KASPERSKY lab

Leitfaden zur Einhaltung der EU-DSGVO

„Die Einhaltung der Datenschutzbestimmungen ist für Unternehmen mit Sitz in der EU nichts Neues."

Ehe wir diese Herausforderung im Detail betrachten, sollten Sie die wichtigsten Änderungen kennen,[1] die Sie betreffen:

- Alle personenbezogenen Daten, die Sie kontrollieren und verwalten – unabhängig davon, ob deren Verarbeitung in der EU stattfindet oder nicht –, müssen fair und transparent verarbeitet werden und einen eindeutigen Nutzungszweck haben, der den betroffenen Personen gegenüber (z. B. Bürgern) benannt werden kann.
- Ein Verstoß gegen die Verordnung führt zu erheblichen Bußgeldern – bis zu 4 % des weltweiten Jahresumsatzes oder bis zu 20 Millionen EUR (der jeweils höhere Wert gilt).
- Für die Nutzung von Daten sind striktere Einwilligungskriterien erforderlich, die von den Bürgern bei Bedarf auf einfache Weise widerrufen werden können.
- Datenschutzverletzungen müssen innerhalb von 72 Stunden gemeldet werden, nachdem der Verantwortliche für die Datenverarbeitung davon Kenntnis erhalten hat.
- Die betroffenen Personen erhalten mehr Rechte, um zu erfahren, wie, wo und zu welchem Zweck ihre Daten verarbeitet werden.
- Die Datenlöschung (oder „das Recht auf Vergessen") wird vereinfacht. Die betroffenen Personen können beantragen, dass ihre personenbezogenen Daten gelöscht oder deren Verarbeitung unterbunden wird (vorausgesetzt ihr Antrag erfüllt bestimmte Bedingungen).
- Es wird eine Datenportierbarkeit ermöglicht, d. h. die Betroffenen erhalten das Recht, ihre personenbezogenen Daten einzusehen.
- Die Datenschutzprozesse (oder „Datenschutz durch Technikgestaltung") müssen bei der Entwicklung und Gestaltung neuer Systeme von Anfang an berücksichtigt und nicht erst als späteres Add-on hinzugefügt werden.
- Datenschutzbeauftragte müssen in Unternehmen vorhanden sein, deren Kernaktivitäten in Verarbeitungsvorgängen bestehen, bei denen eine regelmäßige, groß angelegte und systematische Überwachung der betroffenen Personen durchgeführt wird, oder in manchen Fällen, wenn Unternehmen große Mengen einer „speziellen" Datenkategorie verarbeiten.

Es ist nun beschlossene Sache: Die EU-Datenschutz-Grundverordnung wird kommen und sie wird, unabhängig von dem Arbeitsbereich, in dem Sie tätig sind – ob Personal-, Marketing-, Rechts- oder IT-Abteilung – Auswirkungen auf Sie persönlich und auf Ihre tägliche Arbeit haben. Wenn Sie mit personenbezogenen Daten wie Mitarbeiterdaten, Informationen von Kunden oder Interessenten arbeiten, diese speichern oder anwenden, wird die EU-DSGVO Ihre Arbeitsweise verändern. Und es liegt in Ihrer Verantwortung, für die Einhaltung dieser Änderungen zu sorgen.

Verantwortung für die EU-DSGVO übernehmen

Wie ein persönlicher Trainer soll dieser Leitfaden Sie unterstützen und eine Struktur für eine effektive Umsetzung bieten. Der Leitfaden entwickelt eine Art Plan für die notwendigen Änderungen, führt Sie zum Wesentlichen und sorgt für die erfolgreiche Einhaltung der EU-DSGVO.

Die Einhaltung von Datenschutzrichtlinien ist für Unternehmen in der EU nichts Neues. Wenn aber nun am 25. Mai 2018 die EU-DSGVO in Kraft tritt und die Datenschutzrichtlinie 95/46/EC ersetzt, müssen die Unternehmen einem neuen Ansatz des Datenschutzes folgen, der den EU-Bürgern mehr Kontrolle über ihre personenbezogenen Daten und über den Umgang mit ihnen einräumt.

Was bedeutet diese Richtlinie neben dem allgemeinen Hype und der Konzentration auf die termingerechte Einhaltung der neuen Kriterien für die Unternehmen in ganz Europa – einschließlich der damit verbundenen Bußgelder bei Nicht-Einhaltung – ganz konkret für jeden Einzelnen in einem Unternehmen? Und kann jeder die Verantwortung dafür übernehmen?

Unabhängig von diesen grundlegenden Änderungen ist die Basis dafür bereits in den jetzigen Datenschutzrichtlinien niedergelegt. Die EU-DSGVO sollte nicht als Belastung wahrgenommen werden. Aufgrund ihrer bindenden Natur stellt sie für die Unternehmen eine Chance dar und kann vielfältige Vorteile für einen optimalen Geschäftsbetrieb bieten, wenn sie richtig angewendet wird.

Während die Führungskräfte meist für die Sicherstellung des allgemeinen Rahmens verantwortlich sind, muss sich jeder einzelne Mitarbeiter im Detail darüber informieren, wie er die Herausforderung, seine Daten korrekt zu verwalten, bewältigt. Die Sicherheit und sichere Aufbewahrung von Daten in Ihrem Besitz wird eine noch größere Bedeutung bekommen. Durch die strengen Vorgaben und Ziele der EU-DSGVO müssen das gesamte Unternehmen und die Mitarbeiter diesen wichtigen Meilenstein der Einhaltung zum Ziel haben und die Datenverwaltungspraktiken generell optimieren.

Ebenso wie ein geänderter Lebensstil oder das Ziel, für den Sommer fit und gesund zu werden, lässt sich die Umsetzung der EU-DSGVO auf Abteilungsebene nur schrittweise mit kleinen, aber wichtigen Änderungen erreichen, die in Summe zu einer optimalen Aufstellung im Jahr 2018 führen, wenn die EU-DSGVO in Kraft tritt.

1 http://www.eugdpr.org/key-changes.html

Probleme in Vertrieb und Marketing

„Wird die EU-DSGVO uns nicht ausbremsen und uns zusätzliche Verwaltungsarbeiten auferlegen, wenn wir unsere E-Mail-Kampagnen und Vertriebsteams auf die richtigen Kunden ausrichten möchten?“

Häufige Bedenken

Bei Vertrieb und das Marketing stehen in der Regel die Nutzung von Kunden- und Interessentendaten im Vordergrund, um die Vertriebs-Leads zu fördern und die Markenwahrnehmung beständig zu verbessern. Bei großen Datenbankbeständen und zielgerichteten Kampagnen müssen diese Abteilungen bereits jetzt strenge Datenschutz- und Opt-out-Richtlinien einhalten.

Die Auswirkungen der EU-DSGVO

Wenn Sie personenbezogene Daten für gezielte Marketing- und Vertriebskampagnen nutzen, müssen Sie auf die Einhaltung der neuen Richtlinien achten. Es ist nicht mehr zulässig, vorausgewählte Felder in Formularen zu verwenden oder Personen mit Werbung anzusprechen, die nicht ausdrücklich zugestimmt haben. Für die Verarbeitung personenbezogener Daten ist eine ausdrückliche Einwilligung erforderlich. Für nicht personenbezogene Daten ist eine unmissverständliche Einwilligung ausreichend. Auch Bestimmungen zur Löschung von Daten müssen gemäß dem „Recht auf Vergessen“ ausgeführt werden. Für Einzelne wird es einfacher, die Entfernung ihrer Informationen aus Ihrer Datenbank zu verlangen.

Ihr fünfstufiger Datenfitnessplan

- Personen, die ihre Einwilligung bisher verweigert haben oder nichts unternommen haben, müssen jetzt ihre ausdrückliche Einwilligung geben, wenn Sie sie weiterhin in Ihrer Marketing-Kontaktliste aufführen möchten. Bevor Sie nun Ihre gesamte Datenbank durchforsten, sollten Sie über die optimale Vorgehensweise nachdenken, wie Sie das Ziel einer nützlichen und bereinigten Marketingliste erreichen.
- Die Einträge in Ihrer Datenbank müssen auf Einwilligungen und Reaktionen basieren. Um dies zu erreichen, sind wirksame Handlungsaufforderungen und motivierende Inhalte erforderlich.
- Gemäß der EU-DSGVO muss der dem Werbematerial beigelegte Einwilligungstext klar und verständlich sein, damit die Betroffenen ihre Entscheidung über die Nutzung ihrer Daten einfach und eindeutig treffen können.
- Fertigen Sie ein unmissverständliches Auditprotokoll an und bewahren Sie einen Datensatz der Einwilligungen auf.
- Sie benötigen für Vermarktungszwecke eindeutige Einwilligungen – Besuche bei einer Veranstaltung oder das Hinterlassen von Visitenkarten an einem Messestand sind nicht ausreichend für die Aufnahme in eine Marketing-Mailing-Datenbank. Die Personen müssen entweder ein Kontrollkästchen deaktivieren oder eine andere klare Handlung durchführen oder eine Aussage oder Aktion vornehmen, die klar angibt, dass die betroffene Person mit der Verarbeitung ihrer personenbezogenen Daten einverstanden ist. Beispielsweise könnte die Person ihre E-Mail-Adresse in einem optionalen Bereich eines Onlineformulars angeben, für dessen Nutzung eine besondere Verzichtserklärung gilt.

Entschlackung von Abteilungsdaten

- Wo können Sie anfangen? Sie sollten überstürzte Reaktionen oder „Brachialkuren“ vermeiden, wenn Sie Ihr Datendilemma in den Griff bekommen möchten. Richtig in die Wege geleitet, können ein langfristig optimaler Datenzustand und die Einhaltung der EU-DSGVO einfacher sein, als es zunächst scheint.
- Schrittweise aufgebaute, realistische Umsetzungs- und Optimierungspläne mit klaren Zielen und Meilensteinen können sicherstellen, dass jede Abteilung fit für die Herausforderungen der EU-DSGVO ist. Damit kann das Unternehmen auf Kurs gehalten und ein langfristig optimaler Datenzustand ohne Schwachstellen im Immunsystem des Unternehmens implementiert werden.

Probleme der Rechtsabteilung

„Sicherzustellen, dass unsere Mitarbeiter die Regeln verstehen und befolgen und dass die SLAs mit unseren Vertragspartnern und Lieferanten der EU-DSGVO entsprechen, wird unsere Ressourcen auf die Probe stellen."

Nur 38%
der IT-Entscheider haben hinsichtlich der EU-Datenschutz-Grundverordnung ein tiefergehendes Wissen.

Häufige Bedenken

Die Rechtsabteilung hat bereits mit zahlreichen Richtlinien zu kämpfen, um sicherzustellen, dass das Unternehmen gemäß den Datenschutzgesetzen handelt. Es wäre nachvollziehbar, wenn sie die Auswirkungen der EU-DSGVO auf ihre tägliche Arbeit skeptisch sieht.

Die Auswirkungen der EU-DSGVO

Es sollte nicht alles auf den Schultern der Rechtsabteilung lasten. Dennoch gibt es entscheidende Bereiche, mit denen sie sich befassen muss. Die Verwaltung der Verträge und die Verhandlungen mit Kunden und Lieferanten gehören zu diesen Bereichen. Gemäß EU-DSGVO ist Ihr Unternehmen für jeden Verstoß gegen die Richtlinien im Zusammenhang mit der Datenverarbeitung verantwortlich und zwar unabhängig davon, ob die Daten im Unternehmen oder über Dritte oder Partner weiterverarbeitet werden. Aus diesem Grund ist es entscheidend, die generelle Einhaltung sicherzustellen. Von internen Teams und Marketing-Datenbanken bis hin zu PR-Agenturen und externe Datenzentren: Wenn die Regeln nicht befolgt werden, oder wenn ein Verstoß vorliegt, kann dies erhebliche Auswirkungen auf Ihr Unternehmen haben. Sie müssen sicherstellen, dass Ihre Datensicherungsrichtlinien den neuen Anforderungen standhalten und Priorität besitzen.

Ihr fünfstufiger Datenfitnessplan

- Alle Verträge, die über den Zeitpunkt des Inkrafttretens der EU-DSGVO hinausreichen, müssen überprüft und gegebenenfalls aktualisiert werden, um den neuen Datenverarbeitungsrichtlinien zu genügen.
- Stellen Sie sicher, dass neue Verträge oder Vereinbarungen die EU-DSGVO bereits berücksichtigen, damit Sie nicht im nächsten Jahr unter Druck geraten, wenn die Änderungen vollzogen sein müssen.
- Dies lässt sich bewerkstelligen, indem Sie bereits jetzt bestimmte Klauseln hinzufügen, die dann bei Inkrafttreten der EU-DSGVO einfach abgeändert werden können.
- Sie können sich in dieser Hinsicht auf den Änderungszeitpunkt vorbereiten, indem Sie diesen Termin in Projektplänen oder Zeitplänen vormerken.
- Kontaktieren Sie Ihre Lieferanten, um die Einhaltung der Verordnung sicherzustellen. Diese Verordnung betrifft auch Ihre Lieferanten. In Kooperation mit ihnen können Sie ihre Ressourcen gemeinsam sinnvoll einsetzen und eine stabile Lösung für beide Seiten entwickeln, sodass für jede Partei klar ist, wo die Verantwortlichkeiten im Falle eines Verstoßes liegen und wenn Betroffene Anträge zu ihren Daten stellen.

Finanzabteilung und Buchhaltung als Achillesferse

32%

der IT-Entscheider haben kaum oder gar keine Kenntnis darüber, dass im Rahmen der EU-Datenschutz-Grundverordnung europäische Unternehmen Sicherheitsvorfälle innerhalb von 72 Stunden berichten müssen.

„Die EU-DSGVO wird große Auswirkungen auf unsere Arbeit haben, denn es werden noch mehr Augen auf unsere Abteilung gerichtet sein, um sicherzustellen, dass wir unsere Daten entsprechend den Gesetzen verarbeiten und sichern."

Häufige Bedenken

Die Finanzabteilung ist ein hochgradig regulierter Bereich und bereits heute verschiedensten Richtlinien zur Rechenschaftspflicht unterworfen, da sie täglich große Mengen sensibler, personenbezogener Daten verarbeitet.

Die Auswirkungen der EU-DSGVO

Aufgrund der Menge von personenbezogenen Daten in den Finanz- und Buchhaltungsabteilungen eines Unternehmens wird sich das Augenmerk des Datenschutzbeauftragten und der Regulierungsbehörden, die für die Einhaltung der EU-DSGVO verantwortlich sind, in Zukunft besonders auf diese Abteilungen richten. Die Sicherheit personenbezogener Daten, die quer durch die Systeme transferiert werden, ist der entscheidende Punkt, an der hohe Bußgelder fällig werden können, wenn ein Verstoß auftritt. Mit den Verfahren, die bereits gemäß strengen Richtlinienkontrollen angewendet werden, wird die EU-DSGVO aber nur dazu beitragen, die Leistungsfähigkeit und Transparenz der Finanzabteilung weiter zu stärken.

Ihr fünfstufiger Datenfitnessplan

- Sorgen Sie dafür, dass innerhalb der Abteilung ein klarer Eskalationsprozess besteht, um etwaige Datenschutzverletzungen umgehend den Behörden zu melden.
- Ein Datenaudit kann dazu beitragen, die erforderlichen Änderungen bei den aktuellen Verfahren zu erfassen und so die Einhaltung der Verordnung sicherzustellen. Dies bedeutet nicht, dass neue Richtlinien erstellt werden müssen. Die vorhandenen Richtlinien sollten aber so aktualisiert werden, dass sie der neuen EU-DSGVO entsprechen.
- Die Automatisierung von Prozessen kann eine Unterstützung bei der Reduzierung menschlicher Fehler und der Vermeidung von Risiken darstellen, die zu Datenschutzverstößen – absichtlichen oder unabsichtlichen – führen können.
- Überprüfen Sie die Datenaufbewahrungsverfahren, die die Aufbewahrung und Vernichtung von personenbezogenen Daten regeln. Diese Parameter werden sich unter der EU-DSGVO ändern.
- Stellen Sie den Datenschutz künftig in das Zentrum aller Prozesse und versuchen Sie nicht, dieses Thema in Form von Add-ons zu bewältigen. Es muss zu einem Kernbereich Ihrer Geschäftstätigkeit werden.

Probleme der Personalabteilung

29%
der IT-Entscheider haben kaum oder gar keine Kenntnis darüber, dass die Verordnung auf persönliche Daten, die innerhalb und außerhalb der EU gespeichert sind, angewandt werden kann.

„Das Speichern, Sichern und Löschen von HR-Daten ist bereits heute eine mühevolle Aufgabe und Ursache regelmäßiger Probleme, und sicher wird uns die EU-DSGVO noch mehr Kopfschmerzen bereiten?“

Häufige Bedenken

Die Personalabteilung speichert eine Menge personenbezogener Daten, z. B. die Lebensläufe jetziger und früherer Mitarbeiter und die von nicht erfolgreichen Kandidaten sowie Mitarbeiterdaten aller Art, darunter Kontaktinformationen und Bankkontoangaben.

Die Auswirkungen der EU-DSGVO

Gemäß EU-DSGVO haben Mitarbeiter weitreichendere Rechte in Bezug auf die Verwendung und die Aufbewahrung ihrer Daten. Dies bereitet Arbeitgebern möglicherweise Kopfschmerzen. Obwohl die Auswirkungen für die Personalabteilungen erheblich sind, ist diese Herausforderung nicht unüberwindbar. Die Personalabteilung muss für mehr Transparenz in Bezug auf die Verwendungszwecke der personenbezogenen Daten sorgen und den Mitarbeitern die Möglichkeit geben, Anträge auf deren Löschung zu stellen. Dies gilt für derzeitige wie ehemalige Mitarbeiter.

Ihr fünfstufiger Datenfitnessplan

- Um Druck von der Personalabteilung zu nehmen, ist ein Audit zu den aktuellen Datenverarbeitungsprozessen und -richtlinien der erste logische Schritt zu einem Verständnis der erforderlichen Änderungen.
- Dadurch kann ermittelt werden, wo Updates an Arbeitsverträgen, Handbüchern und Unternehmensrichtlinien erforderlich sind.
- Bevollmächtigen Sie die Betreffenden in Ihrem Team, mehr Informationen an Mitarbeiter und Bewerber herauszugeben, um den Zweck und die gesetzliche Grundlage für die Erhebung ihrer Daten offenzulegen und um sicherzustellen, dass diese ihre Rechte kennen.
- Um eine schnelle Reaktion auf Datenschutzverstöße zu gewährleisten, ernennen Sie einen diesbezüglichen Verantwortlichen oder ein entsprechendes Team.
- Regelmäßige Schulungen zur Ermittlung eines Datenschutzverstoßes und der Reaktion darauf, in Verbindung mit entsprechenden Richtlinien, können sicherstellen, dass dieser Aspekt der Verordnung nüchtern und vertrauensvoll bewältigt wird.

Irritationen in der IT-Abteilung

„Es ist nicht meine Aufgabe, personenbezogene Daten aufzubewahren oder zu verwalten, warum soll ich mich also um die EU-DSGVO kümmern?“

22%

der IT-Entscheider sind sich nicht darüber bewusst, dass ihre Organisationen bis zum 25. Mai 2018 der EU-Datenschutz-Grundverordnung voll entsprechen müssen.

Häufige Bedenken

IT-Mitarbeiter haben die zentrale Aufgabe, die Infrastruktur des Unternehmens am Laufen zu halten und die Robustheit sowie Zuverlässigkeit der Systeme sicherzustellen. Die EU-DSGVO ist dabei nicht unbedingt ihr Thema. Effektive IT-Prozesse sind aber für die Sicherstellung und Gewährleistung der EU-DSGVO-Einhaltung von grundlegender Bedeutung und sorgen für ein optimiertes, sicheres und transparentes Vorgehen.

Die Auswirkungen der EU-DSGVO

Die EU-DSGVO betrifft die IT-Abteilung auf verschiedene Weise. Dabei gibt es sicherlich Überschneidungen mit anderen Abteilungen, wenn diese ihre Prozesse aktualisieren und optimieren. Beispiel: Das Marketingteam fordert eine Unterstützung für seine Opt-in- und E-Mail-Kampagnen an, um sicherzustellen, dass eine Technologie verfügbar ist, mit deren Hilfe die Einwilligungsformulare etc. protokolliert werden können. Durch die größere Beweislast gegenüber Betroffenen, die Zugang zu ihren Informationen oder deren Löschung bzw. die Angabe des Verwendungszwecks verlangen können, müssen die Systeme und Programme, die diese Informationen enthalten, einfach zu bedienen sein und eine vollständige Transparenz bezüglich deren Verwendung aufweisen. Auch die Sicherung der Daten, die im Besitz Ihres Unternehmens sind, ist extrem wichtig.

Ihr fünfstufiger Datenfitnessplan

- Arbeiten Sie mit den anderen Abteilungen im Unternehmen zusammen und ermitteln Sie deren Anforderungen und wie diese Auswirkungen auf die verwendete Software und die verwendeten Systeme haben, und welche Unterstützung sie benötigen, um der EU-DSGVO zu genügen.
- Katalogisieren Sie alle personenbezogenen Daten, um die Transparenz sicherzustellen und einen einfachen Zugang zu den Informationen zu gewährleisten, wie dies für Berichtszwecke oder Anträge von Betroffenen erforderlich ist.
- Legen Sie eindeutige Auditprotokolle für alle personenbezogenen Daten fest, die in Unternehmen oder daraus transferiert werden.
- Wenden Sie spezielle Datenschutzmaßnahmen an, um die Informationen zu schützen und die Wahrscheinlichkeit sowie die Auswirkungen eines Datenschutzverstoßes zu minimieren, einschließlich Verschlüsselung und Anonymisierung.
- Berücksichtigen Sie die Anforderungen der EU-DSGVO in der Planungsphase einer jeden neuen Software oder von Infrastrukturaktualisierungen und stellen Sie so sicher, dass die Verordnung eingehalten wird und die Daten sicher und vollständig aufbewahrt werden.

17%

der IT-Entscheider geben an, dass ihre Organisationen nur wenige oder gar keine Vorbereitungen hinsichtlich der EU-Datenschutz-Grundverordnung getroffen haben.

Handlungsaufforderung: Gruppenübungen

Die vor Ihnen liegende Aufgabe mag abschrecken, aber die Unternehmen und die einzelnen Abteilungen machen bereits gute Fortschritte bei den Vorkehrungen für einen optimalen Datenzustand. Um die Mitarbeiter zu motivieren und das Unternehmen in einem optimalen Zustand zu halten, sollten Verhaltensweisen in Bezug auf die Sicherheit von personenbezogenen Daten generell gestärkt und beibehalten werden.

Ihr fünfstufiger Datenfitnessplan

- **Legen Sie die ganze Strecke zurück** – Langfristig lohnen sich halbherzige Ansätze bei dem Bemühen, Ihr Unternehmen für die EU-DSGVO bereit zu machen, nicht. Machen Sie die neuen Verfahren zukunftssicher. Es kann Ihr Unternehmen schwer beeinträchtigen, wenn Sie jetzt nicht die richtigen Schritte einleiten.
- **Ernennen Sie einen Coach** – Jede Abteilung benötigt einen Ansprechpartner, der alles zusammenfasst, alle auf Kurs und den Plan im Auge behält.
- **Machen Sie Ihren Kopf frei** – Änderungen in den Abteilungen und im Unternehmen setzen eine offene Geisteshaltung voraus und den Willen, die Prozesse zum langfristigen Wohlergehen des Unternehmens zu ändern.
- **Schulen Sie regelmäßig** – Datenschutzrichtlinien müssen regelmäßig aktualisiert und mit allen Abteilungen, Mitarbeitern und Lieferanten deutlich kommuniziert werden.
- **Arbeiten Sie mit einem persönlichen Trainer** – Unterstützung durch Dritte hilft Ihnen nicht nur dabei, Kurs zu halten, sondern auch künftig einen optimalen Datenzustand gewährleisten zu können.

Sofern nicht anders angegeben, basieren die in diesem Whitepaper aufgeführten Statistiken und Daten aus Untersuchungen, die Arlington Research im Auftrag von Kaspersky Lab im April 2017 durchgeführt hat. Insgesamt wurden über 2.300 IT-Entscheider in Europa, aus Unternehmen mit 50 und mehr Mitarbeitern, über Ihre Meinung und Wahrnehmung zur EU-Datenschutz-Grundverordnung (DSGVO) befragt.

For more information about Kaspersky products and services contact your account rep or visit www.kaspersky.com

Kaspersky Lab
Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK
www.kaspersky.com