ANNEX [●]

**Standard contractual clauses**

SECTION I

*Clause 1*

***Purpose and scope***

1. The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2. The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
3. These Clauses apply to the processing of personal data as specified in Annex II.
4. Annexes I to IV are an integral part of the Clauses.
5. These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
6. These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

*Clause 2*

***Invariability of the Clauses***

1. The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
2. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

*Clause 3****Interpretation***

1. Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
3. These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

*Clause 4****Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 5 - Optional****Docking clause***

1. Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.
2. Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.
3. The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

**OBLIGATIONS OF THE PARTIES**

*Clause 6*

***Description of processing(s)***

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

*Clause7*

***Obligations of the Parties***

* 1. **Instructions**

1. The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
2. The processor shall immediately inform the controller if, in the processor’s opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.
   1. **Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

* 1. **Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

* 1. **Security of processing**

1. The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.
2. The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
   1. **Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (“sensitive data”), the processor shall apply specific restrictions and/or additional safeguards.

* 1. **Documentation and compliance**

1. The Parties shall be able to demonstrate compliance with these Clauses.
2. The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
3. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller’s request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
4. The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
5. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.
   1. **Use of sub-processors**

|  |  |
| --- | --- |
|  | OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller’s prior specific written authorisation. The processor shall submit the request for specific authorisation at least Choose an item. prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date. |
|  | OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller’s general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least Choose an item. in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object. |

1. Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
2. At the controller’s request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
3. The processor shall remain fully responsible to the controller for the performance of the sub-processor’s obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
4. The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.
   1. **International transfers**
5. Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
6. The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

*Clause 8*

***Assistance to the controller***

1. The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
2. The processor shall assist the controller in fulfilling its obligations to respond to data subjects’ requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller’s instructions
3. In addition to the processor’s obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
4. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a ‘data protection impact assessment’) where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
5. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
6. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
7. the obligations in Article 32 of Regulation (EU) 2016/679.
8. The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

*Clause 9*

***Notification of personal data breach***

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

* 1. **Data breach concerning data processed by the controller**

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

1. in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
2. in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller’s notification, and must at least include:
3. the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
4. the likely consequences of the personal data breach;
5. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

1. in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.
   1. **Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

1. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
2. the details of a contact point where more information concerning the personal data breach can be obtained;
3. its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller’s obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

*SECTION III*

**FINAL PROVISIONS**

*Clause 10*

***Non-compliance with the Clauses and termination***

1. Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
2. The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
3. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
4. the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
5. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
6. The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
7. Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

*ANNEX I*

**List of parties**

**Controller(s):** [*Identity and contact details of the controller(s), and, where applicable, of the controller’s data protection officer]*

Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Contact person’s name, position and contact details: Click or tap here to enter text.

Signature: Click or tap here to enter text.

Accession date: Click or tap to enter a date.

\* \* \* \*

**Processor(s):** [*Identity and contact details of the processor(s) and, where applicable, of the processor’s data protection officer]*

Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Contact person’s name, position and contact details: Click or tap here to enter text.

Signature: Click or tap here to enter text.

Accession date: Click or tap to enter a date.

\* \* \* \*

*ANNEX II*

**Description of the processing**

*Categories of data subjects whose personal data is processed*

Candidates

Consumers

Dealers' representatives

Employees

Employees' family members

Former employees

Guests

Journalists

Members of the corporate bodies

Proxy holders

Suppliers' representatives (consultants, contractors, agents)

Visitors

*Categories of personal data processed*

Identification information, please specify:

Contact information, please specify:

Family information, please specify:

Professional information, please specify:

Financial information, please specify:

Digital information, please specify:

Sensitive information, please specify below (where applicable):

Other information, please specify:

*Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

*Nature of the processing*

Performance of the services pursuant to the agreement.

*Purpose(s) for which the personal data is processed on behalf of the controller*

*Duration of the processing*

Until the termination of the services, unless otherwise indicated in written by Pirelli.

*For processing by (sub-) processors, also specify subject matter, nature and duration of the processing*

Performance of the services pursuant to the agreement and until its termination, unless otherwise indicated in written by Pirelli.

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller*

[*Where applicable*]

*ANNEX III*

**Technical and organisational measures to ensure the security of the data**

Below is the baseline technical and organizational measures that Pirelli requires suppliers acting as processor(s) (“**Supplier(s)**”) to adopt and implement for ensuring an appropriate level of security of its personal data (“**Pirelli Personal Data**”). The list below shall be read jointly with any other technical document, checklist or certification in place between Pirelli and Supplier on technical and organizational measures applicable to the processing of Pirelli Personal Data.

In case changes to the baseline technical and organizational measures listed below become necessary, Supplier must promptly notify Pirelli in writing about such changes. All changes must remain consistent with the overall baseline security measures below and they shall never lead to a downgrade of said measures.

## **Policies and Procedures**

Supplier shall have in place policies and/or procedures regarding the areas listed below. Such policies and/or procedures shall be subject to periodic review.

### **Accountability**

Supplier must identify, and communicate the relevant details to Pirelli, a “*Point of Contact*” in charge of the IT security of assets and systems used to process Pirelli Personal Data. Supplier shall also communicate in advance to Pirelli the contacts of the personnel in charge for the communication of personal data breaches. To the maximum extent possible, Supplier should also ensure the continuous availability of such personnel on a 24/7 basis – especially in cases of emergency.

### **Business continuity**

Security requirements for guaranteeing system back-up and business continuity planning must be in place, especially with respect to assets used to process Pirelli Personal Data. To that extent, Supplier shall maintain the ability to restore the availability and access to Pirelli Personal Data in a timely manner in order to avoid any service interruption.

### **Security Training and Instructions**

Dedicated training activities for the improvement of IT security awareness within Supplier’s company structure must be performed. Supplier personnel shall receive detailed instructions on the secrecy and integrity of their access credentials, as well as on the diligent custody and protection of their assigned devices, tools and systems – with specific reference to those used to process Pirelli Personal Data.

### **Logging and monitoring**

Systems and tools used by Supplier to process Pirelli Personal Data must have logging and monitoring mechanisms in place. With respect to logs, Supplier shall generate and retain logs for the period required by applicable laws (or otherwise agreed with Pirelli) and, in any case, keep such logs for at least 6 (six) months from their generation. With respect to monitoring, Supplier shall ensure traceability of all operations carried out on Pirelli Personal Data through its systems and tools by adopting and implementing adequate tracking measures.

### **Data loss prevention**

Supplier shall have in place policies and/or procedures that prevent data export outside Supplier’s network. In case of sharing of Pirelli Personal Data, Supplier shall adopt adequate confidentiality measures.

### **Management of Personal Data Breaches**

Supplier shall have in place policies and/or procedures relating to the management of personal data breaches. Said policies and procedures should be known by Supplier’s personnel and periodically reviewed and audited by Supplier.

## **Asset Management**

### **Asset inventory**

Supplier shall have in place and keep updated an inventory of all assets used to process Pirelli Personal Data.

### **Asset protection**

Supplier shall protect the assets used to process Pirelli Personal Data according to international industry standards and best practices. Protective measures shall include at least: use of antivirus software, firewalls, IDS/IPS modules and anti-spam solutions.

### **Asset lifecycle management**

Supplier must ensure all assets that process Pirelli Personal Data, as well as any cybersecurity solution required in Pirelli service delivery (e.g. antivirus, firewalls, IDS/IPS modules) are always updated to the last software version available. Where updates are not possible or not applied yet, Supplier shall define an update plan and an overall risk mitigation plan to manage any relevant risk relevant to system obsolescence (e.g. segregation implementation, monitoring, etc.).

### **Cyber security risk assessments**

Supplier shall carry out a risk assessment on the IT systems used to carry out the services for Pirelli, especially taking into account all the risks that presented by the processing of Pirelli Personal Data. Such risk assessment shall occur either on a yearly basis or when required under applicable laws and regulations.

## **Encryption**

### **Encryption measures**

Taking into account the state of the art of technology and encryption techniques, Supplier shall implement encryption at different levels:

* **Encryption at rest**: Supplier shall have in place proper encryption techniques to protect confidentiality of Pirelli Personal Data at rest at different levels (e.g. full disk encryption on mass drives; transparent data encryption on databases; file-level encryption).
* **Encryption in transit**: Supplier shall have in place proper encryption techniques to protect confidentiality of Pirelli Personal Data in transit (e.g. network encryption, application encryption, etc.).
* **Encryption key management**: Supplier shall have in place proper solutions and a defined process of Encryption key management, ensuring at least the segregation of ownerships between key owners and data owners.
* **Encryption certificates management**: Supplier shall have in place proper solutions and a clear and documented process for the management of encryption certificates. Such process shall be developed according to requirements defined by international industry standards (e.g. minimum length of encryption keys).

## **Identity and Access Management**

### **Access to Pirelli Personal Data**

Supplier shall guarantee that Pirelli Personal Data can be accessed only by authorized personnel with appropriate expertise and experience in data protection matter and that the personnel is subject to confidentiality obligations.

Supplier shall keep and regularly update a list of all the persons (including any employee, agent or contractor) acting under its authority or under the authority of any sub-processors, who have access or otherwise process Pirelli Personal Data.

### **Measures and Principles for user identification and authorization**

Supplier shall implement systems for user authentication and authorization management. Supplier shall assign the minimum access permissions to Pirelli Personal Data according to the principles of “*Least privilege and Need-to-know*” (i.e. allowing access only to the data necessary to perform the relevant work function). Supplier shall also review the permissions to grant users based on their role in the processing of Pirelli Personal Data, as well as in light of any applicable regulatory requirement on user identity and access management.

### **Profile review**

Supplier shall review the consistency and presence of user authorization profiles at least annually and it shall keep track of this activity when it pertains to Pirelli Personal Data.

### **Credentials security**

Supplier shall adopt international standards and best practices on credentials security requirements on all assets used to process Pirelli Personal Data.

### **Individual credentials**

Supplier shall assign only individual credentials on any assets used to process Pirelli Personal Data (especially those with high permissions on systems and applications). The assignment and use of any shared credentials is strictly forbidden.

### **Identity lifecycle**

Supplier shall have a clear process for identity lifecycle management. Such process must ensure that all credentials used to access assets used to process Pirelli Personal Data automatically expire after a pre-determined period of non-use by users.

# **physical security**

### **Security of Data Processing Centers (“DPCs”)**

Supplier shall have in place physical security measures developed according to main industry standards and best practices such as, at least: installation of burglar alarms and CCTVS, both as regards the premises and the entrances to DPCs. Supplier shall also have in place procedures to limit physical access to DPCs (e.g. anti-intrusion turnstiles), preventing unauthorized activities and report access activities (e.g. multiple failed access attempts).

### **Positioning of DPCs**

Supplier shall disclose Pirelli, upon request, the locations of DPCs used to process Pirelli Personal Data. Pirelli must be informed in advance in case of any changes to the location of the DPCs.

# **Security Operations**

### **System security**

Supplier shall have in place proper measures to reduce the vulnerabilities of the assets used to process Pirelli Personal Data by enforcing adequate configurations and avoiding any unauthorized changes (e.g., control of removable device).

### **Security development guidelines**

In case of development of software used to processes Pirelli Personal Data, Supplier shall adopt secure code writing guidelines.

### **Security patch management**

Supplier shall manage the installation and de-installation of patches with a process, developed according to industry best practices and standards that ensures traceability and timing of patching activities.

### **Vulnerability assessment**

Supplier shall provide evidence of vulnerability assessment or penetration test activities performed on its systems.

## **Personal data breaches**

### **Notification to Pirelli**

In case of a personal data breach regarding Pirelli Personal Data, Supplier shall promptly notify Pirelli through [Personal\_Data\_Breach@pirelli.com](mailto:Personal_Data_Breach@pirelli.com). Timing for notification of the breach shall be as follows:

1. **Key information** (simple email communication including at least the elements described in relevant clauses of the SCCs): no later than 12 hours after having become aware of the breach.
2. **Full report** (based on the *Security Incident Report* available at this [link](https://psi-dotcom-prd.s3.eu-west-1.amazonaws.com/suppliers-portal/en-ww/Security_Incident_Report_WW.docx) or, as an alternative, in a dedicated Supplier’s format, which includes the information requested in Pirelli *Security Incident Report*): no later than 48 hours after notification of the key information above.

*ANNEX IV*

**List of sub-processors**

The controller has authorised the use of the following sub-processors:

Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Contact person’s name, position and contact details: Click or tap here to enter text.

Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Click or tap here to enter text.

\* \* \* \*