Binding Corporate Rules ("BCR")

Document Ref.	
Version:	**5**
Dated:	**19 December 2019**

Revision History

Version	Date	Revision Author	Summary of Changes
1	20th May 2018	Waterwhale Europe	Initial document.
2	20th May 2019	Waterwhale Europe	Co-reviewers comments
3	2nd July 2019	Waterwhale Europe	Consolidated draft
4	6th November 2019	Waterwhale Europe	Consolidated draft-ITS comments
5	19th December 2019	Waterwhale Europe	Consolidated draft-Art.8.4

FUJIKURA AUTOMOTIVE EUROPE S.A.U.
Binding Corporate Rules ("BCR")

Content

1. INTRODUCTION 3

2. SCOPE 4

2.1 GEOGRAPHICAL SCOPE 4
2.2 MATERIAL SCOPE 4

3. DEFINITIONS 4

4. PRINCIPLES APPLICABLE TO FAE GROUP PROCESSING OF PERSONAL DATA 6

6. RIGHTS OF THE DATA SUBJECTS 9

6.1 Transparency and information rights 9
6.2 Rights to access, rectification, erasure, restriction, objection and right to data portability 10
6.3 Right to present claims to the Internal Claims Management Process 13

7. RIGHTS OF THE DATA SUBJECTS AS THIRD-PARTY BENEFICIARIES OF THE BCR 13

8. BCR: INTERNAL EFFICIENCY 14

10. DATA PROTECTION GUARANTEES 15

11. ACCOUNTABILITY 18

12. LIABILITY OF THE MAIN ESTABLISHMENT OF THE GROUP 19

13. FINAL PROVISIONS 20

14. CONTACT DETAILS 21

1. INTRODUCTION

FUJIKURA AUTOMOTIVE EUROPE S.A.U. (henceforth, "FAE") is the parent company of a group of companies working on a single economic activity: the production of cables for the automotive industry. FAE and its subsidiaries are fully committed to protecting personal data, for which reason the Group took the decision to pass some "*Binding Corporate Rules*" (**BCR**), with the purpose of regulating intra-group international data transfers. International data transfers are defined as data processing which involves a flow of such data from countries located in the European Economic Area (EEA) to recipients located in countries outside EEA, whether this is data transfer between controllers, or a data transfer performed by a controller to a processor, which processes the data on behalf of the controller.

The FAE Group is an eminently multinational business network, hence for its business to be conducted properly new centralised data storage systems needed to be created which would be accessible from the various companies in the Group. There would also need to be the ability to transfer data between these companies to achieve optimum efficiency and productivity.

These binding corporate rules were approved by the FAE Board of Directors to perform international transfers from companies in the group located within the European Economic Area to companies from the same business or legal group working on a single economic activity and located outside the European Economic Area. These binding corporate rules include all the key principles and enforceable rights and comprise a suitable guarantee for personal data transfers which are undertaken within the business group.

Ensuring the security and privacy of personal data is of singular importance to the Group. The FAE BCR are intended to ensure that personal data is adequately protected when collected, used and/or transferred among the companies in the Group.

Given its importance, the FAE Board of Directors will ensure that all the FAE Group employees apply and take into account the rules detailed in the present document when collecting, holding, using, disclosing, transferring or otherwise handling personal data. In case of violation of these BCR, the procedure to impose a disciplinary sanction shall apply. The particular sanction will be imposed pursuant to the corresponding labour legislation, according to the qualification of the infringement.

The present BCR are developed and implemented in accordance with Regulation (EU) 2016/679 of the European Parliament and the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and the free circulation of such data, which supersedes Directive 95/46/EC (General Data Protection Regulation, **GDPR**).

Likewise, these BCR are part of the Privacy and Personal Data Protection Policy of FAE Group; particularly, they are integrated in Annex G of such Policy, called *Procedure for International Transfer of Personal Data.*

2. SCOPE

2.1 Geographical scope

FAE wants to ensure a consistent approach within the entire FAE organisation where Personal Data are being Processed. Consequently, all FAE Entities, whatever their location or legal jurisdiction, are bound by these BCR.

The BCR are applicable to intra-group data processing and transfers. Specifically, geographical scope refers to any personal data processed by FAE or any of its subsidiaries within and transferred outside of the EEA.

Annex I contains a list detailing all the members of the group (FAE and subsidiaries) to which these rules are applicable.

2.2 Material scope

The type of personal data processing is performed through automatic and manual supports. The personal data which are processed by the group are related, among others, to human resources, management and candidates. Annex II contains a detailed description of these processing activities and the categories of personal data that are subject to international data transfer.

3. DEFINITIONS

In these BCR, the following terms shall be interpreted in accordance with the definitions in the GDPR:

- **FAE Group:** Fujikura Automotive Europe, S.A.U. and each of its subsidiaries.
- **Main establishment of the Group**: the corporate headquarters of the FAE Group, Fujikura Automotive Europe S.A.U., is in Zaragoza (Spain).
- **Members of the Group**: all the companies in the FAE Group detailed in the list in Annex I.
- **European Economic Area**: an association of European countries who have entered into a free trade agreement. This currently comprises the 28 Member States of the European Union plus Iceland, Liechtenstein and Norway.
- **Personal data**: any information relating to an identified or identifiable natural person (a Data subject);

- **Data subject:** an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. As such, Data Subjects include employees (human resources file), clients, suppliers and contact persons (management file) and applicants for job vacancies (candidates file).
- **Processing of personal data**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Restriction of processing**: the marking of stored personal data with the aim of limiting their processing in the future;
- **Pseudonymisation**: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- **Controller**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;;
- **Processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Subcontractor:** the natural or legal person who signs a contract to undertake part or all of the contractual obligations of a data processor;
- **Recipient**: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **Third party**: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons

who, under the direct authority of the controller or processor, are authorised to process personal data;

- **Consent of the data subject**: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **Personal data breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **Special categories of personal data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- **Biometric data:** personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- **Data concerning health**: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- **Binding corporate rules**: the personal data protection policies assumed by a controller or processor located within a Member State for transfers or a series of transfers of personal data to a controller or processor in one or more third countries, within the business or legal group working on a single economic activity;
- **BCR:** throughout this document this expression alludes to the Binding Corporate Rules at the FAE Group;
- **Data exporter:** FAE Group subsidiaries within the EEA which, as controllers, transfer personal data to other Group subsidiaries in third countries outside the EEA;
- **Data importer:** FAE Group subsidiaries in third countries outside the EEA that receive data from data exporters;

4. PRINCIPLES APPLICABLE TO FAE GROUP PROCESSING OF PERSONAL DATA

Under the provisions of the General Data Protection Regulation, international transfers within the scope of the BCR must be in harmony with the following principles that every member of the FAE group is committed to meeting

and respecting in their international data transfers, as well as in the processing of personal data within each company of the group:

- **Basis for personal data processing:** personal data can only be processed if at least one of the following conditions is met:

  * The data subject has given consent to the processing of his or her personal data for one or more specific purposes. At every member of the FAE group, this is the basis for processing when collecting *curricula*.
  * It is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. At every member of the FAE group, this is the basis for processing data from companies, suppliers and clients in terms of data from the persons involved.
  * It is necessary for compliance with a legal obligation to which the controller is subject. At every member of the FAE group, this is the basis for processing data to be sent to the tax authorities, Social Security or other Public Administrations.
  * It is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data – particularly if the data subject is a child. At every member of the FAE group, this is the basis for processing video surveillance, where the legitimate interest is protecting the safety of people and their property.

- Processing of special categories of personal data: the processing of special categories of personal data **is forbidden except when:**

  * the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except when the applicable legislation prohibits it, or
  * processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;, or
  * processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent, or
  * processing is necessary 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 on the basis of Union or Member State law, or

* processing covers data that the data subject has clearly made public or that is necessary for recognising, exercising or defending a right in a legal process.

- **Lawful, fair and transparent:** data must be processed lawfully, fairly and transparently with regard to the data subject.
- **Purpose limitation:** personal data will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data minimisation and accuracy:** data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Equally, they should be accurate and, if necessary, up to date, with all reasonable measures adopted to eliminate or rectify any imprecise data without delay.
  Retention period limit: every member of the FAE Group will ensure that personal data are kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Data protection by design and by default:** in line with the principles established in its Privacy Policy, every member of the FAE Group will ensure that data protection principles by design and by default are effectively contemplated throughout the life cycle of personal data processing for any developments or projects undertaken by every member of the Group.
- **Right to information and transparency:** personal data will be processed transparently, making all opportune information available to the data subjects, as per the terms of clause 6.1.
- **Individual automated decisions:** data subjects have the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning him or her or similarly affects him or her. No member of the FAE Group will take this type of decision.
- **Security and confidentiality:** All the members of FAE Group will implement suitable organisational and technical measures to protect personal data against accidental or deliberate destruction, accidental loss or alteration, disclosure and unauthorised access and against any other illegal processing of these data. Access to and processing of these personal data shall be limited to duly authorised and trained personnel, as per the requirements for data privacy and protection. (Security and confidentiality measures are detailed in clause 10).
- **Restrictions on current and further data transfer by processors and controllers not pertaining to the FAE Group:** every member of the FAE Group will set the conditions that transfers to outside organisations must meet to ensure suitable protection of personal data, as detailed in clause 10.3.
- **Processing by data processors which are members of the FAE Group:** when the local controller with responsibility for personal data instructs

another company within the FAE Group to process these, the provisions of clause 10.2 will be followed.

- **Notification of data security breaches:** in order to have the very highest level of protection for personal data, every member of the FAE Group has established a procedure for attending to notifications of data security breaches, which is detailed in clause 10.4.

6. RIGHTS OF THE DATA SUBJECTS

6.1 Transparency and information rights

a. Transparency with regard to the BCR

In order to process data fairly, every member of the FAE Group must be transparent in collecting and then processing data.

The BCR are available to all data subjects: they are published on the corporate website and on the intranet for companies pertaining to the FAE Group. Likewise, any data subject can request a copy of the BCR from the "Local Data Manager" or the "Data Protection Officer".

b. Information rights vis-à-vis the data subjects

When the personal data is collected from the data subject (article 13 GDPR), he will be provided with the following information when the data is collected:

- the identity and contact details of the controller and, where applicable, its representative,
- contact details of the "*Data Protection Officer*";
- the purposes of the processing for which the personal data are intended and the legal basis for the processing;
- when the processing is based on point (f) of Article 6 (1) GDPR, the legitimate interests pursued by the controller.
- the recipients or categories of recipients of the personal data, if any;
- that their personal data may be subject to an international data transfer by the controller;
- that should their personal data be subject to an international data transfer, the transfer will be governed by the present Binding Corporate Rules (BCR); in these cases, information on their third party beneficiary rights with regard to the processing of their personal data and on the means to exercise those rights, the clause relating to the liability and the clauses relating to the data protection principles shall be provided too;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

When the personal data has not been collected from the data subject (article 14 GDPR), the previous information, as well as the categories of personal data concerned and the source from which the personal data originate, will be communicated as soon as possible and, no later than a month after its collection, unless the data must be used for a communication or if he plans on transferring them to another data processor, in these cases the information must be provided immediately when the communication is made or the data is transferred first time.
In these cases where the data are not collected from the data subject, it won´t be necessary to provide this information when it can be proved that it is impossible, would entail a disproportionate effort or the data subject already has this information.

In any case, the information will be provided in writing and it will be understandable and easily accessible using plain and clear language.

6.2 Rights to access, rectification, erasure, restriction, objection and right to data portability

Data subjects have the rights to access, rectification, erasure and object available to them for all personal data relating to them.

- The **right to access** implies that the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
  (a) the purposes of the processing;
  (b) the categories of personal data concerned;
  (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
  (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;

If requested by the data subject, the controller shall provide a copy of the personal data undergoing processing. For any further copies, a reasonable fee based on administrative costs will be charged.

– The **right to rectification** gives the data subject the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

– The **right to erasure (right to be forgotten)** means the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2) GDPR, and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to Article 21(1) GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) GDPR;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) GDPR.

– According to the **right to restriction of processing,** the data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
Likewise, a data subject who has obtained restriction of processing shall be informed before the restriction of processing is lifted.

- The right to **data portability** means the data subject has the right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
  - the processing is based on consent or on a contract; and
  - the processing is carried out by automatic means.

  In exercising this right, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
- The data subject can exercise the **right to object** under special personal circumstances, where their legitimate interest is of higher value than the legitimate interest of the controller for processing these personal data. In that case, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance to the above, to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

All the members of the Group have established a local level way to proceed in these cases to ensure the aforementioned rights. A request from a data subject for any of these rights to be exercised shall be managed based on these procedures, providing a response without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests, informing the data subject of the extension within one month of receipt of the request, together with the reasons for the delay.

Documents in various formats corresponding to the exercising of these rights will be made available to the data subject.

Should the request be denied on the grounds it is unfounded, the data subject may still appeal to the Internal Claims Management Process, detailed in clause 8.6.

6.3 Right to present claims to the Internal Claims Management Process

Data subjects may present claims or complaints which reference non-compliance with one or more of the rules established in this document by way of the internal claims department created by Fujikura; these will be processed under the terms of clause 8.6.

7. RIGHTS OF THE DATA SUBJECTS AS THIRD-PARTY BENEFICIARIES OF THE BCR

As third-party beneficiaries, the data subject has legal resources available should there be a breach of the provisions of the BCR and by legal provisions for personal data protection.

In particular, data subjects are able to enforce the provisions included in clause 4 (principles applicable to FAE Group processing personal data), clause 6 (rights of the data subjects), clause 8.6 BCR (Internal Claims Management Process), clause 10 BCR (Data Protection Guarantees), clause 11 BCR (Accountability), and clause 13.1 (Actions to take if national legislation impedes fulfilment of the BCR) and clause 13.2 (mutual assistance and cooperation with data protection authorities).

Data subjects may exercise these rights in writing or orally to the corresponding FAE Group subsidiary through the *Local Data Manager* or directly before the *Data Protection Officer*. A written response from the person contacted to the data subject's request will be sent without undue delay and in any event within one month of receipt of the request. Such period may be extended by two further months, taking into account the complexity and the number of requests, in which case the data subject will be informed of such extension.

Additionally, the data subject has legal remedies to request restoration of the damage caused and, where applicable, compensation for material and non-material damages when the legal provisions for personal data protection or the provisions of these BCR are breached.

Actions taken against a controller or processor may be brought by the data subjects before the courts of the Member State in which the controller or processor is based, before a Supervisory Authority of a European Union member in the habitual place of residence or place of work of the data subject, or in the country in which the breach

has occurred. The data subject may also choose to exercise these actions before the courts of the Member State in which they reside.

Furthermore, actions with regard to acts of members of FAE Group located outside the EEA may be directed to the main establishment of the Group, as provided in clause 12.

8. BCR: INTERNAL EFFICIENCY

8.6 Internal Claims Management Process

Parties who wish to present claims regarding non-compliance with the BCR by a company in the Group or with regard to any other related matter are free at any time to contact the *Data Protection Officer* at dpo@eu.fujikura.com or person or body dealing with claims about data protection in any of the companies of the Group at info@eu.fujikura.com or, where applicable, the relevant local contact person for data protection at the corresponding Group company (the corresponding *Local Data Manager,* which will be the human resources manager of the respective company). Claims should be presented in writing, with email correspondence considered acceptable. This internal process is alternative to the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy, which the data subjects may exercise at any time.

The data subject will be given written confirmation their claim has been received by the organisation contacted, information about which will immediately be passed on to the *Data Protection Officer* should the claim is not submitted directly before him/her. In any case, the claim must be processed by the *Data Protection Officer* in collaboration with the corresponding *Local Data Manager* within one (1) month of receiving the claim. This timeframe may be exceeded by up to a maximum of two (2) months for reasons of complexity or number of requests. If this period has passed and no reasoned response has been received from the corresponding FAE Group company, the data subject may resort to the Relevant Courts or corresponding Supervisory Authority, detailing the facts of the matter.

Once the *Data Protection Officer* has received the claim from the data subject, they shall check the facts, requesting, as required, all pertinent information from the corresponding *Local Data Managers* or, where it concerns non-compliance by the FAE Group as a whole, from the department where the supposed irregularity has taken place.

Department personnel participating alongside the *Local Data Managers* and the *Data Protection Officer* in the claims management process will be given the level of independence appropriate to the exercising of their role.

The claims management process concludes with a resolution which will be sent in writing to the person who began the process. In case the complaint is considered as justified, a reasonable compensation proportional to the damage caused will be offered

to the claimant, if any, and internal actions will be taken, including the application of disciplinary sanctions according to the corresponding internal procedures and policies.

Should this resolution fail to satisfy the claimant, then this person may petition the Relevant Courts or corresponding Supervisory Authority, requesting the resolution be reviewed and their rights and legitimate interests protected.

If an investigation is launched, all the members of the Group are required to cooperate with the country's Supervisory Authorities and to respect their opinions.

10. DATA PROTECTION GUARANTEES

10.1 Security and confidentiality

1. One of the main priorities at every member of the FAE Group is to ensure personal data is protected adequately and effectively against any breaches of the legally-established principles enshrined in these BCR. Hence:

- Each local controller must take appropriate technical and organisational measures to ensure data security, protecting the personal data from any accidental or illegal elimination, alteration, accidental loss and any unauthorised usage, disclosure or access. These measures must ensure – in accord with current technical expertise and the cost of applying this – a level of security appropriate to the risks presented by processing and the nature of the data which needs protecting.
- Likewise, to guarantee data security, the FAE Group decided to forbid transfers to subcontractors of any data included in international transfers. In exceptional cases, the main establishment of the Group may give written authorisation for these data transfers, in which case contracts will be drawn up with the corresponding subcontractors to regulate the matter. The mentioned contracts will include provisions to make the BCR binding for the respective subcontractors. In any case, safeguards provided by article 46 GDPR shall be respected, according to the Annex G of the Privacy and Personal Data Protection Policy.
- To ensure adequate technical and organisational measures for data protection, the FAE Group introduced its so-called Privacy and Personal Data Protection Policy, which is binding throughout every member of the Group. The security measures provided, in addition to general assurances, refer to servers, computers, networks, communication links and applications installed at the various FAE Group companies.
- The specific measures introduced to ensure suitable personal data protection include controls for: admission, systems access, data access, transfer, entry, work, availability and segregation.

2. With the intention of ensuring data processing confidentiality, only those personnel who are specifically briefed through the training programmes on data protection and privacy under these BCR and whose work so requires them may gather, process or use personal data. Access authorisation for each individual employee will be

restricted in accordance with the type and scope of their specific tasks at the respective member of the FAE Group.

Thus, no employee may use the personal data for which the company is responsible for any purpose other than pursuing the duties or responsibilities implicit in their work. Equally, they may not transfer or provide access for unauthorised persons to personal data. Such people are understood, aside from unauthorised people not pertaining to the organisation, to be other employees who do not require personal data to perform their own specific tasks. Should any employee fail to meet these obligations, they shall be disciplined appropriately.

This obligation to confidentiality remains in place even after the employee in question no longer works for the company.

3. In any case, extra protection shall be provided for special categories of personal data, such as sensitive information.

10.2 Processing by processors that are FAE Group organisations

When a local controller with responsibility for personal data instructs another company of the Group to process these data, the following precautions will be taken:

- Firstly, it must not be forgotten that when personal data is processed by processors that are FAE Group organisations, the General Data Protection Regulation is applicable to them if both parties are within the EEA, or the BCR when the situation requires an international data transfer. Hence, the requisite guarantees under the terms of the GDPR will be put in place.

- The processor shall provide sufficient guarantees to implement appropriate technical and organisational measures to the controller, in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subject.

- The processor shall not engage another processor without prior specific authorisation of the controller.

- Processing by the processor shall be governed by a contract, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The following duties must also be covered in the agreement that must require the data processor to:
    - processes the personal data only on documented instructions from the controller
    - ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
    - Take all appropriate technical and organizational measures required to guarantee an acceptable level of security.
    - May not contract another data processor (subprocessor), unless exceptional cases, as provided in previous section 10.1 and, when contracting, it must agree with the subprocessor the same terms and conditions relative to data protection.

- Assist the data controller with appropriate technical and organizational measures whenever possible for the fulfilment of the duty of the data controller to answer data subject's requests exercising their rights.
- Assist the data controller with the fulfilment of its obligations regarding security of processing, personal data breaches and data protection impact assessments.
- At the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless the applicable law requires storage of the personal data.
- Make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR regarding data processors and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

- Once the work for which the processing is required has been completed, the organisation must delete all the transferred data or where legally permitted to retain them, this shall be done using appropriate technical and organisational measures to protect them against any breach.

10.3 Restrictions on current and further data transfer to processors or external controllers

When a local controller requests an organisation not pertaining to the FAE Group to process personal data, the following conditions are applicable:

a) If this third-party organisation lies within the EEA or in a country the EU Commission deems to have a suitable level of protection, then it must undertake to sign a written agreement whereby it shall only work in accordance with the instructions from the controller and will implement suitable measures to ensure security and confidentiality. *Local Data Managers*, in concert with the *Data Protection Officer*, may provide templates of the appropriate clauses to the corresponding controller.

b) Transferring personal data from any FAE Group company to a company or officer located outside the EEA that has not been declared as possessing a suitable level of protection will only be permitted if adequate guarantees are given under article 46 of the General Data Protection Regulation.

10.4 Notification of Personal Data Breaches

This procedure is to be used when there is an incident of any type resulting in, or believed to have resulted in a breach of security leading to the accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (security breach).

The GDPR requires that all incidents affecting personal data that involve a risk to the rights and freedoms of natural persons be reported to Supervisory Authorities without delay and, where possible, within 72 hours of becoming aware of such. Should the 72-hour period not be met, reason must be given for the delay.

Likewise, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall communicate it to data subjects without undue delay.

These short notification periods demand a quick response in the moment when the possibility of a security breach is detected, which implies the importance of its knowledge by all the members of FAE group and its employees since, if the case occurs, the instructions contained in the personal data security breach notification and management procedure must be observed (*See regulations in Annex H in the FAE Privacy and Personal Data Protection Policy*).

Any personal data breaches shall be properly documented, including the facts relating to the personal data breach, its effects and the remedial action taking. This documentation shall be made available to the relevant Supervisory Authority on request.

In addition, all the members of FAE Group shall communicate any security breaches to the main establishment of the Group.

11. ACCOUNTABILITY

According to the accountability principle, every members of FAE Group shall be responsible for and able to demonstrate compliance with the BCRs. In compliance with GDPR Article 30 and as an indicator of the willingness of Fujikura Group to comply with the data protection regulation, all the members of FAE Group maintain a Record of Processing Activities. This includes an analysis of each personal data processing action and, where necessary, any possible implication for international data transfers. In particular, the Records of Processing Activities contain the name and contact details of the controller and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures. These Records of Processing Activities shall be maintained in writing, including in electronic form, and shall be made available to the relevant Supervisory Authority on request.

Likewise, all necessary risk analyses have been performed, qualifying the risks for the data which will be transferred internationally at low and medium levels, meaning there has not been obligation to perform data protection impact assessments (Article 35 of the GDPR). However, in case of planning any new processing or if there is a change of the risk represented by processing operations which may imply the necessity to perform an a data protection impact assessment pursuant to article 35 GDPR, the corresponding entity shall perform it. In such a case, the entity shall consult the relevant Supervisory Authority prior to processing, pursuant to article 36 GDPR.

Likewise, bearing in mind the state-of-the-art, the cost and type of application, scope, context and purposes of the processing, and the risks and implications that processing entails for the rights and freedoms of people, the FAE Group applies suitable technical and organisational measures to protect the rights of the data subjects, such as data pseudonymization and minimization.

12. LIABILITY OF THE MAIN ESTABLISHMENT OF THE GROUP

The main establishment of the Group, based in Spain, assumes the liability arising from non-compliance with the BCR by the members of the Group outside the EEA and the data subject will have the rights and remedies against it as if the violation had been caused by them in the European Union.

The burden of proof lies with the main establishment of the Group, which must show that the member of the Group located outside the EEA is not responsible for the non-compliance with the BCR upon which the affected party's claim is based. Should non-compliance be proved, the Group will undertake all necessary measures to repair any material or non-material damages resulting from the violation, paying the corresponding compensation to the affected parties, where applicable.

The courts of the EU Member States or other competent State authorities shall have jurisdiction over cases of non-compliance by a member of the Group from outside the EEA. The data subjects may present their claims:

- before a Supervisory Authority of a European Union member in the habitual place of residence or place of work of the data subject, or in the country in which the breach has occurred, or before the Spanish Supervisory Authority (main establishment of the Group office), at their choice.
- before the courts of the Member State in which the controller or processor has an establishment, or the courts of the Member State in which the data subject has his or her habitual residence, or before the Spanish courts (main establishment of the Group office) , at their choice. .

13. FINAL PROVISIONS

13.1 Actions to take if national legislation prevents the group from complying with the BCR.

When a Group company has reason to believe that the legislation applicable to them will prevent the company from complying with the BCR obligations and will have a notable effect on the guarantees provided therein, it must immediately inform the main establishment of the Group and the relevant Authority (except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation)..

Furthermore, if there is a conflict between national legislation and the commitments in the BCR, the main establishment of the Group will take a reasoned decision on the actions to pursue, informing in any case the Relevant Data Protection Authority (in this case, the Spanish Supervisory Authority). This includes any legally binding request for disclosure of the personal data by a law enforcement authority or state security body. In such a case, the competent Supervisory Authority should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation).

If in specific cases the suspension and/or notification are prohibited, the requested BCR member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested BCR member is not in a position to notify the competent Supervisory Authorities, it must annually provide general information on the requests it received to the competent Supervisory Authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

In any case, transfers of personal data by a BCR member of the group to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

13.2 Mutual assistance and cooperation with Supervisory Authorities

All the members of FAE Group will cooperate with and support each other in the management of requests or complaints from individuals and investigations by Data Protection Authorities.

Likewise, they are committed to working with the Supervisory Authorities and following their advice, as well as accepting to be audited by them, on any matter related to the application or interpretation of the BCR.

13.3 Links between the BCR and local legislation

Personal data processing is governed by the applicable local legislation, where this demands a higher level of protection than that established under the BCR. Each member of the Group will undertake to check that the BCR conform to local legislation and should said legislation provide a lower level of protection than the BCR, then this latter will be applied.

13.4 Entry into force and transitional period

The BCR will enter into force on 12th March 2020, for an undefined length of time.

The Board of Directors may agree to establish an additional transitional period enabling all members of the FAE Group to adapt fully to the requirements detailed in this document. International data transfers will not be performed under these BCR during such transitional period.

14. CONTACT DETAILS

Data subjects may send their queries or complaints to the corresponding "*Local Data Managers*" or to the FAE Group "*Data Protection Officer*" at the following address:

Fujikura Automotive Europe S.A.U.

"Data Protection Officer" dpo@eu.fujikura.com

Avenida de Ranillas nº3

Edificio Dinamiza 3 A, planta 1ª, oficina i

50018 – Zaragoza, Spain