutzverletzungen, Prozess zur Beantwortung von Anfragen durch Datensubjekte, Prozess für Datenschutzverletzungen), ihre Verträge anpassen, den Datentransfer ins Ausland konform ausgestalten, die rechtmässige Verarbeitung von Daten sicherstellen sowie ihre Privacy Organisation innerhalb der Firma stärken. Ein grosses Augenmerk soll auf die Dokumentation der einzelnen Schritte und deren Weiterführung gelegt werden, damit die DS-GVO Konformität stets erhalten bleibt und der Datenschutz innerhalb der Organisation gelebt wird. Im Hinterkopf sollte zudem die Revision des Schweizer Datenschutzes behalten werden. Der derzeitige Entwurf spiegelt in vielen Bereichen die Anforderungen der DS-GVO. Obschon die revidierte, endgültige Fassung des DSG nicht vor 2020 zu erwarten ist, sollten Unternehmen in der Schweiz es nicht verpassen, ihren Fokus auf den Datenschutz genügend früh zu schärfen.

Thomas Bolliger
Partner, Information Governance & Compliance
tbolliger@kpmg.com