Acronis

HÄUFIG GESTELLTE FRAGEN ZUR GDPR (EU-DSGVO)

FAQs (Häufig gestellte Fragen)

F: Was ist die GDPR?

A: Die Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) – auch bekannt unter der nachfolgend verwendeten Abkürzung GDPR (General Data Protection Regulation) – ist eine neues gesetzliches Regelwerk, welches den Schutz von personenbezogenen Daten von in der EU ansässigen Personen verbessert. Sie ersetzt ein bisheriges Sammelsurium von nationalen Datenschutzgesetzen durch ein einziges Regelwerk, welches von jedem EU-Mitgliedstaat direkt durchgesetzt wird.

F: Wann tritt die GDPR in Kraft?

A: Am 25. Mai 2018.

F: Gilt die GDPR nur für Unternehmen mit Sitz in der EU?

A: Die Antwort auf diese häufige Fehlannahme lautet „Nein“. Denn jedes Unternehmen, welches Kunden in der EU hat und personenbezogene Daten erfasst oder anderweitig verarbeitet, ist zur Einhaltung der GDPR verpflichtet.

F: Was wird im Rahmen der GDPR unter „personenbezogenen Daten“ verstanden?

A: Mit personenbezogene Daten sind alle Informationen gemeint, die verwendet werden können, um eine Person zu identifizieren. Die neue Definition geht weit über die klassische hinaus, was unter Informationen zur Identifizierung von Personen zu verstehen ist. Zur neuen Definition gehören neben dem Namen oder der E-Mail-Adresse der betroffenen Person daher auch Daten wie Social Media-Beiträge, physische, physiologische oder genetische Informationen, medizinische Informationen, Standort, Bankverbindungen, IP-Adressen, Cookies oder kulturelle Identität.

F: Was genau regelt die GDPR?

A: Die GDPR regelt die Erfassung, Speicherung, Übermittlung und/oder Nutzung – zusammenfassend als Verarbeitung bezeichnet – aller personenbezogenen Daten, die EU-Bürgern gehören. Jedes Unternehmen, das personenbezogene Daten von EU-Bürgern verarbeitet (wie etwa die Verfolgung von Standorten oder Aktivitäten mithilfe von Browser-Cookies), fällt unter den Geltungsbereich des Gesetzes. Und das auch, wenn sich der physische Standort des Unternehmens nicht auf europäischem Boden befindet.

Das Regelwerk unterscheidet bezüglich der Handhabung der personenbezogenen Daten zwischen „Verantwortlichen“ (englisch „Controller“) und „Auftragsverarbeitern“ (englisch „Processor“). Das Unternehmen, das bestimmt, wie und warum die personenbezogenen Daten zu handhaben sind, ist der Verantwortliche. Jede Drittpartei (z.B. ein Cloud Storage Service Provider), die ein Verantwortlicher zur Verarbeitung ihrer personenbezogenen Daten engagiert, ist ein Auftragsverarbeiter.

F: Welche Auswirkungen hat die GDPR auf personenbezogene Datenschutzrechte?

A: Die GDPR verbessert die Datenschutzrechte von EU-Bürgern erheblich und verpflichtet alle Unternehmen, Institutionen oder Einzelpersonen, die personenbezogene Daten verarbeiten, diese Rechte zu schützen. Die Auftragsverarbeiter von personenbezogenen Daten müssen unter anderem folgende Anforderungen erfüllen:

- **Rechte betroffener Personen:** EU-Bürger haben dank GDPR mehr Kontrolle über ihre personenbezogenen Daten. Dazu gehört auch das Recht, von einem Auftragsverarbeiter Kopien oder Fehlerkorrekturen der eigenen personenbezogenen Daten zu verlangen oder dass personenbezogene Daten auf Anfrage der betroffenen Person vollständig gelöscht werden.
- **Nachweis der Konformität:** Auftragsverarbeiter müssen angemessene Datenschutzrichtlinien und -verfahren implementieren sowie detaillierte Aufzeichnungen über ihre Datenverarbeitungsaktivitäten aufbewahren.
- **Benachrichtigungen über Sicherheitsverletzungen:** Auftragsverarbeiter müssen Datenschutzverstöße nicht nur den jeweiligen lokalen Aufsichtsbehören melden, sondern schwere Verstöße auch direkt an die betroffenen Personen.
- **Geldbußen bei Vorschriftsverstößen:** Die GDPR-Regulierungsbehörden können – in Abhängigkeit von der Schwere des Verstoßes und dem verursachten Schaden – hohe Bußgelder gegen Unternehmen verhängen, die die Verordnung nicht einhalten.

F: Verlangt die GDPR, dass personenbezogene Daten innerhalb der EU verbleiben?

A: Nicht unbedingt. Jedoch kann die GDPR-konforme Übermittlung personenbezogener Daten zu Standorten außerhalb der EU („grenzüberschreitende Datenübermittlung“ genannt) kompliziert sein. Denn dabei müssen einige Regeln beachtet werden: Erstens sind Datenübermittlungen grundsätzlich in solche Empfängerländer erlaubt, die auf der EU-Liste von Bestimmungsländern mit „angemessener“ Sicherheit stehen. Damit sind Länder gemeint, deren Datenschutzbestimmungen die EU-Standards erfüllen. In einigen Fällen kann es sein, dass nicht das komplette Land, sondern nur einzelne Gebiete (z.B. Bundesstaaten) als angemessen eingestuft werden. Anfang 2018 gehörten zur Liste der zulässigen Länder: alle EU-Länder, drei Nicht-EU-Länder, die zum Europäischen Wirtschaftsraum gehören (Island, Liechtenstein, Norwegen) sowie einige weitere Länder und Gebiete (Andorra, Argentinien, Kanada, Färöer-Inseln, Guernsey, Isle of Man, Israel, Jersey, Neuseeland, Schweiz, Uruguay).

Datentransfers sind auch zu Standorten erlaubt, die den EU-Standard der sogenannten „verbindlichen internen Datenschutzvorschriften“ (oft auch BCRs genannt, für Binding Corporate Rules) erfüllen. Bei Einhaltung dieser Vorschriften dürfen bestimmte juristische Personen innerhalb einer Organisation (unter Umständen auch Gruppen von unabhängigen Unternehmen, die eine gemeinsame wirtschaftliche Tätigkeit ausüben), personenbezogene Daten übermitteln. Um sich zu qualifizieren, müssen die bestimmenden BCRs von der zuständigen Aufsichtsbehörde genehmigt werden und die Konsistenzstandards der EU erfüllen.

Andere Datenziele sind zulässig, wenn sie bestimmte „Verhaltenskodizes“ und „Zertifizierungssysteme“ befolgen, die in der Regel von einem Branchenverband oder einer entsprechenden Vertretung erstellt werden und der Zustimmung der jeweiligen GDPR-Regulierungsbehörden bedürfen.

Weitere Datenübermittlungen sind zulässig, wenn diese unter die Rubrik „spezifische Ausnahmen“ (d.h. Ausnahmen von den Standardvorschriften) fallen. Beispiele sind Übertragungen personenbezogener Daten, die folgende Bedinungen erfüllen:

- Die betroffene Person stimmt den damit verbundenen Risiken ausdrücklich zu und versteht diese
- Der Auftragsverarbeiter muss eine vertragliche Verpflichtung oder einen Rechtsanspruch erfüllen
- Die Übertragung liegt im öffentlichen Interesse oder im lebenswichtigen Interesse der betroffenen Person
- Die Übertragung liegt im berechtigten Interesse des Datenverantwortlichen, solange diese Interessen nicht die Rechte der betroffenen Person aushebeln. Der Auftragsverarbeiter der Daten muss die Umstände der Übermittlung bewerten und angemessene Maßnahmen zum Schutz der personenbezogenen Daten ergreifen

Es ist daher für Unternehmen zumeist einfacher, sicherer und billiger, personenbezogene Daten nicht in Länder zu übertragen, die außerhalb der EU und auf der kurzen Liste der zugelassenen Länder liegen. Wenn Sie personenbezogene Daten zu anderen Standorten verschieben, sollten Sie daher auf zusätzliche Ausgaben und Arbeit vorbereitet sein. Und dass Sie den zuständigen Aufsichtsbehörden alles nachweisen können, was Sie zum Schutz der Daten getan haben. Sorgen Sie für eine gute Rechtsberatung, wenn Sie sich auf BCRs, Verhaltenskodizes, Zertifizierungssysteme und/oder spezifische Ausnahmen verlassen wollen, um andere Arten von grenzüberschreitenden Datenübertragungen zu rechtfertigen.

F: Wie beeinflusst die GDPR unsere Reaktionen auf Sicherheitsverletzungen?

A: Die GDPR verlangt von Verantwortlichen und Auftragsverarbeitern, dass diese Systeme zur Abwehr, Überwachung und Berichterstattung möglicher Sicherheitsverletzungen bereitstellen – und Technologien, Richtlinien sowie Verfahren implementieren und dokumentieren, um die Prävention, Erkennung, Berichterstattung und Meldung von Verstößen zu unterstützen. Es gelten strengere neue Offenlegungsvorschriften für alle Vorfälle, die bewirken, dass personenbezogene Daten von Unbefugten (durch Zufall oder Vorsatz) abgerufen, übertragen, verändert oder zerstört werden.

Datenschutzvorfälle können durch technische Fehler (z.B. Festplattenausfälle), menschliche Fehler (z.B. versehentliche Löschung/Beschädigung von Benutzerdateien durch IT-Mitarbeiter) oder durch vorsätzliche, böswillige Sicherheitsverletzungen (z.B. Ransomware-Angriffe durch Cyberkriminelle, die personenbezogene Daten verschlüsseln und für deren Freigabe ein Lösegeld verlangen) verursacht werden.

Grundsätzlich müssen die Verantwortlichen und Auftragsverarbeiter mehr Aufwand betreiben, um Sicherheitsvorfälle, die personenbezogene Daten betreffen, zu erkennen, diese innerhalb von 72 Stunden nach ihrer Entdeckung den zuständigen Aufsichtsbehörden zu melden und bei schwerwiegender Beschädigungen von personenbezogenen Daten (wie Diebstahl oder Verlust) auch alle betroffenen Personen umgehend zu benachrichtigen.

F: Welche neuen Benutzerrechte müssen Auftragsverarbeiter unterstützen?

A: Dank GDPR haben betroffene Personen deutlich mehr Kontrolle und Einsichtsmöglichkeiten darüber, wie Auftragsverarbeiter ihre personenbezogenen Daten verwenden. Verantwortliche sind verpflichtet, bestimmte Benutzeranfragen kostenlos zu erfüllen. Beispiele: um Benutzern mitzuteilen, welche Elemente von ihren personenbezogenen Daten erfasst wurden; um Benutzern ihre personenbezogenen Daten in einem leicht zugänglichen Format bereitzustellen; um Fehler zu korrigieren, die vom Benutzer gemeldet werden; um personenbezogene Daten auf Anfrage zu löschen („Recht auf Vergessenwerden").

F: Was ist ein Datenschutzbeauftragter und benötigen alle Verantwortlichen und Auftragsverarbeiter einen solchen?

A: Ein Datenschutzbeauftragter (DSB) ist ein Mitarbeiter oder externer Berater, den viele Verantwortliche und Auftragsverarbeiter als Hauptverantwortlichen zur Überwachung der GDPR-Konformität ernennen müssen. Für öffentliche Einrichtungen gilt ein noch höherer Standard: fast alle müssen einen DSB ernennen. Private Organisationen müssen nur dann einen DSB haben, wenn sie große Mengen personenbezogener Daten verarbeiten, welche die Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, genetische oder biometrische Daten und/oder strafrechtliche Verurteilungen von betroffenen Personen offenbaren können.

Der DSB sollte ein ausgebildeter Compliance-Experte sein, der Erfahrungen im Datenschutzrecht und bei dessen optimaler Umsetzung hat. Seine Aufgabe ist es, die Verantwortlichen, Auftragsverarbeiter und Mitarbeiter der jeweiligen Organisation über ihre Pflichten bezüglich der GDPR zu informieren, deren Einhaltung zu überwachen und als Verbindungsperson für die zuständige Aufsichtsbehörde zu fungieren.

F: Was passiert, wenn ein Verantwortlicher und/oder Auftragsverarbeiter bei der Nichteinhaltung der GDPR-Auflagen erwischt wird?

A: Die Strafen bei Verstößen gegen die GDPR sind nicht unerheblich. Die örtliche Aufsichtsbehörde kann bei hochgradigen Verstößen (wie fehlende schriftliche Aufzeichnungen, fehlende technische und organisatorische Maßnahmen zur Einhaltung der Konformitätsvorgaben) Geldbußen von 10 Millionen Euro oder 2% des globalen Jahresumsatzes (je nachdem, welcher Betrag größer ist) auferlegen. Die Bußgelder können bis auf 20 Millionen Euro oder 4% des globalen Jahresumsatzes steigen (je nachdem, welcher Betrag höher ist), wenn es zu noch schwerwiegenderen Vorfällen wie großen Datenschutz-verletzungen kommt.

Beachten Sie, dass Bußgelder gleichermaßen gegen Verantwortliche und Auftragsverarbeiter ausgesprochen werden können. Aufsichtsbehörden können eine Strafzahlung aber auch auf einen Verantwortlichen und dessen Auftragsverarbeiter proportional verteilen – in Abhängigkeit von der Verantwortung, die jeder an der Datenschutzverletzung trägt, und den Maßnahmen, die jeder zur Wahrung der GDPR-Konformität getroffen hat.

Neben diesen erschreckenden Geldstrafen drohen Unternehmen, die ihre GDPR-Verpflichtungen bewusst ignorieren oder unterschätzen, eine möglicherweise nachhaltige Rufschädigung sowie Klagen von Privatpersonen wegen materieller oder immaterieller Schädigung, wenn deren personenbezogene Daten von einer Datenschutzverletzung betroffen sind. Die gleichen Strafen und Sanktionen gelten auch für weitere, dritte Auftragsverarbeiter, wenn diese personenbezogene Daten im Auftrag eines anderen Unternehmens verarbeiten. Bedenken Sie, wie die Datenschutzverletzungen in den letzten Jahren exponentiell angestiegen sind!

Die jährliche Summe der illegalen Lösegeldforderungen durch Ransomware-Angriffe ist beispielsweise von ca. 650.000 Euro in 2015 auf prognostizierte 6,5 bis 8,5 Milliarden Euro in 2018 gestiegen. Das Potenzial für Konformitätsverstöße allein aufgrund solcher Vorfälle und nicht gemeldeter Datenschutzverletzungen ist also enorm.

F: Die Aufgabe, GDPR-Konformität zu erreichen, erscheint enorm. Womit sollten Sie beginnen?

A: Als Anbieter professioneller Data Protection-Lösungen ist Acronis der Ansicht, dass eine wichtige Grundlage darin besteht, Ihre Storage- und Backup-Infrastruktur hinsichtlich GDPR-Konformität zu aktualisieren. Den Speicherort Ihrer Daten genau festlegen zu können, Datenschutzverletzungen (wie Ransomware-Angriffe) wirksam verhindern und Daten per starker Verschlüsselung (bei Übertragung und Speicherung) sicher schützen zu können, sind grundlegende Bausteine, die konkrete, positive Auswirkungen auf Ihre GDPR-Konformität haben.

Aber Sie sollten sich bei der Frage, wie Sie Ihre GDPR-Herausforderungen angehen, nicht allein auf uns verlassen. Stellen Sie sicher, dass Sie auch eine qualifizierte rechtliche und fachliche Beratung erhalten.

Beachten Sie, dass diese FAQs nur zu Informationszwecken dienen. Sie sind nicht als Rechtsberatung gedacht und sollten auch nicht als solche verwendet oder ausgelegt werden. Sie sollten nicht allein auf Basis der Inhalte dieser FAQs handeln oder von Handlungen absehen, ohne eine rechtliche oder andere fachliche Beratung in Anspruch zu nehmen.

Acronis

Weitere Informationen finden Sie unter **https://www.acronis.com/de-de/gdpr/.**