Ist Ihr Unternehmen bereit für die DSGVO der EU?

PBJ COMPUTER

panda | BUSINESS PARTNER

Die neue Datenschutzgrundverordnung (DSGVO) ist eine Reaktion auf die Zunahme von Cyberattacken und entspringt dem Bedürfnis nach einer verstärkten Zusammenarbeit zwischen öffentlichen und privaten Organisationen, um dieses Dauerproblem zu lösen.

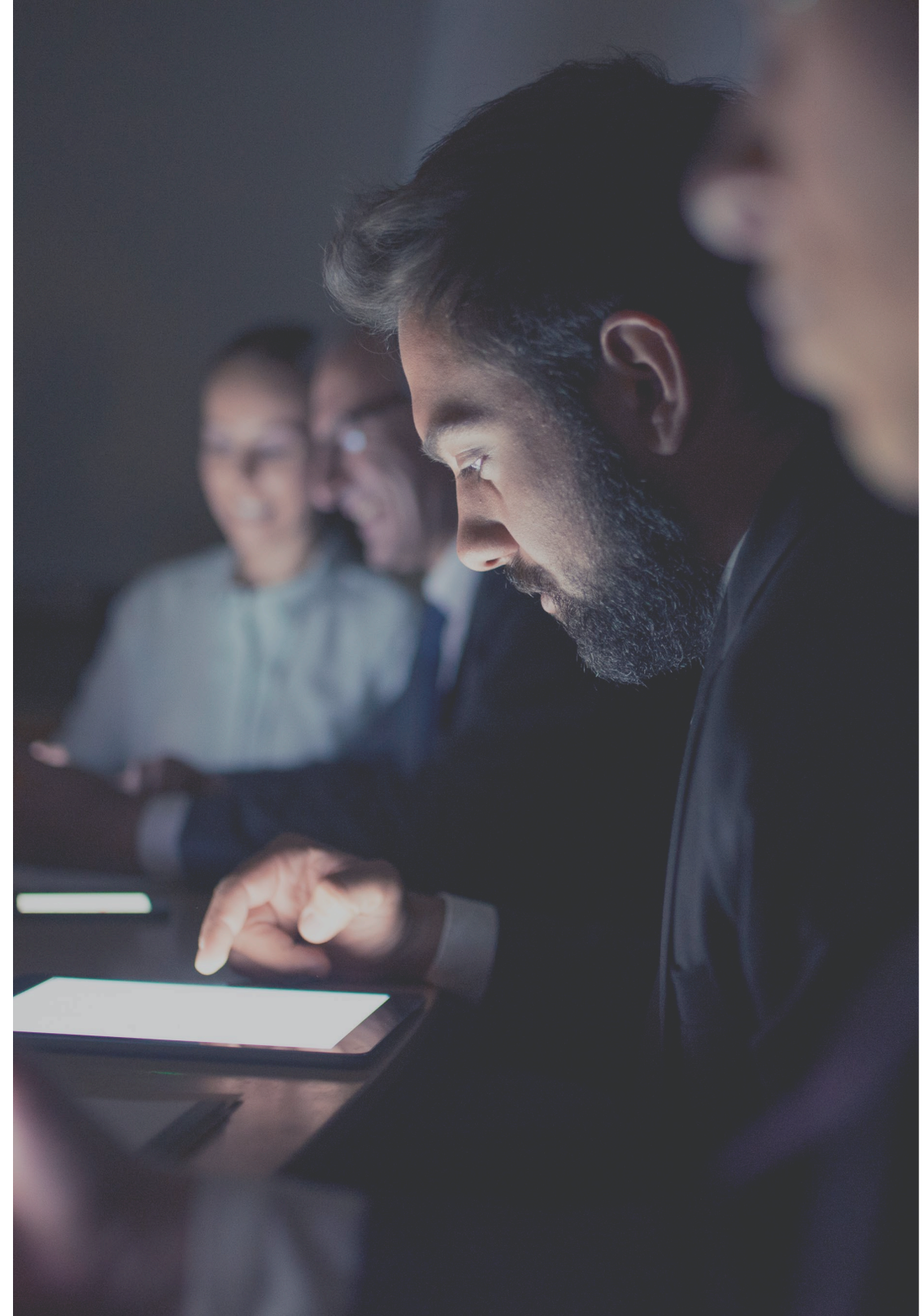
Die Schaffung einer gemeinsamen Regelung ist **eine zusätzliche Sicherheitsbarriere für einen wichtigen und äußerst wertvollen Unternehmenswert: Ihre Daten.**

1. Einführung

Die neue Datenschutz-Grundverordnung wurde vom Europäischen Parlament und dem Rat der EU am 27. April 2016 gebilligt. Sie trat am 25. Mai 2016 in Kraft und wird ab **25. Mai 2018** durchgesetzt.

Die DSGVO setzt Maßstäbe, um ein einheitliches Schutzniveau bei der Verarbeitung von Daten von natürlichen Personen innerhalb der Europäischen Union und beim freien Verkehr solcher Daten innerhalb der Mitgliedsstaaten sicherzustellen.

Wir haben dieses Whitepaper zusammengestellt, um das Verständnis der wichtigsten Inhalte des neuen Rechtsrahmens zu erleichtern und so Unternehmen und staatlichen Institutionen zu helfen, einen Überblick über die Veränderungen zu bekommen, die die neue DSGVO enthalten wird.



2. Wesentliche Schlussfolgerungen

Die neue Datenschutzgrundverordnung (DSGVO) ist eine Reaktion auf die Zunahme von Cyberattacken und entspringt dem Bedürfnis nach einer verstärkten Zusammenarbeit zwischen öffentlichen und privaten Organisationen, um dieses Dauerproblem zu lösen. Die Schaffung einer gemeinsamen Regelung ist eine zusätzliche Sicherheitsbarriere für einen wichtigen und äußerst wertvollen Unternehmenswert: Ihre Daten

Ab dem 25. Mai 2018 müssen Firmen jede Sicherheitsverletzung, die sie erleiden, öffentlich machen und die betroffenen Nutzer innerhalb von 72 Stunden benachrichtigen. Das wird zu einer Erhöhung der Budgets für die Netzwerksicherheit von Unternehmen führen. Ein Regierungsauftrag wie dieser ist in den Vereinigten Staaten bereits in Kraft.

Der Fokus der Firmensicherheit hat sich daher von den Infrastrukturen zu den Menschen verschoben, da die Sicherheit personenbezogener Daten in der Vergangenheit nicht immer angemessen berücksichtigt wurde.

Der Paradigmenwechsel, der zur Einführung der DSGVO geführt hat, basiert also auf der Notwendigkeit, präventive Sicherheitsmaßnahmen im Hinblick auf den Datenschutz von realen Personen zu ergreifen.

Neue Berufsfelder sind in diesem Zuge entstanden, wie zum Beispiel der des Datenschutzbeauftragten (DSB). Der DSB ist verantwortlich für das Reporting und die Beratung bezüglich der Datenschutz-verpflichtungen des Unternehmens. Er überwacht unter anderem die Einhaltung der Vorschriften und verantwortet die Zusammenarbeit mit den Kontrollbehörden.

Damit Unternehmen einen Aktionsplan zur Anpassung ihrer Praktiken an die DSGVO entwickeln und umzusetzen können, müssen die Cybersicherheitslösungen in den Organisationen in Übereinstimmung mit der neuen Regelung sein. Dabei sollten sie in erster Linie proaktive und nicht nur reaktive Sicherheit bieten.

3. Was ist die Datenschutz-Grundverordnung (DSGVO)?

Die EU-Regelung schützt die Grundrechte und -freiheiten von natürlichen Personen, insbesondere ihr Recht auf den Schutz persönlicher Daten, ob sie nun von privaten Organisationen oder öffentlichen Behörden verarbeitet werden. Das Auskunftsrecht, das Recht auf Berichtigung, das Widerrufsrecht, das Widerspruchsrecht und zwei neue Rechte werden anerkannt: das Recht auf Löschung, auch das „Recht auf Vergessenwerden“ genannt, und das Recht auf Datenübertragbarkeit. Die Spezifikationen für die Transparenzanforderungen werden genau beschrieben, ebenso die Einschränkungen bei der Verarbeitung von personenbezogenen Daten zum Zwecke der Archivierung im öffentlichen Interesse, für die wissenschaftliche und historische Forschung oder für statistische Zwecke.

Eine weitere neue Ergänzung ist der Bezug auf die Verarbeitung der Daten von Europäern durch Unternehmen, die in Europa und außerhalb der Europäischen Union niedergelassen sind und innerhalb der EU Aktivitäten ausführen, die die Verarbeitung von personenbezogenen Daten einschließen, auch wenn sie keine physische Präsenz im Hoheitsgebiet des Staatenblocks haben.

Diesem Zusatz ist die Verpflichtung hinzugefügt, dass öffentliche Organisationen in bestimmten Fällen einen „Datenschutzbeauftragten“ (DSB) bestimmen müssen, um die Einhaltung der Regelungen zu gewährleisten. Der Hauptunterschied zum IT-Security Manager ist, dass der DSB Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzen muss.

Diese Maßnahme betrifft fast alle privaten Unternehmen. Obwohl hier auch die Menge der verarbeiteten Daten eine Rolle spielt sowie die Anfälligkeit der Firma für Angriffe.

Außerdem schreibt die DSGVO die Verpflichtung fest, dass die Datenschutzbehörde über alle Sicherheitsvorfälle informiert werden muss, die in einem Unternehmen stattfanden. Durch die Befugnisse dieser Behörde kann sichergestellt werden, dass datenschutzrechtliche Vorfälle nach Bekanntwerden innerhalb von maximal 72 Stunden veröffentlich werden müssen.

4. Eckdaten zur DSGVO

1. Wen betrifft sie?

Die Verordnung betrifft jedes Unternehmen, das personenbezogene Daten von natürlichen Personen verarbeitet, die zur EU gehören, auch wenn sie sich physisch nicht in diesem Gebiet aufhalten.

Der Begriff natürliche Person bezieht sich nicht nur auf Kunden, sondern auch auf Kandidaten, ehemalige Klienten und Nutzer von Produkten und Dienstleistungen, die möglicherweise durch Dritte erworben wurden, sowie auf die Angestellten und Mitarbeiter eines Unternehmens.

2. Wie viel Zeit haben Unternehmen, um die Auflagen zu erfüllen?

Obwohl die Rechtsvorschrift durch das Europäische Parlament und den Rat der EU am 27. April 2016 gebilligt wurde und am 25. Mai 2016 in Kraft getreten ist, wird Sie erst ab dem 25. Mai 2018 Anwendung finden.

3. Was wird als personen-bezogene Daten angesehen und unterliegt damit der DSGVO?

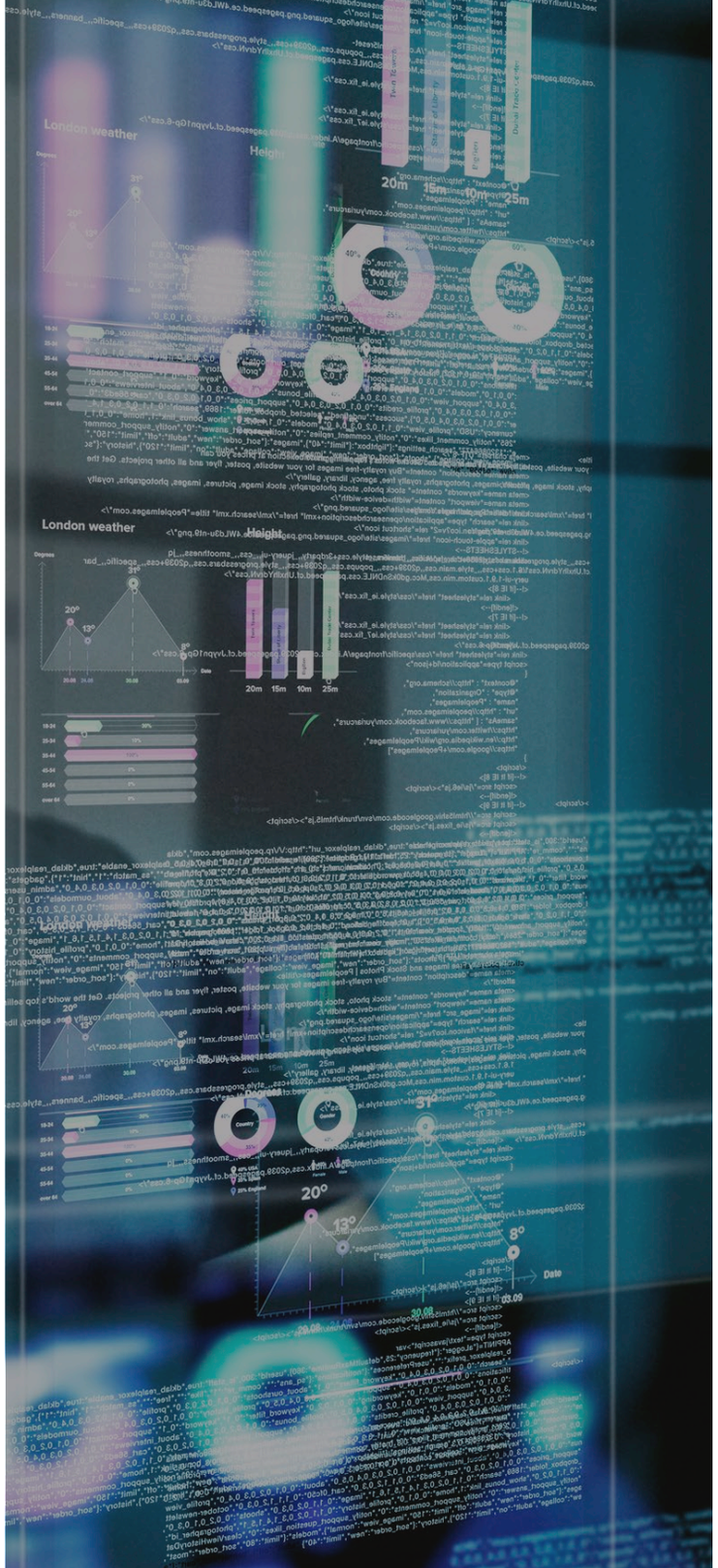
Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Die DSGVO betrifft die Verarbeitung personenbezogener Daten von natürlichen Personen, die sich in der EU niedergelassen haben. Beachten Sie, dass diese Verordnung jedoch nur für lebende Personen gilt.

Sie gilt für Unternehmen, **die personenbezogene Daten von natürlichen Personen in den EU-Mitgliedsstaaten** verarbeiten.

Sie findet **ab 25. Mai 2018** Anwendung.

Sie gilt für die Verarbeitung **personenbezogener Daten von natürlichen Personen innerhalb der EU.**



4. Was wird als sensible personenbezogene Daten angesehen?

Die Verordnung legt spezielle Kategorien von Daten fest, die als sensibel angesehen werden und besonderen Schutz erfordern.

Die Verordnung untersagt die Verarbeitung sensibler personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Auch die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist nicht erlaubt.

Das Verbot gilt nicht in folgenden Fällen: Die betroffene Person hat in die Verarbeitung der personenbezogenen Daten ausdrücklich eingewilligt. Die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person erforderlich. Die betroffene Person hat ihre Daten öffentlich gemacht. Die Verarbeitung der besagten Daten wird berechtigterweise von einer gemeinnützigen Organisation ausgeführt.

Einige Daten werden als sensibel angesehen und benötigen einen besonderen Schutz

5. Welche Konsequenzen hat eine Verletzung dieser Verordnung?

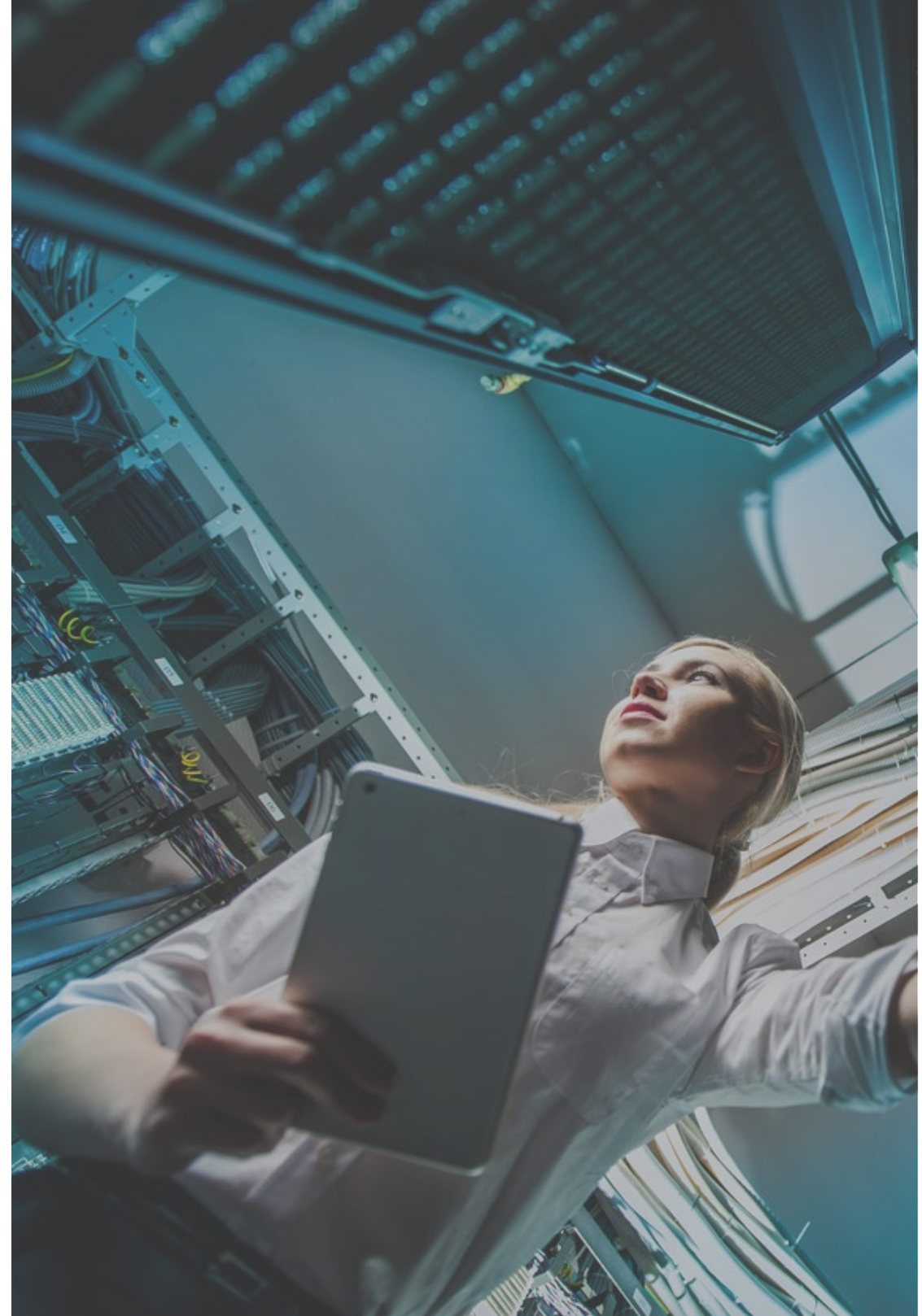
Bei Verstößen gegen die Bestimmungen der DSGVO werden Geldbußen von bis zu 20 Millionen EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher der Beträge höher ist. Sanktionen werden jedoch nicht die einzigen Konsequenzen der Nichteinhaltung sein, wenn die Verordnung 2018 Anwendung findet.

Es gibt Strafen von bis zu **20 Mio €** oder **4 % des gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres

5. Wichtige Rechte und Auflagen der DSGVO

Das Ziel der DSGVO ist es, den Schutz der Daten von EU-Bürgern zu stärken. Dazu müssen Unternehmen eine Reihe von Anforderungen erfüllen, die es natürlichen Personen ermöglichen, deren personenbezogenen Daten von Firmen gesammelt, gespeichert und verarbeitet werden, bestimmte Rechte in Anspruch zu nehmen.

In diesem Abschnitt tragen wir einige wesentliche Anforderungen zusammen, die Unternehmen einhalten müssen, sowie die wichtigsten Rechte von natürlichen Personen, die die neue Verordnung festschreibt. Dieses Wissen wird Ihnen dabei helfen, die Änderungen besser einschätzen zu können und somit die nächsten Schritte zu planen, die zur Umsetzung der DSGVO notwendig sind.



1. Meldepflicht über Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche diese unverzüglich und binnen 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde.

Die Meldung enthält folgenden Informationen:

- Eine Beschreibung der Datenverletzung und ihre Auswirkung
- Die ungefähre Zahl der betroffenen Personen und der betroffenen personenbezogenen Datensätze
- Den Namen und die Kontaktdaten des Datenschutzbeauftragten
- Eine Beschreibung der wahrscheinlichen Folgen der kompromittierten Daten
- Eine Beschreibung der ergriffenen oder geplanten Maßnahmen

2. Aufgaben des Datenschutzbeauftragten (DSB)

Ein Unternehmen muss einen Datenschutzbeauftragten bestimmen, wenn es eine öffentliche Organisation ist oder seine Haupttätigkeit die routinemäßige und systematische umfangreiche Verarbeitung von Daten ist, einschließlich personenbezogener Daten oder Daten, die mit früheren Verurteilungen oder Straftaten verbunden sind.

In der Verordnung ist der Begriff „umfangreich“ nicht eingehend definiert. Deshalb ist es für fast alle Unternehmen erforderlich, einen DSB zu benennen.

Die Funktionen des Datenschutzbeauftragten sind die folgenden:

- Unterrichtung und Beratung derjenigen Beschäftigten, die personenbezogene Daten verarbeiten, hinsichtlich ihrer Pflichten
- Überwachung der Einhaltung dieser Verordnung, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
- Beratungsarbeit im Zusammenhang mit den Folgen des Datenschutzes und Durchführungskontrolle
- Zusammenarbeit mit der Aufsichtsbehörde und Tätigkeit als Anlaufstelle für die Aufsichtsbehörde

3. Prinzip der Transparenz und Einwilligung

Das Prinzip der Transparenz erfordert, dass alle Informationen und Kommunikation bezüglich der Verarbeitung personenbezogener Daten eindeutig und gesetzmäßig sind sowie leicht zugänglich und verständlich.

Folgendes muss eindeutig kommuniziert werden:

- Dass personenbezogene Daten gesammelt, verwendet, abgerufen und verarbeitet werden. Insbesondere müssen dabei folgende Aspekte bezüglich der personenbezogenen Daten kommuniziert werden: der Zweck, die vorgesehenen Fristen, der/die Empfänger, die Logik, die in allen automatisierten Verarbeitungen impliziert ist, und (zumindest dort, wo Profile betroffen sind) die Folgen der Verarbeitung
- Die Risiken, Regeln, Schutzmaßnahmen und Rechte im Zusammenhang mit der Verarbeitung von personenbezogenen Daten
- Die Art und Weise, wie man seine Rechte im Hinblick auf die Verarbeitung personenbezogener Daten durchsetzen kann

4. Anreiz für die Pseudonymisierung

Das Hauptaugenmerk der DSGVO liegt auf den Daten mit Bezug auf eine identifizierbare natürliche Person. Deshalb betrifft die Verordnung nicht die Daten von nicht identifizierten oder identifizierbaren natürlichen Personen.

Aus diesem Grund schafft die DSGVO Anreize für Unternehmen, die Daten, die sie sammeln, zu pseudonymisieren. Die Pseudonymisierung ist die Trennung der Daten von den Kennzeichen, die eine direkte Identifizierung von natürlichen Personen erlauben. Folglich kann Pseudonymisierung die Risiken erheblich senken, die mit der Datenverarbeitung verbunden sind, bei gleichzeitiger Aufrechterhaltung ihres Nutzens. Obwohl die pseudonymisierten Daten nicht völlig von der Verordnung ausgenommen sind, verringert die DSGVO verschiedene Anforderungen für die Kontrolleure, die diese Technik nutzen.

5. Rechte in Bezug auf die Verarbeitung personenbezogener Daten

Unternehmen müssen der betroffenen Person die Mittel für die Ausübung ihrer Rechte bereitstellen. Dies beinhaltet:

1. **Das Recht,** den Zugriff auf ihre persönlichen Daten kostenfrei **zu verlangen** und zu erhalten.
2. **Das Recht,** personenbezogene Daten, die sie betreffen, **zu berichtigen und zu löschen.**
3. **Das Recht auf Vergessenwerden** oder mit anderen Worten, das Recht, dass ihre personenbezogenen Daten gelöscht und nicht weiter bearbeitet werden, wenn sie nicht länger für die Zwecke notwendig sind, für die sie erhoben oder verarbeitet wurden, oder wenn die betroffene Person ihre Einwilligung zur Verarbeitung widerrufen hat.
4. **Das Recht, nicht Gegenstand von Profiling zu sein.** Die betroffene Person hat das Recht, nicht Gegenstand einer Entscheidung zu sein, die ausschließlich auf einem automatisierten Profil basiert. Unter Profiling versteht man die Bearbeitung von Daten, die dabei hilft, bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren oder vorherzusagen.
5. **Das Recht auf Übertragbarkeit** von personenbezogenen Daten, welche das Unternehmen verpflichtet, der betroffenen Person die personenbezogenen Daten in einem gängigen Format zur Verfügung zu stellen und diese Daten an ein anderes Unternehmen zu übermitteln, wenn die betroffene Person dies wünscht.

6. Die Anwendung der DSGVO bei Unternehmen

Alle Unternehmen, die in den EU-Märkten agieren, sind verpflichtet, die Datenschutzpraktiken der DSGVO zu übernehmen.

Unternehmen, die ihre Praktiken nicht anpassen, werden spätestens im Schadensfall die nachfolgend aufgeführten Sanktionen zu tragen haben. Es sollte daher als oberste Priorität angesehen werden, die Umsetzung der DSGVO kurzfristig zu realisieren. Gleichzeitig hilft diese Verordnung dabei, größere Sichtbarkeit und Kontrolle über die eigenen Daten zu erlangen und ein damit zusammenhängendes höheres Schutzlevel zu etablieren.

1. Sanktionen und andere Folgen der Nichteinhaltung

Unternehmen, die die Verordnung nach dem 25. Mai 2018 nicht befolgen, werden möglicherweise mit folgenden Auswirkungen konfrontiert:

- **Direkte oder indirekte wirtschaftliche Konsequenzen**
  Diese könnten aus Sicherheitsvorfällen resultieren, sei es von außen oder durch die Mitarbeiter des Unternehmens.
- **Rufschädigung**
  Der Ruf Ihres Unternehmens könnte durch Sicherheitsvorfälle, die der Öffentlichkeit nicht ordnungsgemäß gemeldet wurden, Schaden nehmen.
- **Kundenverlust**
  Verlust aktueller oder potenzieller Kunden, wenn ein Unternehmen nicht nachweisen kann, dass es die Verordnung einhält.
- **Beschränkung oder Verbot der Datenverarbeitung**
  Diese Maßnahmen können nach Datenschutzüberprüfungen auferlegt werden und die Arbeitsabläufe eines Unternehmens stark beeinträchtigen.
- **Vorübergehende Einstellung der Dienstleistung**
  Dies könnte Ihre Kunden dazu veranlassen, die Zusammenarbeit zu kündigen und/oder rechtliche Schritte einzuleiten.
- **Entschädigungszahlungen**
  Betroffene Personen können im Falle von Rechtsverletzungen Regressforderungen geltend machen.
- **Bußgeldzahlungen**
  Für Regelverletzungen können Bußgelder von bis zu 20 Mio € oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres erhoben werden.

Durch Befolgen der Verordnung können Unternehmen die oben genannten Probleme vermeiden, das Vertrauen ihrer Kunden stärken und sich so einen Wettbewerbsvorteil verschaffen.

Anerkannter Zertifizierungsmechanismus

Die Gesetzgeber haben erkannt, dass für viele Unternehmen der Nachweis, dass sie die DSVGO befolgen, von Vorteil ist. Zu diesem Zweck wurden Datenschutzzertifizierungsmechanismen und -siegel eingeführt.

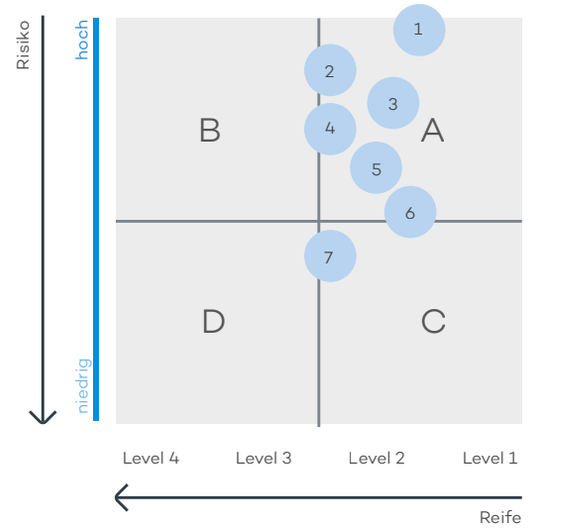
Die DSGVO spricht sogar von der Möglichkeit, ein gemeinsames europäisches Datenschutzsiegel zu entwickeln; und obwohl die DSGVO bisher nur wenige Einzelheiten dazu bekanntgibt, wird erwartet, dass dieser Mechanismus in den kommenden Monaten ausgearbeitet wird.

2. Aktionsplan für die DSGVO

Um ihre Geschäftspraktiken an die DSGVO anzupassen, müssen Unternehmen zunächst ihre aktuelle Position bei der Einhaltung der Verordnung bestimmen. Ein erster Schritt für Unternehmen ist dabei, dass sie die absolute Kontrolle über die Verarbeitung personenbezogener Daten erlangen. Folgende Fragen sollten die Unternehmen beantworten können:

- Welche personenbezogenen Daten werden verarbeitet, einschließlich ihrer Erhebung, Übermittlung und Speicherung?
- Wo befinden sich die Daten und wer hat Zugriff darauf, einschließlich Dritter?
- Wann und wo werden Daten übertragen, einschließlich Dritter und länderübergreifend?
- Welche Sicherheitsmaßnahmen werden im Laufe des Lebenszyklus der Daten ergriffen?
- Wie werden die Daten gespeichert, die es ermöglichen, andere Informationen zu identifizieren?
- Wie werden Datenidentifikation, -modifikation, -löschung und -übertragung der betroffenen Person auf Anfrage gewährt?
- Wie wird der Datenschutz kommuniziert und archiviert und auf welche Weise wird er für die Datenverarbeitung genutzt?

Indem sich Firmen der bestehenden Umsetzungslücken bewusst werden, unternehmen sie den ersten Schritt, um die Risiken ihrer Verarbeitungsmethoden personenbezogener Daten zu bestimmen und auf dieser Grundlage priorisierte Maßnahmenpläne zu entwickeln.



SCHLÜSSEL

Kreise

1. Third-Party-Management
2. Schulung und Bewusstsein
3. Risikomanagement
4. Richtlinien
5. Datenlecks
6. Kunden fair behandeln
7. Vorfallmanagement

Sektoren

A. Höheres Risiko Höhere Reife

B. Höheres Risiko Niedrigere Reife

C. Niedrigeres Risiko Höhere Reife

D. Niedrigeres Risiko Niedrigere Reife

Abbildung 1. Unternehmen stehen in den kommenden Monaten bei der Vorbereitung auf die DSGVO vielen Herausforderungen gegenüber. Der erste Schritt ist die Bestimmung des eigenen aktuellen Status.

7. Inwiefern sind Unternehmen bereits auf die DSGVO vorbereitet?

Eine Umfrage, die der amerikanische Computerhersteller Dell im September 2016 durchgeführt hat, ergab, dass **sowohl KMUs als auch große Unternehmen zu wenig über die neue Datenschutz Grundverordnung der EU wissen.** Befragt wurden insgesamt 821 Datenschutzverantwortliche in europäischen Großunternehmen und KMUs.

Auch heute, wenige Monate vor dem Inkrafttreten der neuen Verordnung, haben viele Unternehmen noch keinen konkreten Aktionsplan und wissen nicht genau, **wie sie sich** auf die Einführung der DSGVO **vorbereiten** sollen. Dabei könnte, wie oben erläutert, der Verstoß gegen die DSGVO beträchtliche Auswirkungen sowohl auf die **Datensicherheit** als auch auf das **Geschäft** haben.

Laut Dell-Studie sind daher 82 % der für die Datensicherheit verantwortlichen Experten über die Einhaltung der neuen Verordnung besorgt. Die Sorge ist am größten in Europa, vor allem in Deutschland und Schweden, und besonders bei **großen Unternehmen.**

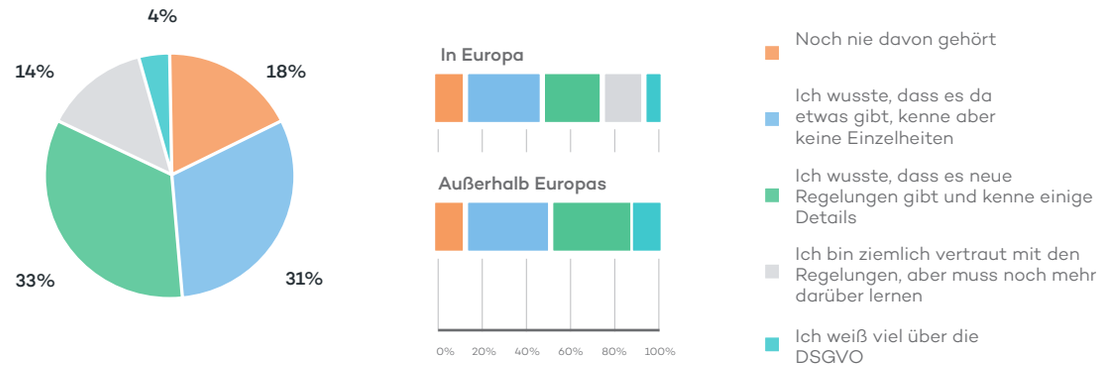


Abbildung 2. Wie würden Sie Ihr Wissen über die DSGVO beschreiben?

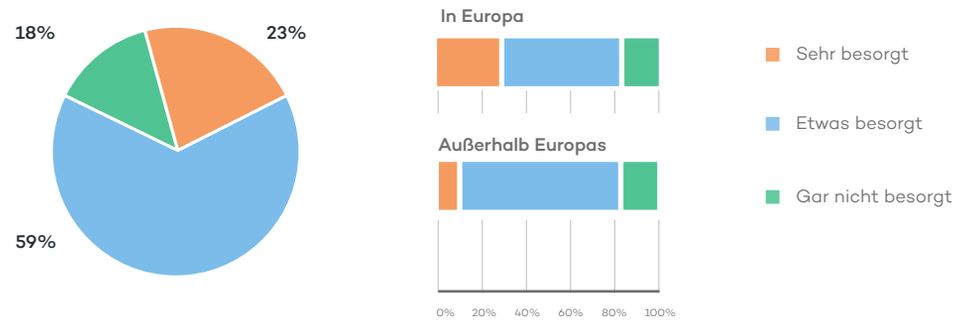


Abbildung 3. Wie besorgt sind Sie über die Einhaltung der DSGVO?

Der Studie zufolge sind die **Deutschen** am besten auf die DSGVO vorbereitet (4 %), während die Befragten in den **Benelux**-Ländern (Belgien, Niederlande und Luxemburg) von sich behaupten, **wenig oder gar nicht vorbereitet** zu sein.

Insgesamt **sagen** mehr als **80 % der Befragten, dass sie wenig oder gar nichts über die Inhalte der neuen DSVGO wissen,** und nur **3 % der IT-Experten sind darauf vorbereitet.**

Die Ergebnisse der Umfrage zeigen zudem, dass den Unternehmen zwar bewusst ist, dass eine Verletzung der DSGVO **Auswirkungen auf die Datensicherheit und ihr Geschäft** haben kann. Andererseits sind sich viele jedoch weder im Klaren darüber, in welchem Umfang sie Änderungen vornehmen müssen, noch wissen sie, welche Strafen bei Nichteinhaltung drohen.

Nur 23 % der Befragten gaben an, dass sie hinsichtlich ihres Umgangs mit der Datensicherheit große Veränderungen erwarten.

Mehr als 80 % der Studienteilnehmer **verfügen über sehr geringe Kenntnisse** über die neue Verordnung und wissen nicht, wie sie diese umsetzen sollen bzw. sind nicht vorbereitet. **Nur 3 % hatten zum Zeitpunkt der Umfrage bereits einen Plan für die Umsetzung.**

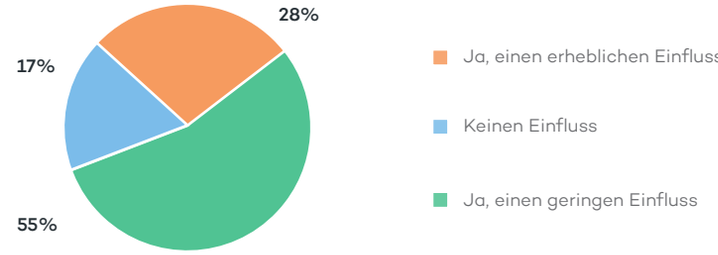


Abbildung 4. Wird die DSGVO Ihrer Meinung nach einen Einfluss auf die Herangehensweise an die Datensicherheit haben?

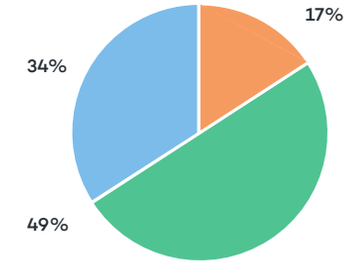


Abbildung 5. Wird die DSGVO Ihrer Meinung nach Auswirkungen auf Ihre Geschäftsergebnisse haben?

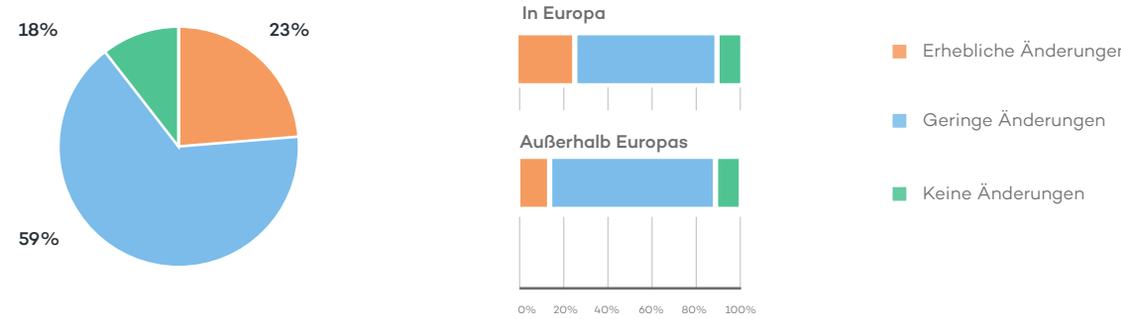


Abbildung 6. Was glauben Sie, wie viele der aktuellen Technologien und Praktiken werden sich als Folge der DSGVO ändern müssen?

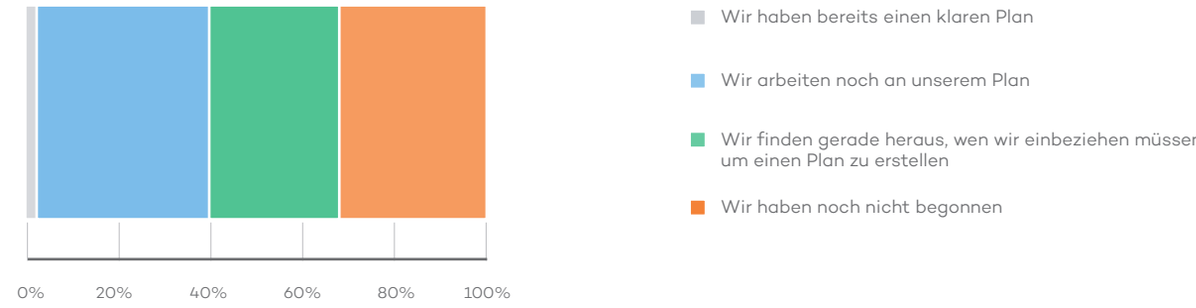


Abbildung 7. Hat Ihr Unternehmen einen Plan, um sich auf die DSGVO vorzubereiten?

8. Pandas Adaptive Defense hilft, die Anforderungen der DSGVO zu erfüllen

Wie in den vorangehenden Abschnitten gezeigt, gibt es einerseits eine Notwendigkeit, die Datensicherheitspraktiken und die bestehenden Technologien an die neue Verordnung anzupassen. Andererseits fehlt Unternehmen das detaillierte Wissen über die neuen Pflichten, die potenziellen Auswirkungen auf ihre Organisationen und die implizierten wirtschaftlichen Risiken.

Der notwendige Anpassungsprozess erfordert große Anstrengungen bei der Bewusstseinsbildung, Schulung, Analyse und Umsetzung der neuen Datenschutzpraktiken. Schlimmer sind jedoch die Konsequenzen, wenn die notwendigen Schritte zur Umsetzung der DSGVO ausbleiben. Dann drohen direkte und indirekte wirtschaftliche Sanktionen, Rufschädigung, Verlust von Kunden, Einschränkungen der Betriebsabläufe, Kundenbeschwerden und Schadenersatzforderungen.

Panda Adaptive Defense minimiert diese Risiken und hilft seinen Kunden, die DSGVO einzuhalten.

Die beiden Schlüsselfaktoren, die für die Einhaltung der DSGVO eine entscheidende Rolle spielen, sind:

1) Kontrolle über die Daten, die in den verschiedenen Abteilungen (HR, Marketing usw.) auf Computern und Servern gesammelt, gespeichert und verarbeitet werden.

2) Einführung der Maßnahmen, die erforderlich sind, um sie vor Angreifern zu schützen.

Der notwendige Anpassungsprozess erfordert von den Unternehmen große Anstrengungen bei der Bewusstseinsbildung, Schulung, Analyse und Umsetzung der neuen Datenschutzpraktiken und -Technologien.

panda

Adaptive Defense 360

Von diesen Schlüsselfaktoren ausgehend können drei Schwerpunkte ausgearbeitet werden, um die Sicherheit der Daten zu gewährleisten:

1. Vorbereitung

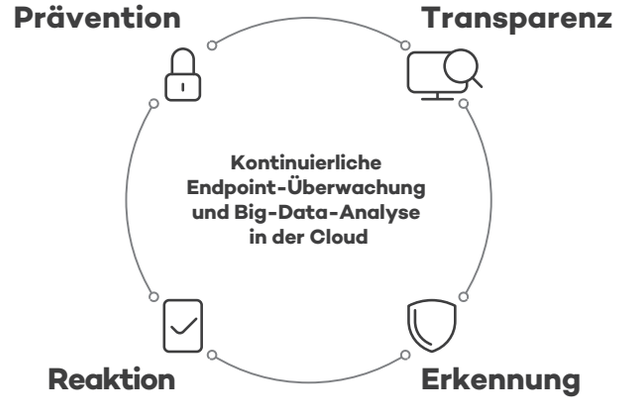
Die Verfügbarkeit eines Systems, welches jederzeit gründliche forensische Untersuchungen durchführen kann, ist der Schlüssel für die schnellstmögliche Neutralisierung eines Angriffes.

Adaptive Defense beinhaltet ein internes Auditsystem, um den Sicherheitsstatus der IT-Infrastruktur jederzeit zu verifizieren. Bei der Umsetzung des Aktionsplanes für die Einhaltung der DSGVO erweist es sich als unschätzbares Tool.

2. Schutz

Effektive Sicherheitslösungen müssen fortschrittliche Technologie mit menschlicher und computergesteuerter Intelligenz kombinieren. Mit anderen Worten, moderne IT-Sicherheit benötigt maschinelles Lernen mit Experten als Supervisor. Damit eine Sicherheitslösung in jeder Situation funktioniert, muss sie eine Kombination aus Prävention, Erkennung, Transparenz und Intelligenz bieten. Nur so können Cyberattacken jeglicher Art zuverlässig gestoppt und verhindert werden.

Adaptive Defense und Adaptive Defense 360 decken folgende Bereiche ab, die notwendig sind, um die Schutzanforderungen eines Unternehmens, einschließlich der der DSGVO, zu erfüllen:



- **Kontinuierliche Überwachung** durch Aufzeichnung und Überwachung aller Aktivitäten von laufenden Prozessen, um nicht vertrauenswürdige Software an ihrer Ausführung zu hindern, fortschrittliche Bedrohungen in Echtzeit zu erkennen, in Sekunden zu reagieren und sofortige Wiederherstellungsmaßnahmen zu ergreifen.
- **Erkennung von nicht vertrauenswürdigen Dateien.** Dies ermöglicht Ihrem Unternehmen, die Eintrittsvektoren für ausgeführte Angriffe zu reduzieren. Die eingesetzte Sicherheitslösung sollte alle auf Ihren Geräten laufenden Anwendungen als vertrauenswürdig oder schädlich klassifizieren können.
- **Intelligente Gefahrenerkennung.** Eine Gefahr ist immer schneller als jedes Gerät, das Sie schützen wollen. Also sollten Sie als Anwender nicht derjenige sein, der die Rückmeldungen überwachen muss. Effektive Sicherheitslösungen müssen in der Lage sein, autonom und automatisch zu arbeiten, und sich an die individuelle Betriebsumgebung Ihres Unternehmens anzupassen.
- **Schnelle und automatisierte Reaktion.** Unternehmen werden mit einer Flut von Vorfällen und Warnmeldungen, die von ihren Systemen generiert werden, überschüttet. Doch wenn ein Cyberkrimineller erst einmal das System infiltriert hat, kann der Datendiebstahl in Sekundenschnelle erfolgen. Deshalb muss die ausgewählte Sicherheitslösung in der Lage sein, eine beginnende Attacke schnell zu identifizieren, Maßnahmen zu ergreifen, um Schaden zu vermeiden und die Arbeitslast für die Systeme zu senken. Auf diese Weise können Sie Kosten reduzieren und Aufgaben automatisieren, für deren Ausführung man zuvor Tage benötigte.

3. Transparenz und Kontrolle

Daten sind etwas Lebendiges. Sie wachsen, verändern und bewegen sich. Sie so zu verwalten, dass sie mit der neuen DSGVO in Einklang stehen, ist nur der Anfang. Wenn alles vorhanden ist, um dies effektiv zu tun, bleibt die Frage, wie man die Daten konstant kontrolliert und wie man jegliche Anomalien erkennt, die auftreten könnten.

Das **Advanced Reporting Tool (ART),** das optionale Modul von Adaptive Defense, ist ein intelligentes Sicherheitstool, das automatisch Reports über alle Endpoint-Aktivitäten erstellt. Es bietet Unternehmen die Möglichkeit, sowohl ungewöhnliches Verhalten und extern gesteuerte Angriffe als auch internes Fehlverhalten schnell und einfach zu erkennen.

Dabei speichert das Advanced Reporting Tool alle Informationen, die es über die auf den Endpoints laufenden Prozesse generiert, und gleicht diese automatisch miteinander ab. Aus diesen Daten leitet die Plattform dann wiederum automatisch Sicherheitsinformationen ab und bietet dem Administrator Tools an, mit deren Hilfe er ungewöhnliches Verhalten oder Probleme identifizieren kann.

Mithilfe des Advanced Reporting Tool (ART) können IT-Administratoren...

- ...gezielt nach relevanten Informationen suchen. Das erhöht die Effizienz der IT-Abteilung, da Sicherheitsrisiken oder Unstimmigkeiten in der Firmeninfrastruktur schnell aufgedeckt werden.
- ...Probleme lokalisieren, indem Verhaltensmuster von Ressourcen und Anwendern analysiert und ihre Auswirkungen auf das Unternehmen identifiziert werden.
- ...Echtzeit-Warnungen über alle Ereignisse, die möglicherweise eine Datenverletzung darstellen, erhalten.
- ... umfassende, individuell konfigurierbare Reports erstellen. Die Reports zeigen den Status der wichtigsten Sicherheitsindikatoren und wie diese sich entwickeln.

Wenn die IT-Sicherheitsabteilung eines Unternehmens ein **SIEM** (Security Information Event Management) nutzt, erleichtert die offene Struktur der Adaptive Defense Plattform die Echtzeit-Integration der Aktivitätsdaten, die auf den Endpoints überwacht werden, in die Logdateien, die im SIEM verwaltet werden.

Dies ermöglicht den Sicherheitsteams des Unternehmens oder des externen Security Operations Centers (SOC):

- **Ihren ganzheitlichen Sicherheitsansatz zu erweitern**, der nicht nur das Perimeter-Netzwerk umfasst, sondern auch die Endpoints.
- **Einen privilegierten Überblick über Angriffe und ihre Gesamtauswirkung zu erhalten,** was die Gelegenheit für eine gründliche forensische Analyse bietet.


TOP10 accessed Files from endpoints

MACHINE	CHILDPATH	COUNT	%
BIOIGIL	SYSTEMDRIVE | \Users\igil\AppData\Local\Google\Chrome\User Data\Default\Login Data	21	0,055%
BIOIGIL	DESKTOPDIRECTORY | \CAU_gestinven_II.mdb	20	0,053%
BIOMARTINEZ	APPDATA | \Mozilla\Firefox\Profiles\u71q2nip1.default\places.sqlite	19	0,050%
BIOIGIL	INTERNET_CACHE | \Content.Outlook\1ZE6EX4F\Visual Studio 2013 and MSDN Licensing Whitepaper - January 2015 (ENG).pdf	19	0,050%
BIOIGIL	INTERNET_CACHE | \IE\609EM715\Office_365_Addons_Customer_Overview.pdf	19	0,050%
BIOIGIL	RECYCLED | \S-1-5-21-20473081-1892483688-328166375-9156\$I3ARFTK.pptx	19	0,050%
BIORDELACASA	DESKTOPDIRECTORY | \nerdos_arcolardo.pdf	18	0,048%
BIOCSAUCIO	DESKTOPDIRECTORY | \20160302_secure.pandasoftware.com.pfx	18	0,048%
BIOJCORDERI	PROFILE | \AppData\LocalLow\LastPass\sites.dat	18	0,048%
BIOIGIL	TEMP | \Temp5835678641E4E54582971667#D9DFCE\1ulppt.ppt	18	0,048%

Abbildung 8. Beispiele für die Sichtbarkeit, die ART bietet

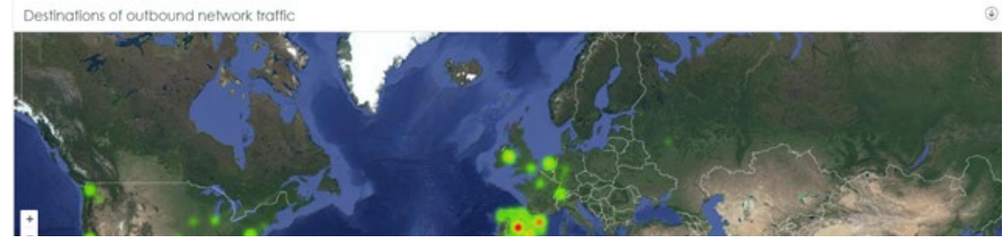


Abbildung 9. Geolokalisierung des ausgehenden Datenverkehrs einer Firma

- **Das Maximum herauszuholen** aus den gesammelten Informationen, um die Situation ihrer IT-Infrastruktur besser zu kennen und Verbesserungsstrategien zu implementieren.
- **Ihre SIEM-Daten anzureichern**, indem diese mit zusätzlichen Daten abgeglichen werden, die von Endpoints stammen, was die Qualität der Corporate Intelligence für Ihre Systeme erhöht.

Panda Adaptive Defense gewährleistet die Sicherheit des Unternehmens und seiner Daten. Die Firmen, die ihr Vertrauen in Adaptive Defense gesetzt haben, sind bereits auf dem richtigen Weg zur Einhaltung der DSGVO. Folgende Leistungen bietet Adaptive Defense diesen Unternehmen hinsichtlich der neuen Verordnung:

- Schutz der personenbezogenen Daten, die in den Systemen eines Unternehmens verarbeitet werden, zum Beispiel durch das **Stoppen der Ausführung jedes nicht vertrauenswürdigen Prozesses.**
- **Risikominimierung** und die Lieferung von **Indikatoren für Schlüsselaktivitäten** sowie den **Endpoint-Status,** was dabei hilft, Sicherheitsprotokolle einzuführen und Administratoren stets über gefährdete Geräte, anomale interne und externe Netzwerkaktivitäten usw. zu informieren.
- **Tools**, um die Anforderung zu erfüllen, **die Behörden über einen Sicherheitsvorfall innerhalb der ersten 72 Stunden nach seinem Auftreten zu informieren.** Dank der forensischen Analyse-Tools, Warnmeldungen, Transparenz und der totalen Kontrolle, die Adaptive Defense/Adaptive Defense 360 bietet, wird Ihr Unternehmen immer mit den entsprechenden Ressourcen ausgestattet sein, um schnell einen Report vorzulegen und einen Aktionsplan zu entwickeln, um zukünftige Störfälle zu verhindern.
- **Kontrollmechanismen und Datenmanagement für den DSB,** der in Echtzeit nicht nur über die Sicherheitsvorfälle informiert wird, sondern auch darüber, ob diese Vorfälle kompromittierte personenbezogene Datendateien einschließen oder nicht. Sowohl das ART, über Echtzeit-Warnungen, Kontrollpanels und Berichte, als auch die SIEM-Benachrichtigungssysteme des Unternehmens werden den DSB über anomale Aktivitäten benachrichtigen, die mit dem Zugriff auf personenbezogene Datendateien einhergehen.

9. FAQs zur DSGVO

1. Wer sind die hauptsächlichen Organisationen und Vertreter, die von der DSGVO betroffen sind?

Die Europäische Datenschutzkommission
Die Kommission besteht aus einer Kontrollinstanz aus jedem der 28 Mitgliedsstaaten und dem Europäischen Datenschutzbeauftragten. Die Rolle der Kommission wird darin bestehen, zu überprüfen, was funktioniert und was nicht, und außerdem zu beraten und zu unterstützen.

Die Datenschutzkontrollbehörde
Unabhängige Behörde, die von einem Mitgliedsstaat gegründet wurde, um die lokalen Rechtsvorschriften durchzusetzen.

Prozessverantwortlicher
Natürliche oder juristische Person, Behörde, Dienst oder andere Gesellschaft, die im Namen des Kontrolleurs personenbezogene Daten verarbeitet. Der Prozessverantwortliche bestimmt weder den Zweck noch die Mittel zur Verarbeitung. Er verarbeitet die Daten nur, wie vom Kontrolleur gewünscht.

Beispiel: Ausgelagertes Lohnbuchhaltungsunternehmen oder Cloud- Provider, wie zum Beispiel Microsoft Azure, wo Daten gesammelt, gespeichert und verarbeitet werden.

Wenn ein Anbieter in Übereinstimmung mit den Anforderungen agiert, ist dieser ein Datenverantwortlicher. Nach der alten Richtlinie würde eine Geldstrafe nur im Falle der Nichtbeachtung des Kontrolleurs auferlegt werden. Nach der neuen Richtlinie ist der Prozessverantwortliche auch für die Erfüllung seiner eigenen Verpflichtungen verantwortlich, wie zum Beispiel angemessene Sicherheitsmaßnahmen zu haben.

Kontrolleur oder Verarbeiter
Die Person oder Abteilung, die dafür verantwortlich ist zu bestimmen, welche personenbezogenen Daten das Unternehmen benötigt und zu welchem Zweck. Ein einfaches Beispiel: Eine Webseite fragt nach Ihrem Namen und Ihrer Adresse, zwecks Versand einer Bestellung. Die Firma, die die Informationen abfragt und festlegt, zu welchem Zweck sie diese benutzen wird, ist für die Daten verantwortlich.

Der Kontrolleur muss nicht nur die Verordnung einhalten, er muss die Einhaltung auch nachweisen. Das ist einer der Hauptunterschiede zwischen dieser Verordnung und bisherigen. Der Kontrolleur muss in der Lage sein, die Einhaltung jederzeit nachzuweisen, indem er den Aufforderungen der Kontrollbehörde oder der interessierten Partei Folge leistet.

2. Was wird mit den Datenschutzgesetzen der Mitgliedsstaaten passieren?

Die Verordnung setzt sie nicht außer Kraft, noch können sie aufgehoben werden. Die Verordnung bewirkt den normgebenden Ersatz der Gesetze der Mitgliedsstaaten bei allem, was im Widerspruch zum Europäischen Regelwerk steht. Doch diese Gesetze werden in Kraft bleiben, bis sie vollständig aufgehoben oder an die DSGVO angepasst werden können.

Infolgedessen wird es notwendig sein, sowohl die DSGVO als auch das Gesetz des Mitgliedsstaates zu berücksichtigen. Wenn es einen Widerspruch zwischen dem einen und dem anderen gibt, dann findet die DSGVO Anwendung anstatt des Gesetzes des Mitgliedsstaates.

3. Sollten Unternehmen ihre Datenschutzerklärungen überarbeiten?

Die kurze Antwort: ja. In den Informationen, die interessierten Parteien zur Verfügung gestellt werden, sorgt die Verordnung für die Einbeziehung von Sachverhalten, die bis dato nicht zwingend notwendig waren. Beispielsweise wird es notwendig sein, die rechtliche Grundlage für die Verarbeitung von Daten zu erklären, ihre Aufbewahrungsfrist festzulegen und die interessierten Parteien darüber zu informieren, dass sie ihre Beschwerden an die Datenschutzbehörden richten können, wenn sie glauben, dass es ein Problem gibt mit der Art und Weise, wie ihre Daten behandelt werden. Es ist wichtig zu bedenken, dass die Verordnung ausdrücklich verlangt, dass die bereitgestellten Informationen leicht zu verstehen sind und in klarer und prägnanter Sprache dargestellt werden.

4. Ändert sich die Art und Weise, wie eine Einwilligung einzuholen ist?

Eine der wesentlichen Grundlagen für die Verarbeitung von personenbezogenen Daten ist die Einwilligung. Die Verordnung verlangt, dass die Einwilligung im Allgemeinen freiwillig, auf einer informierten Grundlage, konkret und unmissverständlich erfolgen muss. Um prüfen zu können, ob die Einwilligung unmissverständlich ist, verlangt die Verordnung, dass es eine Erklärung auf Seiten der interessierten Parteien gibt oder ein positives Anzeichen, dass die interessierte Partei ihre Zustimmung gegeben hat. Eine Einwilligung kann sich nicht aus dem Schweigen oder der Untätigkeit von Klienten oder anderen natürlichen Personen ergeben.

Unternehmen sollten überprüfen, wie die Einwilligung eingeholt und aufgezeichnet wurde.

Es muss berücksichtigt werden, dass die Einwilligung nachweisbar sein muss und dass diejenigen, die personenbezogene Daten sammeln, beweisen können, dass die betroffene Person ihnen ihr Einverständnis gegeben hat. Deshalb ist es wichtig, die Systeme zu überprüfen, die die Einwilligungen aufzeichnen, sodass diese durch ein Audit verifiziert werden können.

5. Darf ich die Verantwortlichkeiten des DSB auslagern oder aufteilen?

Unternehmen mit begrenztem Budget dürfen DSB-Aufgaben auslagern oder teilen. In Deutschland müssen Firmen mit mehr als neun Mitarbeitern laut Bundesdatenschutzgesetz einen DSB bestimmen. Jedoch ist es allgemein üblich, die Aufgabe an spezialisierte Datenfirmen oder Anwaltskanzleien auszulagern.

Die Verordnung legt fest, dass eine Unternehmensgruppe einen einzigen DSB bestimmen darf, solange dieser von jeder Niederlassung aus leicht zu erreichen ist. Sollten Sie beschließen, Ihren DSB auszugliedern, wäre es notwendig, eine Dienstleistungsvereinbarung (DLV) zu treffen, um sicherzustellen, dass Sie die DSGVO einhalten. Die Einhaltung wird nicht nur dadurch erreicht, dass man einen DSB hat. Es muss ein DSB sein, der auf die verschiedenen Anfragen der interessierten Parteien jederzeit reagieren kann.

6. Wann, wie und wem melde ich einen Sicherheitsvorfall?

Wann? Ein Sicherheitsvorfall sollte immer gemeldet werden, wenn personenbezogene Daten natürlicher Personen davon betroffen sind, wenn der Vorfall zu Verlust oder Diebstahl der Daten führt oder wenn einfach auf diese zugegriffen wurde.

Wenn der Vorfall nicht umgehend gemeldet wird, kann dies zu Geldstrafen von bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes führen.

Wem? Es ist wichtig, zu beachten, dass es zwei verschiedene Schwellenwerte gibt: einen für die Benachrichtigung der Kunden oder der allgemeinen Öffentlichkeit und einen für die Alarmierung der Datenschutzbehörde.

- Wenn die personenbezogenen Daten, auf die zugegriffen wurde, Identifizierungszeichen enthalten, zum Beispiel E-Mail-Adressen, Online-Konto-ID oder IP, ist es erforderlich, die betroffenen natürlichen Personen darüber zu informieren.
- Wenn die Informationen Finanzdaten enthalten – Kontonummern oder andere Finanzkennzeichen – dann ist es wahrscheinlich, dass er dem Einzelnen schadet und die Datenschutzbehörde muss informiert werden.

Wie? Neben der Beschreibung der Art des Vorfalls sollte die Meldung die Art der Daten, die Anzahl der Individuen und der gefährdeten Datensätze enthalten. Das Unternehmen sollte die möglichen Konsequenzen der Nichteinhaltung beschreiben sowie alle Maßnahmen, die zur Schadensminderung ergriffen werden müssen.

Wann läuft die Frist ab? Die Benachrichtigung der Datenschutzbehörde muss innerhalb von 72 Stunden nach dem Vorfall erfolgen.

Wie kann ich mich darauf vorbereiten? Sie sollten sicherstellen, dass Sie ein internes Meldeverfahren haben und dass Sie über alle Einzelheiten des Vorfalls verfügen, insbesondere wenn auf personenbezogene Daten zugegriffen wurde. Denken Sie daran, dass Sie Unterlagen einreichen müssen über die Abhilfemaßnahmen, die ausgeführt wurden. Dazu benötigen Sie

Informationen über den Eintrittsweg des Angreifers, das Setup der angegriffenen Workstations und ihre Schwachstellen, die betroffenen Systeme usw. Dies wird es leichter machen, Entscheidungen darüber zu treffen, ob die Öffentlichkeit und die Datenschutzbehörde informiert werden müssen. Angesichts der kurzen Meldefristen für einen Vorfall ist es wichtig, eine stabile Angriffserkennung, eine forensische Analyse, Echtzeitwarnungen sowie ausführliche Berichte zu haben, die analysiert und der Öffentlichkeit und der Datenschutzbehörde präsentiert werden können.

Panda Adaptive Defense ist der beste Verbündete eines Unternehmens im Anpassungsprozess an die DSGVO, denn es bietet:

- Schutz der personenbezogenen Daten, die in den Systemen des Unternehmens verarbeitet werden
- Reduziertes Risiko, Opfer eines Angriffs zu werden
- Tools, um die Anforderungen an die Meldung von Sicherheitsvorfällen innerhalb der ersten 72 Stunden zu erfüllen
- Kontrollmechanismen und Datenmanagement für den DSB, die Benachrichtigungen in Echtzeit bieten, nicht nur über Sicherheitsvorfälle, sondern auch über Vorfälle, bei denen möglicherweise Dateien gefährdet sind, die personenbezogene Daten enthalten

7. Sollten Unternehmen sofort damit beginnen, die in der Verordnung vorgesehenen Maßnahmen durchzuführen?

Nicht unbedingt. Die Verordnung ist in Kraft, wird aber vor dem 25. Mai 2018 keine Anwendung finden.

Es ist jedoch sinnvoll sein, bereits jetzt mit der Bestandaufnahmen sowie der Implementierung von einigen der absehbaren Maßnahmen zu beginnen:

- Führen Sie Risikoanalysen Ihrer Datensysteme durch und stellen Sie fest, wie die Daten verarbeitet werden.
- Führen Sie die Dokumentation der Datenverarbeitung ein.
- Implementieren Sie Folgenabschätzungen oder andere absehbare Maßnahmen.
- Entwickeln und implementieren Sie Prozeduren für die adäquate Benachrichtigung von Behörden oder interessierten Parteien über alle Sicherheitsvorfälle, die sich ereignen könnten.

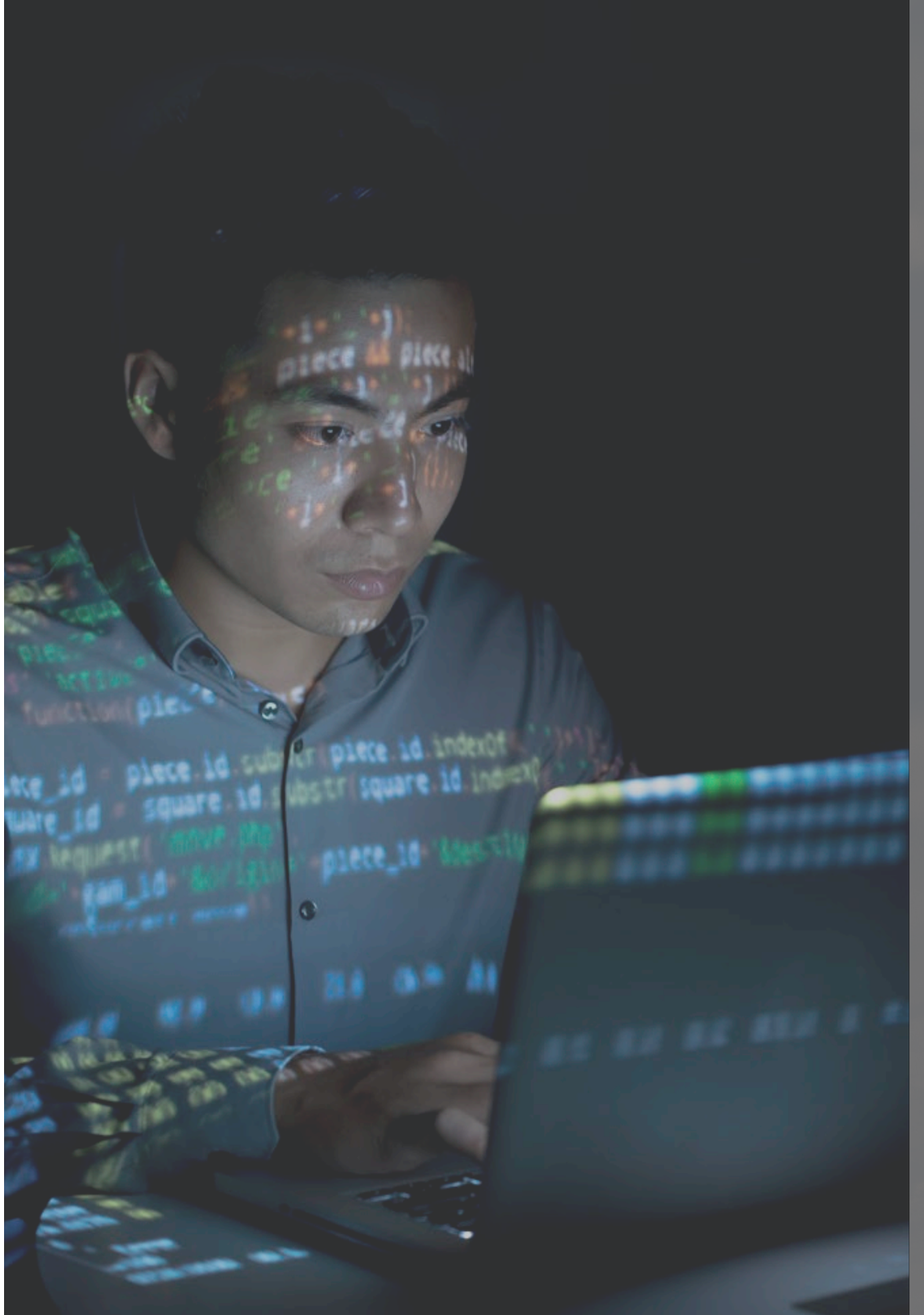
Panda Adaptive Defense sichert den Schutz des Unternehmens und seiner Daten und hilft bei deren Verwaltung. Firmen, die sich auf Adaptive Defense verlassen, sind schon jetzt auf einem guten Weg zur Einhaltung der DSGVO.

10. Über Panda Security

Dieser Bericht nutzt Daten, die von Panda Securitys multidisziplinärem Team gesammelt wurden. Dies ist ein Expertennetzwerk, das 1990 gegründet wurde und dessen Mission es ist, die Komplexität der IT-Security zu vereinfachen, indem es ständig neue und bessere Lösungen zum Schutz seiner Kunden entwickelt.

Wir teilen offen das Wissen unserer Fachexperten des PandaLabs, dem Labor, das Bedrohungen analysiert und in Echtzeit neutralisiert. Wir sind sowohl Entwickler, die sich auf moderne Cybersicherheit spezialisiert haben, als auch Produkt- und Marketingexperten.

Wir erfinden Cybersicherheit neu und machen sie weltweit zugänglich.



Weitere Informationen unter:

pandasecurity.com/germany/enterprise/solutions/adaptive-defense-360/

Rufen Sie uns an:

030-62985786

Kontaktieren Sie uns per E-Mail:

info@pbj.de

PBJ COMPUTER

panda | BUSINESS PARTNER

Adaptive Defense 360

Uneingeschränkte Transparenz, absolute Kontrolle

PBJ COMPUTER

panda | BUSINESS PARTNER

Krampnitzer Weg 96
14089 Berlin
Telefon 030-62985786
Fax 030-62985788
info@pbj.de
https://www.pbj.de