Planday und die Einhaltung der DSGVO

Am 25. Mai 2018 trat die neue EU-Datenschutz-Grundverordnung (kurz: DSGVO) in Kraft. Wir haben in diesem Zusammenhang Fragen von unseren Kunden bekommen, die wissen wollen, was die DSGVO ist und was Planday getan hat, um sie umzusetzen. Um einige dieser Fragen zu beantworten und die Auswirkungen der DSGVO deutlich zu machen, haben wir hier dargelegt, was genau die DSGVO ist. Die hier enthaltenen Informationen dienen nur zu Informationszwecken und sind nicht als Rechtsberatung gedacht. Sie sollten eng mit Ihrem Rechtsanwalt zusammenarbeiten, um genau festzustellen, wie sich die DSGVO auf Sie auswirken könnte.

FAQs zu Plandays DSGVO-Konformität

Um Kunden und Partnern den Umgang mit DSGVO zu erleichtern, haben wir nachstehend die am häufigsten gestellten Fragen beantwortet.

Was sind die DSGVO-Kontaktdaten von Planday?

Name der Firma: Planday A/S

Adresse:
Kuglegårdsvej 7-9-11
building 181
1434 København K
Dänemark

Mail: support@planday.com

Verarbeitet Planday sensible Daten?

Nein, Planday verarbeitet keine sensiblen Daten.

Vergibt Planday Unteraufträge für Verarbeitungstätigkeiten an Dritte?

Verarbeitungstätigkeiten erfolgen ausschließlich innerhalb unserer in Dänemark gehosteten Applikations-/IT-Infrastruktur sowie in allen Software as a Service-Systemen wie beispielsweise in unseren CRM- und ERP-Systemen.

Hat Planday einen Plan zur Sicherstellung von DSGVO-Compliance bis zum 25. Mai 2018?

Ja

Wie fördert Planday das Bewusstsein für Datenschutz?

Planday führt verschiedene Schulungsprogramme für Mitarbeiter zur Datensicherheit, unter anderem Webinare von Compliance-Spezialisten, sowie einen internen Informationsaustausch und Workshops zum Datenschutz durch.

Wie werden personenbezogene Daten gespeichert?

Personenbezogene Daten werden in unseren Datenbanken auf unseren Servern gespeichert.

Werden Daten von Planday außerhalb des EWR weitergegeben?

Planday ist ein globales Unternehmen mit Niederlassungen in Europa, Asien und den USA. Mitarbeiter können an ihren jeweiligen Standorten auf Kundendaten aus unseren CRM- und ERP-Systemen zugreifen; Kunden können weltweit auf ihre Daten zugreifen.

Ist Planday nach ISO/IEC 27001 zertifiziert oder Teil eines freiwilligen Datenschutzsystems?

Planday ist nach ISO 27001 zertifiziert.

Verfügt Planday über einen festgelegten Reaktionsplan zur Behandlung von Datenschutzvorfällen, unbefugter Offenlegung, unbefugten Zugriffs oder Verstößen gegen den Datenschutz?

Ja, Planday verfügt über ein Managementverfahren für alle Arten von Vorfällen, was auch Verstöße gegen den Datenschutz einschließt. Der Plan ist dem Branchenstandard angeglichen.

Welche Sicherheitsverfahren wendet Planday an, um seine Systeme vor Verwundbarkeit und die Daten vor versehentlichem Verlust, Zerstörung oder Beschädigung zu schützen?

Die Daten in unseren SaaS-Systemen werden während der Übertragung und im Ruhezustand verschlüsselt. Wir haben außerdem eine rollenbasierte Zugriffskontrolle und Zwei-Faktor-Authentifizierung für Logins eingerichtet. Die Daten in unserem Produkt werden verschlüsselt übertragen.

Plandays Engagement für Sicherheit und Datenschutz bei der Umsetzung von DSGVO

Plandays Engagement für Sicherheit und Datenschutz bei der Umsetzung von DSGVO

Von unserem Führungsteam bis hin zu unseren Entwicklern nimmt jeder bei Planday die Sicherheit unserer Produkte und den Schutz der personenbezogenen Daten unserer Kunden und Mitarbeiter sehr

ernst. Unsere Kunden vertrauen uns ihre Daten an; der Schutz dieser Daten ist für unser Geschäft von entscheidender Bedeutung.

Wir arbeiten aktiv mit unseren Kunden zusammen, um deren Bedürfnisse im Zusammenhang mit Datenverarbeitung und Datenschutz voll zu verstehen. Darüber hinaus arbeiten wir mit einer spezialisierten Organisation zusammen, um sicherzustellen, dass wir für die von DSGVO eingeführten Änderungen gerüstet sind.

Wir betrachten Datenschutz aus zwei verschiedenen Blickwinkeln: interne Verfahren und technische Entwicklung. Auf einen kurzen Nenner gebracht: Wir tun alles, was wir können, um sicherzustellen, dass wir über die richtigen Personen, Verfahren und Ausbildungen verfügen, um die Daten unserer Kunden zu schützen und gleichzeitig sicherzustellen, dass unser Produkt technisch hieb- und stichfest ist.

Technisches Engagement

Aus technischer Sicht unternehmen wir große Anstrengungen, um sicherzustellen, dass wir unser System mit den in diesem Artikel dargestellten Kontrollmaßnahmen vor internem und externem Missbrauch schützen. Diese Kontrollen spielen eine große Rolle für unsere DSGVO-Compliance und helfen gleichzeitig auch unseren Kunden, DSGVO-konform zu werden, indem wir sicherstellen, dass die Speicherung von Daten der Beschäftigten in Planday den DSGVO-Standards entspricht. Aus rein infrastruktureller Sicht stellen wir Folgendes sicher: dass das Planday-System vor externen Angriffen geschützt ist, dass die Daten im System durch Verschlüsselung geschützt sind und dass wir Datenmanagementverfahren einsetzen, um Daten vor internem und externem Missbrauch zu schützen. Wir lassen auf regelmäßiger Basis umfassende Penetrationstests und ein Sicherheitsaudit durch einen Dritten durchführen.

Planday besitzt eine Zertifizierung von **CyberEssentials** , einem von der britischen Regierung unterstützten Sicherungssystem gegen Cyberangriffe. Wir sind außerdem beim Information Commissioner's Office (ICO) und bei Datatilsynet (der nationalen Datenschutzbehörde Dänemarks) registriert. Des Weiteren arbeitet unser technisches Team an der **ISO 27001** Zertifizierung.

Selbstverständlich erfüllen wir auch die lokalen Datenschutz- und Handelsvorschriften in allen unseren Märkten.

Engagement bei den Verfahren

DSGVO ist Teil unseres unternehmerischen Risikomanagements; dies bedeutet, dass wir DSGVO-Compliance als Teil der Methoden und Verfahren ansehen, mit denen wir Risiken managen und unsere Ziele als Unternehmen erreichen.

Als Teil dieser Compliance verarbeitet Planday nur Daten gemäß unserer Datenverarbeitungsvereinbarung (Data Processing Agreement – DPA). Alle Daten, die wir verarbeiten, sind in unserer Infrastruktur und unseren SaaS-Systemen geschützt – d.h. die Daten, die wir verarbeiten, verlassen nie ein sicheres System.

Außerdem sind alle Zugriffe auf Kundendaten durch Rollen und Berechtigungen innerhalb des Planday-Systems gesichert. Mitarbeiter

von Planday können nur auf Daten, die sie unbedingt kennen müssen und gemäß des „Prinzips der geringsten Privilegien" zugreifen, was bedeutet, dass sie zur Erfüllung ihrer Aufgaben lediglich die minimale Zugriffsstufe auf Daten haben.

Wenn wir Daten verarbeiten und auf sie zugreifen, geschieht dies immer mit Einwilligung, entweder gemäß unserer Datenverarbeitungsvereinbarung oder mit ausdrücklicher Zustimmung des Kunden. Dadurch stellen wir sicher, dass wir unsere gesetzliche Verpflichtung gegenüber unseren Kunden erfüllen, jederzeit ihre Daten zu schützen.

Jeder Zugriff auf Kundendaten innerhalb des Planday-Produkts erfolgt ebenfalls nur mit Einwilligung. Wenn beispielsweise ein Mitglied des Customer Success-Teams auf das Planday-Konto eines Kunden zugreifen muss, hat ihm der Kunde seine Einwilligung zum Zugriff auf diese Daten zu erteilen.

Wir verlangen von allen unseren Mitarbeitern, dass sie eine Schulung zum Datenschutz absolvieren, die vor allem auf die Beziehung zwischen Datenschutz und DSGVO abstellt. Die Mitarbeiter werden routinemäßig in neuen Prozessen und Verfahren geschult und bei späteren Änderungen umgeschult.

Darüber hinaus verlangen wir, dass jede Abteilung sämtliche Vorgänge dokumentiert, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen. Um unser System vor internem Missbrauch zu schützen, stellen wir außerdem sicher, dass die Mitarbeiter von Planday einen minimalen Zugriff auf Daten erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen.

Wir halten DSGVO für unglaublich wichtig und werden weiterhin unsere Datenschutzverfahren fortlaufend überprüfen. Wir betrachten DSGV nicht als einmaliges Projekt, sondern als kontinuierliche Verpflichtung zu Datenschutz und Vertraulichkeit.

Was Planday zur Vorbereitung auf DSGVO unternommen hat

Was Planday zur Vorbereitung auf DSGVO unternommen hat

Jeder bei Planday nimmt die Sicherheit unseres Produktes sehr ernst. Unsere Kunden vertrauen uns ihre Daten an und der Schutz dieser Daten ist für unsere Geschäftstätigkeit sowie für die Unterstützung der Geschäftstätigkeit unserer Kunden von zentraler Bedeutung.

Planday arbeitet seit langem kontinuierlich mit Datenschutzspezialisten und Rechtsberatern zusammen, um ständige Compliance mit DSGVO und anderen weltweiten Datenschutzvorschriften zu gewährleisten. Wir außerdem arbeiten aktiv mit unseren Kunden zusammen, um deren Bedürfnisse im Zusammenhang mit Datenverarbeitung und Datenschutz voll zu verstehen.

Das Führungsteam von Planday engagiert sich für die Compliance von Planday mit der Datenschutz-Grundverordnung.

Unsere Compliance wird auf dem bereits sicheren Produkt aufbauen, das wir jetzt haben; dabei ist gewährleistet, dass die Daten Ihrer Mitarbeiter so sicher wie möglich sind. Planday erfüllt in allen seinen Märkten die nationalen Datenschutzgesetze; wir besitzen eine Zertifizierung von **CyberEssentials,** einem von der britischen Regierung unterstützten Cyber-Schutzsystem, und sind außerdem beim Information Commissioner's Office (ICO) und bei Datatilsynet (der nationalen Datenschutzbehörde Dänemarks) registriert.

Planday bietet Ihnen nicht nur eine sichere Lösung, sondern hilft Ihnen auch dabei, DSGVO-konform zu werden, indem wir sicherstellen, dass die Daten Ihrer Mitarbeiter vollständig geschützt sind.

Nachstehend führen wir die Schritte auf, die wir unternehmen, um sicherzustellen, dass wir DSGVO-konform sind.

Risikoprofil

Die Erfüllung der DSGVO ist für uns nie nebensächlich gewesen. Seit November 2017, als wir zum ersten Mal eine Risikobewertung des Typs der von uns verarbeiteten und gespeicherten Daten durchgeführt haben, arbeiten wir daran, die DSGVO zu erfüllen. Planday verarbeitet weder in großem Umfang sensible Daten noch überwachen wir systematisch Personen auf der Grundlage personenbezogener Daten oder verwenden automatisiertes Profiling.

System-Compliance von Planday

DSGVO ist kein einmaliges Projekt, sondern eine fortlaufende Initiative, die Teil des kontinuierlichen Strebens nach Verbesserung und des unternehmerischen Risikomanagements von Planday ist. Wir sind ständig bestrebt, unser System des Managements von Zwischenfällen und das kontinuierliche Verbesserungsregister zu optimieren.

Zugriffskontrolle

Alle Zugriffe auf Kundendaten sind durch Rollen und Berechtigungen innerhalb des Planday-Systems abgesichert. Mitarbeiter von Planday können nur auf Daten, die sie unbedingt kennen müssen und gemäß des „Prinzips der geringsten Privilegien" zugreifen, was bedeutet, dass sie zur Erfüllung ihrer Aufgaben lediglich die minimale Zugriffsstufe auf Daten haben.

Wir helfen unseren Kunden auch dabei, DSGVO-konform zu werden, indem wir sicherstellen, dass die im System erstellten Rollen nicht versehentlich die Datensicherheit gefährden.

Datenanonymisierung und Pseudonymisierung

DSGVO verlangt, dass bestimmte Daten entweder anonymisiert oder pseudonymisiert werden. Wir wissen, dass dies technische und komplexe Begriffe sind. Sollten Sie deshalb Fragen haben, was sie bedeuten, empfehlen wir Ihnen, **diesen Artikel** zu lesen.

Wir arbeiten mit Obfuskation zur Anonymisierung von Daten. Persönliche Daten wie Bankverbindungen und persönliche Identifikationsnummern werden obfusziert; dies bedeutet, dass lediglich die letzten Ziffern angezeigt (z.B. **** 1234) angezeigt werden.

Darüber hinaus werden die Daten wann immer möglich anonymisiert. Wir werden auch sicherstellen, dass die Daten von Beschäftigten, die das Unternehmen verlassen, anonymisiert werden; dies bedeutet, das wir alle der Identifizierung dienenden Informationen aus den für historische Aufzeichnungen als „notwendig" erachteten Daten entfernen werden.

Beispielsweise sind die Löhne, die ein Manager früher für die Gehaltsabrechnung genehmigt hat, weiterhin für Manager im System sichtbar, aber die personenbezogenen Daten dieses Mitarbeiters werden gelöscht werden. Dies bedeutet, dass unsere Kunden keine wichtigen historischen Informationen verlieren, es aber keine unnötigen persönlichen Informationen in Planday gibt.

Konforme Systeme von Dritten

Wir verwenden nur Systeme von Dritten, die DSGVO-konform sind.

Verschlüsselte Daten

Die Daten unserer Kunden werden durchgängig verschlüsselt. Dies bedeutet: Wenn Sie Informationen in die App eingeben, werden Ihre Daten an einen https-Webprozessor geschickt und dann in einer Datenbank gespeichert. Ihre Informationen werden auf dieser Reise durchgängig verschlüsselt und können deshalb zu keinem Zeitpunkt gelesen werden.

Sichere Passwörter und Verifizierung

Nur Sie können Ihr Passwort sehen; deshalb können nicht einmal Benutzer mit der höchsten Admin-Zugriffsstufe Passwörter anderer Benutzer sehen. Ihr Passwort wird im System und in der Datenbank von Planday immer verschlüsselt bleiben.

Wir verlangen von unseren Benutzern, dass sie ihre E-Mail verifizieren und ein sicheres Passwort verwenden. Wir werden außerdem von bereits bestehenden Benutzern verlangen, dass sie ihr Passwort aktualisieren und ihre E-Mail verifizieren.

Löschen von Endbenutzerdaten

Wir entwickeln das Verfahren der Verarbeitung von Endbenutzerdaten weiter (z.B. Daten von Beschäftigten). Das Löschen personenbezogener Daten von Endbenutzern wird automatisch erfolgen, sobald Beschäftigte ausscheiden. Endbenutzerdaten, die nicht länger relevant oder notwendig sind, werden anonymisiert werden.

Unternehmens-Compliance von Planday

DSGVO ist Teil unseres unternehmerischen Risikomanagements; dies bedeutet, dass wir DSGVO-Compliance als Teil der Methoden und

Verfahren ansehen, mit denen wir Risiken managen und unsere Ziele als Unternehmen erreichen.

DPA

Als Teil dieser Compliance verarbeitet Planday nur Daten gemäß unserer Datenverarbeitungsvereinbarung (Data Processing Agreement – DPA). Alle Daten, die wir verarbeiten, sind in unserer Infrastruktur und unseren SaaS-Systemen geschützt – d.h. die Daten, die wir verarbeiten, verlassen nie ein sicheres System.

Wenn wir Daten verarbeiten und auf sie zugreifen, geschieht dies immer mit Einwilligung, entweder gemäß unserer Datenverarbeitungsvereinbarung oder mit ausdrücklicher Zustimmung des Kunden. Dadurch stellen wir sicher, dass wir unsere gesetzliche Verpflichtung gegenüber unseren Kunden erfüllen, jederzeit ihre Daten zu schützen.

Zugriff des Planday-Mitarbeiters auf Daten

Außerdem sind alle Zugriffe auf Kundendaten durch Rollen und Berechtigungen innerhalb des Planday-Systems gesichert. Mitarbeiter von Planday können nur auf Daten, die sie unbedingt kennen müssen und gemäß des „Prinzips der geringsten Privilegien" zugreifen, was bedeutet, dass sie zur Erfüllung ihrer Aufgaben lediglich die minimale Zugriffsstufe auf Daten haben.

Jeder Zugriff auf Kundendaten innerhalb des Planday-Produkts erfolgt ebenfalls nur mit Einwilligung. Wenn beispielsweise ein Mitglied des Customer Success-Teams auf das Planday-Konto eines Kunden zugreifen muss, hat ihm der Kunde die Einwilligung zum Zugriff auf diese Daten zu erteilen.

Wir verlangen von allen unseren Mitarbeitern, dass sie eine Schulung zum Datenschutz absolvieren, die vor allem auf die Beziehung zwischen Datenschutz und DSGVO abstellt. Die Mitarbeiter werden routinemäßig in neuen Prozessen und Verfahren geschult und bei späteren Änderungen umgeschult.

Darüber hinaus verlangen wir, dass jede Abteilung sämtliche Vorgänge dokumentiert, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen. Um unser System vor internem Missbrauch zu schützen, stellen wir außerdem sicher, dass die Mitarbeiter von Planday einen minimalen Zugriff auf Daten erhalten, die sie zur Erfüllung ihrer Aufgaben benötigen.

Management von Datenschutzverstößen

DSGVO verlangt, dass Unternehmen Benutzer über einen Verstoß gegen den Datenschutz innerhalb von 72 Stunden nach dessen Entdeckung unterrichten. Wir verfügen über alle Verfahren, um dies zu ermöglichen und einfach zu bewerkstelligen.

Einwilligung

Eine der größten Änderungen in DSGVO besteht in der Art und Weise, wie Unternehmen von Kunden die Einwilligung zur Nutzung ihrer personenbezogenen Daten erlangen. Wir haben unser

Verfahren zur Erlangung der Einwilligung von Kunden aktualisiert und sie darüber informiert, wie ihre Daten verarbeitet werden, wenn sie Planday nutzen. Wir werden auch sicherstellen, dass überhaupt nur die notwendigen Daten erhoben werden.

Risikomanagement

Planday arbeitet mit einem „Continuous Improvement Model", einem System, dass es uns ermöglicht, reibungslos Änderungen an Methoden, Prozessen und Verfahren vorzunehmen, um hereinkommende Risiken zu bekämpfen.

Zusätzliche Sicherheitsverfahren

Alle Kundendaten werden verschlüsselt und in Kopie auf einem sicheren Medium gespeichert. Wir verwenden außerdem auf allen Planday-Rechnern Antiviren- oder Malware-Schutz. Alle in der Softwareentwicklung eingesetzten oder mit sensiblen Daten in Berührung kommenden Rechner verwenden verschlüsselte Datenträger.

Wir nehmen das Vertrauen unserer Kunden ernst

Das Vertrauen unserer Kunden ist die Grundlage unseres Produktes und unseres Geschäfts – ohne es können wir unseren Kunden nicht die Lösungen anbieten, die sie benötigen, um ihr Unternehmen besser zu führen. Deshalb haben wir seit der Gründung von Planday Datenschutz und Vertraulichkeit Vorrang eingeräumt und wir werden damit auch während des ganzen Prozesses der DSGVO-Compliance fortfahren. Mit dem von uns entworfenen Plan zur DSGVO-Compliance, dem Input einer spezialisierten DSGVO-Organisation und einem starken internen Sicherheitsteam haben wir alle notwendigen Maßnahmen ergriffen, vollständig konform zu sein.