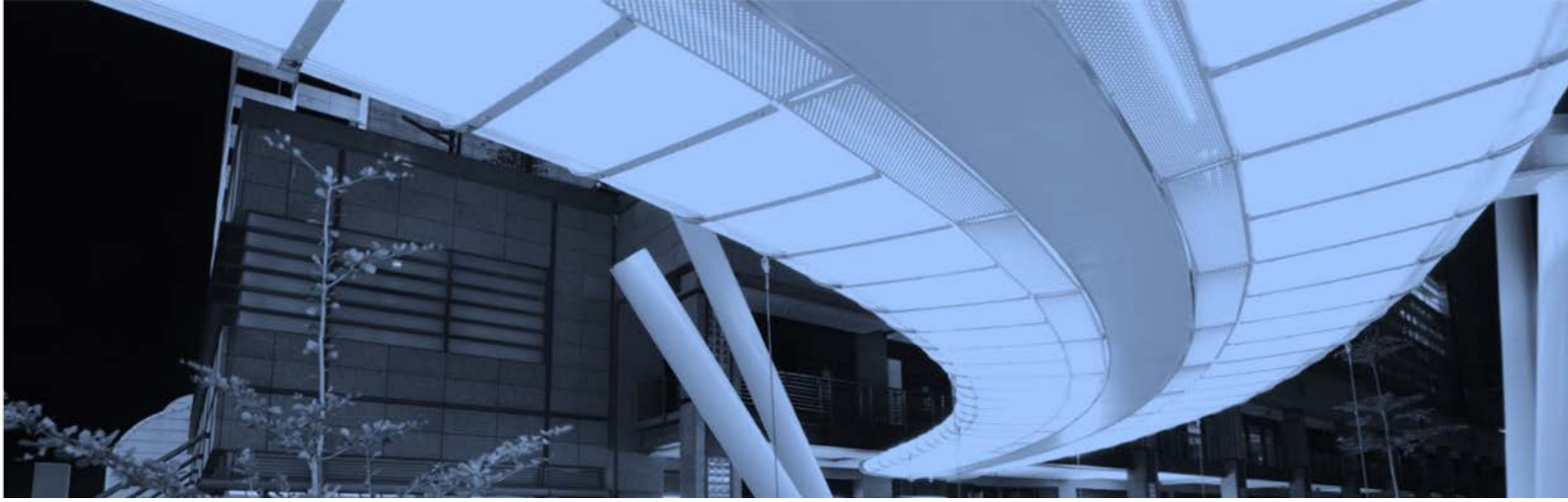
BCD travel

travel smart. achieve more.

Antwort von BCD Travel auf die

Datenschutz-Grundverordnung der Europäischen Union (DSGVO)

November 2017



Unabhängig davon, ob Sie Geschäftsreisender oder Travel Manager sind, Sie haben inzwischen bestimmt schon von der EU-Datenschutz-Grundverordnung (DSGVO) gehört, die am 25. Mai 2018 in Kraft treten wird. Die DSGVO ist ein europäisches Datenschutzgesetz, aber sie hat weltweite Geltung und weltweite Auswirkungen. Die DSGVO ist für die Geschäftsreisebranche ein wichtiges Thema: Nicht nur aufgrund der großen Reichweite, sondern auch aufgrund erhöhter Datenschutzanforderungen und möglicher Konsequenzen für Unternehmen, die gegen sie verstoßen. Im Laufe dieses Jahres werden wir weitere Informationen über die DSGVO veröffentlichen und mit Ihnen teilen.

**Für die Zwecke dieses Dokuments umfasst die Bezeichnung „BCD Travel" BCD Travel, BCD Travel Meetings & Events und Advito.*

Was sind Datenschutzgesetze?

Datenschutzgesetze regeln die Art und Weise, wie Unternehmen personenbezogene Daten über Einzelpersonen erheben, nutzen und weitergeben. Sie sind nichts Neues; nahezu jedes Land hat inzwischen Datenschutzgesetze eingeführt. Die europäische Datenschutzrichtlinie (Richtlinie 95/46/EG) gilt seit 1995. und jeder EU-Mitgliedsstaat hat sie in seine eigene Gesetzgebung umgesetzt. Die DSGVO wird diese Richtlinie im nächsten Jahr ersetzen.

Was genau ist die DSGVO?

Die DSGVO ist eine komplette Überarbeitung der aktuellen EU-Datenschutzrichtlinie. Es handelt sich um die größte Änderung des europäischen Datenschutzrechts der letzten 20 Jahre. Die DSGVO ist eine *Verordnung* – das bedeutet, sie muss innerhalb der gesamten EU *vollständig* befolgt werden. Mit anderen Worten: Es bedarf keiner weiteren Gesetzgebung einzelner EU-Staaten, damit die DSGVO in Kraft tritt.

Die DSGVO ist ein Versuch, das EU-Datenschutzrecht zu stärken, zu vereinheitlichen und zu modernisieren und die Rechte und Freiheiten des Individuums zu erweitern, weil in der EU der Datenschutz ein Grundrecht des Menschen ist. Die DSGVO schreibt unter anderem vor, wie Organisationen personenbezogene Daten erheben, nutzen, speichern und löschen dürfen. Dies wird einschneidende Auswirkungen auf Unternehmen in aller Welt haben.

Die Verordnung tritt zum 25. Mai 2018 in Kraft.

Ein Hinweis zu rechtlichen Definitionen

Die DSGVO nennt die betroffenen Personen auch „Datensubjekte“. Sie werden in diesem Dokument im Folgenden beide Ausdrücke lesen.

Wen betrifft die DSGVO?

Der Geltungsbereich der DSGVO ist sehr groß. Das neue Gesetz betrifft (1.) Unternehmen mit Sitz in der EU und (2.) alle Unternehmen, die an der Verarbeitung personenbezogener Daten in der EU beteiligt sind – unabhängig vom Sitz des Unternehmens und dem Ort, an dem die Datenverarbeitung jeweils stattfindet. Dies bedeutet, dass die DSGVO auf jedes Unternehmen der Welt Anwendung finden könnte. Die DSGVO gilt darüber hinaus für alle Branchen und Sektoren der Wirtschaft.

Was sind die wichtigsten Veränderungen, die die DSGVO bringt?

Die übergreifenden Veränderungen lassen sich wie folgt zusammenfassen:

- **Richtlinie versus Verordnung** – die DSGVO gilt automatisch überall in der EU, ohne dass sie von den EU-Mitgliedsstaaten in ein entsprechendes Gesetz umgesetzt werden muss. Das bedeutet eine stärkere Vereinheitlichung der datenschutzrechtlichen Anforderungen in der EU.

- **Breitere Definition personenbezogenen Daten** – die DSGVO definiert den Begriff „personenbezogene Daten” umfassender als bisher; eingeschlossen sind ab jetzt auch Online-Identifizierungsmerkmale wie IP-Adressen (einmal vergebene Nummern, die es Computern ermöglichen, miteinander im Internet zu kommunizieren).

- **Exterritoriale Wirkung** – die DSGVO gilt für alle Unternehmen, die (1.) einen Sitz in der EU haben, (2.) ihre Waren und Dienstleistungen Bürgern der EU anbieten und (3.) das Verhalten von EU-Bürgern überwachen. Deshalb können auch Unternehmen ohne Präsenz in der EU von den Vorschriften der DSGVO betroffen sein.

- **Wesentlich höhere Strafen** – Zuwiderhandlungen gegen Vorschriften der DSGVO können zu Strafen von bis zu 20 Mio. Euro oder bis zu 4 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres führen.

- **Strengere Anforderungen an die Einwilligung** – die DSGVO legt die Standards für die Einwilligung in die Verarbeitung personenbezogener Daten (Erhebung, Nutzen und Speichern von Daten) durch die betroffene Person hoch. Die DSGVO schreibt vor, dass die Einwilligung eindeutig und durch eine eindeutig bestätigende Handlung des Betroffenen erfolgen muss. Das heißt: Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen keine Einwilligung dar. Außerdem muss es Individuen möglich sein, ihre Einwilligung jederzeit leicht zu widerrufen.

- **Meldepflicht bei Verletzungen des Datenschutzes** – die DSGVO verlangt von einem für die Verarbeitung Verantwortlichen, der zuständigen Aufsichtsbehörde Datenschutzverletzungen umgehend mitzuteilen, wenn möglich, innerhalb von 72 Stunden nach Bekanntwerden, es sei denn, die Datenschutzverletzung wird wahrscheinlich die persönlichen Rechte und Freiheiten der betroffenen Personen nicht gefährden. Unter bestimmten Umständen besteht auch die Verpflichtung, betroffene Personen unverzüglich zu benachrichtigen. Die DSGVO schreibt auch einem

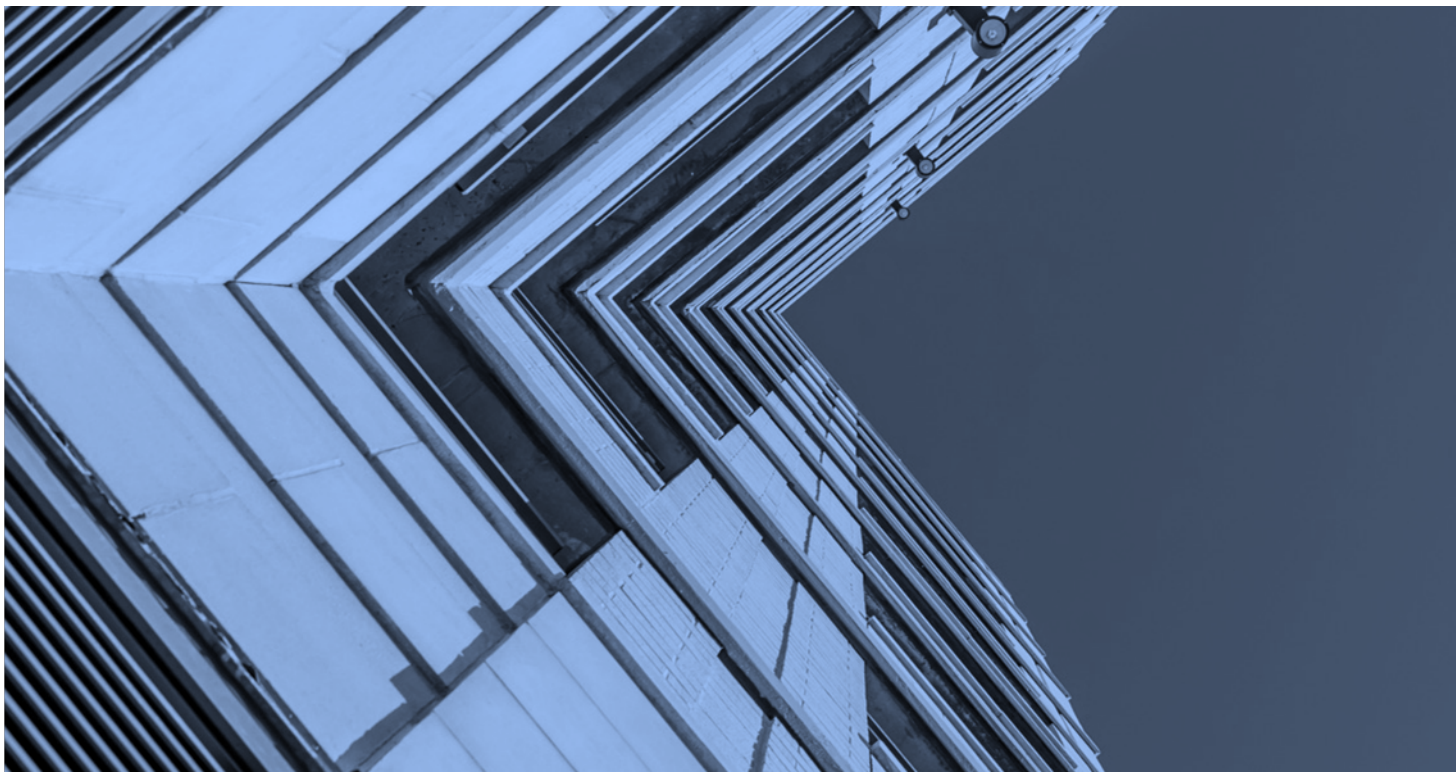
Auftragsverarbeiter vor, dem Verantwortlichen jede Verletzung des Datenschutzes umgehend zu melden.

Was ist der Unterschied zwischen einem Verantwortlichen und einem Auftragsverarbeiter?

- **Erweiterung der Rechte von betroffenen Personen** – die DSGVO stärkt die bisherigen Rechte der betroffenen Personen und führt zusätzliche neue Rechte ein, z. B. das Recht auf Vergessenwerden und das Recht auf Datenübertragbarkeit (Übermittlung von Daten an Dritte).

- **Datenschutz durch Technik und Datenschutz-Folgenabschätzung** – Datenschutz muss von Anfang an berücksichtigt werden, wenn neue technische Verfahren geplant werden, nicht erst im Nachhinein. Die Verantwortlichen müssen Datenschutz-Folgeabschätzungen durchführen, bevor sie personenbezogene Daten verarbeiten, wenn diese Verarbeitung aufgrund der Anwendung neuer Techniken oder wegen Art, Umfang, Kontext oder Zweck der Datenverarbeitung wahrscheinlich zu einem „hohen Risiko“ für die Rechte und Freiheiten der betroffenen Personen führt.

- **Ernennung eines Datenschutzbeauftragten (engl. Data Protection Officer, DPO) –** Die DSGVO schreibt vor, dass alle privaten Stellen (Verantwortliche oder Auftragsverarbeiter) einen Datenschutzbeauftragten ernennen müssen, deren „Kerntätigkeit“ eine der folgenden Aktivitäten beinhaltet: (1.) eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang oder (2.) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten.



Wie bereitet sich BCD Travel auf die DSGVO vor?

„DSGVO-konform“ zu werden, kann eine gewaltige Aufgabe sein – aber dank sorgfältiger Planung, Projektmanagement und dem Setzen von Schwerpunkten ist sie durchaus zu bewältigen.

Als Teil des gesamten Datenschutzprogramms von BCD Travel haben unsere Teams für Daten- und Informationssicherheit bereits aktiv mit der DSGVO-Vorbereitung begonnen. Wir sind uns jedoch darüber im Klaren, dass die Einhaltung der DSGVO ein laufender und niemals endender Prozess ist, für den wir unseren Umgang mit Daten immer wieder überprüfen und auf den neusten Stand bringen müssen.
Wir nehmen unsere Verantwortung sehr ernst, die uns anvertrauten Daten von Kunden, Reisenden und Mitarbeitern zu schützen. Wir sorgen für diesen Schutz durch einen interdisziplinären Ansatz und eine Struktur, die einen weltweiten Datenschutzbeauftragten, IT-Sicherheitsexperten sowie Experten für Recht und Datenschutz umfasst.

Im Folgenden stellen wir Ihnen einige Initiativen und Schwerpunktbereiche unseres Plans zur Vorbereitung auf die DSGVO vor:

- **Beurteilung der Datenverarbeitungsaktivitäten.** Kein Unternehmen kann die Anforderungen der DSGVO erfüllen, solange es nicht genau weiß, welche Daten es aktuell erhebt, wie und wozu es diese Daten nutzt und an wen diese Daten zu welchem Zweck weitergegeben werden. Die Komplexität der Geschäftsreisebranche macht diese Aufgabe zu einer besonderen Herausforderung. Nahezu jede einzelne Transaktion hat mehrere Beteiligte, darunter einzelne Reisende, Reiseeinkäufer, Reisebüros, Geschäftsreiseunternehmen, Anbieter von Online-Buchungstools, globale Computerreservierungssysteme, Zahlungsdienstleister und Lieferanten wie Hotels und Fluggesellschaften. Deshalb führen wir zunächst ein umfassendes Datenmapping-Projekt durch, um ein vollständiges und präzises Verständnis der Daten, die wir erheben und unserer wichtigsten Verarbeitungstätigkeiten zu gewinnen. Am Ende dieses Projekts werden wir die umfangreichen Anforderungen der DSGVO an die Dokumentation der Verarbeitungstätigkeiten erfüllen.

- **Internationale Datentransfers**. Die „Binding Corporate Rules“ (BCR) – in der Datenschutz-Grundverordnung als verbindliche interne Datenschutzvorschriften bezeichnet – sind der EU-„Goldstandard“. Diese Regeln stellen die offiziellen weltweiten Datenschutzstandards eines Unternehmens dar. Wir haben unsere BCR bei der niederländischen Datenschutzbehörde mit der Bitte um Genehmigung eingereicht. Wenn unsere BCR genehmigt werden, werden sie belegen, dass BCD Travel mit seinem Engagement für den Datenschutz die höchsten derzeit praktizierten Standards erfüllt.

- **Schulung und Bewusstsein.** Wir implementieren spezielle DSGVO-Schulungen für alle unsere Mitarbeiter auf Managementebene. Diese Schulung erfolgt beim Onboarding und wird jedes Jahr erneut stattfinden. Die Schulung mit Schwerpunkt DSGVO wird mit sicherheitsorientierten Kursen unseres Teams für Informationssicherheit kombiniert und beinhaltet ein umfassendes und obligatorisches Training zur Verbesserung des Sicherheitsbewusstseins für alle Mitarbeiter, regelmäßige Datenschutz-Newsletter, Artikel aus Firmen-Newslettern und Wettbewerbe zur Sensibilisierung für die interne Sicherheit.

- **Aktualisierung der Datenschutzerklärung.** Wir überprüfen und aktualisieren zurzeit unsere Datenschutzerklärung auf DSGVO-Compliance, einschließlich der Integration der obligatorischen Offenlegungen, welche die DSGVO verlangt.

- **Rechte der betroffenen Personen**. Wir prüfen alle Prozess- und Infrastrukturmaßnahmen, um sicherzustellen, dass wir auf Anfragen von Reisenden, die ihre personenbezogenen Daten einsehen, berichtigen, löschen usw. wollen, angemessen antworten können.

Wie gewährleistet BCD Travel die Datensicherheit?

Die DSGVO verlangt, dass BCD Travel *„geeignete technische und organisatorische Maßnahmen“* ergreift, um die personenbezogenen Daten, die das Unternehmen verarbeitet, zu schützen. Diese Maßnahmen sind unter Berücksichtigung der nachfolgenden Kriterien zu bestimmen: *Stand der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“*..

Zu diesem Zweck hat BCD Travel eine Vielzahlrobuster Maßnahmen eingeführt, um die personenbezogenen Daten seiner Kunden und Reisenden zu schützen:

- Unser Datenschutz-Team entwickelt, implementiert und erstellt laufend Methoden und Sicherheitsmaßnahmen nach ISO 27001 und PCI-DSS (Kreditkarten-Sicherheitsstandard), um für ein angemessenes Niveau an Datensicherheit zu sorgen.

- Alle unsere Rechenzentren werden von unabhängigen Firmen geprüft und halten die internationalen Normen für Sicherheitsmaßnahmen (ISO 27001) und Qualität (ISO 9001) ein.

- Ferner überwachen und evaluieren wir unsere Compliance mit unseren hohen Sicherheitsstandards durch jährliche interne und externe Audits und Sicherheitschecks.

- Unser formalisierter Incident-Response-Plan (Reaktionsplan) beinhaltet die rechtlich notwendigen Benachrichtigungen und die Dokumentation von Maßnahmen zur Behebung und Milderung von Vorfällen. Dieses formal festgelegte Verfahren ermöglicht es uns, auf Datenvorfälle mit angemessener Dringlichkeit und mit funktionsübergreifenden Teams aus BCD Travel Experten zu reagieren.

Als Ergebnis dieser und anderer Datenschutz-Initiativen können wir stolz vermelden, dass wir in puncto Datenschutz vor Kurzem von Bitsight an die Spitze einer kurzen Liste von Geschäftsreiseanbietern gewählt wurden. Bitsight wird von den weltgrößten Investmentbanken, Einzelhändlern, privaten Beteiligungsgesellschaften und Versicherern genutzt, um das Drittschadenhaftpflichtrisiko mit objektiven, belegten Sicherheits-Ratings zu bewerten. Seine Sicherheits-Rating-Plattform analysiert laufend riesige Datenmengen zum Sicherheitsverhalten, um Unternehmen dabei zu helfen, ihr Drittschadenhaftpflichtrisiko und ihre Benchmark-Performance zu messen und Cyber-Versicherungsprämien zu beurteilen und auszuhandeln.

Häufig gestellte Fragen (FAQ)

Diese FAQs erläutern, wie das EU-Datenschutzrecht angewandt auf BCD Travel funktioniert und welche Maßnahmen BCD Travel ergreift, um sich an die EU-Datenschutz-Anforderungen zu halten.

1. Warum ist das Datenschutzrecht für BCD Travel so wichtig?

Das Datenschutzrecht (einschließlich der DSGVO) ist deswegen so wichtig für BCD Travel und seine Kunden, weil BCD Travel als Anbieter von Geschäftsreisen notwendigerweise personenbezogene Daten über Reisende erheben, nutzen und weitergeben muss.

2. Verarbeitet BCD Travel „personenbezogene Daten“?

Die DSGVO gilt für Unternehmen, die „personenbezogene Daten“ verarbeiten (in den USA üblicherweise kurz PII für „personally identifying information“ genannt). Personenbezogene Daten sind laut Definition der DSGVO alle Daten, die dazu führen können, dass man die betroffene Person direkt oder indirekt identifizieren kann. Zu den personenbezogenen Daten zählen Vorname, Initiale(n) und Nachname, Adresse, E-Mail-Adresse, Telefonnummer, Sozialversicherungsnummer, Geburtsdatum, Geburtsort, Führerscheinnummer, Ausweisnummern, Identifizierungsnummer, Login und Kontonummer, Kreditkartendaten, Sicherheitscode, Zugangscode oder Passwort. Personenbezogene Daten haben also einen breiten Geltungsbereich und beinhalten sowohl Daten, die offensichtlich personenbezogen sind (wie der Name oder die Kontaktdaten einer Person), als auch Daten, die man verwenden kann, um eine Person auf indirektem Weg zu identifizieren (wie eine IP-Adresse). Da BCD Travel Dienstleistungen im Bereich Geschäftsreisen, Meetings, Events und Beratung erbringt, erhebt, nutzt und offenbart das Unternehmen notwendigerweise und zwangsläufig personenbezogene Daten über Reisende.

3. Inwiefern beeinträchtigt der Brexit die Compliance in Großbritannien?

Ob und inwiefern der Brexit die Compliance in Großbritannien beeinträchtigt, wird man erst wissen, wenn Großbritannien die EU verlassen hat. Vorläufig jedoch gelten die DSGVO-Anforderungen auch für Großbritannien. Die DSGVO gilt automatisch, solange Großbritannien Mitglied der EU ist, und die britische Regierung hat bereits signalisiert, dass die DSGVO auch danach (fast) ohne Übergang weitergelten soll. Sie gilt dann immer noch für alle britischen Unternehmen, die der EU ihre Dienste anbieten.

4. Wer setzt die Einhaltung der DSGVO durch?

Jede nationale Aufsichtsbehörde der EU ist für die Durchsetzung der Einhaltung der Verordnung verantwortlich und kann bei Verstößen gegen die DSGVO Bußgelder verhängen.

5. Was ist ein Datenschutzbeauftragter (DSB)?

Ein Datenschutzbeauftragter wird von einem Unternehmen ernannt, um als Ansprechpartner des Unternehmens für Anfragen der betroffenen Personen, für den Widerruf einer Einwilligung, für Anfragen zum „Recht auf Vergessenwerden“ und sonstige Rechte ähnlicher Art zu fungieren.

6. Wird BCD Travel einen Datenschutzbeauftragten ernennen?

Ja. Wir werden einen Datenschutzbeauftragten ernennen, der ein Netz von lokalen und regionalen Datenschutzbeauftragten beaufsichtigt und unterstützt. Dieses Team wird in allen Angelegenheiten, die mit der Verarbeitung personenbezogener Daten zu tun haben, eng zusammenarbeiten.