

**SPANISH DATA PROTECTION AUTHORITY
DECISION APPROVING PROCESSOR BINDING CORPORATE RULES OF
AVATURE GROUP**

The SPANISH DATA PROTECTION AGENCY,

Pursuant to the request by Avature Spain S.L.U on behalf of the AVATURE group, received on 21 December 2022, for approval of their binding corporate rules for processor;

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 v Facebook Ireland Ltd and Maximillian Schrems, 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;

Makes the following observations:

1. Article 47(1) of the EU General Data Protection Regulation 2016/679 (GDPR) provides that the Spanish Data Protection Agency 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 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 BCRs, 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 (SA) and, as such, they are not assessed by the competent SA 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 rev.01¹, the Processor BCRs application of AVATURE S.L.U was reviewed by the Spanish Data Protection Agency, as the competent SA for the BCRs (BCR Lead) and by two SAs 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 Processor BCRs of AVATURE GROUP comply with the requirements set out by Article 47(1) of the GDPR as well as the Working Document WP257 rev.01² 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.
 - 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:
 - a) The structure and contact details of the group of undertakings and each of its members are described in the application form WP265 that was provided as part of the file review and Annex 4;

¹ Endorsed by the EDPB on 25 May 2018.

² Endorsed by the EDPB on 25 May 2018.

- 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 I of the BCR;
- c) the legally binding nature, both internally and externally, of the Processor BCRs is recognized in the IGA, Application Form and in the Introduction of the 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 BCRs are detailed in articles Part II, Section A 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 SA 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 BCRs which are set forth in Part II, Section A Rule 4 and Appendix 1 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 BCRs 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 Section C;
- g) how the information on the BCRs, 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 Part II Section A Rule 1.A and Part II, Section C 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 6.A;

- i) the complaint procedures are specified in Part II, Section B Rule 9 and Appendix 3;
- j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the BCRs are detailed in Part II, Section B Rule 8 and Appendix 2. 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 AVATURE headquarters, as well as to the data privacy organization) and are available upon request to the competent SA;
- k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the SAs are specified in Part II, Section B, Rule 11 and Appendix 5;
- l) the cooperation mechanism put in place with the SA to ensure compliance by any member of the group of undertakings is specified in Part II, Section B Rule 10 and Appendix 4. The obligation to make available to the SA the results of the monitoring of the measures referred to in point (j) above is specified in Appendix 2;
- m) the mechanisms for reporting to the competent SA 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 Part II, Section B Rule 12;
- n) finally, provide for an appropriate data protection training to personnel having permanent or regular access to personal data (Part II, Section B Rule 7).

7. The EDPB provided its opinion 15/2024 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 Processor BCRs of AVATURE 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 SA maintains the power to order the suspension of data flows to a recipient in a third country or to an international organisation whenever the appropriate safeguards envisaged by the Processor BCRs of AVATURE GROUP are not respected.

ANNEX TO THE DRAFT DECISION

The Processor BCRs of AVATURE that are hereby approved cover the following:

a. Scope.

Only members of AVATURE GROUP processors and/or sub-processors as part of their regular business activities in the course of providing services to a customer.

b. EEA countries from which transfers are to be made: Spain and Germany (EEA Countries).

c. Third countries to which transfers are to be made: Argentina, Australia, China, Hong Kong, United Kingdom and United States.

d. Purposes of the transfer:

Transfers of customer personal data under this Policy take place between Group Members globally (see the location of all such Group Members [here](#)), whatever the origin of the data,

for the purposes of providing the required services to customers (as agreed via agreement), which entails, among others, accessing to customer personal data in order to: (i) store such data on customers' behalf; (ii) provide them technical support services; (iii) perform configuration or reconfiguration services in the pertinent instances as instructed by the customers; (iv) carry out the processing operations required to provide the various functionalities of the services offered to customers; and (v) provide security and availability of the services.

e. Categories of data subjects concerned by the transfer: current, past and prospective employees or other personnel (such as trainees, secondees or independent contractors) of customers.

f. Categories of personal data transferred: Personal data processed under this Policy includes customer personal data; specifically personal data regarding **current, past and prospective employees or other personnel (such as trainees, secondees or independent contractors)** of customers shared by the latter through the agreed configuration / agreement, which mainly comprises the following data: **(a) personal and contact details** (e.g. name, age, date of birth, contact details, government issued identification numbers (such as social security numbers, driver's license numbers or national identification numbers); **(b) talent, recruitment and application, education and training details** (e.g. educational history, work experience, CV, notes from users in relation to personnel's qualities and qualifications); and **(c) financial information** (e.g. bank account numbers provided by customers' personnel for the sole purposes of receiving salary payments and details of dependents and emergency contacts).

Also, **special categories of personal data** may be processed by the Group Members when necessary and required or permitted by Applicable Local Law for the purposes described in the following section. Specifically, health and medical information (including health insurance identification numbers), or sexual, racial, political, ethnic, ideological or religious orientation of individuals (only for EEO compliance or as required and permitted by laws applicable to the controller in the jurisdictions where the controller collects the data).