SPANISH DATA PROTECTION AUTHORITY
DECISION APPROVING BINDING CORPORATE RULES OF FCC GROUP

The SPANISH DATA PROTECTION AGENCY,

Pursuant to the request by Fomento Construcciones y Contratas S.A. (FCC hereafter), on behalf of the FCC Group for approval of their binding corporate rules 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 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 EU General Data Protection Regulation 2016/679 (GDPR), provides that the SPANISH SA shall approve Binding Corporate Rules (BCRs) 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 must 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 FCC S.A was reviewed by the SPANISH DATA PROTECTION AGENCY, 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.

6. The review concluded that the Controller BCRs of FCC GROUP comply with the requirements set out by Article 47(1) of the GDPR as well as the 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 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 Internal Procedure.

   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 (Part II, Section C of BCR);

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

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

a) The structure and contact details of the group of undertakings and each of its members are described in the Application form that was provided as part of the file review and in Annex 3 of BCR;

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 the Part I of BCR;

c) the legally binding nature, both internally and externally, of the Controller BCRs is recognized in the Application form and in Section 3 of BCR ;

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 Section 4 of the BCR;

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 Section 5 of the BCR;

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 the Introduction and in Part II Section C of the BCR;

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 Section 5.1 of the BCR;

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 Part II, Section B Rule 15.A of the BCR;

i) the complaint procedures are specified in the Part II, Section B, Rule 12 and Appendix 3 of the BCR;

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 Sections 7.2 and 7.3 of the BCR. 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 the board of the audited Group Company, and the board of directors of the parent company) 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 Part II, Section B, Rule 14 and Appendix 5 of the BCR;

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 Section 9 of the BCR. The obligation to make available to the supervisory authority the results of the monitoring of the measures referred to in point (j) above are specified in sections 7.2 and 7.3 and Annex IV of the BCR;

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 Section 9.2 of the BCR;

n) finally, provide for an appropriate data protection training to personnel having permanent or regular access to personal data (Part II, Section B, Rule 10 of the BCR).

7. The EDPB provided its opinion 17/2024 in accordance with Article 64(1)(f) of the GDPR. The Spanish Data Protection Agency took utmost account of this opinion.

DECIDES AS FOLLOWING:

1. The **Spanish Data Protection Agency** approves the Controller BCRs of FCC GROUP 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) GDPR. For the avoidance of doubt, the SPANISH DATA PROTECTION AGENCY 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. In accordance with Article 58(2)(j) GDPR, each concerned SAs 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 FCC GROUP are not respected.

ANNEX TO THE DRAFT DECISION

The Controller BCRs of FCC that are hereby approved cover the following:

a. **Scope:** The purpose of the BCRs is to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when performing International Transfers of Personal Data between FCC Group Companies established in the EEA and FCC Group Companies established outside the EEA, importing such Personal Data in its capacity as Controller or Processor on behalf of Group company adhered to a controller including onward transfers.

b. **EEA countries from which transfers are to be made**: Spain, Portugal, Netherlands, and Norway (EEA countries).

c. **Third countries to which transfers are to be made**: Argelia, Australia, Bosnia and Herzegovina, Chile, Colombia, Dominican Republic, Ecuador, Egypt, Guatemala, Jersey, Kosovo, México, Montenegro, Nicaragua,

Oman, Panamá, Perú, Qatar, Saudi Arabia, Serbia, The Tunisia, United Arab Emirates, United States of América and United Kingdom.

d. **Purposes of the transfer:** The purposes are detailed in Part I of the BCR. They include the following:

- Transfers of **current and former employees and temporary employees'** personal data are mainly made between Group Members in Europe and Group Members globally (including Mexico, the United States of America, Saudi Arabia, Peru, etc.) for the purposes of administering and managing personnel (*e.g.* protecting the health and safety of employees, monitor compliance with internal policies and procedures, etc.), providing and monitoring IT services (including CCTV and door entry systems), providing a wide variety of services to other Group Members (*e.g.* IT technology and systems services, payroll, selection and human resources management services, audit services, document destruction services, document transport services, risk management services, procurement of products and/or services, video surveillance systems management services, management of marketing and communication campaigns, management and coordination services in the field of data protection, etc.), supporting the management of the services provided by the company, verifying the fulfilment of the employee's labour obligations and duties, managing the safety in emergency situations and responding to employee's requests in this context and complying with applicable legal obligations (*e.g.* Labour and Social Security obligations).

- Transfers of **current and former job applicants'** personal data are mainly made between Group Members in Europe and Group Members globally (including Mexico, the United States of America, Saudi Arabia, Peru, etc.) for the purposes of administering and managing the job recruitment process (*e.g.* reviewing CVs, carrying out interviews, etc.) and complying with applicable legal obligations.

- Transfers of **independent contractors, suppliers, customers and vendors'** personal data are mainly made between Group Members in Europe and Group Members globally (including Mexico, the United States of America, Saudi Arabia, Peru, etc.) for the purposes of administering and managing the agreements entered into with these third parties, providing visitors with access to premises, providing a wide variety of services to other Group Members (*e.g.* IT technology and systems services, audit services, document destruction services, document transport services, risk management services, procurement of products and/or services, video surveillance systems management services, electronic invoicing services, management and coordination services in the field of data protection, etc.) and complying with the applicable legislation (*e.g.* commercial, tax, etc.).

In relation to employees, job applicants, independent contractors, suppliers, customers and vendors, **special categories of personal data** may be processed by the Group Members if required in order to properly fulfil its purposes (*e.g.* establishment of suitable conditions in case of physical limitations or special needs, absence management and administration, premises' access control, provision of employment-related health benefits, etc.) and only as necessary for the purposes of carrying out the obligations and exercising specific rights of Group Members or of the data subject in the field of employment and social security and social protection law (as foreseen on Article 9.2(b) GDPR), for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (as foreseen on Article 9.2(f) GDPR) and for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (as foreseen on Article 9.2(h) GDPR). Additionally, special categories of personal data may be processed for the provision of a wide variety of services to other Group Members (*e.g.* occupational risk prevention services and joint medical services, legal advisory services, labor litigation services, whistleblowing line, archiving and document custody services, insurance services, internal reporting management services, corporate security and general services, finance services**,** etc.).

- Transfers of **website visitors'** personal data are mainly made between Group Members in Europe and Group Members globally (including Mexico, the United States of America, Saudi Arabia, Peru, India, Singapore, etc.) for the purposes of contacting the data subjects and answering any queries or doubts they may have.

- Transfers of personal data of **employees (including expatriates) and external collaborators' relatives** are mainly made between Group Members in Europe and Group Members globally (including Mexico, the United States of America, Saudi Arabia, Peru, India, Singapore, etc.) for the purposes of managing internal competitions/contests and events for employees and their relatives, or, with regard to expatriate personnel´s relatives, managing evacuation or repatriation, managing the safety in emergency situations and respond to requests in this context, or the same needs and perks that the expatriate employee might have.

e. Categories of data subjects concerned by the transfer: Those categories are specified in Part I of the BCR. They included:

Employees, job applicants, independent contractors, suppliers, customers and vendors, website visitors and employees (including expatriates) and external collaborator.

f. Categories of personal data transferred: Those categories are specified in Part I of the BCR. They included:

- in relation to **current and former employees and temporary employees' personal data**: **(a) Basic information** (*e.g.* name, surname, date of birth,

ID number, email address, home address, telephone number, emergency contact number, national insurance number, image, nationality, etc.); **(b) Employment data** (*e.g.* profession, job position, etc.); **(c) Financial Information** (*e.g.* bank account details, salary, bonus, pension contributions, etc.); **(d) IT details** (*e.g.* IT and internet user logs, IP address, successful and failed login attempts, etc.); **(e) Business travel information** (*e.g.* credit card information, passport number, expenses incurred, driving license, etc.); **(f) Social circumstance data** (*e.g.* hobbies and lifestyle, driver's license, etc.); **(g) Insurance data**; and **(h) Geolocation data** (information that indicates the geographical position of a terminal equipment used by a data subject such as latitude, longitude or altitude of the equipment);

- in relation to **current and former job applicants' personal data**: **(a) Basic information** (*e.g.* name, surname, data of birth, ID number, email address, home address, telephone number, image, etc.) and **(b) Labour and educational information** (*e.g.* job qualifications, employment history, CV, references, etc.);
- in relation to **independent contractors, suppliers, customers and vendors' personal data**: **(a) Contact information** (*e.g.* name, surname, ID number, professional address, email address, image, etc.); **(b) Personal characteristics data** (age, date of birth, nationality, etc.); **(c) Employment data** (*e.g.* profession, job position, etc.); **(d) Economic, financial and insurance data** (*e.g.* bank account details) **(e) Academic and professional data** (*e.g.* profession category, etc.); **(f) IT information** (*i.e.* IP address); **(g) Visa application information**; and **(h) Complaint data** (*e.g.* personal data provided through internal compliance system).

In relation to employees, job applicants, independent contractors, suppliers, customers and vendors, **special categories of personal data** may be processed by the Group Members when necessary and required or permitted by the applicable law for the purposes described in the following section.

- In relation to **website visitors' personal data**: **Contact details** (*e.g.* name, surname, email address, IP/MAC address, personal data collected through cookies or other similar information storage and retrieval devices etc.); and
- in relation to **employees (including expatriates) and external collaborators' relatives**: **(a) Basic information** (*e.g.* name, surname, ID number, email, image, etc.); **(b) Geolocation data** (information that indicates the geographical position of a terminal equipment used by a data subject such as latitude, longitude or altitude of the equipment) or even **(c) Special categories of personal data** in cases of relatives of expatriate personnel/external collaborators or relatives with certain disability.