AUTORITEIT PERSOONSGEGEVENS - BCR APPROVAL DECISION

Autoriteit Persoonsgegevens

DECISION APPROVING CONTROLLER BINDING CORPORATE RULES

OF AMERICAN EXPRESS GLOBAL BUSINESS TRAVEL

The Autoriteit Persoonsgegevens,

Pursuant to the request by GBT III B.V. on behalf of the group American Express Global Business Travel , received on 11 November 2019 for approval of their binding corporate rules (BCRs) for controller;

Having regard to Articles 47, 57 and 64 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR); Having regard to the Court of Justice of the European Union (CJEU) decision Data Protection Commissioner Maximillian Schrems and Facebook Ireland Ltd, C-311/18 of 16 July 2020;

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021;

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023;

Makes the following observations:

1. Article 47(1) of the GDPR, stipulates that the competent supervisory authority shall approve Binding Corporate Rules provided that they meet the requirements set out under this Article.

2. The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees to controllers and processors established in the EU as to the protection of personal data that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country.

3. Before carrying out any transfer of personal data on the basis of the BCRs to one of the members of the group, it is the responsibility of any data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country of destination in the case of the specific data transfer, including onward transfer situations. This assessment has to be conducted in order to determine whether any legislation or practices of the third country applicable to the to-be-transferred data may impinge on the data importer's and/or the data exporter's ability to comply with their commitments taken in the BCR, taking into account the circumstances

surrounding the transfer. In case of such possible impingement, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures in order to exclude such impingement and therefore to nevertheless ensure, for the envisaged transfer at hand, an essentially equivalent level of protection as provided in the EU. Deploying such supplementary measures is the responsibility of the data exporter and remains its responsibility even after approval of the BCRs by the competent Supervisory Authority and as such, they are not assessed by the competent Supervisory Authority as part of the approval process of the BCRs

4. In any case, where the data exporter in a Member State is not able to implement supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under these BCRs. In the same vein, where the data exporter is made aware of any changes in the relevant third country legislation that undermine the level of data protection required by EU law, the data exporter is required to suspend or end the transfer of personal data at stake to the concerned third countries.

5. In accordance with the cooperation procedure as set out in the Working Document WP263 rev01[1], the Controller BCRs application of American Express Global Business Travel was reviewed by the Autoriteit Persoonsgegevens, as the competent supervisory authority for the BCRs (BCR Lead) and by two Supervisory Authorities (SA) acting as co-reviewers. The application was also reviewed by the concerned SAs to which the BCRs were communicated as part of the cooperation procedure. This review was communicated to American Express Global Business Travel and they have been given the opportunity to incorporate and comment on this feedback throughout the procedure. This process continues until the BCRs fulfil the requirements set out by Article 47(1) of the GDPR as well as the Working Document WP256 rev01.[2]

6. The review concluded that the Controller BCRs of American Express Global Business Travel fulfil the requirements set out by Article 47(1) of the GDPR as well as the Working Document WP256 rev01[3] and in particular that the aforementioned BCRs:

   i) Are legally binding and contain a clear duty for each participating member of the Group including their employees to respect the BCRs by entering in an Intra-Group Agreement (*8. Intra-Group Agreement and 9. Board resolutions*);

   ii) Expressly confer enforceable third-party beneficiary rights to data subjects with regard to the processing of their personal data as part of the BCRs (*GPR - Rights for individuals under EU law; GPR - Questions, complaints or concerns (page 13 f.); GPR - Enforcement and liability. Supporting Documents: 8. Intra-Group Agreement Clause 4 and 9. Board Resolution*);

---

[1] Endorsed by the EDPB on 25 May 2018.

[2] The WP256 rev.01 and WP264 are superseded by the EDPB Recommendation 1/2022. However, since the BCR-C of American Express Global Business Travel had already reached the stage of a "consolidated draft" in accordance with 2.4 of WP 263 rev.01 at the time of publication of the Recommendations, it can be assessed under the previous framework, subject to the EDPB adopting its opinion by the end of 2023 (paragraph 13 of the Recommendations).

[3] Endorsed by the EDPB on 25 May 2018.

iii) Fulfil the requirements laid down in Article 47(2) of the GDPR:

a) The structure and contact details of the group of undertakings and each of its members are described in the Application form WP264 that was provided as part of the file review and *Appendix 1: List of GBT companies and 15. GBT Organizational Structure;*

b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question are specified in *Part 2, section 7 of the application and Part 1, section 2 of the application - "short description of processing and data flows". Supporting Documents: 7. Current List of GBT Group Companies and 15. GBT Organizational Structure;*

c) the legally binding nature, both internally and externally, of the Controller BCRs is recognized in *Part 2, section 4 of the application and Part 1, section 2 of the application, GPR: ENSURING ACCOUNTABILITY (page 15). Supporting documents: 8. Intra-Group Agreement 9. Board resolutions and 11. Employment Contract Template;*

d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules are detailed in articles *GPR - Data Protection and Privacy Principles (page 2 ff);*

e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22 of the GDPR, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules which are set forth in *GPR - Rights granted to individuals (page 13), GPR - Questions, complaints or concerns (page 13 f.) and GPR - Enforcement and liability (page 14 f.);*

f) the acceptance by the controller or processor established on the territory of a Member State of its liability for any breaches of the binding corporate rules by any member concerned not established in the Union as well as the exemption from that liability, in whole or in part, only if the concerned party proves that that member is not responsible for the event giving rise to the damage are specified in *GPR - Questions, complaints or concerns (page 13 f.). Supporting Documents: 8. Intra-group agreement (Clause 6.5);*

g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of Article 47.2 of the GDPR are

provided to the data subjects in addition to Articles 13 and 14 of the GDPR, is specified in *GPR – Rights for individuals (page 13) and GPR - Questions, complaints or concerns (page 13 f.);*

h) the tasks of any data protection officer designated in accordance with Article 37 of the GDPR or any other person or entity in charge of monitoring the compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling are detailed in *GPR - Ensuring Accountability (page 15) and GPR - Questions, Complaints or Concerns (page 13 f.);*

i) the complaint procedures are specified in *GPR – Questions, complaints or concerns (page 13 f.);*

j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the binding corporate rules are detailed in *GPR - Ensuring Accountability (page 15), GPR- Cooperation (page 15) and GPR - Questions, Complaints or Concerns (page 13 f.)*. Such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such monitoring are communicated to the person or the entity referred to in point (h) above and to the board of the controlling undertaking of the group of undertakings (in this situation to American Express Global Business Travel headquarters, as well as to the data privacy organization) and are available upon request to the competent supervisory authority;

k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authorities are specified in *GPR – Changes to the Rules (page 16);*

l) the cooperation mechanism put in place with the supervisory authority to ensure compliance by any member of the group of undertakings is specified in *GPR – Cooperation (page 15)*. The obligation to make available to the supervisory authority the results of the monitoring of the measures referred to in point (j) above is specified in *GPR – Cooperation (page 15)*;

m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules are described in *GPR – Conflict of Laws (page 15 f.);*

n) finally, provide for an appropriate data protection training to personnel having permanent or regular access to personal data in *14. GBT Privacy Training Module.*

7. The EDPB provided its opinion 19/23 in accordance with Article 64(1)(f) of the GDPR. The Autoriteit Persoonsgegevens took utmost account of this opinion.

DECIDES AS FOLLOWING:

1. The Autoriteit Persoonsgegevens approves the Controller BCRs of American Express Global Business Travel as providing appropriate safeguards for the transfer of personal data in accordance with Article 46(1) and (2) (b) and Article 47(1) and (2) of the GDPR. For the avoidance of doubt, the Autoriteit Persoonsgegevens recalls that the approval of BCRs does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which, an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
2. The approved BCRs will not require any specific authorization from the concerned SAs.
3. The Controller BCR of American Express Global Business Travel must be brought in line with the EDPB Recommendations 1/2022 in the framework of the 2023 annual update.
4. In accordance with Article 58(2)(j) of the GDPR, each concerned SA maintains the power to order the suspension of data flows to a recipient in a third country or to an international organization whenever the appropriate safeguards envisaged by the Controller BCRs of American Express Global Business Travel are not respected.

The Hague, 9 January 2024

Yours sincerely,

Autoriteit Persoonsgegevens

On it's behalf,

Legal remedy

If you do not agree with this decision, you can object against this decision taken by the Autoriteit Persoonsgegevens by lodging a notice of objection.[4] The notice of objection must be signed and dated, include the name and address of the person submitting it and should entail a description of the decision against which the objection is being lodged and the grounds on which it is based. You must do this within six weeks after this decision is taken by addressing it to the Autoriteit Persoonsgegevens and submitting the notice via PO Box 93374, 2509 AJ The Hague, The Netherlands.[5] It is also possible to submit a notice of objection via our web form on the website, see https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/bezwaar-maken.

Please note that submitting a notice of objection will not automatically suspend the effect of this decision.

[4] The Dutch General Administrative Act applies to this procedure.
[5] Article 6:7 in conjunction with article 6:8 (1) of the Dutch General Administrative Act.

ANNEX I:

SUMMARY OF BCR CONTROLLER OF AMERICAN EXPRESS GLOBAL BUSINESS TRAVEL

The Controller BCRs of American Express Global Business Travel (GBT) that are hereby approved cover the following:

a. **Scope.**

These BCRs apply to all personal information received and processed by any GBT company or transferred between GBT companies and their employees, wherever those companies are in the world and are designed to provide a global framework and a baseline set of requirements to protect the personal information of all corporate and direct customers and their travellers, meeting attendees, service providers and employees regardless of the requirements of applicable data protection law *(see GPR – Scope and Purpose (page 1)).*

b. **EEA countries from which transfers are to be made:**

Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, the Netherlands, Norway, Poland, and Sweden.

A list of all companies covered by the BCRs can be found in Appendix 1 to the BCRs.

c. **Third countries to which transfers are to be made:**

Europe: Switzerland and the United Kingdom

Asia: China, India, Japan, Singapore, Taiwan, Thailand

Americas: Argentina, Brazil, Canada, Colombia, Mexico, the United States

Australia

A list of all companies covered by the BCRs can be found in Appendix 1 to the BCRs.

d. **Purposes of the transfer:**

The purposes are detailed in *GPR – Scope and Purpose (page 1 f.).*

They include the following:

Customer data:

- To provide GBT's products and services, including:
  - to book travel, organise meetings and events, prepare itineraries and invoices, communicate with travellers about products and services, provide customer service, manage customers' accounts, and provide travellers and their employers with emergency services; and
  - to provide travel, meetings and events, consulting, business insights, and other related services to travellers' employers or travel sponsors, to comply with GBT's agreements with them, to communicate about

GBT products and services, and to help travellers' employers or travel sponsors ensure compliance with their policies.

- To market goods and services to prospective customers;
- To process payments and transactions and provide related customer service;
- To operate websites and mobile applications, including using device data to monitor and improve the performance and content of services, provide updates, analyse trends and usage in connection with services, and measure whether ads and offers are effective; and
- To operate and improve GBT's business, using travellers' information for compliance with GBT company policies and procedures; for accounting and financial purposes; to detect or prevent fraud or criminal activity; to perform, analyse and improve GBT's business and services; and otherwise as required by law.

Employee data

- Administration of employment contracts, payroll and employee benefits, including insurance and pensions;
- Compliance with employment-related legal requirements such as income tax, national insurance deduction and employment and immigration laws and responding to requests and legal demands from regulators or other authorities;
- Administration of the workforce, including training and development, evaluation, rewards, assigning tasks, managing activities, planning, travel and expenses;
- Implementing and maintaining IT systems, including providing IT support, ensuring business continuity, and managing security services and IT access rights and administration of GBT's ethics helpline;
- Verification of the personal data related to former employment, educational history, and professional standing, and completion of background checks;
- Administering health and safety programmes and policies and corporate resource planning; and
- Monitoring GBT's premises and property.
- Post-transfer processing: The personal data transferred will be processed for the administration of human resources functions and the maintenance of GBT's workforce and may be further processed by third party service providers who provide payroll services, health and other insurance, and other benefits to employees.

Service provider data

- Service provider data is maintained in the GBT systems, including compliance tools, payment, expenses and finance systems, so that GBT can engage, screen, manage, and pay vendors.

e. **Categories of data subjects concerned by the transfer:**

Categories of data subjects are described in Appendix 2 to the BCRs.

These include Customers (travellers), Employees (former, current and prospective employees, directors, individual consultants, contingent workers, retirees, job applicants as well as any data given to GBT by such persons relating to third parties, for example dependants, and beneficiaries under employees' life insurance policies or for their emergency contacts), and Service provider data

f. **Categories of personal data transferred**:

Those categories are specified in Appendix 2 to the BCRs.

Customer data: To perform travel-related services, GBT must process personal information relating to the traveller, including his/her name, address, phone, email, nationality, age, passport details, dietary preferences and details of any disability which may affect his/her ability to travel etc., and potentially emergency contact details. Traveller data is also used to provide event management services as part of performance of the GBT Meetings & Events service or, on an aggregated basis, to advise how to structure a customer's travel management policy and reduce company travel costs, as part of the GBT consultancy service. That information must be transferred around the world to wherever travellers wish to go.

Employee data: GBT employs and retains many employees, directors, individual consultants, contingent workers and staff. The nature of the data covered by the BCRs are all the human resource records and information that relate to former, current and prospective employees, directors, individual consultants, contingent workers, retirees, job applicants as well as any data given to GBT by such persons relating to third parties, for example dependants, and beneficiaries under employees' life insurance policies or for their emergency contacts.

Service provider data: GBT contracts various service providers in the course of business. During service provider review, GBT receives basic information for contact purposes, including name, business email and business phone. If determined that the provider has anti-corruption or sanctions risk, information about the service provider's beneficial owner(s) is required to perform proper screening activities.

ANNEX II: DOCUMENTATION FOR EDPB DECISION

1. Application Form;

2. BCR Policy:

GBT Global Privacy Rules, including Appendix 1: List of GBT companies, Appendix 2: Description of Processing and Data Flows, and Appendix 3: Handling data subject inquiries, complaints and requests.

3. Intergroup agreement;

4. Referential (WP256);

5. List of entities.