SOPHOS
Security made simple.

Die neue EU-Datenschutz-Grundverordnung (DSGVO)

Erstellt von Sophos in Zusammenarbeit mit Rechtsanwältin Dr. Bettina Kähler

Im Mai 2016 ist die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft getreten, die das europäische Datenschutzrecht grundlegend verändern wird. Nach einer Übergangsfrist von zwei Jahren endet die Umsetzungsfrist am 25. Mai 2018. Zu diesem Zeitpunkt müssen alle Unternehmen ihre internen Abläufe und Verfahren den neuen Vorgaben der DSGVO angepasst haben.

Es ist das erste Mal seit 1995, dass wieder eine grundlegende europäische Rechtsvorschrift zum Datenschutz verabschiedet wurde - seinerzeit war es die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (Richtlinie 95/46/EG).[i] Rückblickend betrachtet war das Jahr 1995 technologische Steinzeit und dementsprechend hat das Recht mit dieser Entwicklung nicht Schritt halten können. Anders als noch vor 22 Jahren passen heute riesige Speicherkapazitäten in jede Hosentasche und mobile Geräte sind aus unserem Alltag nicht mehr wegzudenken. In Anbetracht der neuen Möglichkeiten von Cloud Computing und allgegenwärtiger, schneller Verfügbarkeit von Informationen und Daten lösen sich die Grenzen von Netzwerken und Geräten auf: Sensible Daten verlassen fast schon routinemäßig die traditionell sicheren vier Wände des Unternehmens. Doch nicht nur der Gebrauch, auch der Missbrauch personenbezogener Daten ist heute ein Leichtes. Fast täglich werden Unternehmen und deren Kunden Opfer von Datenpannen, bei denen persönliche und höchst vertrauliche Daten in die Hände von Kriminellen fallen.

Die DSGVO ist unmittelbar geltendes Recht und löst somit praktisch alle nationale Gesetzgebung ab. Einzelne Bereiche werden in Deutschland durch ein neues Bundesdatenschutzgesetz geregelt, das Ende April 2017 vom Bundestag verabschiedet wurde.

Der vollständige Text der DSGVO ist hier[1] veröffentlicht.

Zeit für Reformen

Vor diesem Hintergrund wurde in den letzten Jahren immer deutlicher, dass die alten Regeln für Datenschutz und Datensicherheit nicht mehr ausreichen, um europaweit für einen angemessenen Schutz von personenbezogenen Daten und Rechtssicherheit für die Unternehmen zu sorgen. Auch nationale Rechtsgrenzen scheinen immer mehr aufgelöst von der Dominanz des technisch Machbaren. Hier soll die DSGVO nunmehr Abhilfe schaffen.

Das Ziel

Ziel der Datenschutzverordnung ist es, die Datenschutzrechte von EU-Bürgern zu stärken, das Vertrauen in die digitale Wirtschaft wiederherzustellen und Kundendaten durch Einführung neuer Datenschutzprozesse und -kontrollen in Unternehmen besser zu schützen.

Ein so grundlegend neues Gesetzeswerk wirft viele Fragen auf, zumal es - bezüglich der Etablierung technischer und organisatorischer Sicherheitsmaßnahmen - neue und detailliertere Anforderungen festschreibt, die Unternehmen künftig zu beachten haben. In diesem Whitepaper möchten wir Ihnen nunmehr die zentralen Änderungen und Anforderungen vorstellen, die ab Mai 2018 von den Unternehmen umgesetzt sein müssen. Anschließend gehen wir der Frage nach, welche Schritte für die Umsetzung erforderlich sind.

Kernelemente der Reform

Die DSGVO basiert auf vier zentralen Säulen. Diese sind:

- Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, die Zweckbindung und Richtigkeit von personenbezogenen Daten
- Transparenz der Datenverarbeitung und Betroffenenrechte
- Daten- und Systemsicherheit
- Kontrolle der Umsetzung der DSGVO, Meldepflichten gegenüber Aufsichtsbehörden und Betroffenen sowie Rechenschaftspflichten.

[1] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=de, zuletzt abgerufen am 07. April 2017

Die DSGVO gilt für alle Unternehmen und Behörden, die vollautomatisiert oder teilautomatisiert personenbezogene Daten verarbeiten. Auch im Fall der nichtautomatisierten Datenverarbeitung ist die DSGVO anwendbar, sofern diese in einem Dateisystem stattfindet. Grundsätzlich ist die neue Verordnung daher von jedem Unternehmen aus jeder erdenklichen Branche zu beachten, das selber oder im Auftrag von anderen personenbezogene Daten verarbeitet. Die Definition des Begriffs der personenbezogenen Daten umfasst nunmehr nicht nur die Merkmale, die eine Person direkt identifizieren (Name und Anschrift z.B.), sondern auch die Angaben, die sie mittelbar identifizierbar machen, wie z.B. IP-Adressen, Cookies, RFID-Tags, Standortdaten.

Ausschlaggebend für die räumliche Anwendung der DSGVO ist, dass die Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung eines Unternehmens in der Europäischen Union erfolgt. Neu ist insoweit, dass die Verordnung unabhängig davon gilt, ob die Datenverarbeitung auch tatsächlich innerhalb der Union stattfindet. Auch Unternehmen mit Sitz außerhalb der EU müssen die Vorgaben der Verordnung beachten, wenn sie sich mit ihrem - kommerziellen oder nicht-kommerziellen - Angebot an EU-Bürger richten oder, z.B. im Rahmen des Webtracking, deren Verhalten überwachen. Dieser Aspekt ist insbesondere für die Schweiz von Bedeutung: das Nicht-EU-Mitglied Schweiz erwirtschaftet einen großen Teil seines Bruttosozialprodukts durch Handel mit EU-Staaten und wird aufgrund dieser Neuerung mit Sicherheit an vielen Stellen ebenfalls die neuen Regeln der EU-Verordnung einhalten müssen.

Die vier Säulen

Verglichen mit dem in Deutschland, Österreich und der Schweiz noch geltenden Datenschutzrecht beinhaltet die DSGVO erheblich gesteigerte Anforderungen an Unternehmen, die personenbezogene Daten verarbeiten, diese Daten technisch und organisatorisch gegen Verlust, Veränderung und Manipulation zu schützen. Unternehmen werden daher zukünftig deutlich mehr Überlegung und Aufwand in die dann vorgeschriebenen Risikoanalysen, Verfahrensdokumentationen, Folgeabschätzungen und datenschutzfreundliche Techniken investieren müssen. Hinzu kommen Nachweispflichten und Informationspflichten an die von der Datenverarbeitung betroffenen Personen sowie an die Aufsichtsbehörden im Fall von Datenpannen, die ausgeweitet wurden. Die in der Verordnung formulierten gesteigerten Anforderungen lesen sich in Teilen wie eine Antwort auf die Missstände und Regelungslücken der vergangenen Jahre.

Im Einzelnen:

- **Einwilligung:** Als Rechtsgrundlage für die Erlaubnis zur Verarbeitung personenbezogener Daten wird vorherige Einwilligung der betroffenen Personen die vorrangige Rechtsgrundlage für Datenverarbeitungen. Verlangt wird eine ausdrücklich erteilte Einwilligung der Betroffenen. Die Einwilligung ist zweckgebunden und darf nur zu vorher eindeutig festgelegten Zwecken eingeholt werden. Das datenverarbeitende Unternehmen trägt zudem die Beweislast dafür, dass eine wirksam erteilte Einwilligung vorliegt. Neben der Einwilligung sind weitere Erlaubnisse zur Datenverarbeitung vorgesehen, wie z.B. zum Zweck der Vertragserfüllung.

- **Transparenz und Information:** Neu sind umfangreiche datenschutzrechtlichen Transparenz- und Informationspflichten. Datenverarbeitende Unternehmen müssen zukünftig beispielsweise bei der ersten Erhebung von Daten den von der Datenverarbeitung betroffenen Personen zahlreiche Mindest-Informationen über den Umgang mit ihren Daten mitteilen, wie z.B. die Zwecke und Rechtsgrundlage der Datenverarbeitung, bestehende Rechte auf Auskunft, Löschen und Widerruf sowie mögliche Datenübermittlungen an Dritte. Anders als unter der jetzt gültigen Rechtslage müssen die Unternehmen die Betroffenen im Fall von Datenpannen nicht nur benachrichtigen, wenn besonders sensible Daten betroffen sind, sondern in jedem Fall, sofern eine Beeinträchtigung der Rechte zu erwarten ist.
- **Compliance:** Auf der technischen Seite sind die datenverarbeitenden Unternehmen weitreichender als bisher verpflichtet, technische und organisatorische Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten zu ergreifen und vor allem auch deren Einhaltung nachzuweisen. Die Compliance-Maßnahmen müssen mindestens alle zwei Jahre überprüft, ggf. aktualisiert und regelmäßig dokumentiert werden.
- **Technische Sicherheitsmaßnahmen:** Die zu implementierenden technischen und organisatorischen Sicherheitsmaßnahmen orientieren sich an den Schutzzielen der Vertraulichkeit, der Integrität und Authentizität der personenbezogenen Daten. Die Unternehmen müssen eine Sicherheitspolitik etablieren, die auf der Grundlage einer Risikoanalyse unter anderem die nachfolgend genannten Punkte umfasst:
  - Die Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen
  - die Fähigkeit, die Verfügbarkeit und den Zugang zu Daten im Falle eines physischen oder technischen Zwischenfalls rasch wiederherzustellen
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Im Ergebnis sind Unternehmen damit verpflichtet, ein Informationssicherheits-Managementsystem und ein Risikomanagement zu etablieren, um den Anforderungen der DSGVO zu genügen. Diese Verpflichtung trifft nicht nur Unternehmen, die ihre eigenen Daten verarbeiten, sondern ausdrücklich auch diejenigen, die die Daten im Auftrag anderer verarbeiten.

- **Datenschutz durch Technik:** Die Unternehmen müssen sicherstellen, dass die von ihnen zur Verarbeitung personenbezogener Daten eingesetzten Systeme und Prozesse, von Beginn an datenschutzfreundlich ausgestaltet sind („privacy by design"). Wiederum auf der Grundlage einer Risikoanalyse sind „geeignete" technische und organisatorische Sicherheitsmaßnahmen zu bestimmen, die dafür ausgelegt sind, den Anforderungen der Verordnung zu genügen und die Rechte der betroffenen Personen zu wahren.

- **Die Folgen abschätzen:** In Fällen, in denen Unternehmen Datenverarbeitungen durchführen, die ein hohes Risiko für die Rechte der betroffenen Personen bergen, sind nach der DSGVO datenschutzrechtliche Folgenabschätzungen durchzuführen. Dies gilt beispielsweise für die umfangreiche Verarbeitung von Gesundheitsdaten oder die Profilbildung. Die DSGVO gibt dabei beispielhaft vor, welche Punkte mindestens zu prüfen sind, darunter eine systematische Beschreibung der geplanten Verarbeitungen und deren Zweck, verbunden mit einer Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung in Bezug auf den Zweck.
- **Haftung:** Für Unternehmen, die als Auftragsdatenverarbeiter für andere Unternehmen tätig sind, wird die Haftung verschärft. Neben generell strengeren Anforderungen an den Einsatz von Auftragsdatenverarbeitern, haftet mit der DSGVO neben dem Verantwortlichen (dem Auftraggeber der Datenverarbeitung) nunmehr grundsätzlich auch der Auftragnehmer gegenüber den Betroffenen auf Schadensersatz, sollte es zu Datenverlusten und der damit einhergehenden Verletzung von Rechten kommen.

Womit ist bei Datenschutzverstößen zu rechnen?

Die Datenschutz-Aufsichtsbehörden erhalten mit der DSGVO eine Reihe von Befugnissen, die sie gegenüber Unternehmen bei vermuteten oder tatsächlichen Verstößen gegen die Verordnung einsetzen können. Diese reichen vom Hinweis, dass eine Datenverarbeitung unzulässig sein könnte, über die Verwarnung im Fall von Verstößen bis zu Bußgeldern. Die Höhe der Geldbußen wurde dabei deutlich angehoben. Je nach Art und Schwere des Verstoßes können bis zu 10 Millionen Euro oder 2 % des „gesamten, weltweiten" Jahresumsatzes des betroffenen Unternehmens als Geldbuße verhängt werden - je nachdem, welcher Betrag höher ist. Dies gilt z.B. für den Fall der Nicht-Durchführung einer Datenschutzfolgenabschätzung. Für andere Verstöße (z.B. die Missachtung der Informationspflichten der von der Datenverarbeitung betroffenen Personen) können bis zu 20 Millionen EUR oder 4% des gesamten, weltweiten Jahresumsatzes als Geldbuße fällig werden, wiederum je nachdem, welcher Betrag höher ist. Die Datenschutz-Aufsichtsbehörden sind dabei ausdrücklich angewiesen, sicherzustellen, dass die Verhängung von Geldbußen „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" ist.

Die Bedeutung des neuen EU-Rechts für die Schweiz

Die Schweiz verfügt als Nicht-EU-Mitglied über ein Datenschutzgesetz[ii] , das in seinen wesentlichen Inhalten den noch geltenden deutschen und österreichischen Datenschutzgesetzen entspricht. Dies gilt insbesondere für die Vorgabe, personenbezogene Daten durch angemessene technische und organisatorische Maßnahmen gegen unbefugtes Verarbeiten, Vernichtung und Verlust zu schützen. Die Anforderungen unterscheiden sich derzeit also nicht wesentlich vom Rest Europas. Mit der Umsetzung der DSGVO gelten deren Vorschriften auch für Unternehmen außerhalb der EU unter anderen dann, wenn die Datenverarbeitung in der EU „ansässige" Personen betrifft und „dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten" oder „die Personen zu überwachen". Der räumliche Kontext von Datenverarbeitung ist damit weitgehend aufgehoben und Schweizer Unternehmen müssen schon dann das neue EU-Recht berücksichtigen, wenn sie personenbezogene Daten von EU-Bürgern verarbeiten, um beispielsweise Dienstleistungen in der EU anzubieten. Da die Schweiz in den EU-Staaten ihre wichtigsten Handelspartner hat[iii] , ist es auch für Schweizer Unternehmen empfehlenswert, im Detail zu überprüfen, ob und wie die neuen Regeln ihre internen Abläufe beeinflussen und diese ggfls. anzupassen.

Darüber hinaus steht zu erwarten, dass mittelfristig auf der Grundlage der Anforderungen der DSGVO branchenspezifische „Best-Practice" Modelle und Zertifizierungsverfahren entwickelt werden, deren Einhaltung dann standardmäßig auch von Schweizer Unternehmen erwartet wird.

Wie sollten Unternehmen sich vorbereiten?

Es ist nur noch etwas mehr als ein Jahr Zeit um die Anforderungen der DSGVO in den Unternehmen umzusetzen. Eine gute Vorbereitung setzt bei den unternehmensinternen Prozessen an und bezieht alle datenschutzrechtlich relevanten Abläufe im Unternehmen ein. Dabei sollte zunächst eine Ist-Analyse den gegenwärtigen Stand in Bezug auf die Umsetzung und Einhaltung von Datenschutzvorgaben erfolgen. Auf der Grundlage einer Risikoanalyse sollten dann bereits etablierte Sicherheitsmaßnahmen überprüft und dokumentiert werden. Wichtig ist, systematisch und zielgerichtet entlang der einzelnen Prozesse vorzugehen. Bei der Planung von neuen Maßnahmen ist auf den Einsatz datenschutzfreundlicher Technologien von Anfang an zu achten.

Weder die zurzeit gültigen Datenschutzgesetze noch die DSGVO schreiben konkret bezeichnete technische Kontrollmechanismen vor. Zentral ist aber in beiden Fällen die von den Datenschutzgesetzen geforderte Absicherung der personenbezogenen Daten gegen unbefugte Verarbeitung, Veränderung, Zerstörung und Verlust. Insofern sind Unternehmen gut beraten, Kontrollmechanismen auszuwählen und zu implementieren, die von Anfang an verhindern, dass Unbefugte personenbezogene Daten lesen, kopieren, verändern oder vernichten können. Vorbild kann das Vorgehen der Unternehmen sein, die aufgrund ähnlich strenger gesetzlicher Vorgaben schon heute hohe technische Sicherheitsstandards umsetzen müssen. Der Payment Card Industry Data Security Standard (PCI DSS) und das US-Bundesgesetz Health Insurance Portability and Accountability Act (HIPAA) für das Gesundheitswesen in den USA, sind nur zwei Beispiele für Vorschriften, die Datenschutzkontrollen ähnlich wie diejenigen im Vorschlag zur Reform des EU-Datenschutzrechts vorsehen. An diesen Standards können sich Unternehmen bei der Auswahl konkreter Sicherheitsmaßnahmen daher orientieren.

Parallel zur Überprüfung der technischen Sicherheitsmaßnahmen kann ein Unternehmen dann auf der Grundlage der Ist-Analyse der unternehmensinternen Prozesse beginnen, die Anforderungen der DSGVO in Bezug auf die Informations- und Transparenzpflichten umzusetzen. Auch dafür ist die detaillierte Kenntnis unternehmensinterner Abläufe unabdingbar. Zu prüfen ist, wie die neuen Anforderungen in bestehende Prozesse eingefügt werden können oder ob neue Verfahren geschaffen werden müssen. Nicht aus dem Blick geraten darf dabei die Notwendigkeit der Dokumentation der erfolgten Schritte: Sie kann auf bestehender Dokumentation aufbauen. Sofern keine ausreichende Dokumentation im Unternehmen vorhanden ist, muss auch hier nachgebessert werden.

Sophos-Lösungen zur Umsetzung Ihrer Sicherheitsmaßnahmen

Die Entscheidung, welche technischen Sicherheitsmaßnahmen zu etablieren sind um den Anforderungen der EU-DSGVO gerecht zu werden, muss auf der Grundlage einer umfassenden Risikoanalyse und im Rahmen einer unternehmensweiten Sicherheitsstrategie erfolgen. Bei der Etablierung technischer Sicherheitsmaßnahmen können Sophos-Lösungen als wichtige Bausteine zum Einsatz kommen. Welche Lösung an welcher Stelle sinnvoll einzusetzen ist, muss im Einzelfall geprüft und entschieden werden.

Um bei der Einhaltung der DSGVO zu helfen, setzen die Lösungen von Sophos an 3 zentralen Bereichen an:

1. Bekämpfung der Hauptursache von Datenverlusten
2. Rechtzeitiges Stoppen von Bedrohungen
3. Schutz bei menschlichem Versagen

1. Bekämpfung der Hauptursache von Datenverlusten

Feindliche Angriffe von außen und versehentliche Offenlegungen von personenbezogenen Daten durch interne Fehler sind die zwei Hauptursachen für Datenpannen. Sophos Central Device Encryption ist die einfachste Methode zur zentralen Verwaltung Ihrer Festplattenverschlüsselung für alle PCs und Macs. Die Festplattenverschlüsselung sorgt dafür, dass personenbezogene Daten im Falle eines Geräteverlusts- oder diebstahls unlesbar bleiben.

Sophos Mobile bietet einen vergleichbaren Schutz für Daten auf mobilen Geräten und ermöglicht darüber hinaus eine Remote-Ortung, -Zurücksetzung oder -Sperrung verloren gegangener Geräte. Mit minimalem Zeitaufwand können mobile Geräte gesichert und verwaltet werden.

Sophos Intercept X kann gemeinsam mit schon bestehenden Antivirus-Produkten genutzt werden und schützt effektiv vor Malware, Exploits und Ransomware.

Alle diese Lösungen sind in Sophos Central integriert und können über eine zentrale benutzerfreundliche Management-Konsole verwaltet werden.

2. Rechtzeitiges Stoppen von Bedrohungen

Da Malware-Angriffe immer raffinierter und aggressiver werden, ist eine mehrschichtige Sicherheitsstrategie erforderlich, die Angriffe auf allen Ebenen des Netzwerks stoppen kann. Die XG Firewall schützt Netzwerk-Geräte, indem sie die Angriffe direkt an der Netzwerkgrenze abfängt - also noch bevor sie auf Geräte gelangen können.

Die Sophos Email Appliance blockiert oder verschlüsselt sensible E-Mails und Anhänge (z.B. PDFs) automatisch, damit der Schutz der Daten immer sichergestellt ist. Zudem werden verdächtige E-Mails gestoppt, bevor sie in die Posteingänge der Benutzer gelangen können.

3. Rechtzeitiges Stoppen von Bedrohungen

Eine E-Mail kann – auch ganz ohne böse Absicht - schnell bei einem falschen Empfänger landen. Wenn die Mail vertrauliche Daten enthält, können eigentlich harmlose Fehler schnell weitreichende Folgen haben. Die dateibasierte Verschlüsselung von Sophos SafeGuard sorgt dafür, dass Daten auch dann geschützt bleiben, wenn sie die Geräte oder das Netzwerk (z.B. E-Mail-Anhang, Cloudspeicher) verlassen.

Fazit

Seit Jahren beherrschen gravierende Datenpannen mit alarmierender Häufigkeit die Schlagzeilen. Im Rahmen der EU-DSGVO drohen betroffenen Unternehmen im Falle von Datenpannen empfindliche Geldstrafen in Höhe von bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes.

Die rechtzeitige Vorbereitung auf die Veränderungen im Datenschutzrecht, die ab Mai 2018 in den Unternehmen etabliert sein müssen, hat daher viele Vorteile. Unternehmen verbessern schon jetzt ihre Compliance in puncto Datenschutz und Datensicherheit und müssen nicht später der neuen Rechtslage hinterherhinken.

Jedes Unternehmen, das Daten von EU-Bürgern vorhält, ist zur Einhaltung der neuen Verordnung verpflichtet. Daher sollten auch insbesondere Schweizer Unternehmen prüfen, ob und an welcher Stelle die neue DSGVO für sie gilt und sich entsprechend vorbereiten.

Die Verschlüsselungs- und Datenschutztechnologien von Sophos können für alle betroffenen Unternehmen als wichtige Bausteine dienen, um die Anforderungen der Datenschutz-Grundverordnung zu erfüllen.

Anhang: Wortlaut Datenschutz-Grundverordnung
Auszug aus den Vorschriften für technische und organisatorische Sicherheit personenbezogener Daten

Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit")

Art. 32 DSGVO Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

(a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

(b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

(c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

(d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Art. 25 DSGVO Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Personenbezogene Daten müssen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

iText der EU-Datenschutzrichtlinie von 1995: http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:31995L0046&from=de; zuletzt abgerufen am 07. April 2017

iiBundesgesetz über den Datenschutz: https://www.admin.ch/opc/de/classified-compilation/19920153/index.html; zuletzt abgerufen am 12. April 2017

iii„Die Schweiz gehört zu den Ländern mit den höchsten Anteilen des Aussenhandels am Bruttoinlandprodukt (BIP). Die Haupthandelspartner des grenzüberschreittenden Warenverkehrs sind die Industriestaaten; eine besonders wichtige Stellung hat dabei die EU": https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/aussenhandel.html; zuletzt abgerufen am 12. April 2017

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 (0)611 58 58-0 | +49 (0)721 255 16-0
E-Mail: sales@sophos.de

17-05-15 WPDE (PS-2550)

SOPHOS