DSGVO – physische Sicherheits- und Datenschutzvorkehrungen

Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union verlangt von Organisationen rund um die Welt, ihren Zugriff auf personenbezogene Daten sowie deren Nutzung und Pflege zu überdenken. Dieses Whitepaper beschreibt Szenarien von Datenrisiken, die in administrativer Intervention und Strafgebühren im Rahmen der Neuregelung resultieren könnten. Es untersucht auch Best Practices im Zusammenhang mit physischer Sicherung und Datenschutz, da sie einen wichtigen, aber häufig übersehenen Bereich des Datenschutzes repräsentieren. Die Kombination von administrativen, Cybersicherheits- und physischen Schutzmaßnahmen kann zum Schutz sensibler personenbezogener Daten beitragen und das Engagement einer Organisation für den Datenschutz demonstrieren.

Wichtige Erkenntnisse:

- Finden Sie heraus, was die DSGVO zur physischen Sicherung und zum Schutz von personenbezogenen Daten sagt.
- Erfahren Sie, was Branchenexperten für ein angemessenes Maß von Datenschutz halten.

Leben in einer datenbasierten Welt
Die Mehrzahl der Organisationen sammelt und nutzt personenbezogene Daten als einen normalen Aspekt der heutigen Geschäftsabwicklung – seien es Daten über Personal, Kunden, potentielle Neukunden oder Dritte. Diese Daten werden typischerweise in elektronischer Form gespeichert und sind für die Organisation[1] und externe Parteien zugänglich. Darüber hinaus besteht die Hauptaufgabe einiger Organisationen im Sammeln und in der Analyse von personenbezogenen Datenvolumen.

Wenngleich Menge und Art der von jeder Organisation erfassten Daten variieren, besteht weitgehend Einvernehmen darüber, dass es noch nie einfacher war, sie zu finden. Menschen hinterlassen eine enorme Spur von Daten, wenn sie Social-Media-Profile erstellen, an Online-Communities teilnehmen, im Internet suchen, Umfragen beantworten und Werbeangebote oder “kostenlose” Dienste wie zum Beispiel zum Speichern von Fotos und Musik-Streaming nutzen.

Die Technologie unterstützt den Aufbau robuster Personenprofile weiter mit Fortschritten bei künstlicher Intelligenz, e-Markern, Web-Beacons, Cookies und anderen Überwachungstools.

Technologie und Data-Mining zusammen haben Organisationen die Ansammlung enormer Mengen personenbezogener Daten ermöglicht. Diese Repositorien können Aufschluss über das Alter einer Person, Ehestand, Geburtstag, Bildung, Hobbys, Religion, Berufslaufbahn, politische Neigungen, Kaufpräferenzen, bevorzugte Nachrichtenquellen, Einkommen, kriminellen Hintergrund und vieles mehr geben.

Viele dieser Daten sind zwar in Unternehmensdatenbanken zentralisiert, aber Datenpakete sind oft über die Lieferkette und unterschiedliche Systeme verstreut – häufig ohne jeden Mechanismus, der zukünftigen Empfängern der Daten verrät, wie oder weshalb sie ursprünglich gesammelt wurden. Dabei werden Daten Verwendungsarten ausgesetzt, die weit vom ursprünglichen Zweck entfernt sind, für den sie erhoben wurden.

Eine Vielzahl von Personen innerhalb einer Organisation kann tagtäglich auf die gespeicherten Daten zugreifen – vielleicht um ein Gehalt auszuzahlen, Marktforschung zu betreiben, eine E-Mail-Marketingaktion zu veranstalten oder die Kundentreue zu verfolgen. Jeder Zugriffspunkt zu diesen Datenpools repräsentiert eine Gelegenheit für den Missbrauch von personenbezogenen Daten oder dafür, dass sie in die falschen Hände gelangen.

Fakten im Kurzüberblick

Was ist die DSGVO?
Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union verfolgt das Ziel, die Privatsphäre von in der Europäischen Union (EU) wohnhaften Personen zu schützen.

Wann tritt sie in Kraft?
25. Mai 2018

Wer ist von ihr betroffen?
Alle Unternehmen – ungeachtet ihres Standorts –, die personenbezogene Daten von betroffenen Personen in der Europäischen Union kontrollieren oder verarbeiten.

Was konstituiert personenbezogene Daten?
Jegliche zu einer natürlichen Person oder betroffenen Person in Bezug stehende Informationen. Es kann alles von einem Namen, einem Foto, einer E-Mail-Adresse, Bankdetails, Posts auf Websites von sozialen Netzwerken, medizinischen Informationen bis zur IP-Adresse eines Computers sein.

Welche Auswirkung hat sie?
Eine Strafgebühr von 20 Millionen Euro oder bis zu 4 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist). Dies ist die maximale Strafgebühr, die für die schwersten Verstöße verhängt werden kann.

Wo erhalte ich weitere Informationen?

- Ein Überblick über die Regelung
- Lesen Sie die Regelung
- Physische Sicherheitslösungen

65 %
der Befragten gaben an, dass Verletzungen des Datenschutzes zu einem Verlust ihres Vertrauens in die betroffene Organisation führen.[5]

Erwägen Sie die folgenden Szenarien, um sich ein Verständnis der physischen Sicherheitsrisiken zu verschaffen, mit denen Organisationen konfrontiert sind:

Ein Mitarbeiter empfängt am Flughafen sensible Daten auf seinem Handy und bemerkt nicht, dass jemand seinen Bildschirm anschaut.

- Ein Mitarbeiter verliert seinen Laptop und die Daten auf dem Laufwerk sind nicht verschlüsselt.
- Ein Mitarbeiter geht von seinem Schreibtisch weg, um sich eine Tasse Kaffee zu holen. Er lässt dabei Kundenkontaktdaten auf seinem Monitor angezeigt oder auf seinem Schreibtisch liegen und ein unbefugter Betrachter geht vorbei.
- Ein unzufriedener Mitarbeiter fotografiert Dokumente, die auf einem Kopierer liegen gelassen wurden, auf einem Bildschirm angezeigte Informationen und an einen Computermonitor geklebte Anmeldedetails.
- Veraltete Laptops oder Desktop-Computer werden zu karitativen Zwecken gespendet, ohne die Festplatten vollständig zu löschen.
- Eine Arztpraxis schließt und wirft Patientenakten in den Mülleimer, ohne sie zu schreddern.

2016 bedrohten Hacker
1 Milliarden Datensätze [2]

Derartige Szenarien sind zunehmend besorgniserregend, da Verstöße gegen die Datenschutzvorschriften in der heutigen digitalen Welt allzu häufig sind. Forrester meldete 2016, dass in nur 12 Monaten über eine Milliarde Akten von Hackern bedroht waren. In der ersten Hälfte von 2017 wurde berichtet, dass 918 Datenschutzverstöße in der weltweiten Bedrohung von 1,9 Milliarden Datensätzen resultierten. Dies repräsentiert eine Zunahme von 164 Prozent im Vergleich mit den ersten sechs Monaten von 2016.[2]

Mit jeder neuen Vertraulichkeitsverletzung wächst die Besorgnis, dass der Schutz von Daten nahezu verloren ist. Laut einer jüngsten Studie fühlen Menschen ihre Privatsphäre durch Sicherheits- und Vertraulichkeitsprobleme bedroht. Tatsächlich fürchten 91 Prozent, dass die Einzelperson die Kontrolle darüber verloren hat, wie ihre personenbezogenen Daten von Unternehmen gesammelt und genutzt werden. Fast genauso viele glauben, dass es sehr schwierig wäre, ungenaue Informationen über sie selbst online zu entfernen.[3] Nicht nur maßgebliche Verstöße erregen Bedenken. Kleinunternehmen halten vielleicht weniger Informationen über den Einzelnen, aber für die Betroffenen ist es nicht weniger wichtig, wenn sie gestohlen oder missbraucht werden.

Diese Bedenken nehmen weiter zu, obwohl es seit mehr als einem Jahrzehnt strikte Datenschutzrichtlinien und -vorschriften gibt. Der Health Insurance Portability and Accountability Act (HIPAA), der Fair Credit Reporting Act und die Datenschutzrichtlinie der Europäischen Union sind einige bekannte Beispiele.

Die Datenschutzrichtlinie umreißt Prinzipien wie etwa die Anforderung, dass Daten sicher sein müssen, nur zu begrenzten Zwecken verarbeitet und nicht länger als nötig aufbewahrt werden dürfen. Da es sich jedoch um eine “Richtlinie” und nicht um ein Gesetz handelt, fällt die Implementierung und Durchsetzung in jedem europäischen Land unterschiedlich aus.

Dann kam die DSGVO
Die DSGVO ist die umfassendste zum Schutz von personenbezogenen Daten eingeführte Regelung mit globaler Wirkung. Ihre Schaffung beruht auf der allseitigen Überzeugung, dass jeder ein Grundrecht auf den Schutz seiner Privatsphäre hat. Ihr Ziel ist der Schutz der Privatsphäre von in der EU wohnhaften Personen anhand der Durchsetzung einer neuen Regelung des Schutzes, der Verarbeitung und der Nutzung von personenbezogenen Daten durch Unternehmen.

Die DSGVO ist möglicherweise die wichtigste Fortentwicklung in der Datensicherheits- und Datenschutzregelung seit 20 Jahren – sowohl im Hinblick auf ihre Anforderungen an die Datenpflege als auch auf ihre potentiellen finanziellen Auswirkungen. Angesichts von zwei Stufen von Bußgeldern können Organisationen Strafen in Höhe von 2 Prozent ihres weltweiten Jahresumsatzes/10 Millionen Euro auferlegt werden für Verstöße wie:

- Unterlassen der Benachrichtigung einer Aufsichtsbehörde und betroffener Einzelpersonen über eine Verletzung des Datenschutzes
- Unterlassung der Berufung eines Datenschutzbeauftragten, sofern die Organisation diesen benötigt

Organisationen kann ein Bußgeld von 4 Prozent ihres weltweiten Jahresumsatzes/20 Millionen Euro auferlegt werden für Verstöße wie:

- Unterlassen der Gewährung der Rechte betroffener Personen
- Nichtbefolgung einer Weisung einer Aufsichtsbehörde
- Nichterfüllung der Anforderungen für internationale Datenübertragungen[4]

Diese Strafgebühren gehen mit dem Verlust von Ruf, Markenwert und Vertrauen einher – was für Unternehmen unter dem Strich genauso verheerend sein kann. Berichten zufolge führen Verletzungen des Datenschutzes bei 65 Prozent der Personen zum Verlust ihres Vertrauens in die betroffene Organisation.[5]

Die Befolgung der DSGVO ist kein kleines Unterfangen, da sie Organisationen dafür verantwortlich macht, wie sie personenbezogene Daten sammeln, nutzen, pflegen und löschen und sie dabei sicher halten. Auch diejenigen, die bereits Datenschutz- und Sicherungsprogramme implementiert haben, müssen ihre Prozesse neu bewerten. Die DSGVO

Die DSGVO ist die umfassendste zum Schutz von personenbezogenen Daten eingeführte

Regelung mit globaler Wirkung.[1]

fordert von Organisationen ausdrücklich die Implementierung angemessener technischer und organisatorischer Maßnahmen zur Verhinderung des Verlustes oder der unbefugten Nutzung von personenbezogenen Daten.

Viele stellen deshalb Fragen wie die folgenden:

F. Was konstituiert personenbezogene Daten?
A. Jegliche Informationen in Bezug auf eine identifizierte oder identifizierbare natürliche Person.[6] Diese könnten Kennungen (wie einen Namen oder eine Kennnummer) oder Daten umfassen, aus denen rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Zugehörigkeit zu einer Gewerkschaft, genetische Daten, Gesundheitsdaten oder Straftaten hervorgehen; Vorhersagen der Arbeitsleistung, wirtschaftliche Lage, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel.[7]

F. Was ist Pseudonymisierung und weshalb sollte ich mich darum kümmern?
A. Mit der DSGVO wird der Begriff 'Pseudonymisierung' 15-mal erwähnt – ein Verfahren, bei dem in einem Datensatz enthaltene identifizierende Felder durch eine oder mehrere künstliche Kennungen bzw. Pseudonyme ersetzt werden. Die DSGVO empfiehlt die Anwendung einer Pseudonymisierung auf personenbezogene Daten, um die Risiken betroffener Personen zu reduzieren und um Verantwortlichen und Auftragsverarbeitern bei der Erfüllung ihrer Datenschutzobligationen zu helfen.[8]

F. Können Organisationen die Einwilligung von Einzelpersonen zum Sammeln ihrer personenbezogenen Daten einholen?
A. Ja, aber die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Bereits angekreuzte Kästchen oder Untätigkeit stellen keine Einwilligung dar.[9] Organisationen müssen einen Nachweis des Erhalts der Einwilligung führen und sicherstellen, dass Ersuchen um Einwilligung von anderen Ersuchen unterscheidbar sind und in einer klaren und einfachen Sprache erfolgen.[10] Artikel 13 legt umfangreiche Informationen dar, die der betroffenen Person zum Zeitpunkt der Sammlung personenbezogener Daten bereitgestellt werden müssen, wie zum Beispiel den Zweck der Erhebung der Informationen, die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und die Dauer der Speicherung der Daten.

F. Was ist eine Datenschutz-Folgenabschätzung?
A. Eine Datenschutz-Folgenabschätzung, die für mit einem hohen Risiko behaftete Aktivitäten erforderlich ist, hilft Organisationen bei der Bewertung des Ursprungs, des Wesens, der Besonderheit und des Schweregrads von Risiken und der Implementierung angemessener Maßnahmen zur Minderung der Risiken, wie zum Beispiel Verschlüsselung. Bei der Bewertung von Datensicherheitsrisiken sollten die Risiken erwogen werden, die sich durch die Verarbeitung von personenbezogenen Daten ergeben, wie zum Beispiel Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übertragen, gespeichert oder auf sonstige Weise verarbeitet werden, wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.[11]

F. Muss ich einen Datenschutzbeauftragten berufen?
A. Die Benennung eines Datenschutzbeauftragten muss erfolgen, wenn die Datenverarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird (mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln) oder für ein Unternehmen, dessen Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erforderlich machen. Ein Datenschutzbeauftragter ist ebenfalls für alle Unternehmensgruppen erforderlich, die sensible Daten in Bezug auf Gesundheit oder religiöse oder politische Überzeugungen in großem Umfang verarbeiten. Im Einzelnen gilt für den Datenschutzbeauftragten Folgendes:

- Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt.
- Der Datenschutzbeauftragte kann ein Personalmitglied oder ein externer Dienstleister sein.
- Kontaktdetails müssen der relevanten Aufsichtsbehörde gemeldet werden.
- Dem Datenschutzbeauftragten müssen angemessene Ressourcen zur Ausübung seiner Aufgaben und Pflege seiner Fachkenntnisse bereitgestellt werden.
- Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene.
- Der Datenschutzbeauftragte darf keine anderen Aufgaben ausüben, die zu einem Interessenkonflikt führen könnten.[12]

Physische Sicherheits- und Datenschutzanforderungen
Was sollten Organisationen zur Verhinderung von Verletzungen des Datenschutzes tun? Artikel 24 der DSGVO umreißt die Verantwortlichkeit einer Organisation für die Implementierung "geeigneter technischer und organisatorischer Maßnahmen" zur Gewährleistung einer nachweislich ordnungsgemäßen Verarbeitung von personenbezogenen Daten. Artikel 32 geht einen Schritt weiter und erklärt, "bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden."

Ein wichtiger Aspekt dieser Regelung ist die Betonung der Verhinderung eines unbefugten Zugangs. Hier ist physische Sicherheit ausschlaggebend. Sie kann insbesondere zum Schutz der Daten gegen interne und externe menschliche Bedrohungen beitragen, die auf die Ausnutzung von Lücken im Schutzwall Ihrer Organisation oder bei Ihrem Personal abzielen. Dazu gehören Einschränkungen im Hinblick darauf, welche Daten beobachtet oder gestohlen werden können oder zugreifbar sind. Führen Sie eine Revision der folgenden Aspekte durch und beurteilen Sie, ob Ihr Personal die geeigneten, zur Regelbefolgung erforderlichen technischen und organisatorischen Maßnahmen implementiert hat.

Setzen Sie Datenschutz vom Design her und standardmäßig ein:
Zum standardmäßigen Schutz von Daten dürfen Organisationen proaktiv nur die für den vorgesehenen Zweck erforderlichen personenbezogenen Daten identifizieren und sammeln sowie die Daten nur solange aufbewahren, wie es erforderlich ist (Minimierungsprinzip), und sie sollten sicherstellen, dass personenbezogene Daten keiner unbestimmten Zahl von Personen zugänglich gemacht werden. Dazu wird es wahrscheinlich erforderlich sein, sicherzustellen, dass Datenschutzrisiken im Vorab identifiziert und Systeme zur Minderung dieser Risiken entwickelt werden, dass eine angemessene Pseudonymisierung und Anonymisierung erfolgt und dass Transparenz innerhalb der Verarbeitungsfunktionen geschaffen wird sowie spezifische Personen oder Funktionen identifiziert werden, die Zugang zu den Daten benötigen. Fragen Sie sich: Ziehen Sie Datenschutzrisiken für Einzelpersonen in Betracht, bevor Sie Ihre Informationssysteme, Geschäftspraktiken und physische Auslegung konzipieren? Haben Sie gegenwärtige Systeme und Verarbeitungsaktivitäten mit Ihrem IT-Personal überprüft und besprochen, ob weitere Schritte erforderlich sind, um zu dokumentieren, wie personenbezogene Daten über den gesamten Informationsdaten-Lebenszyklus hinweg geschützt werden?

Verwenden Sie physische Sicherheitsvorkehrungen:
Cybersicherheits-Kontrollmechanismen wie Datenverschlüsselung und komplexe Passwörter sind zwar entscheidend, aber administrative und physische “Low-Tech”-Kontrollmechanismen sind von gleicher Wichtigkeit. Fragen Sie sich, wo auf sensible Informationen zugegriffen wird, um zu bestimmen, wo physische Barrieren erforderlich sind. Beispielsweise verwenden Mitarbeiter häufig Mobilgeräte von überall aus für den Zugriff auf und die gemeinsame Nutzung von Daten. Eine zunehmende Zahl dieser Mitarbeiter greift an öffentlichen Orten und häufig für andere deutlich sichtbar auf sensible Informationen zu. Auch im Büro besteht ein höheres Risiko der Offenlegung von Daten. Übliche Großraumbüros entfernen die physischen Barrieren, die in der Vergangenheit zur Abschirmung von Computerbildschirmen beigetragen haben. Fragen Sie sich: Haben Sie Computerbildschirme von Fenstern, Türen und für die Öffentlichkeit zugänglichen Bereichen entfernt positioniert? Statten Sie Monitore und Bildschirme von Mobilgeräten mit Blickschutzfiltern aus, um die auf ihnen angezeigten Informationen vor potentiellen Beobachtern zu schützen? Sind gemeinsam genutzte Drucker, Kopier- oder Faxgeräte in geschützten Bereichen aufgestellt oder mit verschließbaren Abdeckungen versehen? Bewahren Sie physische Kopien von Daten in einer Einrichtung mit Zugangskontrolle auf? Werden Aktenvernichter standardmäßig in allen Geschäftsbereichen bereitgestellt, insbesondere neben Druckern, Kopier- und Faxgeräten, und sind sie eine Grundvoraussetzung für alle Telearbeiter oder Personen, die über Fernverbindungen auf Unternehmensdatenbestände zugreifen?

Planen Sie die Mitarbeiterschulung:
Schulungsprogramme sollten drei zentrale Aspekte abdecken: Best Practices für Beobachtung, physischen Zugang und Diebstahlverhinderung. Beispielsweise sollten Mitarbeiter daran erinnert werden, sich ihrer Umgebung bewusst zu bleiben, wenn sie an öffentlichen Orten über ihre Laptops, Tablets und Smartphones auf vernetzte Geräte zugreifen und sie verwalten. Gerätebildschirme sollten nicht den Blicken von Passanten oder potentiellen Beobachtern ausgesetzt werden, insbesondere wenn Anmeldedetails eingegeben oder sensible Kontodetails angezeigt werden. Hinsichtlich des physischen Zugangs sollten Organisationen ihre Mitarbeiter darin schulen, nach Meetings Informationen von Whiteboards zu löschen und vertrauliche Papiere einzusammeln, sich Passwörter zu merken, statt sie aufzuschreiben, Aktenschränke und Laptops abzuschließen, Blickschutzfilter an Computerbildschirmen zu verwenden, eine Richtlinie zum aufgeräumten Schreibtisch zu befolgen und sich von unbeaufsichtigten Geräten abzumelden. Fragen Sie sich: Ist Situationsbewusstsein in Ihr Schulungsprogramm einbezogen, damit Mitarbeiter lernen, auf ihre Umgebung zu achten, und verdächtiges Verhalten erkennen und darauf reagieren können? Verstehen Ihre Mitarbeiter die Erwartungen Ihrer Organisation hinsichtlich der Richtlinie zum “aufgeräumten Schreibtisch”? Erinnern Sie Mitarbeiter häufig an gute Sicherheitspraktiken, die sie befolgen müssen?

Erarbeiten Sie klare Richtlinien:
Zur Demonstration des Engagements einer Organisation für die Implementierung angemessener Sicherheits- und Datenschutzmaßnahmen müssen ihre Richtlinien die Gebote und Verbote im Zusammenhang mit dem Betrachten und der Nutzung von Informationen durch Mitarbeiter und Vertragspersonal sowohl am Arbeitsplatz als auch vom Arbeitsplatz entfernt umreißen. Personalverträge sollten spezifische Aussagen über die Verantwortlichkeit für den Schutz von sensiblen und vertraulichen Informationen enthalten.[13] Fragen Sie sich: Haben Sie sich mit Einzelpersonen über Ihre Erklärung zum Datenschutz und zu Sicherheitspraktiken ausgetauscht, die erläutert, wie Ihre Organisation personenbezogene Daten schützt, teilt, entsorgt und Zugang zu ihnen gewährt? Wenden Sie eine BYOD-Richtlinie (Bring your own Device) an, die das Verhalten von Mitarbeitern und erforderliche Sicherheitskontrollen bei ihrem Zugriff auf Unternehmensressourcen über ihre persönlichen Geräte regelt? Verlangen Sie im Rahmen Ihrer Sicherheitsrichtlinie, dass Mitarbeiter sowohl visuelle als Cybersicherheits-Kontrollmechanismen verwenden?

Legen Sie Datenspeichergrenzen fest:
Legen Sie fest, wie lange personenbezogene Daten – nach geltendem Recht – gespeichert werden. Stellen Sie sicher, dass alle personenbezogenen Daten, die nicht unbedingt zur Unterstützung der geschäftlichen Zwecke, für die sie gesammelt wurden, benötigt werden, sicher gelöscht werden. Fragen Sie sich: Welche technischen Kontrollen haben Sie implementiert, damit Daten zum richtigen Zeitpunkt gelöscht werden? Erfüllen die Vernichtungsprozesse Ihrer Organisation strikte Sicherheitsrichtlinien wie etwa in NIST Special Publication 800-88 definiert, zum Beispiel die physische Vernichtung von Festplatten, die das Ende ihrer Gebrauchsdauer erreicht haben?

Überprüfen Sie Drittlieferanten:
Verwenden Sie nur Auftragsverarbeiter, die hinreichende Garantien hinsichtlich Fachwissen, Zuverlässigkeit und Ressourcen für die Implementierung technischer und organisatorischer Maßnahmen, einschließlich der sicheren Verarbeitung, bereitstellen können. Fragen Sie sich: Haben Sie ein Anbietermanagementprogramm implementiert, das vertragliche Verpflichtungen einbezieht und die Beaufsichtigung von Dritten mit Zugang zu personenbezogenen Daten festlegt?

Erstellen Sie ein Datenschutzverstoßprotokoll:
Organisationen müssen bereit sein, die Aufsichtsbehörde ohne unnötige Verzögerung zu benachrichtigen, wenn sie sich bewusst werden, dass eine Verletzung des Schutzes von personenbezogenen Daten erfolgt ist (soweit möglich, nicht später als 72 Stunden). Oder sie müssen nachweisen können, dass es unwahrscheinlich ist, dass die Verletzung des Schutzes von personenbezogenen Daten in einem Risiko für die Rechte und Freiheiten natürlicher Personen resultiert. Bei einem hohen Risiko muss die betroffene Person bzw. müssen die betroffenen Personen ebenfalls ohne unnötige Verzögerung über die Verletzung des Schutzes von personenbezogenen Daten benachrichtigt werden.[14] Fragen Sie sich: Wann haben Sie die Richtlinien und Pläne Ihrer Organisation zu Notfällen und zur Meldung von Verstößen zuletzt einer Revision unterzogen? Wissen Mitarbeiter Ihrer Organisation, wer zu verständigen ist, wenn ihr Gerät kompromittiert wurde oder sie sich einer Datenschutzverletzung bewusst werden? Haben Sie einen aktuellen Notfall- und Verstoßmeldeplan implementiert, um festzulegen, wann und wie Behörden über eine Datenschutzverletzung benachrichtigt werden?

Seien Sie sich der Rechte des Einzelnen bewusst:
In der EU wohnhafte Personen haben ein Recht auf Einsicht in die personenbezogenen Daten, die Organisationen in Bezug zu ihnen besitzen – und unter bestimmten Umständen auf die Löschung ihrer Daten. Das Recht auf Löschung fordert von Organisationen, alle Verknüpfungen zu oder Kopien oder Replikate von diesen personenbezogenen Daten zu löschen. Organisationen sollten Personen ermöglichen, Ersuchen auf elektronischem Weg einzureichen, insbesondere, wenn personenbezogene Daten elektronisch verarbeitet werden.[15] Fragen Sie sich: Versteht Ihre Organisation, was als “personenbezogene Daten” erachtet wird und wie auf Anfragen in Bezug auf personenbezogene Daten zu reagieren ist?

Schlussfolgerung:

Die DSGVO ist die bedeutsamste Änderung der Datenschutzvorschriften der letzten 20 Jahre. Sie verlangt, dass personenbezogene Daten in einer Weise verwaltet werden, die zu einer angemessenen Sicherheit und Vertraulichkeit beiträgt – eine Aufgabe, die sowohl technische als auch organisatorische Ressourcen erfordert. Und die Strafgebühren für eine Nichtbefolgung könnten verheerend sein. Bei den im Regelwerk umrissenen Best Practices handelt es sich jedoch einfach um gute Geschäftspraktiken. Niemand wünscht den Missbrauch seiner Daten, und keine Organisation wünscht die Rückwirkungen einer Verletzung des Datenschutzes. Organisationen, die Datenschutz nicht als eine behördliche Bürde sondern als eine unternehmerische Verantwortlichkeit sehen, können ihn als einen strategischen Vorteil zur Verbesserung ihres Rufs und Markenwerts nutzen und bessere Mitarbeiter sowie letztendlich das Vertrauen der Öffentlichkeit gewinnen.

www.3m-blickschutz.de

[1]Forrester, Lessons Learned from the World’s Biggest Security Breaches and Data Abuses, 9. Januar 2017
[2]2017 Gemalto Breach Level Index, http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
[3]GfK Privacy Panel, Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014.
[4]Artikel 83, der DSGVO, 2017
[5]Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, gesponsert von Centrify, 2017.
[6]Artikel 4, der DSGVO, 2017
[7]Randnummer 75, der DSGVO, 2017
[8]Randnummern 26 und 28, der DSGVO, 2017
[9]Randnummer 32, der DSGVO, 2017
[10]Artikel 7, der DSGVO, 2017
[11]Artikel 35 und Randnummern 83-84, der DSGVO, 2017
[12]Artikel 37-38, der DSGVO, 2017
[13]Randnummer 74, 77-78, der DSGVO, 2017
[14]Randnummer 81, der DSGVO, 2017
[15]Randnummer 59, 63, 65, 66 der DSGVO, 2017