Kingston TECHNOLOGY

Datenschutz und Cybersicherheit nach der DSGVO

Datenschutz und Cybersicherheit nach der DSGVO

Vorwort

Unzählige Unternehmen und Organisationen haben hart gearbeitet – und viele Stellen geschaffen – um sich auf die DSGVO vorzubereiten. Vielleicht war auch Ihr Unternehmen eines von diesen. Doch die sich ständig weiterentwickelnden Cyberbedrohungen bedeuten, dass Sie es sich nicht leisten können, innezuhalten und Luft zu holen. Die Einhaltung der DSGVO ist kein Abarbeiten einer To-Do-Liste, sondern ein Rahmen, anhand dessen Sie Ihre kontinuierlichen Bemühungen um Datenschutz und Cybersicherheit beurteilen können. Es gibt keinen Platz für Selbstzufriedenheit.

In diesem kurzen eBook bündeln wir das Wissen einiger der erfahrensten Kommentatoren Großbritanniens im Bereich der Cybersicherheit, um zu erörtern, wie sich der Datenschutz seit der Einführung der DSGVO verändert hat. Wir berichten auch darüber, wie Unternehmen ihre Mitarbeiter über die Notwendigkeit der Einhaltung von Vorschriften aufklären und diskutieren, wie IT-Abteilungen und Technologieanbieter die IT-Infrastruktur besser sichern und Endbenutzer über neue Sicherheitsherausforderungen aufklären können.

Datenschutz und Cybersicherheit nach der DSGVO

Mitwirkende

Dieses kurze eBook wurde von fünf Experten für Datenschutz und Cybersicherheit zusammengestellt.

Rob Allen
@Rob_A_kingston

Rob ist Direktor für Marketing und technische Dienste bei Kingston Technology und gehört dem Unternehmen seit 1996 an. In seiner Funktion ist Rob verantwortlich für die Bereiche PR, Soziale Medien, Channel-Marketing mit digitalen Marketingmedien und Kreatives für alle Kingston Marken und Produkte.

Tara Taubman-Bassirian
@clarinette02

Tara trägt viele Titel: Anwältin, Rechtsanwältin, Mediatorin, Forscherin, Beraterin, Rednerin und Schriftstellerin. Mit ihrer unglaublichen Expertise in Bereichen wie Privatsphäre, geistiges Eigentum und Datenschutz hat sie sich in mehreren Regionen der Welt einen Namen gemacht, vor allem in Großbritannien, Frankreich und den USA.

Rafael Bloom
@rafibloom73

Rafael ist der Direktor von Salvatore Ltd. In dieser Funktion unterstützt er Unternehmen bei der Bewältigung der strategischen, wirtschaftlichen und verfahrenstechnischen Herausforderungen und Chancen, die sich aus dem technologischen und regulatorischen Wandel ergeben.

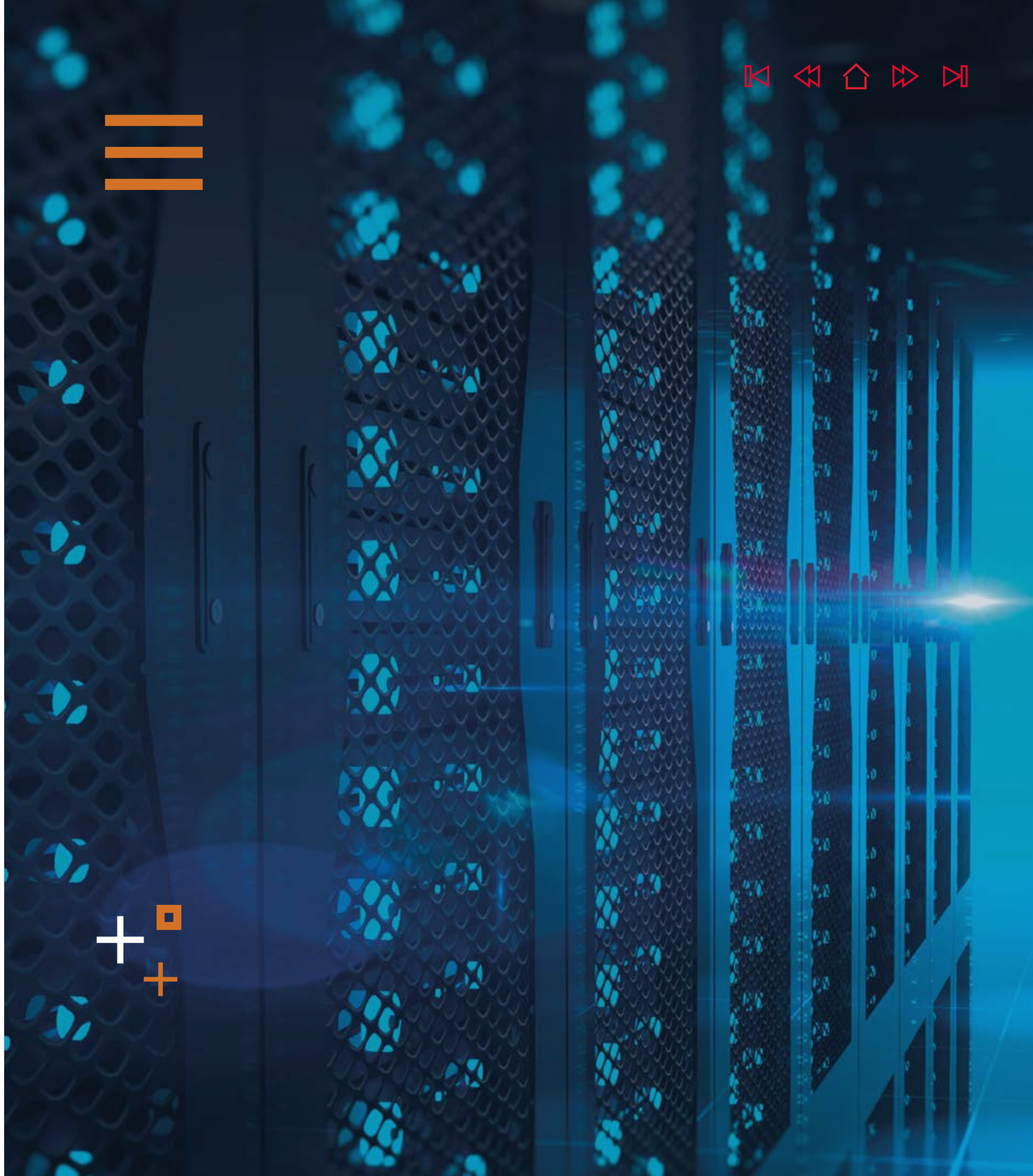
Miriam Brown
@Kingston_MBrown

Strategischer B2B-Marketing-Manager bei Kingston Technology, die seit 1997 im Unternehmen tätig ist. In ihrer Funktion ist Miriam für die Marketingstrategie, den Inhalt und die Kampagnen für alle Kingston B2B-Produkte verantwortlich.

Sally Eaves
@sallyeaves

Prof. Sally Eaves wurde als Wegbereiterin für ethische Technologie beschrieben. Sie bringt umfassende Erfahrungen aus ihren Funktionen als Geschäftsführerin und Technische Direktorin, sowie als Professorin für aufstrebende Technologien und als globale strategische Beraterin mit. Sally ist eine preisgekrönte internationale Hauptrednerin, Autorin, Forscherin und Influencerin, die eine eigenständige und authentische Vordenkerrolle einnimmt.

Inhaltsverzeichnis



Abschnitt 1 – Wie hat sich der Datenschutz seit der DSGVO verändert?

Unternehmen haben schon einen weiten Weg zurückgelegt. In den letzten zwei Jahren wurden die juristischen Teams vergrößert, die Einstellung von Datenschutzbeauftragten ist in die Höhe geschnellt[1] und die Konsultation von externen Datenschutzbeauftragten hat zugenommen. Die Durchführung von Datenschutzfolgenabschätzungen (DPIAs) ist inzwischen Tausenden von Organisationen und Unternehmen bekannt.

Aber es liegt noch ein langer Weg vor uns.

Eine der größten Herausforderungen der DSGVO ist, dass man immer fokussiert bleiben muss. In den meisten Organisationen könnte fast jeder Mitarbeiter jederzeit gegen die Regeln verstoßen. Das Problem ist in Sektoren größer, in denen die Arbeitskräfte überlastet sind oder in denen es ein hohes Maß an Autonomie gibt – wie etwa im Gesundheitswesen, im Bildungswesen und im Rechtswesen. Im Rechtswesen werden sich beispielsweise viele Anwälte nichts dabei denken, sensible Falldaten über einen einfachen E-Mail-Anhang auszutauschen. Angehörige der Gesundheitsberufe tauschen Patientendaten oder die Ergebnisse eines MRT-Scans über ungesicherte E-Mail-Adressen aus. In Organisationen mit hohem Stress ist nur ein wenig zusätzlicher Druck auf der To-Do-Liste nötig, damit die Einhaltung der Vorschriften aus dem Blick gerät. Die Produktivität – so scheint es – ist wichtiger als das Protokoll.

Das muss sich ändern.

Dann ist da noch die Frage des Bewusstseins im Wohltätigkeitsbereich. Allzu oft scheinen Wohltätigkeitsorganisationen zu glauben, dass sie von der DSGVO ausgenommen sind. Selbst wenn sie verstehen, dass die DSGVO für jede Organisation des privaten, öffentlichen und NRO-Sektors gilt, zögern sie – vielleicht verständlicherweise – Geld von ihrem Anliegen abzuziehen und es in den Datenschutz zu investieren. Das ist edel, aber auch naiv. Die möglichen Bußgelder für Verstöße gegen die DSGVO stellen die wahrscheinlichen IT-Ausgaben in den Schatten.

Seit 2016 ist die Nachfrage nach Datenschutzbeauftragten (DSB) in die Höhe geschnellt und um über 700 % gestiegen.

Tara Taubman-Bassirian
@clarinette02

Berater für DSGVO, Datenschutz und geistiges Eigentum

„Viele Organisationen des NRO-Sektors sagen: 'Die DSGVO gilt nicht für uns, wir sind nur eine Wohltätigkeitsorganisation.' Selbst bei der Einhaltung der Website-Compliance versuche ich ihnen zu sagen, dass es nicht um die Daten geht, die Sie sammeln wollen, sondern um die Dritten, denen sie den Zugriff auf die Daten Ihrer Besucher gestatten."

1. Varonis: Ein Jahr im Leben mit der DSGVO: Wissenswerte Fakten und Schlüsselthemen www.varonis.com/blog/gdpr-effect-review/ [Abfrage am 26.11.19]

Wie hat sich der Datenschutz seit der DSGVO verändert?

Die Datenminimierung ist ein ermutigender Trend

Wir leben in einer Zeit ungeheurer Datenerfassung. Die „Big Four" (Google, Apple, Facebook und Amazon) verfügen über riesige Mengen an Kundendaten. Andere Organisationen könnten die „Big Four" nachahmen und so viele Daten wie möglich sammeln. Doch je mehr Daten Sie zur Verfügung haben, desto mehr Risiken setzen Sie sich aus. Einer der positivsten Trends seit der Einführung der DSGVO ist der Widerstand gegen die übermäßige Datenerfassung. Kluge Unternehmen setzen sich für ein Ethos der Datenminimierung ein: Wenn man sie nicht braucht, sammelt man sie nicht.

Tara Taubman-Bassirian
@clarinette02

Berater für DSGVO, Datenschutz und geistiges Eigentum

„Die Datenminimierung ist wahrscheinlich eines der besten Prinzipien der DSGVO. Jede Erstellung einer Datenbank bedeutet, dass ein Risiko entsteht."

Rob Allen
@Rob_A_kingston

Direktor für Marketing und technische Dienste, Kingston Technology

„Wir haben strenge Regeln für die Löschung von Daten. Ja, geschäftskritische Daten müssen korrekt gespeichert werden. Aber alles andere auch? Nach einem Jahr sind sie weg. Was bringt es, die Daten zu behalten?"

Die Vorteile gehen sogar über die Risikominimierung hinaus. Nehmen wir zum Beispiel das Marketing. Wenn Ihre Marketingdatenbank nicht gepflegt wird, verfügen Sie möglicherweise über veraltete Daten. Wenn Ihre Datenbank Zehntausende von Personen umfasst und Sie häufig E-Mail-Marketingkampagnen durchführen, summieren sich die Kosten. Außerdem verzerrt sich die Leistungsstatistik Ihrer Kampagne.
Die Datenminimierung gilt auch für physische Daten. Seien Sie vorsichtig, was Sie ausdrucken (z. B. Scans von Kundenpässen) und seien Sie vorsichtig, was Sie aufschreiben (z. B. Kontopasswörter). Wenn Sie eine physische Kopie von etwas benötigen, bewahren Sie sie sicher auf. Der Berg an Papierkram auf Ihrem Schreibtisch mag imposant aussehen. Aber sicher ist er nicht.

Rafael Bloom
@rafibloom73

Direktor,
Salvatore Ltd.

„Wir beobachten eine völlig anderes Verständnis über die Schnittstelle zwischen Technologie und dem, was ein Unternehmen tatsächlich tut. Es muss unbedingt ein hoher Grad an digitaler Reife innerhalb der Unternehmensführung erreicht werden."

Auswirkungen der Exposition: von der Führungsebene zum Verbraucher

Datenschutz als Regulierungskonzept gibt es seit Jahrzehnten. Aber durch die hohen Bußgelder, die Unternehmen wie Google[1], British Airways und der Marriott-Hotelkette[2] auferlegt wurden – und die Berichterstattung darüber in den Medien – wurde die Aufmerksamkeit der Führungsebene auf die DSGVO gelenkt. Dies hat zu einem tieferen und weitreichenderem Verständnis für die DSGVO gesorgt.

1. Varonis: Ein Jahr im Leben mit der DSGVO: Wissenswerte Fakten und Schlüsselthemen www.varonis.com/blog/gdpr-effect-review/ [Abfrage am 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [Abfrage am 26.11.19]

Wie hat sich der Datenschutz seit der DSGVO verändert?

Fortsetzung...

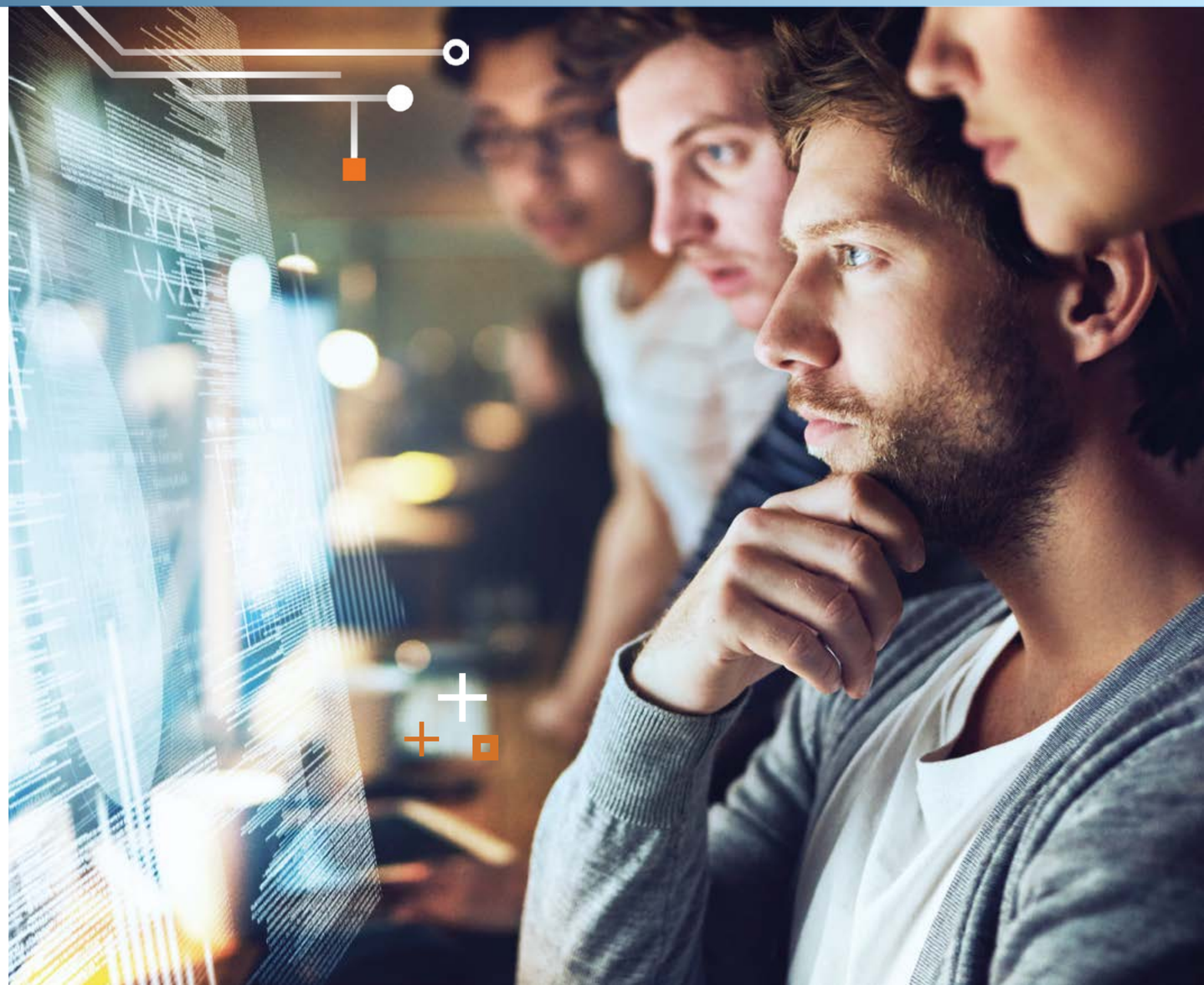
Eine weitere treibende Kraft hinter der Einführung eines starken Datenschutzes sind Kooperationen. Große Unternehmen führen nun eine umfassende Due Diligence-Prüfung zur Integrität der Datensicherheit eines potenziellen Lieferanten durch, da sie nicht für Datenverletzungen durch die Zusammenarbeit mit Dritten haftbar gemacht werden wollen.

Es gibt auch eine Kehrseite des verstärkten kommerziellen Bewusstseins der DSGVO: Die Verbraucher sind sich ihrer Rechte an ihren Daten bewusster. Sie wissen, dass sie, wenn ein Unternehmen die Kontrolle über seine Daten verliert, Anspruch auf Entschädigung haben und es ist dabei zu beachten, dass nicht unbedingt ein Verstoß vorliegen muss. Unternehmen müssen ihre Konzentration aufrechterhalten.

Sally Eaves
@sallyeaves

CEO und Direktor,
Sally Eaves Consultancy

„Datenschutz ist zu einer geschäftlichen Pflichtübung geworden, mit dem Vertrauen gewonnen oder verloren werden kann."



Abschnitt 2 – Wie schulen Unternehmen ihre Mitarbeiter?

Mitarbeiterschulung: ein Wort, das bei Ihren Mitarbeitern Augenrollen verursachen kann.

Ein weiterer Grund, um sicherzustellen, dass Ihre Schulung für Ihre Mitarbeiter interessant und informativ ist. Gut geschulte Mitarbeiter vernachlässigen seltener wirksame Datenschutzpraktiken. Falls es eine Datenschutzverletzung gibt, wird die Beurteilung der Datenschutzbehörde (ICO) für Sie günstiger ausfallen, wenn Sie nachweisen können, dass Sie sich bemüht haben, Ihre Mitarbeiter in Sachen Datensicherheit zu schulen.

Rafael Bloom
@rafibloom73

Direktor,
Salvatore

„Ich sehe Daten gerne als ein Element der Lieferkette, bei dem ihre Herkunft und ihr gesamter Lebenszyklus einer angemessenen Kontrolle unterliegen müssen. Es ist gut und schön, wenn Sie Ihr Team für eine halbe Stunde in einen Raum holen und ihnen sagen, was sie zu tun haben, wie „bitte schreddern Sie nichts, bitte verwenden Sie ein anständiges Passwort". Sicher, Sie haben das Risiko für das Unternehmen gesenkt. Aber gibt es später wirklich einen wesentlichen Unterschied, abgesehen von der anfänglich kleinen Wirkung, die Sie den Menschen irgendwie aufgezwungen haben? Nein."

Im April 2019 hat die Digitalministerin Margot James aber angedeutet, dass nur drei von zehn britischen Organisationen Mitarbeiter für den Umgang mit Cyberbedrohungen geschult haben[1]. Es ist an der Zeit, die Schulung ernst zu nehmen.

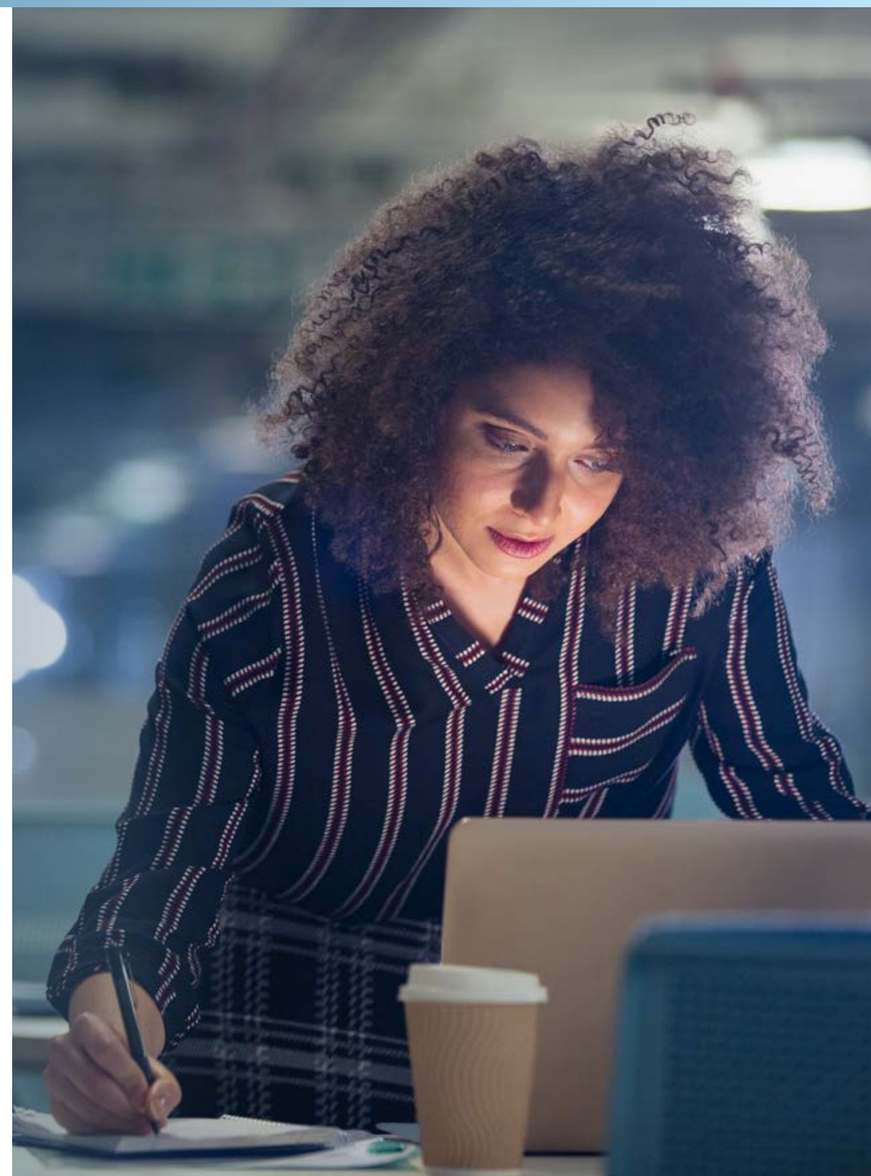
Es geht um die Schaffung einer Kultur, nicht um eine Schulung, bei der man Kästchen ankreuzen muss.

Bei der Schulung geht es darum, echte Veränderungen im Verhalten und der Unternehmenskultur zu erreichen, nicht darum, etwas anzukreuzen. Es ist einfach, ein Online-Schulungspaket mit einigen einfachen Fragen zum Datenschutz zu erwerben, die jeder richtig beantworten kann. Aber wird das wirklich zum Schutz Ihrer Organisation beitragen?

Gutes Datenschutzverhalten umfasst zwei grundlegende Bestandteile. Erstens: Eine Schulung, die interessant und auf die besonderen Herausforderungen Ihrer Organisation ausgerichtet ist. Zweitens, die Erkenntnis, dass die DSGVO eine tief greifende Frage der Arbeitsplatzkultur ist, die alle Mitarbeiter jeden Tag betrifft. Es geht darum, mit den Daten das Richtige zu tun, den richtigen Weg in der gesamten Organisation zu finden. Nehmen wir zum Beispiel die Personalabteilung. Denken Sie an all die persönlichen Details der Stellenbewerber, die gerade auf den E-Mail-Servern liegen.

Der Datenschutz liegt in der Verantwortung aller.

1. Intelligenter CISO: Welche Auswirkungen hatte die DSGVO ein Jahr später auf die Datensicherheit? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [Zugriff am 26.11.19]



Wie schulen Unternehmen ihre Mitarbeiter?

Hinter allen Daten stehen Personen

Im ersten Abschnitt haben wir festgestellt, dass die Verbraucher sich ihrer Datenrechte immer bewusster werden. Eine gute Möglichkeit, Datenschutzschulungen wirkungsvoll zu gestalten, besteht darin, Ihren Mitarbeitern zu helfen, die Verbindung herzustellen, dass hinter den Daten immer eine Person steht. Bitten Sie Ihre Mitarbeiter, über jede Organisation nachzudenken, an die sie Daten weitergegeben haben, dann wird ihnen klar werden, dass es beim Datenschutz um die persönliche Privatsphäre geht.

Notfallplan zur Hand haben

Sally Eaves
@sallyeaves

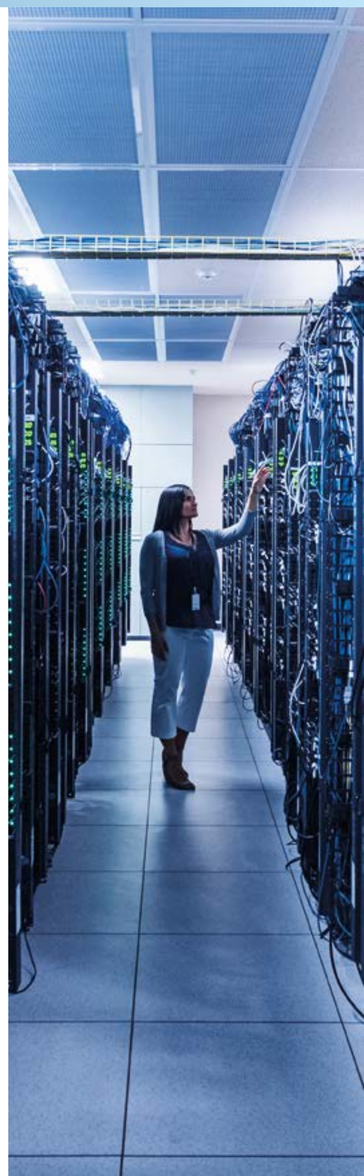
„Die kontinuierliche Schulung der Mitarbeiter über Datensicherheit und -schutz ist Pflicht für ein Unternehmen. Dies darf keine einmalige, einmal im Jahr stattfindende Schulung sein, sondern muss zu einer proaktiven, interaktiven und informativen Kultur werden, die die tägliche Arbeitsumgebung durchdringt. Die Mitarbeiter müssen in den Dialog zum Thema einbezogen werden, was wir abmildern, managen und verteidigen wollen."

Miriam Brown
@Kingston_MBrown

„Ich denke, es ist während der Schulung interessant, wenn Sie die Leute fragen: „Was wäre, wenn das Ihre Daten wären?" Wenn mein Bankmanager von zu Hause aus auf seinem Laptop arbeiten würde und sensible Informationen auf diesem Laptop hätte, würde ich mir wünschen, dass sie auf einem verschlüsselten Laufwerk liegen."

Rob Allen
@Rob_A_kingston

„Behandeln Sie Daten, als wären es Ihre eigenen."



Abschnitt 3 – Können IT-Abteilungen Geräte besser sichern?

Fernarbeit ist die neue Normalität.

Ihre Mitarbeiter haben wahrscheinlich über mehrere verschiedene Geräte Zugang zu ihrer Arbeitswelt – einschließlich persönlicher Geräte, die leicht im Zug liegen bleiben oder im Taxi verloren gehen können. Ihre Herausforderung besteht darin, einen Weg zu finden, wie Sie Ihren Mitarbeitern helfen können, effizient zu arbeiten, ohne sich Sicherheitsrisiken und Datenverletzungen auszusetzen. Eine einzige Person reicht aus, um Ihre Datenschutzbemühungen zum Scheitern zu bringen.

Sally Eaves
@sallyeaves

CEO und Direktor,
Sally Eaves Consultancy

„Daten müssen während der Übertragung, im Ruhezustand und bei der Nutzung geschützt werden – es ist entscheidend, einen allumfassenden Sicherheits-, Wiederherstellungs- und Datenlöschungsplan zu haben, der all diese Kontexte abdeckt. Besonders wichtig ist es, die Aufmerksamkeit auf Risikobereiche zu lenken, die oft unterschätzt werden, z. B. unverschlüsselte USB-Sticks und -Laufwerke, die Verwendung von E-Mails für den Versand unverschlüsselter Anhänge und Webbrowser-Funktionen, die sensible Benutzerdaten offenlegen. Bei so vielen verbundenen Geräten und der ständigen Veränderung von Arbeitsweisen ist es von entscheidender Bedeutung, dass die auf einem Mobiltelefon gespeicherten Daten so sicher sind wie die auf einem Unternehmensserver gespeicherten Daten."

Zwei-Faktor-Authentifizierung

Für ein durchschnittliches Unternehmen ist es bei weitem das Beste und Einfachste, den Netzwerkperimeter zu schützen – und das kann wirklich so einfach sein wie die Verwendung von Passwortmanagern und Zwei-Faktor-Authentifizierung. Ein gutes Beispiel für die Zwei-Faktor-Authentifizierung ist, wenn ein Benutzer aufgefordert wird, ein Passwort auf einem Laptop sowie einen Passcode einzugeben, der an sein Mobiltelefon gesendet wird, sobald ein Passwort erfolgreich eingegeben wurde.

VPNs und verschlüsselte SSDs/USB-Laufwerke

VPN-Netzwerke sind bei KMUs zunehmend beliebt. Sie sind besonders geeignet für Mitarbeiter, die über öffentliche WLAN-Netze auf Geschäftsdaten zugreifen. Aber Unternehmen müssen sich davor hüten, die Fähigkeiten von VPNs zu überschätzen. Sie sind eher ein Teil als die ganze Lösung. Zu oft setzen Unternehmen VPNs ein, nur damit mobil arbeitende Mitarbeiter Notebooks oder Laptops ohne jegliche Hardware-Verschlüsselung nutzen können. Fast jeder speichert Dateien auf seinem Laptop. Was passiert, wenn dieses Gerät gehackt, verloren oder gestohlen wird? Verschlüsselte USB-Sticks und SSDs sind nur geringfügig teurer als die Standardversionen. Die Bereitstellung verschlüsselter USB-Sticks und die Ausstattung der Notebooks Ihres Unternehmens mit hardwareverschlüsselten SSDs ist ein langer, langer Weg, um die Herausforderungen der Remote-Arbeit zu bewältigen. Falls ein Gerät verloren geht oder gestohlen wird, können Sie sicher sein, dass niemand Zugriff auf die verschlüsselten Dateien hat. Sie können sogar verlorene USB-Sticks aus der Ferne zerstören.

„Ich habe einmal einen Cyber-Sicherheitsexperten getroffen, der versuchte, den CEO eines Unternehmens zur Zwei-Faktor-Authentifizierung zu überreden, nur um dann auf Widerstand zu stoßen: „Nein, wir machen es nicht, das ist umständlich, das ist ein zusätzlicher Schritt, das will ich nicht."" Bald darauf wurden sie Opfer eines Betrugs in der Höhe von 40.000 Pfund."

Rafael Bloom
@rafibloom73

Direktor, Salvatore Ltd.

„Letztendlich ist die beste Methode, das Sicherheitsbewusstsein zu erhöhen, Gespräche mit den Mitarbeitern zu führen und Strategien zu finden, die sowohl sicher als auch produktiv sind."

Rob Allen
@Rob_A_kingston

Direktor für Marketing und technische Dienste, Kingston Technology

Können IT-Abteilungen Geräte besser sichern?

Private Server und MSPs

Immer mehr große Organisationen gehen wieder dazu über, eigene Server vor Ort zu haben. Das bedeutet, dass sie die volle Kontrolle über ihren Serverbestand haben, wobei nichts in der öffentlich zugänglichen Cloud gespeichert wird. Dann gibt es hybride Serverlösungen, bei denen nicht-sensible Daten in der Cloud bleiben, persönliche Daten aber vor Ort bleiben. Für KMUs und Organisationen des NRO-Sektors kann es zu teuer sein, einen eigenen Server zu unterhalten. Hier kommen die Anbieter von verwalteten Diensten und virtuellen privaten Servern ins Spiel. Diese verstärken den Fokus auf die Sicherheit, ohne Ihre Betriebskosten dramatisch zu erhöhen.

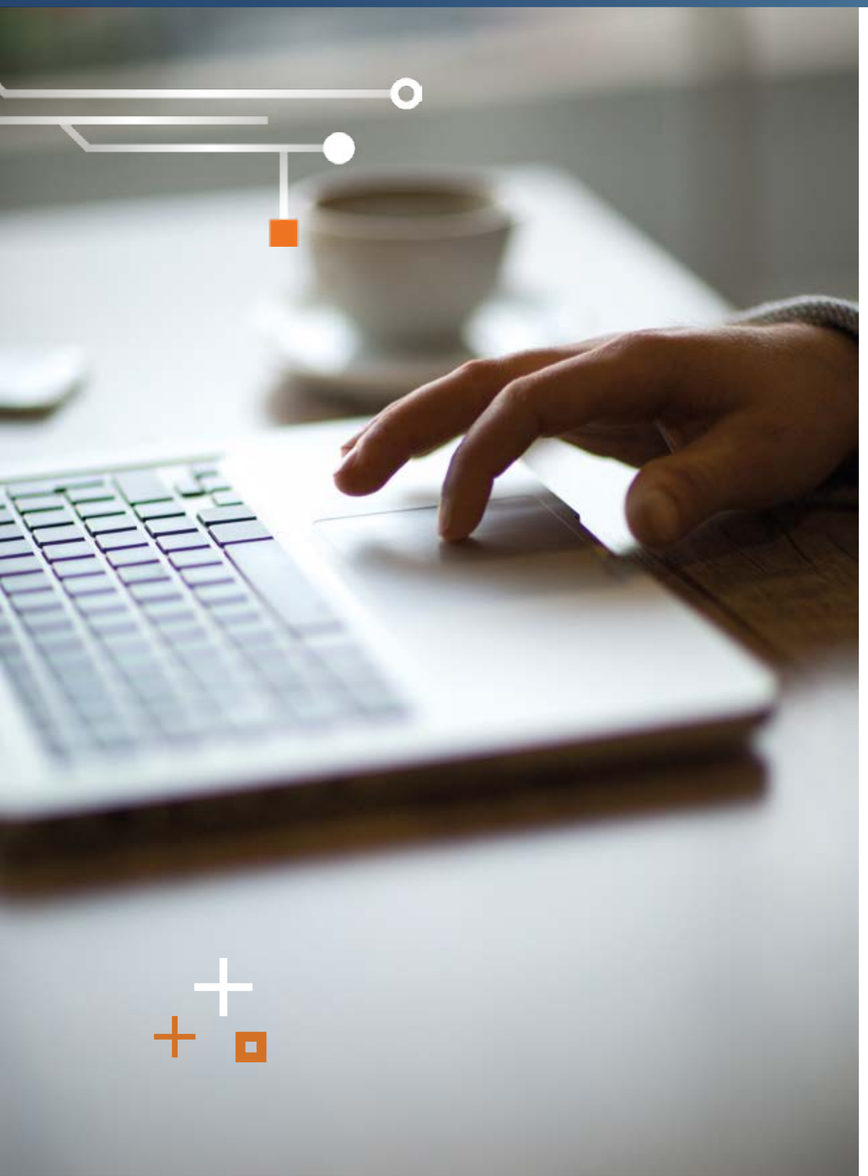
Automatische Markierung abgelaufener Daten

Einer der Grundsätze der DSGVO ist die Notwendigkeit, alte Daten zu löschen. Bestimmte Arten von persönlichen Daten dürfen beispielsweise nicht länger als sieben Jahre aufbewahrt werden. Was wäre, wenn Sie automatisch aufgefordert würden, wenn die Frist für Daten bald „ablaufen" würde? Mit der richtigen Datenbank wäre es für Ihr IT-Team ein Leichtes, eine Aktion zu erstellen, die eine automatisch generierte E-Mail an den DSB sendet, wenn sich das Datum einer Sperrfrist für die Datenspeicherung nähert.

Zusammenarbeit mit den richtigen Anbietern

Wenn es um IT-Sicherheit geht, gibt es unzählige Hersteller und Anbieter. Recherchieren Sie. Es geht darum, ein System zu haben, das von einem vertrauenswürdigen Anbieter mit dem spezifischen Fachwissen in Ihrer Branche stammt. Stellen Sie sicher, dass der/die von Ihnen gewählte(n) Anbieter nicht nur über die Technologie verfügt bzw. sie besitzt, sondern auch die Herausforderungen bei der Umsetzung der Datensicherheit versteht.

Abschnitt 4 – Wie können Technologieanbieter ihre Prozesse und ihr Verständnis verbessern?



TLC für den DSB

Seit 2016 ist die Nachfrage nach Datenschutzbeauftragten in die Höhe geschnellt und um über 700 % gestiegen.[1] In ganz Europa sind heute über 500.000 Datenschutzbeauftragte beschäftigt – das ist sechsmal so viel wie noch 2017 prognostiziert wurde.[2] Und doch wird die Bedeutung der Rolle des Datenschutzbeauftragten oft übersehen und bagatellisiert.

Ein DSB benötigt einen vollständigen Einblick in die Sicherheits- und Datenschutzumgebung Ihres Unternehmens. Es ist eine Vollzeitbeschäftigung. Doch in einigen Organisationen ist „DSB" einfach ein Etikett, das dem Mitarbeiter, der die Technologie am besten versteht, verliehen wird. Sie sind für den Datenschutz ihres gesamten Unternehmens verantwortlich, während sie gleichzeitig die regulären Aufgaben ihrer täglichen Arbeit erfüllen müssen.

Die Realität sieht so aus, dass es eine Reihe von professionellen Dienstleistungen und Instrumenten zur Unterstützung dieser neuen Art von DSB geben muss. Selbst wenn Sie einen Vollzeit-DSB haben, gibt es rasante Veränderungen bei der Datensicherheit, und es wird immer Herausforderungen geben, die eine zweite Meinung erfordern. Die Zusammenarbeit mit einem externen Beratungsunternehmen oder einem Berater für Datensicherheit kann ein langer Weg sein, aber zuerst müssen Sie die Dinge intern so gut wie möglich in Ordnung bringen.

Klarheit, Kontingenz und Kohäsion

Ihre IT-Infrastruktur ist nur so stark wie ihr schwächstes Glied. Deshalb sollte Ihr Technologieanbieter bei jeder Neuerung in Ihrem IT-Ökosystem volle Klarheit über die potenziellen Sicherheitsbedrohungen und klare Ratschläge zur sicheren Nutzung Ihres neuen Produkts geben.

Tara Taubman-Bassirian
@clarinette02

Berater für DSGVO, Datenschutz und geistiges Eigentum

„Ich versuche den Leuten, die überall CCTV-Kameras installieren, zu erklären, dass dies nicht unbedingt sicher ist, denn oft werden sie ohne Passwort installiert. Sie können sich also einfach auf einer Website einloggen und zuschauen. Solche Kameras sind eine Einladung für Einbrecher:
Komm und sieh nach, wann ich nicht da bin!"

1. Varonis: Ein Jahr im Leben mit der DSGVO: Wissenswerte Fakten und Schlüsselthemen
   www.varonis.com/blog/gdpr-effect-review/ [Abfrage am 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go?
   www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [Abfrage am 26.11.19]

Wie können Technologieanbieter Prozesse und das Verständnis verbessern?

Es gibt das Problem der Notfallmaßnahmen. Was passiert, wenn ein Produkt das Ende seiner Lebensdauer erreicht oder aktualisiert werden muss? Technologieanbieter sollten Ratschläge für den Fall geben, dass ihre Produkte unbeabsichtigt die darauf enthaltenen Daten gefährden oder die Sicherheit Ihres größeren IT-Ökosystems gefährden. Nehmen Sie zum Beispiel einen MRT-Scanner. Er könnte mit einer vier Terabyte großen verschlüsselten SSD zum Speichern von Patientenbildern ausgestattet sein. Aber was passiert, wenn dieser Speicher voll ist?

Auch die Technologieanbieter und Unternehmen selbst müssen ein Umfeld des digitalen Zusammenhalts und der Datenkohäsion schaffen – sowohl innerhalb der Organisation als auch bei der Zusammenarbeit mit externen Anbietern und Partnern. Das ist besonders für vielschichtige, abteilungs- und standortübergreifende Organisationen wie den NHS (National Health Service, Großbritannien) von entscheidender Bedeutung.

Miriam Brown
@Kingston_MBrown
Strategischer B2B-Marketing-Manager bei Kingston Technology

„Wir haben viele Produkte an den NHS verkauft – aber es gibt deutliche Unterschiede von einer Stiftung zur nächsten, wenn wir fragen, welche Datenschutzrichtlinien und Protokolle sie anwenden."

Die Zukunft im Blick

Die Technik verändert sich schnell, manchmal schneller als die Sicherheit. Bei neu aufkommenden Technologien – wie z. B. der Bezahlung durch Gesichtserkennung in China – ist es manchmal so, dass Organisationen losrennen, um sich die Technologie zu sichern, bevor sie die möglichen Auswirkungen auf Sicherheit und Datenschutz in Betracht gezogen haben. Die weit verbreitete Verfügbarkeit von 5G-Netzen ist nur noch ein oder zwei Jahre entfernt, in denen Edge-Computing und verteilte Datensilos Realität werden. Technologieanbieter müssen in der Lage sein, Unternehmen dabei zu unterstützen, von neuen Technologien sicher zu profitieren, ohne ihre eigene Datenintegrität oder IT-Sicherheit zu gefährden.

Sally Eaves
@sallyeaves

CEO und Direktor, Sally Eaves Consultancy

„Ich glaube, wir werden eine Veränderung der DSGVO erleben, weg von der reinen Verringerung der Umsetzungsschwierigkeiten, hin zu einer Konzentration auf die Optimierung der Vorteile, wie z. B. verbesserte IT-Prozesse, Backup und Wiederherstellung und erhöhte Sicherheit, und diese als Differenzierungspunkt gegenüber den Branchenkollegen nutzen."

Fazit

Die DSGVO hat die Geschäftswelt zum Besseren verändert, indem sie die Aufmerksamkeit der Führungsebene und der Verbraucher gleichermaßen auf den Datenschutz und die Netzwerksicherheit gelenkt hat. Die Einhaltung von Vorschriften erfordert jedoch, dass konstant die Datensicherheit im Auge behalten werden muss – Tag für Tag – von allen Mitarbeitern. Die sich ständig weiterentwickelnde Technologie und die immer neuen Cyber-Bedrohungen bedeuten, dass eine gute Sicherheitsinfrastruktur und eine gute Schulung – unterstützt durch eine gute beratende Unterstützung im Bereich Technologie und Datenschutz – geschäftskritisch ist. Wenn die Mitarbeiter daran erinnert werden, dass hinter Daten immer eine Person steht, kann viel dazu beitragen, eine Kultur des Datenschutzes in Ihrer Belegschaft zu verankern. Und ein kultureller Wandel ist weitaus effektiver als ein reines Abhaken von Aufgaben bei einer Schulung.

Über Kingston

Mit 32 Jahren Erfahrung verfügt Kingston über das Wissen, um Ihre Herausforderungen bei der Remote-Arbeit zu identifizieren und zu lösen – so können Ihre Mitarbeiter von überall sicher arbeiten, ohne Ihr Unternehmen zu gefährden.

#KingstonisEverywhere