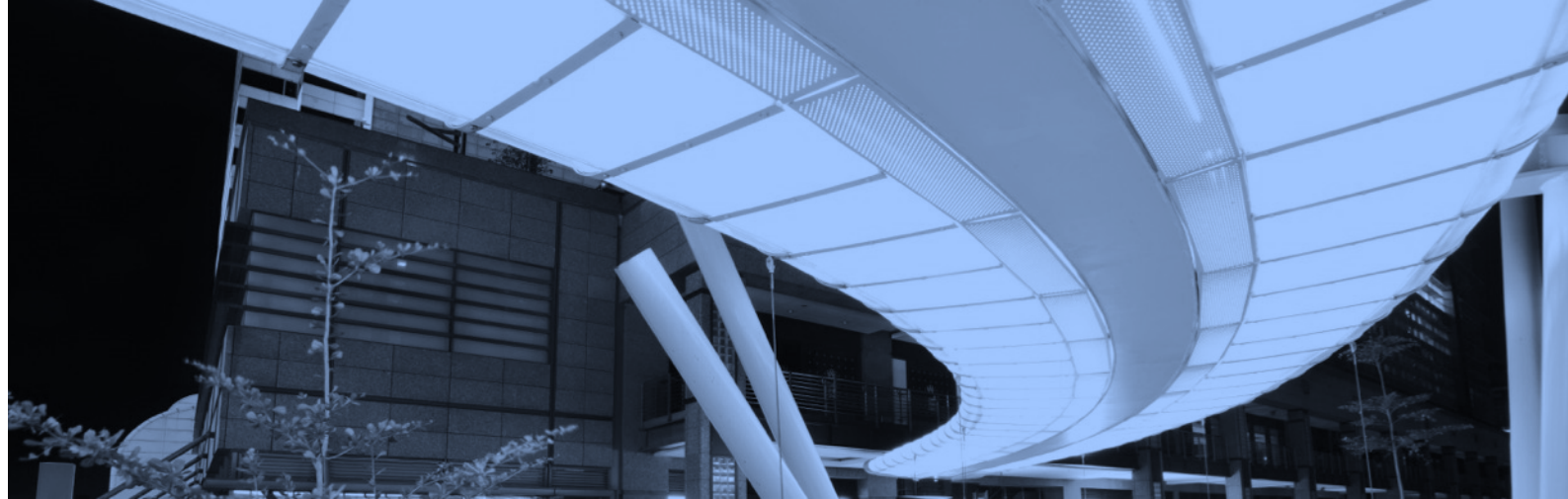




BCD Travel's Response to the EU General Data Protection Regulation (GDPR)

November 2017



Whether you're a business traveler or you manage a corporate travel program, by now, you've very likely heard of the European Union's General Data Protection Regulation (GDPR), set to go into effect May 25, 2018. While the GDPR is a European privacy law, it will have global reach and impact. This broad reach, increased privacy standards and the potential for large fines and penalties for companies that do not comply, mean that the GDPR has become a key topic of focus for the business travel community. Later this year, we will issue additional communications about the GDPR and how it will impact BCD Travel and our customers.

**For the purposes of this document, "BCD Travel" includes BCD Travel, BCD Travel Meetings & Events and Advito.*

What are data protection laws?

Data protection laws are a set of laws that govern the way that businesses collect, use and share personal data about individuals. They are nothing new; almost every country has privacy regulations in place. In the European Union since 1995, these laws have been based on the Data Protection Directive (Directive 95/46/EC), which every EU member state has implemented within its own national legal regime. Next year, the GDPR will replace the Directive.

What exactly is GDPR?

The GDPR is a major overhaul of the current EU data protection law. In fact, it's the biggest change in EU data protection law in over 20 years. The GDPR is a *Regulation* – which means it must be followed *in its entirety* throughout the EU. In other words, no further enabling legislation by individual EU countries is needed for the GDPR to become law.

The GDPR is an attempt to strengthen, harmonize, and modernize EU data protection law and enhance individual rights and freedoms, consistent with the European understanding of privacy as a fundamental human right. The GDPR regulates, among other things, how organizations may obtain, use, store, and eliminate personal data of individuals. It will have a significant impact on businesses around the world.

It will apply from May 25, 2018.

The GDPR refers to “individuals” as “data subjects,” so you’ll see both terms used in this document.

Who does the GDPR affect?

The scope of the GDPR is very broad. It will affect (1) organizations established in the EU, and (2) all organizations involved in processing personal data of individuals in the EU – regardless of where the organization is established, and regardless of where its processing activities take place. This means the GDPR could apply to any organization anywhere in the world. The GDPR also applies across all industries and sectors.

What are the main changes introduced by the GDPR?

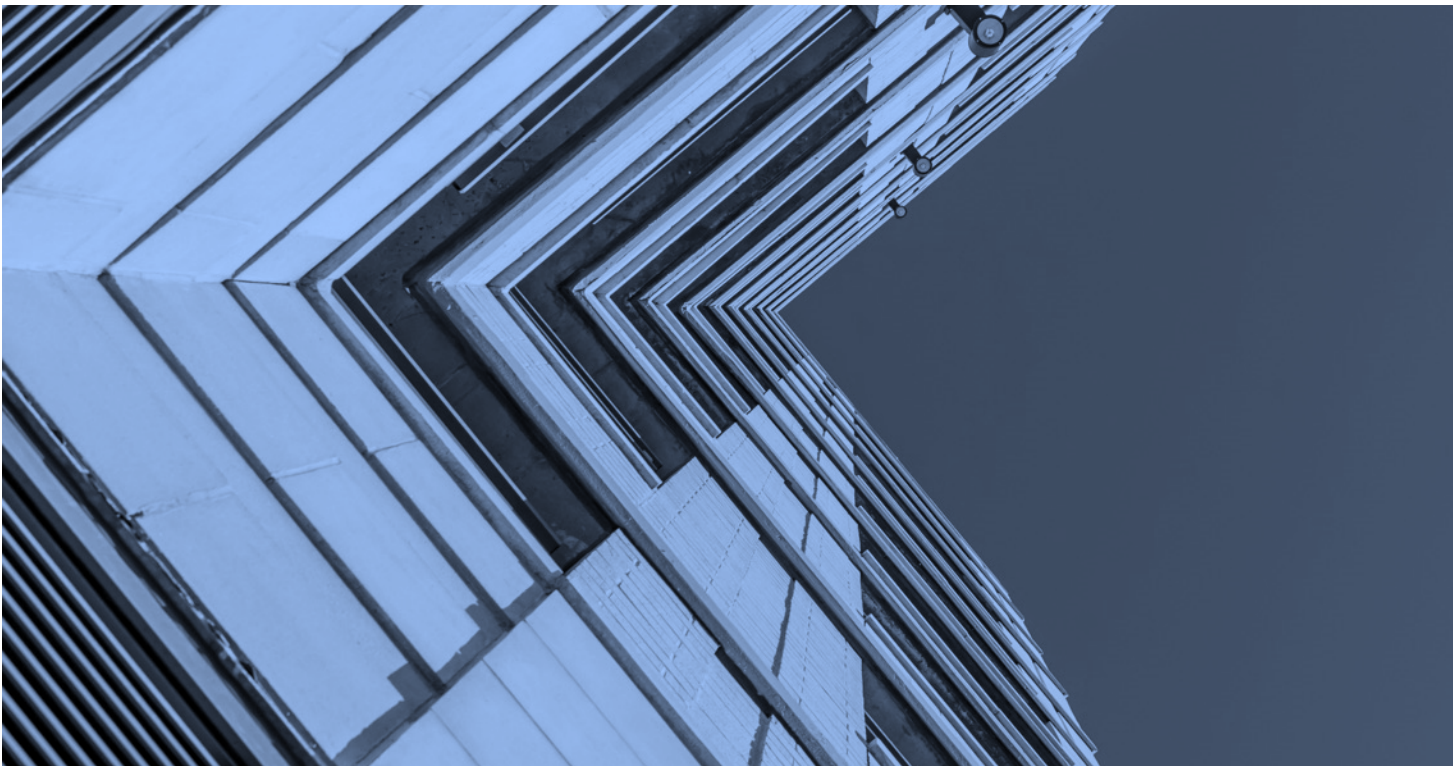
The over-arching changes can be summarized as follows:

- **Directive vs. Regulation** – the GDPR will become law without the need for implementing legislation in each EU member state. This means a greater degree of harmonization of data protection law requirements across the EU.
- **Broader definition of personal data** – the GDPR defines “personal data” more widely than at present, and includes online identifiers such as IP addresses (unique identifying numbers that allow computers to communicate over the internet).
- **Extra-territorial effect** – the GDPR applies to entities that: (i) have an establishment in the EU; (ii) offer goods and services to individuals in the EU; or (iii) monitor the behavior of individuals in the EU. Accordingly, entities without an EU presence may be subject to the GDPR's requirements.
- **Substantially increased fines** – failure to comply with the GDPR's requirements can lead to fines of up to 20 million EUR or up to 4% of total worldwide annual turnover of the preceding financial year.
- **Stricter consent requirements** – the GDPR sets a high standard for consent for processing (collecting, using and storing) personal data. The GDPR is clearer that consent must be unambiguous and involve a clear affirmative action. Silence, pre-ticked boxes or inactivity cannot be used to imply consent. Individuals must also be able to easily revoke consent.
- **Breach notification obligations** – the GDPR requires a controller to report a data breach to the data protection authority without undue delay and, where feasible, within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of the affected individuals. There is also an obligation to notify affected data subjects without undue delay in certain circumstances. The GDPR also requires a processor to notify the controller of any data breach without undue delay.
-

What is the difference between a controller and processor?

European data protection law establishes the concept of “controllers” and “processors.”

- A “controller” is an entity that alone or jointly with others determines the “purposes and means” of the processing of personal information (or, put another way, “why and how” personal information is processed).
 - A “processor” is an entity that processes personal information only on behalf of a controller and strictly in accordance with its instructions, normally pursuant to a service agreement.
-
- **Expansion of data subjects (individuals)’ rights** – the GDPR bolsters existing data subject rights and introduces new ones such as the right to be forgotten and the right to data portability (transfer of data to another third party).
 - **Privacy by design and data protection impact assessments** – data protection must be considered from the outset when new technologies are designed, rather than as an after-thought. Controllers must conduct data privacy impact assessments before processing personal data where the processing is likely to result in a “high risk” for the rights and freedoms of individuals due to the use of new technologies or the nature, scope, context and purposes of the processing.
 - **Appointment of a Data Protection Officer (DPO)** –The GDPR requires the appointment of a DPO by all private bodies (whether controllers or processors) whose “core activities” consist of either of the following two processing activities: (i) regular and systematic monitoring of data subjects on a large scale; or (ii) processing on a large scale of special categories of data and data relating to criminal convictions or offences.



What is BCD Travel doing to prepare for GDPR?

Getting “GDPR ready” may seem a daunting task – but with careful planning, project management and prioritization, it is an achievable one.

As part of BCD Travel’s overall data protection program, our privacy and information security teams have already taken active steps towards GDPR readiness. However, we recognize that GDPR compliance will be an ongoing process of constantly reviewing and updating the way data is handled.

We take very seriously our responsibility to protect the customer, traveler and employee data we hold, and we see to that protection through an interdisciplinary approach and structure that includes a global data protection officer IT security specialists and legal and privacy experts.

Below are some initiatives and focus areas of BCD Travel’s GDPR readiness plan:

- **Assessment of data processing activities.** No company can become GDPR-compliant unless it first knows what data it collects today, how and where it uses that data, with whom it shares that data and for what purpose. The complexity of the corporate travel industry makes this task particularly challenging. Almost every transaction involves many players, including individual travelers, travel buyers, travel management companies, online booking tool providers, global distribution systems, payment solution providers and suppliers such as airlines and hotels. Therefore, we are undertaking a comprehensive data mapping project to ensure a complete and accurate understanding of the data we collect and the core processing activities we perform. Completion of this project will help enable us to comply with the comprehensive data recordkeeping requirements and standards imposed by the GDPR.
- **International data transfers.** Binding Corporate Rules (BCR) are the EU “gold standard” for corporate privacy compliance. In effect, they outline a company’s official global privacy policy and governance. We’ve filed our BCR with the Dutch Data Protection Authority. Once approved, they will document BCD Travel’s commitment to comply with the highest data protection standards available today.
- **Training and awareness.** We require GDPR-focused training for all management-level staff. Training is required at onboarding and is renewed on an annual basis. This GDPR-focused training is coupled with security- oriented programs led by our Information Security team, including comprehensive and mandatory security awareness training for all staff, regular information security email bulletins, company newsletter articles, and internal security awareness contests.
- **Updating privacy notice.** We are in the process of reviewing and updating our privacy notice for GDPR compliance, including incorporating the mandatory disclosures required by the GDPR.
- **Data subject rights.** We are looking into process and infrastructure measures to ensure that we can respond to requests from travelers seeking to access, correct, delete (etc.) their personal data.

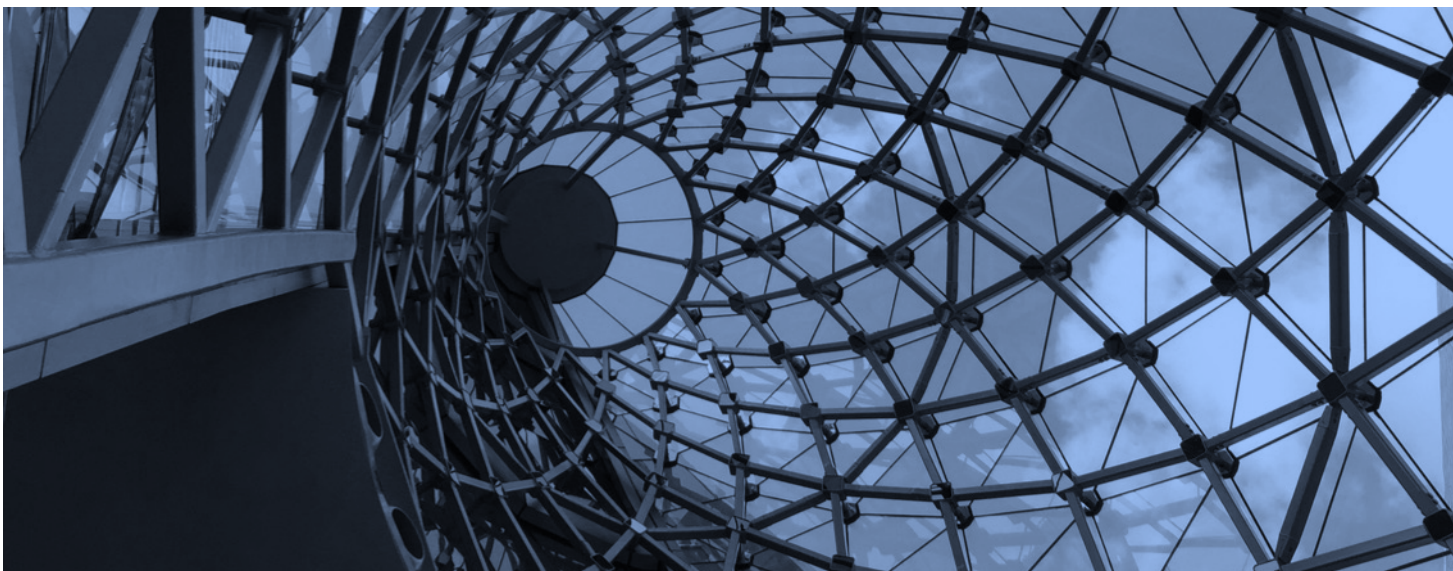
How does BCD Travel maintain the security of its data?

The GDPR requires that BCD Travel must implement “*appropriate technical and organizational measures*” to protect the personal data that it processes, and that these measures must “[take] into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.”

To this end, BCD Travel has in place a number of robust measures to protect the personal data of its customers and travelers:

- Our Information Security Team continues to develop, implement and provide methods and security measures in line with ISO 27001 and PCI-DSS (Payment Card Industry Data Security Standard) to ensure an appropriate level of security.
- All of our data centers are independently audited and maintain international certifications for operations in security (ISO 27001) and quality (ISO 9001).
- Further, we monitor and validate our compliance with our high security standards through annual internal and external audits and security checks.
- Our formalized incident response plan includes notification needed to comply with applicable laws and documentation of measures implemented to correct and mitigate incidents. This formalized procedure enables us to respond to data incidents with appropriate urgency by functional teams comprised of BCD Travel subject matter experts.

As a result of these and other data security initiatives, we’re proud to have recently been ranked by Bitsight at the top of a short list of travel management companies for data security. Bitsight is used by the world's largest investment banks, retailers, private equity companies and insurers to evaluate the security risk of their third parties with objective, evidence-based security ratings. Its Security Rating Platform continuously analyzes terabytes of data on security behaviors in order to help organizations manage third-party risk, benchmark performance, and assess and negotiate cyber insurance premiums.



Frequently Asked Questions

These FAQs explain more about how EU data protection law applies in the context of BCD Travel's services and the measures BCD Travel takes to comply with EU data protection requirements.

1. Why is data protection law relevant to BCD Travel and its customers?

At a global level, data protection law (including the GDPR) is relevant to BCD Travel and its customers because, in the course of providing travel services, BCD Travel must necessarily collect, use and disclose personal data about travelers.

2. Does BCD Travel process “personal data”?

The GDPR applies to businesses that process “personal data” (commonly called personally identifying information, or PII, in the U.S.). Personal data, as defined in the GDPR, is any information that can lead to identifying, directly or indirectly, an individual (data subject). Examples of personal data include: first name or initial and last name, address, email address phone number, social security number, birthdate, place of birth, driver's license number, passport number, identification number, login and financial account number, credit card information, security code, access code or password). Personal data is, therefore, broad in scope, and includes data that is obviously personal (such as an individual's name or contact details) as well as data that can be used to identify an individual indirectly (such as an individual's IP address). In the course of providing travel management, meetings, events and consulting services, BCD Travel inevitably and necessarily collects, uses and discloses personal data about travelers.

3. How does Brexit affect compliance in the U.K.?

How Brexit will affect compliance is something that will require further assessment after the U.K. leaves the EU. However, for now, GDPR standards will apply in the U.K. The GDPR will apply automatically while the U.K. is part of the EU, and the U.K. government has indicated that it will be transposed (almost) directly once the U.K. leaves the EU. It will still apply to U.K.-based companies offering services to the EU.

4. Who enforces compliance with the GDPR?

Each national supervisory authority in the EU is responsible for enforcing compliance and imposing administrative fines for violations of the GDPR.

5. What is a Data Protection Officer (DPO)?

A Data Protection Officer is a person appointed by an organization that acts as an organization's point of contact for an individual's inquiries, withdrawals of consent, right to be forgotten requests, and other related rights.

6. Will BCD Travel appoint a DPO?

Yes. We will appoint a Global Data Protection Officer to supervise and support a network of Local Privacy Managers and Regional Privacy Experts. This team will cooperate in all matters relating to the processing of personal data.