APTIV

DATED JANUARY 26, 2026

APTIV
BINDING CORPORATE RULES
(BCR)

Published: January 2026

TABLE OF CONTENTS

BACKGROUND

1. Aptiv Group, is a global technology and mobility company serving the automotive sector with offices worldwide. In order to share and transfer Personal Data between the entities in the Aptiv Group, Aptiv has decided to adopt Binding Corporate Rules ("**BCR**").

2. Aptiv Global Operations Limited ("**AGOL**"), located in Dublin, Ireland has delegated authority and primary liability for compensation claims, demands, and/or actions related to non-compliance with the BCR by a Participating Company located outside of the EEA.

3. The Privacy Office (as defined below) is in charge of coordinating compliance with the General Data Protection Regulation ("**GDPR**") within the Group as well as adopting and implementing the BCR at EEA level.

1. DEFINITIONS

The terms and expressions in capital letters used in the BCR shall have the meaning as set forth below. Words in singular include the plural and vice versa.

Notwithstanding the above, these terms and expressions shall always be interpreted in accordance with the GDPR.

(a) "**Adoption Agreement**" means the adoption agreement, which the Participating Companies sign (either directly or through an Adherence Agreement) to adopt the BCR.

(b) "**AGOL**" means Aptiv Global Operations Ltd, the EEA headquarters of Aptiv, located at 5 Hanover Quay, Grand Canal Dock, Dublin 2, registered in Ireland under the registration number 574123.

(c) "**Applicable Law**" means any applicable law, statute, bye law, regulation, order, regulatory policy (including any requirement or notice of any Supervisory Authority), guidance, guidelines or industry code of practice, rule of court or directives, delegated or subordinate legislation in force from time to time.

(d) "**Aptiv**" or "**Aptiv Group**" means all Aptiv's technology and mobility solutions companies, including all Participating Companies.

(e) "**Aptiv Privacy Program Standards**" is Aptiv's organisational document for the Aptiv Privacy Program.

(f) "**BCR**" means these Binding Corporate Rules for Aptiv as a Controller and an Internal Processor and the appendices.

(g) "**BCR Lead Supervisory Authority**" means the Irish Data Protection Commission which acts as the lead Supervisory Authority for the purposes of Aptiv's BCRs.

(h) "**Competent Supervisory Authority**" means the Supervisory Authority competent for the Participating Company exporting Personal Data and "**Competent Supervisory Authorities**" shall be construed accordingly.

(i) "**Concerned Supervisory Authority**" means a Supervisory Authority in a country from which a transfer made by a Participating Company takes place pursuant to the BCR, and "**Concerned Supervisory Authorities**" shall be construed accordingly.

(j) "**Consent**" means any freely given, specific, informed and unambiguous indication by which the Data Subject signifies their agreement to Personal Data relating to them being Processed.

(k) "**Controller**" means 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.

(l) "**Corporate Internal Audit**" means Aptiv's global internal audit team.

(m) "**Data Subject**" means an identified or identifiable natural person, which is a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific

to his physical, physiological, mental, economic, cultural or social identity.

(n) "**EEA**" means the European Economic Area.

(o) "**EU**" means the European Union.

(p) "**Executive Champions**" means the Chief Compliance Officer, the Chief Information Officer and the Chief Human Resources Officer.

(q) "**External Processor**" means a Processor which is not an Aptiv Group company.

(r) "**GDPR**" means the European Union Regulation 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.

(s) "**Internal Processor**" means a Processor which is a Participating Company and which is acting on behalf of a Controller that is also a Participating Company.

(t) "**Member State**" means a member state of the EU and/or the EEA.

(u) "**Model Clauses**" means the contractual clauses approved by the European Union Commission in the Annex to Commission Implementing Decision (EU) 2021/914 and any successors or replacements thereto.

(v) "**Participating Company**" means an Aptiv Group company that has signed the Adoption Agreement or an Adherence Agreement and acts as: (i) a Controller; or (ii) an Internal Processor. A list of these companies is set out at Schedule 2 and "**Participating Companies**" refers to all these companies collectively.

(w) "**Personal Data**" means any information which may identify, directly or indirectly, a natural person, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The Personal Data Processed by Aptiv pursuant to the BCR are set out in Schedule 3 (Description of Data Processing Activities).

(x) "**Personal Data Breach**" means 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.

(y) "**Privacy Liaison**" means a designated role with data protection responsibility that acts as a liaison between the Privacy Office and a single Aptiv company or across a number of functions or Aptiv entities in a particular region.

(z) "**Privacy Leader**" means an experienced Aptiv employee within the Aptiv Group who is responsible for managing business awareness and

compliance with applicable data protection laws and Aptiv privacy policies, procedures and guidelines, especially the BCR at the Aptiv Group level. The contact details of the Privacy Leader can be found in Schedule 1 (Privacy Office).

(aa) "**Privacy Office**" means the function within the Aptiv Group which coordinates the global data protection and privacy compliance at the Aptiv Group level and which has overall responsibility for designing, developing and maintaining a system of procedural documents (policies, directives, and work instructions) that ensure that Participating Companies are proactively managing data protection and notably GDPR and BCR compliance. The Privacy Office benefits from a high level of independence within the Aptiv Group. The contact details of the Privacy Office can be found at Schedule 1 (Privacy Office).

(bb) "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and "**Process**" and "**Processed**" shall be construed accordingly.

(cc) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller, which shall include Internal Processors and External Processors.

(dd) "**Recipient**" means a natural or legal person to whom Personal Data are disclosed.

(ee) "**Relevant Employees**" means Aptiv employees that handle Personal Data in the ordinary course of the performance of their role.

(ff) "**Special Categories of Personal Data**" means Personal Data revealing, directly or indirectly, the racial or ethnic origin, political, philosophical or religious 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.

(gg) "**Supervisory Authority**" means the competent independent Supervisory Authority established in each Member State pursuant to Article 51 of the GDPR and "**Supervisory Authorities**" shall be construed accordingly.

(hh) "**Supplier Code of Conduct**" means the Aptiv Supplier Code of Conduct which may be amended from time to time.

(ii) "**Technical and Organizational Measures**" means the technical, physical and organizational measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of Personal Data over a network, and against all other unlawful forms of Processing, and includes Aptiv's Cybersecurity Policy.

(jj) "**Third Party**" means any natural or legal person, public authority, agency or body other than the Data Subject, the Controller, the Processor and persons who, under the direct authority of the Controller or Processor, are authorised to Process Personal Data.

2. SCOPE AND APPLICATION OF THE BCR

2.1 Material scope

The BCR applies to all Processing of Personal Data by Participating Companies acting as a Controller or Internal Processor in relation to Aptiv employees, employees of vendors and customers and visitors to Aptiv premises or websites for the purposes set out in Schedule 3. For the sake of clarity, the BCR does not apply to Aptiv as a Processor for services provided to its customers.

The BCR will apply to all Data Subjects whose Personal Data are transferred within the scope of the BCR from a Participating Company under the scope of application of Chapter V of the GDPR.

2.2 Geographical scope

The BCR applies to all transfers of Personal Data between the Participating Companies. For more information see Schedule 3 (Description of Processing Activities).

2.3 Compliance with the BCR

No transfer of Personal Data shall be made to an Aptiv company until the company is effectively bound by the BCR, becomes a Participating Company and can deliver compliance with the BCR unless alternative appropriate safeguards to govern the transfer of Personal Data are in place such as Model Clauses.

2.4 Withdrawal

Upon withdrawal of a Participating Company from the BCR, the Participating Company and any Internal or External Processor shall delete or return all the Personal Data Processed pursuant to the BCR and delete the copies thereof according to the Group's then-applicable data retention and disposal policies. If Applicable Law in the third country requires the Participating Company or any Internal or External Processor to continually store the Personal Data, then the Participating Company and any Internal or External Processors shall agree with the Participating Company exporting the Personal Data that the Personal Data may be retained by the Participating Company. The Participating Company shall warrant that: (i) the Personal Data will be retained in accordance with the provisions of section 5.2; and (ii) it will, and will ensure any Internal or External Processors will, guarantee the confidentiality of the Personal Data and will not further Process the Personal Data otherwise than as required by the relevant law.

3. DATA PROTECTION PRINCIPLES

Participating Companies undertake to follow the below principles when Processing Personal Data:

3.1 **Transparency, fairness and lawfulness**

Personal Data shall be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject and in accordance with sections 4.1 to 4.12.

3.2 **Purpose limitation**

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a way incompatible with such purposes; further Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall not be considered to be incompatible with the initial purposes.

3.3 **Legal basis for Processing Personal Data**

Processing of Personal Data is only permissible if at least one of the following grounds is fulfilled:

(a) the Data Subject has given Consent to the Processing of Personal Data for one or more specific purposes after receiving, in clear and plain language all necessary information;

(b) Processing is necessary for the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject prior to entering into a contract;

(c) Processing is necessary for compliance with a legal obligation to which the Controller is subject;

(d) Processing is necessary to protect the vital interests of the Data Subjects or of another natural person;

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; or

(f) Processing is necessary to pursue the legitimate interests of 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, in particular where the Data Subject is a child.

3.4 **Processing Special Categories of Personal Data and data relating to criminal convictions and offences**

Special Categories of Personal Data may not be Processed as a general principle.

The general principle that Special Categories of Personal Data may not be processed does not apply where there is a legal basis for the Processing pursuant to section 3.3 and one of the following exemptions applies:

(a) the Data Subject has given explicit Consent to the Processing of those Personal Data for one or more specified purposes, except where EU or Member State law provides that the prohibition on Processing Special Categories of Personal Data may not be lifted by the Data Subject; or

(b) the 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 (e.g. a medical emergency); or

(c) the 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 EU or Member State law or pursuant to a contract with a health professional who is subject to the obligation of professional secrecy under EU or Member State law or rules established by national competent bodies or by another person also subject to the obligation of professional secrecy under EU or Member State law or rules established by national competent bodies; or

(d) the Processing relates to Personal Data which are manifestly made public by the Data Subject; or

(e) the Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(f) the 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 authorized by EU 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

(g) the Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy; or

(h) the Processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject; or

(i) the Processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the Processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the Special Categories of Personal Data are not disclosed outside that body without the Consent of the Data Subjects; or

(j) the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

based on EU or Member State law which purposes shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

Processing of Personal Data relating to criminal convictions and offences or related security measures based on section 3.3 shall be carried out only under the control of official authority or when the processing is authorised by EU or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

3.5 **Data minimization and limited storage periods**

In accordance with the principle of data minimization, Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and/or further Processed.

In accordance with the principle of storage limitation, Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data were collected or for which they are further Processed. Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of Technical and Organizational Measures to safeguard the rights and freedoms of the Data Subject.

Aptiv undertakes to specify (e.g. in a minimum standard notice or records retention schedule) a time period for which certain categories of Personal Data may be kept.

Promptly after the applicable storage period has ended, the Personal Data shall be:

(a) securely deleted or destroyed; or

(b) anonymized.

3.6 **Data protection by design and by default**

Aptiv shall adopt internal policies and shall implement appropriate measures, which meet the principles of data protection by design and data protection by default. This means that:

(a) both at the time of the determination of the means for Processing and at the time of the Processing itself, Aptiv shall implement appropriate Technical and Organizational Measures and procedures in such a way that the Processing will meet the requirements of the BCR and ensure the protection of the rights of the Data Subjects; and

(b) Aptiv shall implement appropriate Technical and Organizational Measures for ensuring that, by default, only those Personal Data are Processed which are necessary for each specific purpose of the Processing and are not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the Personal Data and the time of their storage. Aptiv mechanisms shall

ensure that by default Personal Data are not made accessible to an indefinite number of individuals.

An approved certification mechanism may be used as an element to demonstrate compliance with the principle of data protection by design and by default.

3.7 **Data accuracy**

Personal Data must be accurate, complete and kept up-to-date to the extent reasonably necessary for the purposes for which the Personal Data are Processed. Data Subjects will be actively encouraged to inform Aptiv when Personal Data changes or is incorrect, e.g. by inviting them to update their contact details. It is the responsibility of Aptiv, once informed by a Data Subject, to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.

3.8 **Security**

Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data pursuant to section 6.1.

3.9 **Onward transfers**

Personal Data shall only be transferred to Third Parties or External Processors not bound by the BCR pursuant to section 5.2.

4. RIGHTS OF DATA SUBJECTS

4.1 **Transparency and access to the BCR**

All Participating Companies shall Process Personal Data in a transparent manner. Aptiv shall ensure that Data Subjects are adequately informed about the purposes for which their Personal Data are Processed and shall provide any other information to the Data Subjects which may be required. All Data Subjects whose Personal Data are Processed pursuant to these BCR shall be provided with following information, at minimum:

(a) the definitions set out in section 1 and well as the list of Participating Companies in Schedule 2, the scope of the BCR in section 2 and the description of data processing activities in Schedule 3;

(b) the data protection principles set out in sections 3, 5.2 and 6.1 including relating to transparency, fairness and lawfulness; purpose limitation; legal basis for Processing; Processing of Special Categories of Personal Data; data minimization and limited storage periods; data protection by design and by default; data accuracy; security and data breach notification; and onward transfers of data;

(c) the data subject rights in section 4.2 to 4.12, including the transparency information set out in section 4.3;

(d) the information on third-party beneficiary rights set out in section 7.3 and the means to exercise those rights set out in section 7.4; and

(e) information on how Aptiv handles liability set out in section 7.5.

The BCR shall be made available to Data Subjects via the Aptiv intranet and Aptiv corporate website. Furthermore, a Data Subject will always be able to obtain, upon request, a copy of the BCR from the Privacy Office. Data inquiries can be addressed to a central email address privacy@aptiv.com.

In addition, Data Subjects may receive appropriate information through the following applicable channels:

(f) *Employees*: through (i) email; (ii) intranet postings, (iii) notice board; (iv) team meetings for employees without company email; and (v) employee information events (e.g. town hall meetings) all based on templates provided by the Privacy Office.

(g) *Personnel/Staff of Suppliers*: through the supplier portal or email via the Privacy Leader and/or the supplier account manager.

(h) *Personnel/Staff of Customers*: by email, through the Privacy Leader and/or the customer account manager.

(i) *Visitors:* through in building notices and website privacy notices.

4.2 Rights of Data Subjects

Every Data Subject shall be clearly informed as to how they can exercise their rights. Employees shall be made aware of how they can exercise their rights through the Employee Privacy Policy. Suppliers, including their personnel/staff, are made aware of their rights in the Notice of Privacy Practices available through the Supplier portal.

All requests from Data Subjects should be acknowledged and promptly. Where the Controller has reasonable doubts concerning the identity of the Data Subject making the request, the Data Subject may be asked to provide additional information to verify their identity.

All requests must be responded to without undue delay and in any event within one month from receipt of the request. In exceptional circumstances, this period may be extended by two further months where necessary, taking into account the complexity and number of the requests in which case the Data Subject will be notified of this within the initial one month period.

Any response to a Data Subject request should outline the reasons for the delay in response (if applicable) or the reasons for the response including any redactions.

Specific guidelines and procedures shall be in place within Aptiv Group to provide for the exercise of the rights specified below. In particular, identified Aptiv employees shall be trained to recognize any Data Subject rights request.

The Privacy Office, shall always be at the disposal of both the Controllers and Data Subjects to provide any help.

4.3 Information right

The Controller shall provide or make available to the Data Subject at least the following information, except where the Data Subject already has such information:

(a) the identity and contact details of the Controller and of its representative (where applicable);

(b) the contact details of the relevant Privacy Liaison, if any has been appointed by the Controller or the contact details of the Privacy Leader;

(c) the purposes of the Processing for which the data are intended, and, when appropriate, the purpose(s) of the transfer(s) outside the EEA;

(d) the lawful basis for the Processing;

(e) the Recipients or categories of Recipients of the Personal Data;

(f) the categories of Personal Data concerned, where Personal Data have not been obtained from the Data Subject;

(g) where the Processing is based on legitimate interests, the legitimate interests pursued by the Controller or by a Third Party;

(h) where applicable, which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;

(i) where applicable, the fact that the Controller intends to transfer Personal Data to a non-EEA country or international organization, the reference to the appropriate or suitable safeguards and the means by which to obtain a copy of such safeguards or where they have been made available;

(j) the period for which the Personal Data will be stored, or the criteria used to determine that period;

(k) 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;

(l) where the Processing is based on the Consent of the Data Subject, the existence of the right to withdraw Consent at any time;

(m) the right to lodge a complaint with a Supervisory Authority;

(n) 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 the possible consequences of failure to provide such Personal Data;

(o) the existence of automated decision-making, including profiling and, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

A Data Subject may already have such information where, for example, a service provider of Aptiv has provided the Data Subject a notice with this information.

Where the Personal Data are obtained directly from the Data Subject the information above shall be provided to the Data Subject at the time when the Personal Data are obtained. Where the Personal Data has not been directly obtained from the Data Subject, the Controller will provide the information above: (i) within a reasonable time after, and at least within one month of obtaining the Personal Data, having regard to the specific circumstances in which the Personal Data are Processed; (ii) if Personal Data are to be used for communication with the Data Subject, at the latest at time the time of the first communication to the Data Subject; or (iii) if a disclosure to another Recipient is envisaged, at the latest when the Personal Data are first disclosed.

The right to information where the Personal Data has not been directly obtained from the Data Subject does not apply, in exceptional cases where the provision of such information proves impossible or would involve a disproportionate effort, in particular for Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or where this obligation is likely to render impossible or seriously impair the achievement of the objectives of that Processing. Information may also not be provided if recording or disclosure is expressly laid down by law, which law provides appropriate measures to protect the Data Subject's legitimate interests.

4.4 **Right of access**

Every Data Subject shall have the right to obtain from the Controller within the timeline set out in section 4.2, confirmation as to whether or not Personal Data relating to them are being Processed, and where this is the case, access to at least the following information:

(a) the purposes of the Processing;

(b) the categories of Personal Data concerned;

(c) the Recipients or categories of Recipients to whom the Personal Data are disclosed in particular Recipients in third countries or international organisations and the right to be informed of the appropriate safeguards in place;

(d) the period for which the Personal Data will be stored;

(e) the rights granted to the Data Subject, including the right to request rectification or erasure of Personal Data, to request restriction of Processing of Personal Data and to object to Processing of Personal Data;

(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;

(h) as the case may be, the existence of automated decision-making, including profiling, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

The Controller shall provide a copy of the Personal Data undergoing Processing. For any further copies requested by the Data Subject, the

Controller may charge a reasonable fee based on administrative costs. Where the Data Subject makes the request by electronic means, and unless otherwise requested by the Data Subject, the information shall be provided in a commonly used electronic form. The right to obtain a copy of Personal Data shall not adversely affect the rights and freedoms of others.

4.5 **Right to rectification**

Data Subjects shall have a right to obtain from the Controller, without undue delay, the rectification of inaccurate Personal Data concerning them. 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 Controller shall communicate any rectification of Personal Data request 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.

4.6 **Right to erasure ("right to be forgotten")**

Data Subjects shall have the right to request the Controller erase Personal Data concerning them, without undue delay, where:

(a) the Personal Data are no longer necessary in relation to the purposes for which they were collected or Processed;

(b) the Data Subject has withdrawn their Consent to the Processing and there is no other legal ground for Processing;

(c) the Data Subject objects to the Processing and there are no overriding legitimate grounds for Processing or the Data Subject objects to the Processing of Personal Data for direct marketing purposes;

(d) the Personal Data have been unlawfully Processed;

(e) the Personal Data have to be erased for compliance with a legal obligation to which the Controller is subject;

(f) the Personal Data have been collected in relation to the offer of information society services to children.

Where the Controller has made the Personal Data public and is obliged on request to erase the Personal Data, the Controller , taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, unless this proves impossible or involves disproportionate effort, to inform Recipients Processing the Personal Data that the Data Subject has requested the erasure of any links to, or copy or replication of, those Personal Data. The Controller shall inform the Data Subject about those Recipients if the Data Subject requests.

4.7 **Right to restriction**

Data Subjects shall have the right to request the Controller restrict the Processing of their Personal Data where:

(a) the accuracy of the Personal Data is contested by the Data Subject in which case Processing shall be restricted for a period enabling the Controller to verify the accuracy of the Personal Data;

(b) the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;

(c) the Controller no longer needs the Personal Data for the purposes of the Processing for which it was kept, but it is required to be kept by request of the Data Subject for the establishment, exercise or defence of legal claims;

(d) the Data Subject has objected to processing pursuant to the first paragraph of section 4.9 of the BCR pending verification of whether the legitimate grounds of the Controller override those of the Data Subject.

Where Processing has been restricted, the 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 set out in the law of origin of the Personal Data.

A Data Subject shall be informed by the Controller before the restriction of Processing is lifted.

The Controller shall communicate any restriction of Processing request 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.

4.8 **Right to data portability**

Data Subjects shall have the right to receive from the Controller Personal Data concerning them, which they have provided to the Controller, in a structured, commonly used and machine-readable format and request this Personal Data is sent to another entity, where:

(a) the Processing is based on Consent or necessity for the performance of a contract; and

(b) the Processing is carried out by automated means.

4.9 **Right to object**

Data Subjects have the right to object at any time to the Processing of Personal Data relating to them on grounds relating to their particular situation where such Processing is based on the performance of a task carried out in the public interest or the Controller's or a Third Party's legitimate interest pursuant to sections 3.3(e) and (f) of the BCR. The Controller shall no longer Process the Personal Data unless the Controller demonstrates that compelling legitimate grounds for the Processing which override the interests of the Data Subject, or for the establishment exercise or defence of legal claims.

At any time, a Data Subject may object to the Processing of Personal Data for direct marketing purposes, which includes profiling to the extent that it is related to the direct marketing. Where the Data Subject objects to Processing for direct

marketing purposes, the Personal Data shall no longer be Processed for such purposes.

Where Personal Data are Processed for scientific or historical research purposes or statistical purposes, the Data Subject, on grounds relating to his or her particular situation, shall have the right to object to Processing of Personal Data concerning him or her, unless the Processing is necessary for the performance of a task carried out for reasons of public interest.

4.10 Right to withdraw Consent

Data Subjects shall have the right to withdraw their Consent at any time where Processing of their Personal Data is based on Consent. Withdrawal of Consent shall not affect the lawfulness of Processing based on Consent before its withdrawal.

4.11 Automated individual decisions including profiling

Data Subjects shall have a right not to be subjected to a decision which has legal consequences for them, or which similarly significantly affects them, if this decision has been taken solely on the basis of automated Processing of Personal Data including profiling, e.g. with regard to their creditworthiness, reliability or conduct.

Automated individual decision-making may take place only if: (1) the decision is necessary for the entering into, or performance of, a contract between the Controller and the Data Subject; (2) it is authorized by law to which the Controller is subject and which sets forth suitable measures to safeguard the Data Subjects' rights and freedoms and legitimate interests; or (3) it is based on the Data Subjects' explicit Consent. Automated decision-making shall not be based on Special Categories of Personal Data.

In order to implement suitable measures to safeguard the Data Subjects' rights and freedoms and legitimate interests, the Controller will at least provide the right to obtain human intervention on the part of the Controller, so that the Data Subject may express his or her point of view and contest the decision if they wish.

4.12 Internal complaint mechanism

If a Data Subject believes that their Personal Data are not processed in accordance with the BCR or the applicable national laws they may contact the Controller to make a complaint.

Data Subjects may lodge a complaint with the Privacy Office via the "contact us" section of the Aptiv website or using the contact details of the Privacy Office set out in Schedule 1. If a Data Subject contacts an Aptiv employee directly to make a complaint, the Data Subject should be directed to submit their complaint via the "contact us" form on the Aptiv website.

The Privacy Office evaluates and responds to complaints with assistance from business and IT owners and maintains copies of all complaints and notes the details of complaints in a log.

All complaints should be responded to within the timelines set out in section 4.2 above.

If, after review by the Privacy Office and the relevant business owners, it is considered that a complaint contains substantive claims, the Privacy Office will consider what corrective measures are reasonable and necessary to remediate the basis for the complaint. The Privacy Office will then inform the Data Subject of the proposed corrective measures to be taken and it is recommended that the response also includes their rights set out in section 7.4.

Where it is decided that the substance of the complaint is not justified the Data Subject will be informed the complaint has been rejected and of their rights set out in section 7.4.

A Data Subject is not obliged to utilize Aptiv's internal complaint handling process and may also choose to bring their complaint directly before a Supervisory Authority and/or a competent court at any time as set out in to section 7.4.

5. TRANSFERS OF PERSONAL DATA

Aptiv Group shares Personal Data in the normal course and scope of business with other Participating Companies as well as Third Parties, which may be located in countries both within, and outside of, the EEA.

Transfers of Personal Data to countries outside the EEA that do not ensure an 'adequate' level of data protection and all other transfers of Personal Data within the Aptiv Group will be subject to the BCR or, in some cases, to appropriate Model Clauses for any transfers that are not subject to the BCR.

5.1 Relationship with Processors

The Controller transferring Personal Data to a Processor wherever located is obliged to enter into a written contract with the Processor. Participating Companies may provide a power of attorney to AGOL to enter into written contracts with Processors on their behalf.

The written processor contract must at least include the following provisions:

(a) the Processor shall Process Personal Data only in accordance with the Controller's documented instructions and for the purposes authorized by the Controller;

(b) the Processor shall keep the Personal Data confidential either under an appropriate statutory duty of confidentiality or on the basis of an imposed duty of confidentiality on persons authorized to Process the data;

(c) the Processor shall take appropriate technical and organizational measures to protect the Personal Data and assist the Controller in complying with its obligations under the BCR, in so far as this is possible for the fulfilment of the Controller's obligation to respond to requests for exercising Data Subject rights;

(d) the Processor shall only enlist a sub-Processor with the prior written consent of the Controller and impose on the sub-Processor the same obligations as imposed on the Processor under the written contract, whereas the initial Processor shall remain fully liable to the Controller for the performance of the sub-Processor's obligations;

(e) the Processor shall assist the Controller in complying with its obligations to respond to Data Subject's rights, such as rights of access and rectification;

(f) the Controller has the right to review compliance by the Processor with the obligations under the Processor agreement, including the security measures taken by the Processor and, the Processor shall submit its relevant data processing facilities to audits and inspections by the Controller , an external auditor appointed by the Controller or any Concerned Supervisory Authority;

(g) the Processor shall promptly inform the Controller without undue delay of any actual or suspected Personal Data Breach;

(h) the Processor shall, in the event of any actual or suspected Personal Data Breach, take adequate remedial measures as soon as possible and shall promptly provide the Controller with all relevant information and assistance as requested by the Controller regarding the Personal Data Breach;

(i) the Processor shall assist the Controller in ensuring compliance with its obligations under the BCR and applicable data privacy laws; and

(j) the Processor shall, upon the Controller's request, delete or return all the Personal Data to the Controller after the end of the provision of data processing services, and delete existing copies unless the law applicable to the Processor requires storage of the Personal Data.

5.2 **Onward transfers to Third Parties and External Processors**

Transfers of Personal Data to a Third Party or an External Processor outside the EEA are only permitted if one of the following applies:

(a) the European Commission has decided that the country, territory or one or more specified sectors within that country, or the international organization in question ensures an adequate level of protection;

(b) in the absence of an adequacy decision pursuant to (a) above, the Controller or Internal Processor has provided appropriate safeguards, and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available which may include:

(i) standard data protection clauses (i.e. the Model Clauses) adopted by the European Commission;

(ii) standard data protection clauses adopted by a Supervisory Authority and approved by the European Commission;

(iii) an approved code of conduct together with binding and enforceable commitments of the Third Party or External Processor to apply the appropriate safeguards, including as regards Data Subjects' rights; or

(iv) an approved certification mechanism together with binding and enforceable commitments of the Third Party or External

Processor to apply the appropriate safeguards, including as regards Data Subjects' rights.

(c) in the absence of an adequacy decision pursuant to (a) or of appropriate safeguards pursuant to (b), the transfer may take place only if one of the following conditions applies:

(i) the Data Subject has explicitly Consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards. Such information should include: the purpose of the transfer; the identity of the transferring Participating Company; the identity of, or categories of, Third Parties and/or External Processors to which the Personal Data will be transferred; the categories of Personal Data that will be transferred; the country to which the Personal Data will be transferred; and the fact that the Personal Data will be transferred to a Third Party or an External Processor located in a country without an 'adequate' level of data protection;

(ii) the transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;

(iv) the transfer is necessary for important reasons of public interest;

(v) the transfer is necessary for the establishment, exercise or defence of legal claims;

(vi) the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving Consent;

(vii) the transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

The derogations in (c) above should be interpreted restrictively and may only be used as a legal basis for occasional, not repetitive transfers. If the transfer takes place on a structural basis, other measures, such as Model Clauses, must be taken.

6. EFFECTIVENESS OF THE BCR

6.1 Security and Personal Data Breaches

Ensuring that Personal Data is appropriately protected from Personal Data Breaches is a top priority for Aptiv. Each Participating Company shall implement appropriate Technical and Organizational Measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected. Special Categories of Personal Data shall be processed with enhanced and specific security measures.

AGOL has developed an Aptiv Cybersecurity Policy which applies within the Aptiv Group. It includes security policies that set up all appropriate physical and logical measures with a view to preventing and/or deterring Personal Data Breaches. These policies and procedures shall be regularly audited.

Access to Personal Data shall be limited to disclosure to Recipients for the sole purpose of performing their professional duties. Disciplinary sanctions may apply if an Aptiv employee or any Recipient acting on behalf of Aptiv fails to comply with the appropriate information security policies and procedures.

After becoming aware of a Personal Data Breach, a Participating Company shall notify:

(a) the Controller (where relevant), AGOL and the Privacy Leader without undue delay;

(b) the BCR Lead Supervisory Authority for breaches outside the EEA or the relevant Supervisory Authority for breaches within the EEA, without undue delay, and where feasible, not later than 72 hours after becoming aware of it; and

(c) the Data Subjects where the Personal Data Breach is likely to result in a high risk to their rights and freedoms, without undue delay.

Any Personal Data Breaches should be documented (comprising the facts relating to the breach, its effects and the remedial action taken) and the documentation should be made available to a Supervisory Authority on request.

6.2 Record of processing and data protection impact assessments

In order to demonstrate compliance with the BCR, Participating Companies acting as Controllers shall maintain a record of all categories of Processing activities carried out. This record should be maintained in writing, including in electronic form, and should be made available to a Supervisory Authority on request. This record should contain all of the following information:

(a) the name and contact details of the Controller and, the Controller's representative and the data protection officer (if applicable);

(b) the purpose of the Processing;

(c) a description of the categories of Data Subjects and of the categories of Personal Data;

(d) the categories of Recipients to whom the Personal Data have been or will be disclosed including Recipients in non-EEA countries or international organizations;

(e) where applicable, transfers of Personal Data to a non-EEA country or an international organization, and the documentation of suitable safeguards if relevant;

(f) where possible, the envisaged time limits for erasure of the different categories of Personal Data; and

(g) where possible, a general description of the technical and organizational measures in place.

Aptiv shall assess the potential data protection impact of proposed Processing operations, which, by virtue of their nature, scope and/or purposes, are likely to present a high degree of risk to the rights and freedoms of Data Subjects. The assessment shall contain at least a systematic description of the proposed Processing operations, an assessment of the risks to the rights and freedoms of Data Subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with these BCR, taking into account the rights and legitimate interests of Data Subjects, and an assessment of the necessity and proportionality of the Processing operations in relation to the purposes.

Where a data protection impact assessment indicates that the proposed Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk, the Controller shall consult the relevant Supervisory Authority prior to Processing.

6.3 Training programs

Relevant Employees are trained on the types of Personal Data Processed by the Aptiv Group, enabling them to identify the data protection implications of their specific job roles. For instance, during training, Aptiv Group highlights the types of Personal Data employees in customer support, human resources, or development may encounter and emphasizes the need to handle such Personal Data appropriately. In addition, employees are trained on appropriate steps to take in cases where they suspect a Personal Data Breach or receive a request for access to Personal Data by public authorities and who to contact within the Aptiv Group if they have questions about the appropriate use, access or transfer of Personal Data.

Appropriate handling of Personal Data is part of training that will be provided to personnel that have permanent or regular access to Personal Data that are involved in the collection of Personal Data or in the development of tools used to Process Personal Data covered by the BCR both before they take up a relevant role (where possible) and on a periodic basis. Aptiv employees undertake receive annual training on the Employee Code of Ethical Business Conduct which covers data privacy and the BCR. Aptiv maintain a record of attestations for employees that have completed training.

The training and materials used will be reviewed and approved by the Privacy Office. Any changes to the BCR will be documented and reflected in the training as necessary.

In addition to Aptiv policies on data protection and data security, the BCR will be made available to all employees and contractors on the Aptiv intranet and internet corporate website. Specifically contractors are bound by the Supplier Code of Conduct.

6.4 Audit program

Aptiv measures performance of its privacy program through ongoing monitoring, KPIs and periodic audits. Audits will verify compliance with all aspects of the BCR by Participating Companies (including applications, IT systems, databases that Process Personal Data, or onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with the BCR, review of the contractual terms used for the transfers outside of the Aptiv Group to Controllers or Processors of Personal Data, methods and actions plans ensuring that corrective actions have been implemented).

Corporate Internal Audit, the Privacy Leader and other relevant stakeholders set the audit programme depending on the nature and scope of audit work.

Audits are performed by Corporate Internal Audit on an annual basis and throughout the year, for example, in response to an incident.

The Privacy Leader, Chief Information Security Officer, Chief Compliance Officer, Chief Audit Executive and functional owner of the data processing activity will receive audit results depending on scope of work. The Chief Audit Executive will report these results to the board of directors of AGOL and, where appropriate, to the Audit Committee of the board of directors of AGOL's parent company, Aptiv PLC.

The Privacy Office coordinates with Human Resources and Legal to ensure that any workforce disciplinary action related to noncompliance with Aptiv policies and standards are proportionate to the risk for harm.

The results of an audit will be made available to any Concerned Supervisory Authority on request. The Concerned Supervisory Authorities are also granted the authority to carry out a data protection audit of any Participating Company if required and each Participating Company shall assist in any such audit.

7. BINDING NATURE OF THE BCR

7.1 Compliance and supervision of compliance

Aptiv commits to designate a Data Protection Officer where required pursuant to Applicable Law or any other person or entity (such as a Chief Privacy Officer) with responsibility to monitor compliance with the BCR which role shall enjoy the highest management support for the fulfilling of their tasks. Such Data Protection Officer should not have any tasks that could result in a conflict of interest with their role and should not be in charge of carrying out data protection impact assessments, or BCR audits, if such situation could result in a conflict of interest.

Aptiv has determined it is not required to and has not appointed a Data Protection Officer at this time but has appointed a Privacy Leader which role is accountable for the oversight and enforcement of the Aptiv Privacy Program including the BCR. The Privacy Leader oversees the Privacy Office and is based in Dublin, Ireland. More information on the Privacy Office is set out in Schedule 1 (Privacy Office).

Compliance with the BCR shall be supervised by all Concerned Supervisory Authorities. If non-compliance is identified through an audit, by a Concerned Supervisory Authority or otherwise, the Participating Company shall rectify the identified non-compliance without undue delay. Such non-compliance shall be notified to the Privacy Leader. The Privacy Leader will be kept informed of resolution measures, will oversee resolution measures and will direct any suspension and resumption of data transfers to and from that Participating Company. If non-compliance persists and is not resolved without undue delay, then the Privacy Leader shall remove the Participating Company from the BCR and the Privacy Leader will notify the BCR Lead Supervisory Authority in the annual update.

7.2 Compliance with the BCR by employees

Aptiv provides data protection policies and information security protocols which Relevant Employees (i.e. those with exposure to Personal Data as part of their employment) are required to comply with. Employees are made aware of such requirements and the sanctions in case of non-compliance in various ways, including, where applicable: via internal policies which employees are required to observe.

Any policies which support the BCR may be updated from time to time. The most recent electronic version of a document is the controlling version and the version with which employees are expected to comply.

Non-compliance with the BCR by employees may be regarded as a serious breach and may result in a direction to cease Processing Personal Data, a sanction (such as suspension) or other disciplinary measures up to and including dismissal.

Non-compliance by members of staff that are not employees may result in termination of the relevant contract with this member of staff.

Staff will not be penalized for raising issues relating to compliance with the BCR.

7.3 Third party beneficiary rights

Every Data Subject whose Personal Data is Processed by Aptiv shall have a right to enforce, as a third party beneficiary, the following provisions of these BCR:

(a) duty to respect the general data protection principles relating to transparency, fairness and lawfulness; purpose limitation; legal basis for Processing; Processing of Special Categories of Data; data minimization and limited storage periods; data protection by design and by default; data accuracy; security and data breach notification; and onward transfers of data (sections 3, 6.1 and 5.2 BCR);

(b) duty to ensure transparency and easy access to the BCR by ensuring all Data Subjects are provided with the information on how their data is processed set out in , information on their third party beneficiary rights and on the means to exercise those rights, information on how they can hold the Participating Company liable and information relating to the data protection principles described in (a) above (sections 4.1, 4.2, 4.3 and 7.3 BCR);

(c) duty to respect rights of access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right to withdraw Consent and right not to be subject to decisions based solely on automated processing (including profiling) (sections 4.3 to 4.11 BCR);

(d) duty to assess whether national legislation prevents fulfilment of the obligations under the BCR before data transfers take place and on an ongoing basis (sections 8.1 to 8.4 BCR);

(e) duty to be transparent if national legislation prevents the Participating Company from fulfilling its obligations under the BCRs including by: (i) reporting to the Competent Supervisory Authority if national legislation is likely to have a substantial adverse effect on the guarantees provided by the BCR and (ii) notifying the Competent Supervisory Authority of any legal requirement that the Participating Company is subject to in a non-EEA country that is likely to have a substantial adverse effect on the guarantees provided by the BCR, including any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body (section 8.4 BCR (Government Access Requests));

(f) duty to respect the right to complain through the internal complaint mechanism (section 4.12 BCR);

(g) duty to cooperate with Concerned Supervisory Authorities to ensure compliance by Participating Companies with the BCR (sections 7.1 and 7.6 BCR);

(h) duty to inform Data Subjects of any update to the BCR (section 9 BCR);

(i) with respect to the liability and jurisdiction provisions under which Data Subjects may enforce the BCR against a Participating Company and AGOL accepts responsibility for actions of Participating Companies outside of the EEA and agrees to pay compensation for damages resulting from the violation of the BCR by a Participating Company outside of the EEA (sections 7.4 and 7.5 BCR); and

(j) this third party beneficiary rights provision (section 7.3);

(k) the remedies set out in section 7.4.

These rights do not extend to those elements of the BCR pertaining to internal mechanisms, such as details of training, audit programme, compliance network, and mechanism for updating the BCR.

7.4 **Data Subject remedies**

A Data Subject has a right to receive full and effective compensation for material and non-material damage that results from a breach of the BCR by any Participating Company.

Without prejudice to any other administrative, judicial or non-judicial remedy, every Data Subject has the right to:

(a) lodge a complaint with a Supervisory Authority, in particular in the Member State where:

(i) the Data Subject habitually resides;

(ii) the Data Subject has their place of work; or

(iii) the alleged infringement occurred; and

(b) seek redress and, where appropriate, compensation, by bringing proceedings before the competent courts of the Member State where:

(i) the Controller or Processor is established; or

(ii) the Data Subject habitually resides.

If a Participating Company outside of the EEA violates the BCR, then section 7.5 applies.

Data Subjects shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of Data Subjects' rights and freedoms with regard to the protection of their Personal Data to lodge the complaint on their behalf, to exercise the rights referred to in this section 7.4 on their behalf where provided for by Member State law.

7.5 **Liability**

Each Participating Company may be liable for material and non-material damage resulting from a breach of the BCR committed by it (or under its direction). For the purposes of engagement with Data Subjects and Concerned Supervisory Authorities, AGOL shall assume primary responsibility for non-compliance with the BCR by Participating Companies outside the EEA as set out in this section 7.5.

AGOL agrees to take necessary action(s) to remedy the acts of other Participating Companies outside of the EEA that are bound by the BCR and to pay compensation for damages resulting from the violation of the BCR by a Participating Company.

If a Participating Company outside the EEA violates the BCR, the courts or other Concerned Supervisory Authorities in the EEA will have jurisdiction and the Data Subject will have the rights and remedies against AGOL as if the violation had been caused by AGOL in Ireland instead of by the Participating Company outside of the EEA.

The burden of proof lies with AGOL, with cooperation from the relevant Participating Companies, to show, as required, that the Participating Company is not liable for the breach of the BCR on which the Data Subject's claim for damages is based. If AGOL can prove that the Participating Company is not liable for the violation of the BCR, it may be discharged from any responsibility.

7.6 Mutual assistance and cooperation with Supervisory Authorities

Participating Companies shall cooperate and assist each other to handle a request or complaint from a Data Subject.

Each Participating Company will:

(a) cooperate with and accept and submit to audits and inspections (including on-site) by any Supervisory Authority;

(b) to take into account advice of the Supervisory Authorities;

(c) on request, provide the Supervisory Authorities with any information about the processing operations covered by this BCR;

(d) abide by decisions of the Supervisory Authorities on any issue relating to the BCR; and

(e) reply to any request by a Supervisory Authority within such time as stated by the Supervisory Authority or otherwise within a reasonable period of time.

The Concerned Supervisory Authorities shall receive, upon request, an updated copy of the BCR and/or any related policies, procedures, guidelines, codes of conduct.

Any dispute related to the Supervisory Authorities' exercise of supervision of compliance with the BCR will be resolved by the courts of the Member State of that Supervisory Authority, in accordance with that Member State's procedural law. The Participating Companies agree to submit themselves to the jurisdiction of these courts.

8. LOCAL LAWS AFFECTING BCR COMPLIANCE AND GOVERNMENT ACCESS REQUESTS

8.1 Warranty on compliance with BCR

(a) Participating Companies will use the BCR as a tool for transfers only where they have assessed that the law and practices in the third country of destination applicable to the processing of the Personal Data by the Participating Company importing Personal Data, including any requirements to disclose Personal Data or measures authorizing access by public authorities, do not prevent it from fulfilling its obligations under the BCR. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms of Data Subjects, and do not exceed what is necessary and proportionate in a democratic society to safeguard national security, defence or public security, are not in contradiction with the BCR.

(b) Before a Participating Company can rely on the BCR for a transfer of Personal Data outside of the EEA, the Participating Company engaged in the Processing that requires a transfer of Personal Data outside of the EEA will warrant that they have no reason to believe that the laws and practices in the non-EEA country of destination applicable to the Processing of the Personal Data by the Participating Company importing the data (including any requirements to disclose Personal Data or measures authorizing access by public authorities) prevent the Participating Company importing the data from fulfilling its obligations under the BCR.

8.2 **Continual transfer risk assessment in order to rely on the BCR**

(a) The Aptiv Group will facilitate Participating Companies to undertake and document an assessment to determine if the laws and practices of the non-EEA countries of destination in which Participating Companies are located (including any requirements to disclose Personal Data or measures authorizing access by public authorities) would prevent a Participating Company from fulfilling its obligations under the BCR. An assessment does not need to be undertaken for each transfer and one assessment may apply to the same transfer of a specific type of data to the same country.

(b) If the laws in the country in which the Processing occurs provide for a higher level of protection than the protection offered by the BCR, the Participating Company subject to such local laws undertakes to apply such higher standards. If the applicable local laws provide a lower level of protection for Personal Data than the BCR, then the standards of the present BCR shall apply. In any event, the Participating Companies undertake to Process Personal Data in compliance with the BCR.

(c) If it is found that the laws or practices of the non-EEA country of destination do not provide an essentially equivalent level of protection as that provided in the EEA, then the Participating Companies involved in such proposed transfer will put in place supplemental technical, organizational and/or contractual measures to ensure such level of protection for transfers of Personal Data is provided. Where any safeguards in addition to those envisaged under the BCR should be put in place AGOL and the Privacy Office and/or relevant member of the Privacy Liaison will be informed and involved in such assessment.

(d) The Participating Company which proposes to export the data shall not engage in the transfer if it considers that no appropriate safeguards for such transfer can be ensured.

(e) These transfer risk assessments shall be based on the general principles outlined in **Error! Reference source not found.** (Transfer Risk Assessment) and will be adapted from time to time. Assessments shall be documented appropriately along with any supplementary measures. A non-privileged summary of such assessments and supplementary measures will be made available to a Concerned Supervisory Authority on request.

(f) Each Participating Company importing Personal Data from the EEA shall continually assess whether it has reason to believe that it is, or has become, subject to laws or practices in the country of destination

applicable to the Processing of the Personal Data by the Participating Company importing the data, including following a change in the laws of the country or measures (such as a disclosure request) indicating an application of such laws in practice that is not in accordance with the warranty in section8.1(b). If this is the case, the Participating Company shall promptly notify the Participating Company exporting the data from the EEA and AGOL.

(g) Upon verification of such notification in sub-clause (f), the Participating Company exporting the data, the Participating Company importing the data, AGOL and a member of the Privacy Office shall promptly identify appropriate supplementary measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the parties in order to enable them to fulfil their obligations under the BCR. The same applies if a Participating Company exporting the data has reasons to believe that the Participating Company importing the data can no longer fulfil its obligations under the BCR.

(h) The Participating Company exporting the data from shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can ensure compliance with the BCR, or if instructed by a Competent Supervisory Authority to do so. The Participating Company importing the data will promptly inform the Privacy Leader of the issue in accordance with section 8.4(a). The Privacy Leader will inform AGOL and report the issue to the Competent Supervisory Authority unless prohibited by law. In the event that notification to the Competent Supervisory Authority is prohibited, the Privacy Leader and the Participating Company will follow the process in 8.4(b).

(i) Following such a suspension in accordance with sub-clause (h), the Participating Company exporting the data must end the transfer or set of transfers if the BCR cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, Personal Data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the Participating Company exporting the data, be returned to it or destroyed in their entirety.

(j) Where the Participating Company importing the data is in persistent breach of the BCR or the fails to comply with a binding decision of a competent court or Supervisory Authority, the Participating Company exporting the data may request the immediate return or deletion of the Personal Data that has been transferred under the BCR in their entirety. The same commitments should apply to any copies of the data. The Participating Company importing the data should certify the deletion of the data to the Participating Company exporting the data. Until the data is deleted or returned, the Participating Company should continue to ensure compliance with the BCR. In case of local laws applicable to the Participating Company that prohibit the return or deletion of the transferred Personal Data, the Participating Company warrants that it will continue to ensure compliance with the BCR, and will only Process the data to the extent and for as long as required under that local law.

(k) AGOL and the Privacy Office will inform all other Participating Companies of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same

type of transfers is carried out by any other Participating Company or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

(l) Participating Companies exporting data must monitor, on an ongoing basis, and where appropriate in collaboration with Participating Companies importing data, developments in the third countries to which the Participating Companies have transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

8.3 **Government access requests**

(a) Without prejudice to the obligation of a Participating Company to inform the Participating Company exporting the data of its inability to comply with the commitments contained in the BCR in accordance with sections 8.1 and 8.2 above, where a Participating Company:

(i) receives a legally binding request by a public authority under the laws of the county destination or of another third country, for disclosure of the Personal Data transferred pursuant to the BCR; or

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the BCR,

it shall comply with the obligations in this document.

(b) Participating Companies acknowledge that transfers of Personal Data by a Participating Company to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

8.4 **Transparency when Participating Company cannot comply with the BCR**

(a) The Participating Company importing Personal Data agrees to notify the Participating Company exporting Personal Data promptly if, after having commenced transfers of data pursuant to the BCR, prevent the Participating Company from fulfilling its obligation under, or otherwise have a substantial adverse effect on the guarantees provided by the BCR, including where it has reason to believe that the laws and practices in the non-EEA country of destination applicable to the Processing of the Personal Data by the Participating Company importing the data (including any requirements to disclose Personal Data or measures authorizing access by a public authority). The Participating Company importing the data shall notify the Privacy Leader who will inform AGOL and any Concerned Supervisory Authority about the request, including information about the data requested, the requesting body, and the legal basis for disclosure unless otherwise prohibited by law.

(b) In the event notification to the Competent Supervisory Authority is prohibited, the Privacy Leader and the Participating Company will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can as soon as possible and to be able to demonstrate that it did so. If, despite having used its best

efforts, the Privacy Leader on behalf of the Participating Company is not in a position to notify the Competent Supervisory Authority, the Privacy Leader on behalf of the Participating Company shall annually provide general information on the requests it received to the Competent Supervisory Authority including the number of applications for disclosure, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.

9. Updates of the BCR

In case of changes in laws or Aptiv's internal procedures or regulatory requirements, the terms of the BCR may be updated on the initiative of the Privacy Leader, in coordination with the Privacy Office.

Any update of the BCR shall be recorded and kept by the Privacy Office and communicated to Participating Companies without undue delay. The Privacy Office will provide any information to Data Subjects or Concerned Supervisory Authorities on request. The Privacy Office will also keep a fully updated list of the Participating Companies. Where a modification would possibly affect the level of the protection offered by the BCR or significantly affect the BCR (i.e. changes to the binding character), such change must be promptly communicated to the Supervisory Authorities in advance, via the BCR Lead Supervisory Authority with a brief explanation of the reasons for the update. In this case, the Supervisory Authorities will also assess whether the changes made require a new approval. On an annual basis, a confirmation on sufficient assets together with either: (i) an explanation of the reasons for the changes to the BCR and/or the Participating Companies or (ii) a confirmation of no change to the BCR and/or Participating Companies must be reported to the Supervisory Authorities, via the BCR Lead Supervisory Authority.

SCHEDULE 1

PRIVACY OFFICE

1. **Aptiv Global Operations Limited**

2. **Privacy Leader**

Vice President, Global Data Privacy and Protection Email : Privacy@aptiv.com
Tel : +353 (01) 259 7013
By Post : Aptiv,5 Hanover Quay, Dublin D02 VY79, Ireland

3. **Central Email**

privacy@aptiv.com

4. **Responsibilities**

The responsibilities of the Privacy Leader, the Privacy Office and the Privacy Executive Council are set out in the Aptiv Privacy Program Standards and are summarised here:

(a) Aptiv formally appoints a Privacy Leader to be accountable for the oversight and enforcement of the Aptiv Privacy Program (including the BCR) including informing and advising the highest levels of management on issues relating to the BCR, dealing with Competent Supervisory Authorities' investigations and monitoring and annually reporting on compliance with the BCR at a global level.

(b) The Privacy Leader overseas the Privacy Office and is based in Dublin, Ireland.

(c) The Privacy Office is made up of the Privacy Leader and Legal Lead based in Dublin, Ireland as well as Leads from certain countries in which Aptiv has SME operations. The Privacy Office defines and maintains standards for Aptiv's privacy capabilities against privacy laws and regulations as it is either regionally or functionally applicable. It standardizes privacy policies, procedures and controls and provides meaningful advice and guidance on privacy best practices and expectations for the Aptiv Group.

(d) Local Privacy Liaisons are in charge of handling local complaints from Data Subjects, reporting major privacy issues to the Privacy Leader and monitoring training and compliance at a local level.

(e) The Privacy Leader reports to the Privacy Executive Councils and is responsible for improving the privacy program, developing policies, procedures and training, developing enterprise-wide privacy risk assessments and serves as an escalation point for Data Protection Impact Assessments (DPIAs).

(f) The Privacy Executive Council is made up of executive champions including the Chief Compliance Officer. It has defined responsibilities to establish corporate strategy for privacy; review strategy to implement privacy enhancing technologies; serve as an escalation resource to review high-risk initiatives; review results of any group-wide privacy risk assessments; assist the Aptiv Privacy Office in addressing cross-

functional budget and resource needs; review reports from the Aptiv Privacy Program on the status of the program.

SCHEDULE 2

LIST OF PARTICIPATING COMPANIES

EEA COMPANIES		
Company Name	**Domicile**	**Office Address**
Aptiv Components Sweden AB	Sweden	NORD Bolagstjänst AB, Storgatan 73 A, 852 33, Sundsvall, Sweden
Aptiv Connection Systems Hungary Kft	Hungary	Búzavirág u. 13, Tatabánya, 2800, Hungary
Aptiv Connection Systems Services Austria GmbH	Austria	Stallhofner Strasse 4, 5230, Mattighofen, Austria
Aptiv Connection Systems Services Italia S.P.A.	Italy	Strada Del Francese 137, Torino CAP 10156, Italy, Italy
Aptiv Contract Services Sweden AB	Sweden	Molndalsvagen 36, 402 26, Gothenburg, Sweden, Sweden
Aptiv Global Financing Designated Activity Company	Ireland	5 Hanover Quay, Grand Canal Dock, Dublin 2, D02 VY79, Ireland
Aptiv Global Holdings Limited	Ireland	5 Hanover Quay, Grand Canal Dock, Dublin 2, D02 VY79, Ireland
Aptiv Global Operations Limited	Ireland	5 Hanover Quay, Grand Canal Dock, Dublin 2, D02 VY79, Ireland
Aptiv Holdings (Austria) GmbH	Austria	Industriestrasse 1, 7503 Grosspetersdorf, Austria, Austria
Aptiv Holdings Deutschland 2 GmbH	Germany	Am Technologiepark 1, 42119, Wuppertal, Germany
Aptiv Holdings France SAS	France	Z.I. des Longs Réages, 28230, Epernon, France
Aptiv Italia Holdings s.r.l.	Italy	Strada Del Francese 137, Torino CAP 10156, Italy, Italy
Aptiv Malta Holdings Limited	Malta	Office 10, Verdala Business Park Centre, Level 1, LM Complex, Brewery Street, Zone 3 Central Business District, Birkirkara, CBD 3040, Malta
Aptiv Mobility Services Austria MAT. GmbH	Austria	Stallhofner Strasse 4, 5230, Mattighofen, Austria
Aptiv S&P Mobility Services Spain, S.L.	Spain	Polig Industrial Landaben,, calle A S/N Pamplona/Iruña,, 31012-Navarra, Spain, Spain
Aptiv S&P Solutions Holdings (Spain), S.L.	Spain	Polig Industrial Landaben,, calle A S/N Pamplona/Iruña,, 31012-Navarra, Spain, Spain
Aptiv Services (Ireland) Limited	Ireland	5 Hanover Quay, Grand Canal Dock, Dublin 2, D02 VY79, Ireland
Aptiv Services 2 France SAS	France	Z.I. des Longs Réages, 28230, Epernon, France
Aptiv Services Austria GPD. GmbH & Co KG	Austria	Industriestrasse 1, 7503 Grosspetersdorf, Austria, Austria
Aptiv Services Belgium N.V.	Belgium	Parklaan 43/306, 2300 Turnhout, Belgium
Aptiv Services Deutschland GmbH	Germany	Am Technologiepark 1, 42119, Wuppertal, Germany
Aptiv Services Hungary Kft.	Hungary	Zanati Ut 29/A, Szombathely, Hungary, 9700, Hungary
Aptiv Services Italia 2 S.R.L.	Italy	Strada Del Francese 137, Torino CAP 10156, Italy, Italy
Aptiv Services Italia S.r.l.	Italy	Strada Del Francese 137, Torino CAP 10156, Italy, Italy
Aptiv Services Netherlands B.V.	Netherlands	Vanadiumweg 11 c, 3812 PX , Amersfoort, Netherlands
Aptiv Services Poland S.A.	Poland	Ul. Powstancow Wielkopolskich 13 D, 30-707, Krakow, Poland
Aptiv Technology Services & Solutions S.R.L.	Romania	11 Garii Street, Sannicolau Mare, 305600 , Romania

Aptivport Services, S.A.	Portugal	Pólo Tecnológico de Lisboa, Rua António Champalimaud, lote quatro, 1600-514, Lisbon, Portugal, Portugal
Cyprium France SAS	France	Z.I. des Longs Réages, 28230, Epernon, France
Cyprium Germany GmbH	Germany	Am Technologiepark 1, 42119, Wuppertal, Germany
Cyprium Hungary Kft.	Hungary	Búzavirág u. 13, Tatabánya, 2800, Hungary
Cyprium Poland sp. Z o.o.	Poland	Wielicka Street 28B, 30-552, Kraków, Poland
Cyprium Spain S.L.	Spain	Polig Industrial Landaben,, calle A S/N Pamplona/Iruña,, 31012-Navarra, Spain, Spain
EDSCP Manufacturing Unipessoal Lda.	Portugal	Pólo Tecnológico de Lisboa, Rua António Champalimaud, lote quatro, 1600-514, Lisbon, Portugal, Portugal
gabo Systemtechnik GmbH	Germany	Am Schaidweg 7, 94559, Niederwinkling, Germany
Gabocom Sarl	France	1 Allée de Stockholm, 67300 Schiltigheim, France, France
Harwich Holding GmbH	Germany	Grosser Moorweg 45, 25436, Tornesch, Germany
Harwich Holdings S.A.S.	France	2 Rue des Hêtres, CS 80543 (78197 Trappes Cedex), 78190, Trappes, France
HellermannTyton Aktiebolag	Sweden	Box 7037, Isafjordsgatan 5, 164 07, Kista, Sweden, Sweden
HellermannTyton Aktiebolag Sivuliike Suomessa	Finland	Äyritie 12 B, Vantaa, Finland, FIN-01510, Finland
HellermannTyton AS	Norway	Nila Hansens vei 13, Oslo, Norway, 0667, Norway
HellermannTyton BV	Netherlands	Vanadiumweg 11 c, 3812 PX , Amersfoort, Netherlands
HellermannTyton Engineering GmbH	Germany	Grosser Moorweg 45, 25436, Tornesch, Germany
HellermannTyton España, S.L.U.	Spain	Avda. de la Industria 37 - 2a2a, Alcobendas 28, 28108, Madrid, Spain
HellermannTyton GmbH	Austria	Rennbahnweg 65, 1220, Vienna, Austria
HellermannTyton GmbH & Co. KG	Germany	Grosser Moorweg 45, 25436, Tornesch, Germany
HellermannTyton Holdings AB	Sweden	Box 7037, Isafjordsgatan 5, 164 07, Kista, Sweden, Sweden
HellermannTyton Kft	Hungary	Kisfaludy u. 13, Budapest, Hungary, 1044, Hungary
HellermannTyton Rohvel SL	Spain	Calle la Granja, 100, Alcobendas, 28108, Madrid, Spain, Spain
HellermannTyton SAS	France	2 Rue des Hêtres, CS 80543 (78197 Trappes Cedex), 78190, Trappes, France
HellermannTyton Sp. z.o.o.	Poland	Kounia 111, 62-400, Słupca, Poland
HellermannTyton Srl	Italy	Via Visco 3/7, 35010, Limena (PD), Italy, Italy
HellermannTyton Verwaltungs GmbH	Germany	Grosser Moorweg 45, 25436, Tornesch, Germany
HellermannTyton, Filial af HellermannTyton AB, Sverige	Denmark	Industrivej 44 A 1, 4000, Roskilde, Denmark, Denmark
Höhle OÜ	Estonia	Rapla vald, Löiuse küla,, Torupollu, Estonia, 79405, Estonia
Intercable Automotive Solutions s.r.l.	Italy	Brunico (BZ) Via Dei Campi, Della Rienza 21 CAP 39031, Italy
Intercable s. r. o.	Slovakia	Kriván 565, Kriván, 962 04, Slovakia (Slovak Republic)
Movimento Europe GmbH	Germany	Herdweg 76, 70174 , Stuttgart, Germany
Movimento Group AB	Sweden	Box 14044, 400 20, Göteborg, Sweden
Potio Holding GmbH	Germany	Am Schaidweg 7, 94559, Niederwinkling, Germany
Rebafin GmbH	Austria	Rennbahnweg 65, 1220, Vienna, Austria

Wind River AB	Sweden	Kistagången 20B S-164 40 Kista Sweden, Kista, Sweden
Wind River GmbH	Germany	Business Campus , Emmy-Noether-Ring 24, 85716, Unterschleissheim, Germany
Wind River Netherlands, B.V.	Netherlands	Spaces Amsterdam Zuidas II, Barbara Strozzilaan 101, 1083, HN Amsterdam, Netherlands
Wind River S.R.L.	Italy	Lungo Dora Colletta 75, 10153, Torino, Italy, Italy
Wind River SARL	France	2-12 rue du Chemin des Femmes, Immeuble Odyssée – Bâtiment F, 91300, Massy, France, France
Wind River Systems Romania SRL	Romania	41, Alexandru Ioan Cuza Street, Galati, Romania, 800010, Romania

Non-EEA Companies		
Company Name	**Domicile**	**Office Address**
A.E. Enterprises, LLC	United States	5725 Innovation Drive, Troy MI 48098, United States
Alambrados y Circuitos Eléctricos, S. de R.L. de C.V.	Mexico	Av. Hermanos Escobar #5756, Colonia Fovissste Chamizal, Cd. Juárez, Chihuahua, 32310, Mexico
Antaya Technologies Corp.	United States	333 Strawberry Field Road, Warwick RI 02886, United States
Aptiv (Changshu) Technology Company Limited	China	No. 2 Yunshen Road, Southeast Street, Changshu, Jiangsu Province, China, Changshu, China, China
Aptiv (China) Holding Company Limited	China	Section A, Building C, #118 De Lin Road, Pilot Free Trade Zone, Shanghai, PuDong, 200131, China
Aptiv (China) Technology Company Limited	China	Section A, Building C, #118 De Lin Road, Pilot Free Trade Zone, Shanghai, PuDong, 200131, China
Aptiv (Shanghai) International Management Company Ltd.	China	Building #2, No. 60 Yuan Guo Road, Anting Town, Jiading District, Shanghai, 201814, China
Aptiv (Suzhou) Enterprise Management Co., Ltd.	China	2F, Building 22, 123 Changyang Street, Suzhou Industrial Park, Jiangsu Province, China, China
Aptiv (UK) Holdings Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Aptiv Arabia Gulf Limited	Saudi Arabia	Ground Floor, VJ6W+G&Q, Abu Bakr Al Siddiq, Narjis View, An Narjis, Al-Kharj, Riyadh, 13336, Saudi Arabia
Aptiv Brazil Ltda.	Brazil	Rodovia dos Tamoios, km 21.8, Jambeiro, Sao Paulo, 12.270-000, Brazil
Aptiv China Holdings (US) LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Components (Shanghai) Company Limited	China	Building #2, No. 60 Yuan Guo Road, Anting Town, Jiading District, Shanghai, 201814, China
Aptiv Components India Private Ltd.	India	Plot No.-7, Sector-6,, Dharuhera Industrial Area, District - Rewari, Dharuhera, Haryana, 122106, India
Aptiv Connection Systems (Nantong) Ltd.	China	No. 9 Hebin Road, Tongzhou Economic Development Zone, Nantong, China, China
Aptiv Connection Systems (Shanghai) Ltd.	China	Section A, Building C, #118 De Lin Road, Pilot Free Trade Zone, Shanghai, PuDong, 200131, China
Aptiv Connection Systems Holding Hong Kong Limited	Hong Kong	Unit No.19, Level 26, Tower 1, Millennium City 1, No.388 Kwun Tong Road, Kwun Tong, Kowloon, Hong Kong, Hong Kong
Aptiv Connection Systems Holdings (US) LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States

Aptiv Connection Systems India Private Limited	India	7/60-A & 60-B, Arakkunnam Pulikkamali Road, Arakkunnam P.O, Mulanthuruthy, Ernakulam, Kerala, 682313, India
Aptiv Connection Systems Korea LLC	Korea, Republic of	3 Hyundai-Kia-ro, Paltan-myeon, , Hwaseong-si, Gyeonggi-do, Korea, Republic of
Aptiv Connection Systems Morocco S.A.S.	Morocco	Lot n° 170 Zone Franche, Tanger Automotive City, Tanger, Morocco, Morocco
Aptiv Connection Systems Services Japan, Ltd.	Japan	Dai-Ichi Ito Building, 24-13,, Asahi-cho, 1-chome,, Atsugi-shi, Kanakawa, 243-0014, Japan
Aptiv Connection Systems Yancheng Company Limited	China	No.1 Ganjiang East Road, Yanan High-tech Zone, Yancheng, China
Aptiv Connections Systems Wuhan Company Limited	China	103-176 Commercial Building, Xiaojunshan Community, Junshan Street Wuhan Economic and Technological DZ, Hubei Province, China, China
Aptiv Contract Services Ciudad Juarez, S. de R.L. de C.V.	Mexico	Av. Hermanos Escobar #5756, Colonia Fovissste Chamizal, Cd. Juárez, Chihuahua, 32310, Mexico
Aptiv Contract Services d.o.o. Leskovac	Serbia	Zelena Zona Prva 1, Leskovac, Serbia, Serbia
Aptiv Contract Services de Mexico, S. de R.L. de C.V.	Mexico	Av. Hermanos Escobar #5756, Colonia Fovissste Chamizal, Cd. Juárez, Chihuahua, 32310, Mexico
Aptiv Contract Services Matamoros, S. de R.L. de C.V.	Mexico	Av. Hermanos Escobar #5756, Colonia Fovissste Chamizal, Cd. Juárez, Chihuahua, 32310, Mexico
Aptiv Contract Services Noreste, S. de R.L. de C.V.	Mexico	Av. Hermanos Escobar #5756, Colonia Fovissste Chamizal, Cd. Juárez, Chihuahua, 32310, Mexico
Aptiv Contract Services Nuevo Laredo, S. de R.L. de C.V.	Mexico	Av. Hermanos Escobar #5756, Colonia Fovissste Chamizal, Cd. Juárez, Chihuahua, 32310, Mexico
Aptiv Contract Services Tamaulipas, S. de R.L. de C.V.	Mexico	Av. Fomento Industrial, Col. Parque Industrial del Norte, Reynosa, Tamaulipas, Mexico
Aptiv Contract Services Tijuana, S.A. de C.V.	Mexico	Privada Misiones 15351 Parque Industrial, Misiones de California, Tijuana, Baja California, 22425, Mexico
Aptiv Contract Services Zacatecas, S. de R.L. de C.V.	Mexico	Calz. de la Revolucion Mexicana No. 63, Ejidal Guadalupe, Zacatecas, 98600, Mexico
Aptiv Contract Services, S. de R.L. de C.V.	Mexico	Av. Hermanos Escobar #5756, Colonia Fovissste Chamizal, Cd. Juárez, Chihuahua, 32310, Mexico
Aptiv Corporation	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Electric Systems Company Ltd.	China	Building #2, No. 60 Yuan Guo Road, Anting Town, Jiading District, Shanghai, 201814, China
Aptiv Electrical Centers (Shanghai) Co. Ltd.	China	Building 4, 6, 7, 8, 11, 12, 14, 15, 16, 17, No. 60, Yuanguo Road, Anting, Jiading District, Shanghai, China, China
Aptiv Electronics (Suzhou) Co. Ltd.	China	No. 123 Chang Yang Road, Suzhou Industrial Park, Jiangsu Province, China
Aptiv European Holdings (UK) Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Aptiv Financial Holdings (UK) LLP	England and Wales	1 Park Row, Leeds, LS1 5AB, United Kingdom
Aptiv Financial Investment Services (UK) Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom

Aptiv Financial Services (UK) Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Aptiv Global Holdings (UK) Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Aptiv Global Holdings GmbH	Switzerland	c/o Aptiv Technologies AG, Spitalstrasse 5, 8200, Schaffhausen, Switzerland
Aptiv Global Real Estate Services (US), LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Holdfi (UK) Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Aptiv Holdings (UK) Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Aptiv Holdings (US), LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Holdings Limited	Barbados	C/o PricewaterhouseCoopers Services Inc., The Financial Services Centre, Bishop's Court Hill, St. Michael, Barbados, BB14004, Barbados
Aptiv Holdings Mexico, S. de R.L. de C.V.	Mexico	Av. Hermanos Escobar #5756, Colonia Fovissste Chamizal, Cd. Juárez, Chihuahua, 32310, Mexico
Aptiv Holdings US Limited	Jersey	13 Castle Street, St Helier, JE1 1 ES, Jersey
Aptiv International Financial Services (UK) LLP	England and Wales	1 Park Row, Leeds, LS1 5AB, United Kingdom
Aptiv International Services Company, LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Korea LLC	Korea, Republic of	2302, Yonggudaero, Giheung-gu, Yongin-si, Gyeonggi-do, 446-912, Korea
Aptiv Luxembourg Holdings (UK) Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Aptiv Malaysia Sdn. Bhd.	Malaysia	Lot 3089, Kawasan Perindustrian Cendering, 21080 Kuala Terengganu, Terengganu Darul Iman, Malaysia
Aptiv Manufactura e Servicos de Distribuicao Ltda.	Brazil	Rua José Monfardini, nº 3.845, Espirito Santo do Pinhal, Sao Paulo, 13.990-000, Brazil
Aptiv Manufacturing Management Services S.à r.l.	Switzerland	c/o Aptiv Technologies AG, Spitalstrasse 5, 8200, Schaffhausen, Switzerland
Aptiv Manufacturing Services El Salvador, S.A. de C.V.	El Salvador	Paseo General Escalón, Apto. Local 33, , Colonia Escalón, Edificio Millenium Plaza, Nivel 21, , San Salvador Centro, San Salvador , El Salvador
Aptiv Manufacturing Services Honduras S.A. de C.V.	Honduras	Parque Industrial Green Valley, Santa Bárbara, Quimistán, Honduras, KM 23, Honduras
Aptiv Medical Systems, LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Mexican Holdings (US) LLC	United States	40600 Ann Arbor Road E, Suite 201, Plymouth MI 48170-4675, United States
Aptiv Mobility Services d.o.o. Novi Sad	Serbia	Laze Nancica 34-36, Novi Sad, Serbia
Aptiv Mobility Services Japan, Ltd.	Japan	Sasazuka-Taiyo Bld. 6F,, 1-48-3 Sasazuka, Shibuya-ku, Tokyo, 151-0073, Japan
Aptiv PLC	Jersey	13 Castle Street, St Helier, JE1 1 ES, Jersey
Aptiv Properties Management Services (US) LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States

Aptiv Safety & Mobility Services Singapore Pte. Ltd.	Singapore	501 Ang Mo Kio Industrial Park 1, Singapore, 569621, Singapore
Aptiv Services 3 (US), LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Services 4 US, LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Services 5 US, LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Services Czech s.r.o.	Czech Republic	Cechova 235, Bakov nad Jizerou, Czech Republic, 294 01, Czech Republic
Aptiv Services Guatemala, S.A.	Guatemala	Diagonal 6, 10-50 Zona 10, Edificio Interamericas, Torre Norte, Nivel 8, Oficina 802, Guatemala, Guatemala
Aptiv Services Honduras, S. de R.L. de C.V.	Honduras	Zona Libre Green Valley, Edif#7, Quimistan, Honduras, Honduras
Aptiv Services Kenitra S.A.	Morocco	Kenitra Atlantic Free Zone Ilot 1, Lots 30 et 31, Route Nationale 4, Commune Ameu Safia, Ameu Safia, Morocco, Morocco
Aptiv Services Macedonia DOOEL Skopje	North Macedonia, Republic of	Technological Industrial Development Zone, no.Skopje 1-no.22/1/ Ilinden, Ilinden, Macedonia, Republic of North Macedonia
Aptiv Services Maroc S.A.	Morocco	Tangiers. Km. 7, route de Rabat, Morocco, Morocco
Aptiv Services Meknes S.A.S.U.	Morocco	Lot UL-1, Axe 1, Axe A, Agropolis Business Park, Meknes, Morocco, Morocco
Aptiv Services Morocco S.A.S.U.	Morocco	LOT N 33, 34 ET 35 ZONE, FRANCHE D'EXPORTATION DE TANGER TECH COMMUNE, AOUAMA PROVINCE TANGER-ASSILAH, Tanger, Morocco, Morocco
Aptiv Services Oujda S.A.S.U.	Morocco	Lot n° 157, zone d'accélération industrielle d'Oujda, dite Cleantech, Oujda-Maroc, Morocco
Aptiv Services Tanger S.A.	Morocco	Illot 53, Lot No. 1, Zone Franche d'Exportation de Tanger, Morocco, Morocco
Aptiv Services Tunisia S.A.R.L.	Tunisia	Nouvelle Zone Industrielle, Medjez El Bab, Béja, 9070, Tunisia
Aptiv Services UK Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Aptiv Services Ukraine LLC	Ukraine	8 Sumgaitska Street, Cherkasy, Cherkaska Oblast, Ukraine
Aptiv Services US, LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Swiss Holdings Limited	Jersey	13 Castle Street, St Helier, JE1 1 ES, Jersey
Aptiv Technologies AG	Switzerland	Spitalstrasse 5, 8200, Schaffhausen, Switzerland
Aptiv Technologies Holdings AG	Switzerland	c/o Aptiv Technologies AG, Spitalstrasse 5, 8200, Schaffhausen, Switzerland
Aptiv Trade Management Services (US), LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv Transaction Services GmbH	Switzerland	c/o Aptiv Technologies AG, Spitalstrasse 5, 8200, Schaffhausen, Switzerland
Aptiv Turkey Teknoloji Hizmetleri Limited Şirketi	Turkey	Hasanağa OSB Mahallesi, 12. Cad., No: 1, NİLÜFER/BURSA, Turkey, Turkey
Aptiv US Operations Holdings, LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Aptiv US Services General Partnership	United States	5725 Innovation Drive, Troy MI 48098-2815, United States

Asux Safety Components India Private Limited	India	P-24, Green Park Extension, New Delhi, Delhi, 110016, India
Auburn Enterprises, LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Centro Técnico Herramental, S. de R.L. de C.V.	Mexico	Carretera, Saltillo-Piedras Negras, Km. 8.54 No. 8540, Ramos Arizpe, Coahuila, Mexico, 25900, Mexico
Control-Tec LLC	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Cyprium China Holdings GmbH	Switzerland	c/o Aptiv Technologies AG, Spitalstrasse 5, 8200, Schaffhausen, Switzerland
Cyprium Corporation	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Cyprium Holdings Limited	Jersey	13 Castle Street, St Helier, JE1 1 ES, Jersey
Cyprium International Services Company, LLC	United States	c/o The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington DE 19801, United States
Cyprium Korea LLC	Korea, Republic of	2302, Yonggudaero, Giheung-gu, Yongin-si, Gyeonggi-do, 446-912, Korea
Cyprium LLC	United States	c/o The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington DE 19801, United States
Cyprium Swiss Holdings Limited	Jersey	13 Castle Street, St. Helier, Jersey, JE1 1ES
Cyprium Treasury GmbH	Switzerland	c/o Aptiv Technologies AG, Spitalstrasse 5, 8200, Schaffhausen, Switzerland
Cyprium US Holdings, LLC	United States	c/o The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington DE 19801, United States
Cyprium US Services General Partnership	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Daehan Electronics Yantai Co., Ltd.	China	Yongda Street, Fushan District, Yantai City, Shangdong, China
El Components Corporation LLC	United States	125 E Harmon Ave, #31814, Las Vegas NV 89109, United States
Gabocom Ltd	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Harwich Holdings, LLC	United States	
HellermannTyton (Proprietary) Limited	South Africa	36 Milky Way Avenue, Linbro Business Park, Sandton, South Africa, South Africa
HellermannTyton (Wuxi) Electrical Accessories Company Limited	China	No. 231 Xing Chuang Ba Lu, Wuxi Singapore Industrial Park, Wuxi, Jiangsu Province, Republic of China, Republic of China
HellermannTyton Australia Pty Ltd	Australia	Unit 2 & 6, 12-16 Mangrove Lane, Taren Point NSW 2229, Australia
HellermannTyton Canada Inc.	Canada	205 Industrial Parkway North, Unit #4, Aurora ON L4G 4C4, Canada
HellermannTyton Chile SpA	Chile	Av. Apoquindo 5950, Comuna de Las Condes, Oficina 19-120, Santiago, Región Metropolitana, 7560949, Chile
HellermannTyton Co. Ltd	Japan	602, Kanchenjunga Building, 18, Barakhamba Road, New Delhi, Delhi, 110001, India
HellermannTyton Corporation	United States	7930 N. Faulkner Road, Milwaukee WI 53224, United States
HellermannTyton Data Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom

HellermannTyton Elektrik Ticaret Limited Sirketi	Turkey	Inkilap Mah., Dr. Adnan Büyükdeniz Cad. 2., Blok No: 4 İç Kapı No: 14, Ümraniye / Istanbul, Turkey, Turkey
HellermannTyton Finance PLC	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
HellermannTyton Gridbow (Proprietary) Limited	South Africa	36 Milky Way Avenue, Linbro Business Park, Sandton, South Africa, South Africa
HellermannTyton Group PLC	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
HellermannTyton Holdings Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
HellermannTyton Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
HellermannTyton Ltda	Brazil	Av. José Benassi, 100 - Parque Industrial, Jundiaí-SP, Brazil, 13213-085, Brazil
HellermannTyton Manufacturas, S. de R.L. de C.V.	Mexico	Av. Internacional 140, General Escobedo, Nuevo Leon, 66053, Mexico
HellermannTyton Maroc S.àr.l.	Morocco	174 Boulevard Zerktouni, Casablanca, Casablanca, 100000, Morocco
Hellermanntyton Morocco SARL AU	Morocco	Bureau No. 10, ILOT No. 101 Zone Franche Automotive City Commune, Jouamaa Province Fahs Anjra,, Tanger, Tangier, Morocco
HellermannTyton Private Limited	India	602, Kanchenjunga Building, 18, Barakhamba Road, New Delhi, Delhi, 110001, India
HellermannTyton Pte Ltd.	Singapore	545 Yishun Industrial Park A, Yishun Ave 7, Singapore, 768741545, Singapore
HellermannTyton Services SARL AU	Morocco	Zone Franche d'Exportation, Lot 40a, ZF Business Centre, 2°Etage Bureau no. B3,, Tanger, Tangier, 90090, Morocco
HellermannTyton SRL	Argentina	Monteagudo 748/766, Villa Lynch, Buenos Aires, Argentina, 1650, Argentina
HellermannTyton YH	Korea, Republic of	12-28 Venture-ro, Yeongsu-gu, Incheon, Korea, 22011, Korea
HellermannTyton, S. de R.L. de C.V.	Mexico	Av. Anillo Periferico Sur 7980, Edificio 6ª, Sta. Ma. Tequepexpan, San Pedro Tlaquepaque, Jalisco, 45601, Mexico
Intercable (Ningbo) New Energy Automotive Technology Co., Ltd.	China	228, Jinshan Rd., Jiangbei District, Ningbo, CN-315033, China
Intercable Automotive Solutions (Shanghai) Co., Ltd.	China	Room J7200, 4F, No. 4229 Bao'an Road, Jiading District, Shanghai, Shanghai, 201814, China
KUM LLC	Korea, Republic of	17, Yangdeungnongong-gil, Sangbuk-myeon, Ulju-gun, Ulsan, 44908, Korea, Republic Of
KUMAP Co., Ltd.	Korea, Republic of	1838, Unbuk-ro,, Bugan-myeon, Yeongcheon, Gyeongsangbuk-do, 38907, Korea
Movimento International, S. de R.L. de C.V.	Mexico	Paseo Totoltepec No. 11, San Pedro Totoltepec, Toluca, Mexico, 50226, Mexico
Movimento, Inc.	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Myrna Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Myrna Trading Holdings Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom

Packard Japan G.K.	Japan	160 Como Square West 3F, Kitamachi 2-chome, Toyota-shi, Aichi, Japan
Particle Design, Inc.	United States	500 Wind River Way Alameda, CA 94501, United States
Phoenix Assets Holdings, Ltd.	Virgin Islands, British	68 Water Street, Norwalk CT 06854, United States
PT Aptiv Components Indonesia	Indonesia	Wijayakusuma Industrial Estate Jl. Raya Semarang, Kendal KM 12 Block B.06 Ex. Randugarut district., Tugu, Semarang City, Central Java., Indonesia, 50153, Indonesia
Rio Bravo Eléctricos, S. de R.L. de C.V.	Mexico	Av. Rio Bravo 1420, Col. Parque Industrial Rio Bravo, Cd. Juárez, Chihuahua, Mexico
S.W. Tooling Limited	England and Wales	Griffin House, 135 High Street, Crawley, West Sussex, RH10 1DQ, United Kingdom
Unwired Holdings, Inc.	United States	1209 Orange Street, Wilmington DE 19801, United States
Westerly, LLC	United States	1209 Orange Street, Wilmington DE 19801, United States
Winchester Holding, Inc.	United States	68 Water Street, Norwalk CT 06854, United States
Winchester Interconnect (M) Sdn. Bhd.	Malaysia	No.1651,, Lorong Perusahaan Maju 8, Prai Industrial Estate, Phase IV, 13600 Penang, Malaysia
Winchester Interconnect (Shanghai) Co. Ltd	China	37, Lane 799, Jiasong Middle Road, Huaxin Town, Qingpu District, Shanghai, China
Winchester Interconnect (Suzhou) Co., Ltd.	China	Unit 3, No. 179, Suhong West Road, Suzhou Industrial Park, Suzhou, Jiangsu Province, China
Winchester Interconnect (Thailand) Co., Ltd.	Thailand	20/3 Non-Tower Building B, Tiwanon, Talat Khwan, Mueang Nonthaburi, Nonthaburi, 11000, Thailand
Winchester Interconnect CM CA, Inc.	United States	1810 Diamond Street, San Marcos CA 92078, United States
Winchester Interconnect CM Corporation	United States	349 Lake Road, Dayville CT 06241, United States
Winchester Interconnect Corporation	United States	185 Plains Road, Milford CT 06461, United States
Winchester Interconnect E.C. LTD	Israel	Kherut St 1, Yavne, Israel, 8121217, Israel
Winchester Interconnect EC Corp	United States	PO Box 5677, Caguas Puerto Rico 00726-5677, United States
Winchester Interconnect EC LLC	United States	12691 Monarch ST, Garden Grove CA 92841, United States
Winchester Interconnect Hermetics, LLC	United States	3950 Dow Road, Melbourne FL 32934, United States
Winchester Interconnect Micro LLC	United States	1872 N Case St, Orange CA 92865, United States
Winchester Interconnect RF Corporation	United States	68 Water Street, Norwalk CT 06854, United States
Winchester Interconnect Ruggedized Corporation	United States	2150 Parkes Drive, Broadview IL 60155, United States
Wind River Hong Kong Holding Ltd.	Hong Kong	Room 1919, 19/F, Lee Garden One, 33 Hysan Avenue, Causeway Bay, Hong Kong, Hong Kong
Wind River Inception Technology (Shanghai) Co., Ltd.	China	Room JT6481, 4F, No. 4229 Bao'an Road, Jiading District, Shanghai, Shanghai, 201814, China

Wind River International Limited	Canada	425 Legget Dr, Ottawa ON K2K 3C9, Canada
Wind River K.K.	Japan	Ebisu Prime Square Tower, 1-1-39 Hiroo Shibuya-ku, Tokyo, Tokyo, 150-0012, Japan
Wind River Sales Co., Inc.	United States	500 Wind River Way Alameda, CA 94501, United States
Wind River Software Technology (Beijing) Co., Ltd.	China	Unit 1902, 19F, Hyundai Motor Tower,, No. 38 Xiaoyun Road, Chaoyang District, Beijing, China, 100016, China
Wind River Software Technology (Chengdu) Co., Ltd.	China	14F, Building 7, Zone D, Tianfu Software Park, High-Tech Zone, Chengdu, China, 610041, China
Wind River Systems Costa Rica S. de R.L.	Costa Rica	Condominio Vertical Comercial (Oficinas) Plaza Rob, Edificio El Patio, 2nd Floor, San Rafael de Escazu, 10203, Costa Rica
Wind River Systems International, Inc.	United States	500 Wind River Way Alameda, CA 94501, United States
Wind River Systems Korea, Inc.	Korea, Republic of	2F, Sambo building, 638,, Yeongdong-daero, Gangnam-gu, Seoul, Korea
Wind River Systems, Inc.	United States	500 Wind River Way Alameda, CA 94501, United States
Wind River UK Limited	England and Wales	PURE offices, Kembrey Park, London, SN3 4JL, United Kingdom
Wind RiverX Corporation	United States	1250 H Street NW, Suite 620, Washington DC 20005, United States
Wolfhound Holdings, Inc.	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Wolfhound Intermediate, Inc.	United States	5725 Innovation Drive, Troy MI 48098-2815, United States
Wolfhound Parent, Inc.	United States	5725 Innovation Drive, Troy MI 48098-2815, United States

SCHEDULE 3

DESCRIPTION OF PROCESSING ACTIVITIES

Employee; Vendors and Customers and General Public and Visitor Data

Aptiv Group is an Irish-American organisation operating in approximately 50 different countries around the world (as listed in Schedule 2). The vast majority of Aptiv employees work in manufacturing roles where their personal data is processed in their own jurisdiction. However, there are manufacturing premises in locations that do not have local support services, like HR. In those cases, HR issues and even vendor management, may be dealt with by central HR operations based in the US. It may also be the case that grievances or disputes relating to key personnel are dealt with centrally in the US where input is required from more senior management. In terms of EEA data, Aptiv has a large manufacturing and shared service site in Poland, Germany, Hungary and Romania and therefore data relating to employees and local vendors of this site may be transferred to the US where necessary for the purposes set out in this schedule.

PART A: EMPLOYEE

Categories of data for:

- Current employees (whatever the type of employment contract, e.g. fixed term, permanent, internship);
- Former employees;
- Individuals applying for employment with the Group;
- Dependents, beneficiaries and family members of current and former employees;
- Emergency contact persons of current and former employees of the Participating Company exporting the data.

Category of Data	Type of Data	Purpose of Processing	Third Countries
Name and Initials	First name / initial Middle name / initial	- Recruitment and job application management;	

	Last name Initials	- To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	Every Participating Company inside of the EEA may transfer personal data described in this section to Participating Companies in the US for the purposes described in the preceding column. In addition, ad hoc transfers of employee data to other countries in which Participating Companies are located may occur in limited cases for example to facilitate a secondment.
Education, and Professional Qualifications	Degrees and schooling Information Licenses and professional memberships Professional certification	- Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not	

		limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - Identity Validation and Management, IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	
Personal characteristics	Name Age Date of birth Gender National Identifiers/Passports Marital status Nationality Leisure and interests Photographs Biometric information, such as fingerprint or retina image Family information	- Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; managing legal/regulatory compliance requirements. - Management and development of employees, and other processing as	

		required for the employment relationship; - Identity Validation and Management, IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	
Personal White Page Information	Home postal address	- Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and	
	Personal telephone number		
	Personal electronic mail address		
	Contacts and interactions		
	Personal cellular, mobile or wireless number		

		administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	
Business White Page Information	Business postal address	- Recruitment and job application management; - To comply with specific requests made by prospective employees prior to entering into an employment agreement; - Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops),	
	Business telephone number		
	Business facsimile number		
	Business electronic mail address		
	Business cellular, mobile or wireless number		
	Personal assistant contact information		

		management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	
Health Related Information	Information about physical or psychological state of health, disease state, medical history, medical treatment, or diagnosis by a health care professional	- Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; managing legal/regulatory compliance requirements. - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	
	Health insurance identification or account number		
Professional and Employment	Occupation / title	- Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as	
	Income / salary / service fees / other compensation		
	User identification and / or employee number as assigned by an employer		

	User employee account or other password Employment history, evaluations and disciplinary actions Employer or taxpayer identification number Digitized or other electronic signature Date of hire Calendar information/Call logs Information relating to employee job (such as job title, company, department number, supervisor, work phone and business email) Standard hours CCTV Audio-Visual Streaming and Recording Whistle-blowing matters Emergency contact details Payroll information Absences and leaves Information relating to benefits Information relating to expenses Information relating to bonus Resume and summary of work experience and education	required for the employment relationship; managing legal/regulatory compliance requirements, investigations and audit; cyber and physical security management. - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	

	Training courses completed		
	Use of Company Group assets and facilities		
	Work product		
	Digital communications and devices using company assets		
	Job position being applied for		
Confidential Personal Information	Sexual behavior or sexual preference	- Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; managing legal/regulatory compliance requirements. - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures. - Information on sexual behaviour or sexual preference or racial or ethnic	
	Racial or ethnic origin		
	Religious beliefs		
	Trade union membership		
	Health insurance number		
	Background checks		
	Criminal convictions		
	Children's Data		

		origin may be provided by an employee on a voluntary basis in relation to legal dispute, HR grievance or investigation particularly relating to discrimination claims.	
Other Confidential Information	National identification number State/province-issued identification number Driver's or operator's license number Passport number Migration/Citizenship information Other government-issued identification number (e.g. country-identification) Credit report information Insurance claim history IP address Password/Security hint/questions	- Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies; - Management and development of employees, and other processing as required for the employment relationship; managing legal/regulatory compliance requirements. - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	
Financial Information/Payment Card Industry Information	Financial institution account details	- Management and development of Group business including, but not limited to, reporting and analysis to increase operational efficiencies;	

	Details of financial transactions or account Information (e.g., account balance Information, payment history, overdraft history, and credit or debit card purchase information)	- Management and development of employees, and other processing as required for the employment relationship; managing legal/regulatory compliance requirements. - IT and information processing support, IT applications and systems maintenance, and data storage relating to: internal management and administration in relation to employees and staff, employee support, recruitment, hiring and compensation, benefits management and administration, company physical asset management (e.g. laptops), management forecasting, training, succession planning, career development and compliance with respect to company policies and procedures.	
	Company credit / debit card data		

PART B: VENDORS AND CUSTOMERS

Categories of data for:

- Vendor's current and former employees and vendors / contractors; and
- Customer's current and former employees and vendors / contractors.

Category of Data	Type of Data	Purpose of Processing	Third Countries
Name and Initials	First name / initial	- Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.	Every Participating Company inside of the EEA may transfer personal data described in this section to Participating Companies in the US for the purposes described in the preceding column.
	Middle name / initial		
	Last name		
	Initials		
Education, and Professional Qualifications	Licenses and professional memberships	- Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.	
	Professional qualifications and certification		
Personal characteristics	Photographs	- Management and development of Group business relations;	

	Biometric information, such as fingerprint or retina image	- Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.	
Business White Page Information	Business postal address	- Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.	
	Business telephone number		
	Business facsimile number		
	Business electronic mail address		
	Business cellular, mobile or wireless number		
	Personal assistant contact information		
Professional and Employment	Occupation / title	- Management and development of Group business relations; - Decision-making with regards to the development and operation of Group business; - Providing goods and services to Group or Group's customers as described in contracts.	
	User identification and / or employee number as assigned by an employer		
	User employee account credentials		
	Digitized or other electronic signature		
	Information relating to employee job (such as job title, company,		

	department number, supervisor, work phone and business email)		

PART C: GENERAL PUBLIC AND VISITORS

Categories of data for:

- Visitors to our physical premises; and
- Visitors to our websites.

Category of data	Type of data	Purpose of Processing	Third Countries
Personal interests and website visitors' behaviour	Cookies Information	Improvement of user experience Improvement of web facing products	Every Participating Company inside of the EEA may transfer personal data described in this section to Participating Companies in the US for the purposes described in the preceding column.
	IP address		
	Preferences		
Personal identification of people to physical premises	Pictures and video recording	Test Driving Activities Security CCTV AV Media	

	Names, Contact Details	Access to Facilities	

10.