EU-DSGVO: Zeit zum Handeln

Die ab Mai 2018 in allen EU-Mitgliedstaaten geltende Datenschutz-Grundverordnung bringt zahlreiche Neuerungen mit sich. Sie gilt auch für Schweizer Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, und erfordert auf Unternehmensseite vielfach eine Anpassung von IT-Infrastrukturen, Geschäftsprozessen und Compliance-Richtlinien.

Von Eva-Maria Scheiter

Schweizer Unternehmen mit Tochtergesellschaften oder Niederlassungen in Mitgliedstaaten der Europäischen Union und Unternehmen, die Daten von EU-Bürgern verarbeiten, müssen sich den 25. Mai 2018 vormerken. Ab dann tritt die EU-Datenschutz-Grundverordnung (EU-DSGVO) in Kraft. Sie gilt für alle Unternehmen weltweit, die personenbezogene Daten von EU-Bürgern erfassen, speichern oder anderweitig verarbeiten.

Auch Schweizer Vorentwurf greift die EU-Anforderungen auf

Darüber hinaus greift auch der vorliegende Vorentwurf des neuen Schweizer Datenschutzgesetzes (DSG) die verschärften Anforderungen der EU-Verordnung auf: Das gilt insbesondere hinsichtlich der Pflichten für Unternehmen und der Rechte natürlicher Personen. Viele Unternehmen hierzulande werden sich daher sowohl im Hinblick auf die Datenschutz-Grundverordnung der EU als auch bezüglich des revidierten Schweizer Datenschutzgesetzes neuen und vor allem strengeren Sicherheitsanforderungen stellen müssen – und dies trotz des anerkannt hohen Datenschutzniveaus in der Schweiz.

An öffentlich verfügbaren Informationen zur EU-DSGVO, die im Mai 2016 veröffentlicht wurde, mangelt es eigentlich nicht. Dennoch herrscht auch bei einigen betroffenen Schweizer Unternehmen noch Unklarheit bezüglich der Auswirkungen und der notwendigen Massnahmen zur Erfüllung der geforderten anspruchsvollen Vorgaben. Während sich eine Reihe von Unternehmen bereits mit den Anforderungen und deren Umsetzung befasst und mit einiger Wahrscheinlichkeit die Ziele auch in der vorgegebenen Frist erreichen wird, zögern andere noch.

Personenbezogene Daten unter die Lupe nehmen

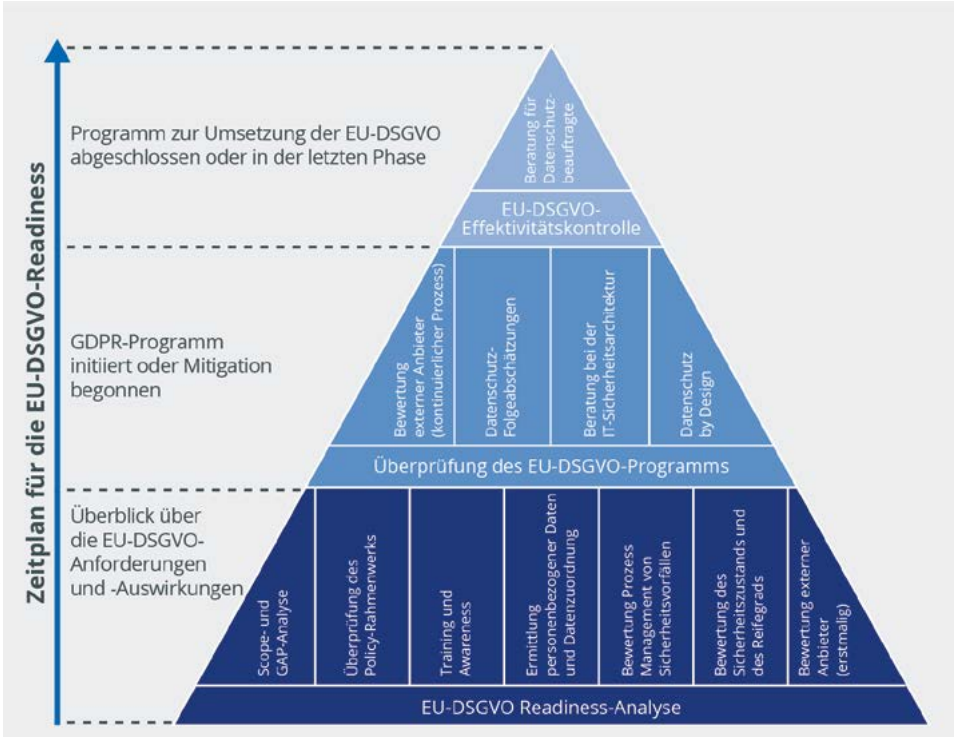
Zum Teil liegt dies auch daran, dass nach wie vor verschiedene Missverständnisse hinsichtlich der konkreten Anforderungen der EU-DSGVO bestehen. Einige Unternehmen wiegen sich in Sicherheit, wenn sie die internationale Norm DIN ISO/IEC 27001 oder die PCI-DSS-Vorgaben umgesetzt haben. Damit ist ein guter Anfang zur Umsetzung der notwendigen technisch organisatorischen Massnahmen gemacht, daraus entsteht aber keine automatische Konformität mit der EU-DSGVO. Schweizer Unternehmen, für welche die EU-DSGVO gilt, sollten zusätzlich dazu all ihre Strukturen und Prozesse, bei denen personenbezogene Daten involviert sind, auf den Prüfstand stellen – das Spektrum dabei erstreckt sich von der Erfassung, Speicherung, Veränderung, Bereitstellung und Löschung oder Vernichtung dieser Daten über Regeln für den Zugriff und reicht bis hin zu Massnahmen, die Unternehmen für den Umgang mit Datenschutzpannen vorgesehen haben. Als personenbezogene Daten gelten Informationen über sachliche oder persönliche Verhältnisse von bestimmten oder bestimmbaren Personen, beispielsweise von Kunden, Lieferanten, Geschäftspartnern und Mitarbeitern eines Unternehmens. Beispiele dafür sind Anschrift, Telefonnummer, E-Mail-Adresse, Geburtsdatum, Personalausweis- und Sozialversicherungsnummer.

Der Weg zur Compliance beginnt mit einem Self-Assessment

Der Ausgangspunkt eines Datenschutzprogramms, das den EU-DSGVO-Anforderungen entspricht, ist in vielen Fällen ein Self-Assessment. Unternehmen erhalten damit einen Überblick über ihre Datenschutzkonformität bezüglich zentraler Aspekte der neuen europäischen Vorgaben – und als willkommene Nebenwirkung auch einen Einblick hinsichtlich der Anforderungen, die mit dem kommenden Schweizer Datenschutzgesetz auf sie zukommen. Den Reifegrad der eigenen Organisation und der implementierten Massnahmen zu kennen, steht zu Beginn aller Aktivitäten auf dem Weg zur Rechtskonformität beim Datenschutz und der Datensicherheit.

Egal, an welchem Punkt sich ein Unternehmen auf dem Weg zur Umsetzung gesetzlicher Vorgaben gerade befindet: Eine Analyse hilft, vorhandene Handlungsbedarfe zu erkennen. Die Vorgehensweise sieht dann so aus, dass zu Beginn die vorhandenen und die geplanten Massnahmen mit den EU-DSGVO-Anforderungen abgeglichen werden. Als Ergebnis der Analyse zeigen sich dann organisatorische und technische Leistungsanforderungen, mit denen Unternehmen vom aktuellen oder geplanten Zustand auf den erforderlichen Stand kommen können.

Modulare Services rund um die EU-DSGVO von externen Anbietern können



Quelle: NTT Security

Dieses EU-DSGVO-Servicemodell unterstützt Unternehmen bei jedem Schritt auf dem Weg zur Compliance.

sich für Unternehmen als eine wichtige Hilfe erweisen. Ungeachtet dessen, ob eine Organisation über genügend qualifizierte interne Mitarbeiter verfügt, die ein EU-DSGVO-Compliance-Programm in Eigenregie entwickeln und umzusetzen können oder sich diese Mitarbeiter bei speziellen Fragen und Vorhaben zusätzlich externen Rat einholen wollen. Oft ist in der Anfangsphase eine Unterstützung bei der Ermittlung des Projektumfangs gefragt. In anderen Fällen kommt es vor, dass Organisationen externe Unterstützung anfordern, um ihre Prozesse (zum Beispiel zur Sicherstellung der Rechte der Betroffenen oder zur Reaktion auf Datenschutzpannen) überprüfen oder überarbeiten zu lassen.

Parallel zur Behandlung von personenbezogenen Daten sieht die EU-DSGVO darüber hinaus strenge Informationspflichten, erweiterte Nutzerrechte und ein «Recht auf Vergessenwerden» vor. Auch diese Vorgaben müssen Organisationen umsetzen. Eine Nichtbeachtung der Vorgaben kann für ein Unternehmen Geldbussen von bis zu 20 Millionen Euro beziehungsweise vier Prozent des global erzielten Umsatzes nach sich ziehen. Die in Planung befindlichen Schweizer Strafbestimmungen sehen hingegen nur Bussen von bis zu 500 000 Schweizer Franken vor; geht es um Kunden, die EU-Bürger sind, gelten die schärferen EU-Bestimmungen.

Das Angebotsspektrum von Services, die sich mit der Umsetzung der EU-DSGVO befassen, verteilt sich auf drei Kategorien:

Bestandsaufnahme: In einem ersten Schritt sollten sich Unternehmen einen Überblick verschaffen und detailliert ermitteln, in welchem Umfang und in welchem Detail ihre Organisation bereits auf die Neuerungen vorbereitet ist. Ein wichtiger Bestandteil ist die Betrachtung der organisatorischen und technischen Massnahmen, die einer besonderen Aufmerksamkeit bedürfen. Gap-Analysen verfolgen das Ziel, potenzielle Handlungsbedarfe zu identifizieren und präsentieren Massnahmenempfehlungen, wie Unternehmen die Vorgaben einhalten können. Gegenstand vertiefender Analysen kann die Ermittlung der personenbezogenen Daten sowie die Bestimmung der Datenquellen und der Datenflüsse sowohl in den fachlichen als auch in den IT-Prozessen sein.

Assessment eines in der Umsetzung befindlichen EU-DSGVO-Programms: Verschiedene Unternehmen haben die Bestandsaufnahme bereits hinter sich gebracht und befinden sich mitten in der Umsetzungsphase. Mit den für diese Stufe verfügbaren Services können Unternehmen prüfen, ob das Vorhaben geeignet ist, um das Ziel der Compliance zu erreichen. Auch hier wiederum existieren Gap-Analysen, die Licht ins Dunkel bringen, auf Lücken aufmerksam machen und Best Practices vorschlagen, um den Handlungsbedarfen zu begegnen. Im Hinblick auf die technischen Aspekte wünschen Unternehmen oft eine Beratung zur Sicherheitsarchitektur. Diese unterstützt Unternehmen bei der Etablierung von Datenschutzmassnahmen in der Design- und in der Entwicklungsphase von Applikationen und Systemen.

Effektivitätskontrolle der vorhandenen Massnahmen: Im Herbst 2017 haben nur die Vorreiter EU-DSGVO-Projekte weitgehend abgeschlossen. Für diese sind Analysen interessant, die den Erfüllungsgrad der implementierten Regeln gemessen an den EU-DSGVO-Vorgaben ermitteln. Sollten Unternehmen externe Dienstleistungen in Anspruch nehmen, so sind auch diese auf DSGVO-Compliance zu prüfen.

In Anbetracht des möglicherweise beträchtlichen Aufwands mögen einige Unternehmen die Umsetzung der EU-DSGVO-Vorgaben als Pflichtübung ansehen. Die durchgreifenden Verbesserungen der fachlichen und IT-Prozesse stellen zugleich jedoch auch eine nicht zu unterschätzende Chance dar. ■

EVA-MARIA SCHEITER
Executive Consultant GRC bei NTT Security