**SPANISH DATA PROTECTION AUTHORITY**
**DECISION APPROVING 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 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 S.A 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 AVATURE 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 AVATURE 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. (Application Form, Intra-Group Agreement or IGA and Introduction of the BCR)

   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.1 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 4;

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, the IGA and in the Introduction 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 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 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 Part II, Section A, Rule 5 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 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.2 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 Part II, Section B, Rule 2.A and Part II Section C.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 7.A of the BCR;

i) the complaint procedures are specified in the Part II, Section B, Rule 10 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 Part II Section B, Rule 9 and Appendix 2 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 12 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 Part II, Section B, Rule 11 and Appendix 4 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 the Appendix 2 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 Part II, Section B, Rule 13 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 8 of the BCR).

7. The EDPB provided its opinion 16/2024 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 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 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 AVATURE GROUP are not respected.

ANNEX TO THE DRAFT DECISION

The Controller BCRs of AVATURE 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 AVATURE Group Companies established in the EEA and AVATURE 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 from importing entities to other importing entities.

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

- Transfers of **current and former employees, contractors and temporary employees'** personal data 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 **(a) managing work activities and personnel generally** (*e.g.* recruitment, appraisals, performance management, promotions, succession planning and career development, payroll management, administering internal mobility, leaves / absences, transfers and secondments, compiling and managing existing employee directories, planning and monitoring of training requirements and career development activities and skills, managing and reporting disciplinary matters and terminations, reviewing employment decisions, ascertaining and making decisions related to employees' fitness to work and workplace adjustments, making business travel arrangements, managing business expenses and reimbursements, facilitating business communications, negotiations, transactions and conferences, monitoring compliance with internal policies and procedures and other monitoring activities as required / allowed for by applicable laws (e.g. internal reporting systems), performing workforce analysis and planning, performing background checks as required / allowed for by applicable laws, etc.); **(b) carrying out aggregated segmentations, statistics and analysis regarding employees' activity data** (*e.g.* for projection of the interview processes, candidate sources, performance, etc.) in order to improve understanding of, and inform decisions about, the employee population in regards to, among others, talent recruitment, career planning and succession planning; **(c) supporting the management of the services provided by the Avature Group and its business operations** (*e.g.* managing and allocating company assets and human resources, operating, managing and securing IT and communication systems and infrastructure, office equipment and other property, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to manufacturing and other business activities, budgeting, financial management and

reporting, communications, managing mergers, acquisitions, and re-organizations or disposals, etc.); **(d) complying with applicable legal obligations and other requirements** (*e.g.* Labour and Social Security obligations, record keeping and reporting obligations, conducting audits, ensuring compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claim, etc.); and **(e) providing a wide variety of services to other Group Members** (*e.g.* IT technology and systems, payroll, Human Resources selection and management, internal audit and compliance, document destruction, document transport, as well as legal management and coordination services in certain areas such as data protection, etc.).

- In relation to employees' **special categories of personal data,** such 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 (Article 9.2(b)) 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 (Article 9.2(h)). Additionally, special categories of personal data may be processed for the provision of a wide variety of services to other Group Members (e.g. legal advisory services, labour 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 **employees' relatives'** personal data personal data 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 managing payroll benefits affecting personnel´s relatives.
- Transfers of **current and former job applicants'** personal data 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 **(a) managing recruitment activities generally** (*e.g.* evaluating applications and making hiring decisions, communicating with applicants in relation to the recruitment process and/or their application(s), etc); **(b) carrying out aggregated segmentations, statistics and analysis regarding candidate's activity data** (*e.g.* in preparation of the interview processes, candidate sources, etc.); **(c) managing membership for the Talent Community** (*e.g.* offering the possibility to voluntarily join the Talent Community and (only under consent) consider joiners for future job opportunities and send them job recommendations or other related information); **(d) complying with applicable legal obligations and other requirements** (*e.g.* conducting audits, ensuring compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claim, etc.); (**e) providing a wide variety of services to other Group Members** (*e.g.* IT technology and systems, Human Resources selection and management, internal audit and compliance, document destruction, document transport, as well as legal management and coordination services in certain areas such as data protection, etc.).

- Transfers of **customers, prospects, suppliers, providers, partners, business associates and advisors (including their employees, representatives and/or agents)**' personal 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 **(a) managing the contractual relationship with them generally** (*e.g.* performing agreements in place and /or taking steps to enter into such agreements, for business purposes and communications, establishing, renewing, maintaining or terminating the business relationships, providing access to Internet-based activities and our premises, maintaining business records, conducting auditing, accounting, financial and economic analysis, performing payment and related accounting functions, etc.); **(b) managing and ensuring security** (*e.g.* safeguarding IT infrastructure, office equipment and other property, etc.); **(c) managing business operations** (*e.g.* operating and managing the IT and communications systems, managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to manufacturing and other business

activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, and re-organizations or disposals, etc.); **(d) planning and executing marketing strategies generally** (*e.g.* marketing research, planning campaigns and developing marketing strategies, monitoring and reporting on the success of campaigns, etc.); **(e) complying with the applicable legislation** (*e.g.* commercial, tax, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claim, etc.); and **(f) providing a wide variety of services to other Group Members** (*e.g.* IT technology and systems, internal audit and compliance, document destruction, document transport, risk management, procurement of products and/or services, electronic invoicing, management of marketing and communication campaigns, as well as legal management and coordination services in certain areas such as data protection, etc.).

- Transfers of **website users**' personal data 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 **(a) managing the provision of services generally** (e.g. developing and providing the online features and content, managing websites, dealing with inquiries and requests, providing support, etc.); **(b) managing and ensuring security** (*e.g.* safeguarding IT infrastructure, ensuring the security and integrity of systems, servers and websites, etc.); **(c) carrying out aggregated segmentations, statistics and analysis** (*e.g.* understanding how the services are being used, improving and developing website and service features, enhancing performance and available support, etc.); **(d) planning and executing marketing strategies generally** (*e.g.* marketing research, planning campaigns and developing marketing strategies, monitoring and reporting on the success of campaigns, etc.); **(e) complying with the applicable legislation** (*e.g.* commercial, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claim, etc.); and **(f) providing a wide variety of services to other Group Members** (*e.g.* IT technology and systems, internal audit and compliance, management of marketing and communication campaigns, as well as

management and coordination services in certain areas such as data protection, etc.).

e. **Categories of data subjects concerned by the transfer:** Those categories are specified in Part I of the BCR. They included: current and former employees, contractors and temporary employees, employees' relatives, current and former job applicants, customers, prospects, suppliers, providers, partners, business associates and advisors, and website users.

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, contractors and temporary employees'** personal data: **(a) Personal and contact details** (*e.g*. first name, middle name, surname, mother's maiden name, title, gender, date of birth, nationality, national identification numbers (*e.g.* national ID number, Social Security Number, passport number, driver's license number and/or other government issued identification numbers), email address, home address, home and mobile telephone numbers, nationality, hobbies, etc.); **(b) Employment data including work history and contact details** (*e.g.* company provided email, desk and mobile telephone numbers, skype user, description of current position, title, salary plan, pay grade or level, unit/department, location, supervisor(s) and subordinate(s), employee identification number, employment status and type, terms of employment, employment contract, work history, re-hire and termination date(s), length of service, retirement eligibility, performance reviews and ratings (including feedback from managers, stakeholders and other people that work with the employee), promotions and disciplinary records, right to work / immigration data such as permits or visas, etc.); **(c) Talent, recruitment and application, education and training details** (*e.g.* details contained in letters of application and resume/CV, personal website or LinkedIn profile directly provided by employees, previous employment background and references, education history, professional qualifications, language and other relevant skills, details on performance management ratings, development plan and willingness to relocate, personal data derived from employees' participation in Avature Group's recruitment process such as, for example, those obtained during personal interviews and the emails exchanged with regarding applications or the conversations, etc.); **(d) Audio and visual information** (*e.g.* voice and likeness as captured in photographs, video or audio recordings in the context of interviews or meetings conducted over phone or via videoconference, etc.); **(e) Financial Information including payroll and compensation details** (*e.g.* bank account details, base salary, bonus, benefits, pay enhancement for dependents, salary step within assigned grade, details on stock options, stock grants and other awards, currency, pay frequency, effective date of current compensation, salary reviews, tax ID social security number and tax code, etc.); **(f) Work schedule data** (*e.g.* record of hours worked (where legally required / allowed for), records of holidays, personal days off, medical leaves and other leaves employees have

taken, and proof of the reasons (if applicable), overtime and shift work and termination date, etc.); **(g) Travel related data** (*e.g.* frequent flyer information (such as alliance airline program and frequent flyer number), usual pick-up and drop-off location, etc.); **(h) Security and IT details** (*e.g.* information captured through entry systems and security cameras, information captured through IT usage including access and authentication information, Internet browsing history, phone numbers dialled, documents and files stored on company systems or networks (including computer desktops), emails transmitted from and received on the company's email accounts (to the extent legally permitted), logs, IP address, successful and failed login attempts, information collected through cookies or other similar tracking technologies, etc.); and **(i) Any other information voluntarily provided by data subjects** (e.g. via complaints, enquiries, interests, etc.).

Also, **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 **employees' relatives' personal data**: **(a) Personal and contact details** (e.g. name, surname, contact details such as emergency contact number, etc.); **(b) Other information about the employees in relation or about their family where legally required / allowed for** (e.g. family group, name and other relevant information about children and other dependants (including them and/or their children's birth certificates), marital status, legal or de facto spouse, marriage certificate, etc.);.
- In relation to **current and former job applicants**' personal data: **(a) Personal and contact details** (*e.g.* first name, surname, country, state and city of residence, email address, home address, home and mobile telephone numbers, nationality, etc.); **(b) Employment data including work history** (*e.g.* current position, title, location and company and work history, salary plan, pay grade or level, right to work / immigration data such as permits or visas, etc.); **(c) Talent, recruitment and application, education and training details** (*e.g.* details contained in letters of application and resume/CV, personal website or LinkedIn profile directly provided by job applicants, previous employment background and references, education history, professional qualifications, language and other relevant skills, details on performance management ratings, development plan and willingness to relocate, personal data derived from job applicants' participation in Avature Group's recruitment process such as, for example, those obtained during personal interviews and the emails exchanged with regarding applications or the conversations, etc.); and (**d) Audio and visual information** (e.g. voice and likeness as captured in photographs, video or audio recordings in the context of interviews conducted over phone or via videoconference, etc.).
- In relation to **customers, prospects, suppliers, providers, partners, business associates and advisors' (including their employees, representatives and/or agents)** personal data: **(a) Personal and contact details** (*e.g.* name, surname, telephone number, email address, postal address, etc.); **(b) Professional details** (*e.g.* position / job title, company details, professional contact details, etc.); **(c) Contractual data** (*e.g.* purchase orders, invoices, contracts and other agreements that may contain personal data regarding these data subjects, etc.); **(d) Financial and payment information**

(*e.g.* bank account details, credit card details, etc.); **(e) Audio and visual information** (*e.g.* voice and likeness as captured in photographs, video or audio in the context of meetings conducted over the phone or via videoconferencing, or for security purposes (including information captured through entry systems and security cameras, etc.); **(f) IT information** (*e.g.* IP address, user ID, passwords, logs (including profile details) of Avature group websites or portals, etc.); and **(g) Other details about the professional relationship with Avature Group** (*e.g.* complaint data, shared communications, etc.).

- In relation to **website users'** personal data: **(a) Personal and contact details** (*e.g.* name, surname, telephone number, email address, postal address, etc.); **(b) Professional details** (*e.g.* position / job title, company details, professional contact details, etc.); **(c) IT information** (*e.g.* IP address, user ID, passwords, logs about usage (including profile details) of Avature group websites or portals, data collected via Avature application including data resulting from the access to users' camera and/or photo library (provided they expressly authorized such access) and other information users may provide that is useful for the future development of the app and for support purposes, etc.); (**d) Navigation and usage data** (*e.g.* information collected automatically from data subjects (i.e. through cookies or other similar technologies) regarding their use of websites, IP address, etc.); and **(e) Other details about their relationship with Avature Group** (*e.g.* queries, interests, shared communications, etc.).
- In relation to **current and former employees, contractors and temporary employees'** personal data: **(a) Personal and contact details** (*e.g.* first name, middle name, surname, mother's maiden name, title, gender, date of birth, nationality, national identification numbers (*e.g.* national ID number, Social Security Number, passport number, driver's license number and/or other government issued identification numbers), email address, home address, home and mobile telephone numbers, nationality, hobbies, etc.); **(b) Employment data including work history and contact details** (*e.g.* company provided email, desk and mobile telephone numbers, skype user, description of current position, title, salary plan, pay grade or level, unit/department, location, supervisor(s) and subordinate(s), employee identification number, employment status and type, terms of employment, employment contract, work history, re-hire and termination date(s), length of service, retirement eligibility, performance reviews and ratings (including feedback from managers, stakeholders and other people that work with the employee), promotions and disciplinary records, right to work / immigration data such as permits or visas, etc.); **(c) Talent, recruitment and application, education and training details** (*e.g.* details contained in letters of application and resume/CV, personal website or LinkedIn profile directly provided by employees, previous employment background and references, education history, professional qualifications, language and other relevant skills, details on performance management ratings, development plan and willingness to relocate, personal data derived from employees' participation in Avature Group's recruitment process such as, for example, those obtained during personal interviews and the emails exchanged with regarding applications or the conversations, etc.); **(d) Audio and visual information** (*e.g.* voice and likeness as captured in photographs, video or audio recordings in the context of interviews or meetings

conducted over phone or via videoconference, etc.); **(e) Financial Information including payroll and compensation details** (*e.g.* bank account details, base salary, bonus, benefits, pay enhancement for dependents, salary step within assigned grade, details on stock options, stock grants and other awards, currency, pay frequency, effective date of current compensation, salary reviews, tax ID social security number and tax code, etc.); **(f) Work schedule data** (*e.g.* record of hours worked (where legally required / allowed for), records of holidays, personal days off, medical leaves and other leaves employees have taken, and proof of the reasons (if applicable), overtime and shift work and termination date, etc.); **(g) Travel related data** (*e.g.* frequent flyer information (such as alliance airline program and frequent flyer number), usual pick-up and drop-off location, etc.); **(h) Security and IT details** (*e.g.* information captured through entry systems and security cameras, information captured through IT usage including access and authentication information, Internet browsing history, phone numbers dialled, documents and files stored on company systems or networks (including computer desktops), emails transmitted from and received on the company's email accounts (to the extent legally permitted), logs, IP address, successful and failed login attempts, information collected through cookies or other similar tracking technologies, etc.); and **(i) Any other information voluntarily provided by data subjects** (e.g. via complaints, enquiries, interests, etc.).

Also, **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 employees' relatives' personal data: **(a) Personal and contact details** (e.g. name, surname, contact details such as emergency contact number, etc.); **(b) Other information about the employees in relation or about their family where legally required / allowed for** (e.g. family group, name and other relevant information about children and other dependants (including them and/or their children's birth certificates), marital status, legal or de facto spouse, marriage certificate, etc.);.