stratio

DATA PROCESSING AGREEMENT

This document sets out the Data Processing Agreement ("**DPA"**) for the processing of personal data during the execution and after the termination of the Contract entered into between STRATIO and Customer, as required by article 28, no. 3 of GDPR.

1. Definitions

1.1. In addition to the terms defined in the Contract, in this DPA all the definitions set forth in article 4 of GDPR shall be adopted, namely the terms "**Personal Data**", "**Data Subjects**", "**Processing**", "**Personal Data Breach**", "**Pseudonymization**", "**Controller**" and "**Processor**".

1.2. In addition to the above, the following definitions shall be adopted:

"**Data Protection Law**"	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, commonly known as the "**General Data Protection Regulation**" or "**GDPR**" as well as any other applicable national rule and legislation on the protection of personal data in the European Union or locally that is already in force or that will come into force during the term of this DPA, including any measure, guideline and opinion issued by the European data protection authorities or by the European Data Protection Board ("**EDPB**").
"**Persons in Charge of Data Processing**"	means the employees and any natural persons who, authorized by the Processor and/ or its sub-processors, if any, can process the Processed Data;
"Processed Data"	all the personal data processed by the Processor on behalf of the Controller under the Services, as better defined in **Appendix I.a – Description of Processing**.
"**Security Measures**"	means the security measures and any other obligations under the Data Protection Law for the purposes of guaranteeing the security and confidentiality of the Processed Data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures, as well as procedures and activities to be performed in case of a personal data breach to prevent and reduce the adverse effects of the breach on the affected data subjects, in particular, those identified in **Appendix I.b – Security Measures**;
"**Sub-Processor**"	means the legal person, company or independent professional who, authorized by the Controller and engaged with the Processor, is allowed to carry out activities entailing the process of the Processed Data, as permitted under Data Protection Law and this DPA. Authorized sub-Processors are detailed in **Appendix I.c – General Authorization for Sub-processing**

"**Standard Contractual Clauses**"	means the Standard Contractual Clauses based on the Commission Implementing Decision (EU) 2021/914, of 4 June 2021, as amended or updated from time to time, and similar clauses enacted pursuant to the Data Protection Law.

2. Scope

2.1. STRATIO shall act as the Processor in relation to the processing of Processed Data on behalf of the Customer which is qualified as the Controller, exclusively for the purposes of executing the Contract or as required by law, according to the terms and conditions of this DPA and of the Data Protection Law.

2.2. The type of personal data and processing activities to be handled by the Processor are exhaustively described in Appendix I.a – Description of Processing. Any amendment to this list must be done in writing by the signature of both Parties, and a copy of said updated list must be enclosed on the final versions of this DPA.

2.3. In relation to any processing of Processed Data carried out by the Processor or by a Sub-processor, directly or through the respective Persons in charge of the Data Processing, for purposes other than those within the scope of this DPA and the Service engaged, and on the basis of different relationships with data subjects, the Processor or its subsequent Subcontractors shall not act as processors of the Controller in relation to the Processed Data, but as independent data controllers, or processors of entities other than the Controller, as the case may be.

3. Term

3.1. This DPA shall be effective from the Effective Date of the Contract for the provision of the Services up to the end of the transitional period of 90 (ninety) days granted after the termination of such Contract or its related services.

3.2. During the transitional period the Controller will be able to delete, remove or transfer the Processed Data from the Platform, as provided for in the Contract. After such transitional period, the Processor will permanently delete all the Processed Data from the Platform and all the existing copies, unless any applicable law requires storage of the Processed Data.

3.3. The Processor shall ensure that all Persons in Charge of the Processing, its Sub-Processors, if any, and their Persons in Charge of the Processing, comply with the obligations laid down in this DPA, as applicable, in the manner and in accordance with the timing indicated thereunder.

4. Obligations of the Controller

4.1. The Controller undertakes to:

4.1.1. Ensure that the collection and further processing of all Processed Data is done in a lawful manner;

4.1.2. Provide clear and timely written instructions to the Processor regarding the Processed Data;

4.1.3. Assist and cooperate, within a reasonable manner, with the Processor whenever required under the processing of the Processed Data, namely if it suspects of any data breach that could undermine the availability,

integrity, privacy and/or security of the Processed Data;

4.1.4. Inform the Processor of any restriction required to the processing of any Processed Data, regardless if required by a Data Subject or instructed by a relevant data protection supervisory authority;

4.1.5. Keep the processor up to date about the Processed Data or any other relevant information for its processing by the Processor or by its Sub-processors, namely about any notification or request for information from a relevant data supervisory authority.

5. Obligations of the Processor

5.1. The Processor undertakes to:

5.1.1. Process the Processed Data for the sole purpose of performing the Services, subject to the limits of this DPA and the Data Protection Law, and in strict compliance with the written instructions given by the Controller and shall immediately inform in writing the Controller should it deem that any of the aforesaid instructions is in breach of the Data Protection Law or, in general, of any applicable law;

5.1.2. Process exclusively the Processed Data that is strictly necessary for correctly and fully performing the Service or meeting the obligations provided for by Data Protection Law or other applicable law;

5.1.3. Process the Processed Data lawfully, fairly and in full compliance with the principles applicable to data processing, with the requirements laid down by the Data Protection Law and the information on the processing of the Processed Data provided to the relevant data subjects by the Controller;

5.1.4. Assist and cooperate, within a reasonable manner, with the Controller whenever required under the processing of the Processed Data, namely if it suspects of any data breach that could undermine the availability, integrity, privacy and/or security of the Processed Data;

5.1.5. Inform the Controller of any restriction required to the processing of any Processed Data, regardless if required by a Data Subject or instructed by a relevant data protection supervisory authority, unless if prohibited by law;

5.1.6. Keep the Controller up to date about the Processed Data or any other relevant information, namely about any notification or request for information from a relevant data supervisory authority;

5.1.7. Cooperate with and assist the Controller in the response to any notifications from a supervisory authority in connection with the Processed Data, including, without limitation, the provision of supporting documentation to be submitted to the relevant supervisory authority as evidence that the Processor is legally bound by the terms of this DPA;

5.1.8. Provide to the Controller, upon request, all the information in its possession or control referring to the processing of the Processed Data under this DPA, namely for the latter to assess whether such processing is carried out in accordance with this DPA.

5.1.9. Disclose the information reasonably required by the Controller for the performance of privacy impact assessments concerning the processing activities and cooperate on the implementation of mitigation actions

agreed by the Parties to address privacy risks which may have been identified.

5.1.10. Permit, provide information for and cooperate with the Controller regarding audits, including any inspections conducted by the Controller or another auditor mandated by the Controller.

5.2. With regard to the Persons in Charge of the Processing, the Processor further undertakes to:

5.2.1. guarantee that the Persons in Charge of the Processing can access and process only the Processed Data that is strictly necessary for correctly and fully performing the Services or meeting the legal requirements, in each case, subject to the limits and in accordance with the conditions of this DPA, the principal agreement between Controller and Processor for the provision of the Services and the Data Protection Law;

5.2.2. guarantee that the Persons in Charge of the Processing are subject to confidentiality undertakings or professional or statutory obligations of confidentiality;

5.2.3. consent that the Processed Data are processed only by the Persons in Charge of Processing who

(i) on the basis of their experience, capabilities and training, can ensure compliance with the Data Protection Law and need to access the data for the purpose of performing the Service;

(ii) attended periodically training courses on the obligations prescribed by the Data Protection Law;

5.2.4. adopt any physical, technical and organizational measure aimed at enabling:

5.2.4.1. each Person in Charge of the Processing to access exclusively the Processed Data that he/she is authorized to process, by taking into account the activity that he/she is required to carry out to perform the Service;

5.2.4.2. any processing of the Processed Data that is in breach of the DPA and/or the Data Protection Law to be promptly identified and reported to the Controller; and

5.2.4.3. upon termination of the Services and, with respect to each Person in Charge of the Processing, upon termination of the appointment of such Person in Charge of the Processing, including, without limitation, when the employment or collaboration relationship between the Person in Charge and the relevant Processor or Sub-Processor is terminated, ensure total confidentiality, availability and integrity of the Processed Data.

6. Sub-processors

6.1. Regarding the Processed Data, the Processor undertakes to engage and work only with sub-processors to which the Controller did not reasonably oppose in writing to said collaboration.

6.2. Sub-processors identified in Appendix I.c – General Authorization for Sub-processing are hereby authorized by the Controller to process Processed

Data provided that said sub-processor:

6.2.1. has committed to confidentiality obligations and enters into a written agreement providing the same data protection obligations as set out in this DPA and other obligations as may be required by the Controller under the instructions of the Processor.

6.2.2. acts exclusively on behalf of the Controller or the Processor instructions;

6.2.3. provides adequate guarantees with reference to the technical and organizational measures adopted for the processing of the Processed Data, including, without limitation, ensuring that the Sub-Processor immediately ceases the processing of the Processed Data should such guarantee be no longer available.

6.3. In case of any intended changes concerning the addition or replacement of any of the Sub-processors identified in Appendix I.c – General Authorization for Sub-processing, the Processor undertakes to notify the Controller, giving the Controller the opportunity to reasonable object to such change within 30 (thirty) days counting from said notification. If the Controller notifies the Processor of any objection to the proposed appointment, the Parties shall work together to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor. Costs related to his change, if any, will be borne by the Controller.

6.4. The Processor shall correctly and completely adopt all the Security Measures in compliance with the Data Protection Law and this DPA.

7. Security measures

7.1. Without limiting the foregoing, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing of the Processed Data, and the likelihood and severity of the risk to the rights and freedoms of natural persons, Processor shall implement appropriate technical and organizational measures to ensure a level of security that is proportionate to the risk associated with the processing of the Processed Data, including, without limitation, the measures provided for by Article 32, paragraph 1 of the GDPR, and in particularly including, but not limited to, the measures identified in Appendix I.b – Security Measures.

8. Processed Data Breach

8.1. In the event of a Personal Data Breach or any other incidents that may compromise the security of the Processed Data (such as loss, damage or destruction of the Processed Data in an electronic or hard copy format, third party unauthorized access to the Processed Data or any other breach of the Processed Data) including, without limitation, any breach or other incident resulting from the conduct of, if any, the Processor's Sub-Processors and/or its Persons in Charge of the Processing, the Processor shall:

8.1.1. immediately and without undue delay inform the Controller by email which shall include at least information regarding the type and description of the Personal Data Breach, identification of the Processed Data and of the Data Subjects affected and potential consequences of said breach, as well as any remedies already put in place (if any). Where and insofar is not

possible to provide all the relevant information at the same time, the information may be provided in phases without undue delay;

8.1.2. in collaboration with the Controller, adopt immediately, and in any case without undue delay, all necessary measures to minimize any type of risk that may derive for the Data Subjects from such breach or incident, remedy such breach or incident and mitigate any possible adverse effect.

8.2. The Controller is fully liable, whenever required, for notifying such Personal Data Breach to the relevant data protection supervisory authority and to the Data Subjects, if applicable.

9. Data Subjects' Rights

9.1. The Controller shall ensure that the rights granted to the Data Subjects by the Data Protection Law are effectively executed. The Processor undertakes to notify the Controller in writing within 5 (five) Business Days of receipt of any request made in this respect by the Data Subjects.

9.2. The Processor shall cooperate with the Controller to ensure that all requests by Data Subjects exercising their rights under the Data Protection Law (including, without limitation, the right to object to the processing and the right to the Processed Data portability) are complied with within the time period and in accordance with all other requirements provided for by the Data Protection Law.

10. Audits

10.1. The Processor acknowledges and accepts that the Controller may assess the organizational, technical and security measures adopted by the Processor in the processing of the Processed Data by way of audit no more frequent than annually (unless if in the context of a Processed Data breach). To this end, upon no less than ten (10) Business Days' prior written notice (except if there is a reasonable urgency of the Controller for an earlier prior notice), the Controller will be entitled to request information about the processing of the Processed Data, if Controller reasonably deems it necessary to verify compliance by the Processor and/or one of its Sub-Processors with this DPA and the Data Protection Law or to ascertain any breach of the Processed Data.

11. Transfers of Processed Data outside the EEA

11.1. The Processor will carry out the processing only in the European Economic Area ("EEA") and agrees not to transfer the Processed Data outside the EEA, without the Controller's prior written consent or unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

11.2. When the Processor transfers personal data with the Controller's consent, as provided for in clause 11.1 above, such transfer is made in accordance with the provided for in Chapter V of the GDPR and with the instructions given by the Controller in relation to such transfer.

11.3. When any of the Sub-processors identified in Appendix I.c, as amended

pursuant to clause 6.3, is established outside the EEA, the Processor, acting as data exporter, shall ensure that whenever there is no adequacy decision in place as set forth in article 45 of the GDPR, it will execute Standard Contractual Clauses as timely approved by the European Commission.

11.4. Further to the cases abovementioned, where appropriate safeguards are applicable the Processor agrees that its sub-processors will only process personal data in accordance with article 49 of the GDPR.

12. Miscellaneous

12.1. Governing law: this DPA will be governed by the same laws governing the Contract.

12.2. Dispute resolution: any dispute arising from or in connection with the negotiation, signature, execution, performance or termination of this DPA shall be governed by the same Jurisdiction applicable to the Contract

12.3. STRATIO may from time to time propose new and updated versions of any Appendixes of this DPA as follows:

12.3.1. In case Customer and STRATIO agree on any change to the Services which subsequently affects or changes the Processed Data, STRATIO will circulate a new and updated version of Appendix I;

12.3.2. If STRATIO changes any of the sub-processors identified in Appendix I.c;

12.3.3. If STRATIO updates any of the Security Measures set forth in Appendix I.b.

12.4. STRATIO will notify Customer of any update to the Appendixes as set out above, and shall give to Customer a prior 30 days' notice before the new Appendix version enter in effect. During that period, Customer has the right to refuse the modification(s), in which case STRATIO has the option to: a) accept the refusal of the Customer, hence the previous clauses will continue to apply, b) negotiate the amends required by Customer in an autonomous document or c) terminate the Contract.

Appendix I.a - Description of processing

Brief description of the processing activities	Purpose of the processing	Categories of Data Subjects involved	Type of Personal Data
Implementing the Services	Providing Customer with the necessary tools to gain access to the Services; provide the services to Customer	• Drivers using Customer's vehicles • Other employees and individual contractors of Customer	• Plate number • Vehicle Identification Number (VIN) • Tachograph • Geolocation • ID number (encrypted by Customer and to which STRATIO does not have the private decrypting key)
Providing Support & Maintenance assistance	Providing Customer with support to the Services as required or convenient. Providing maintenance and upgrading to the Services as required or convenient	• Employees and other individuals who may be working to Customer or acting on its behalf	• Name • Surname • Professional email • Phone number • Mobile number • Job position • Professional address
Negotiating upgrades and changes to the Services	Negotiating new order forms and/or statement of works to amend or upgrade the Services provided to Customer	• Employees and other individuals who may be working to Customer or acting on its behalf	• Name • Surname • Professional email • Phone number • Mobile number • Job position • Professional address

(**Version:** October 2021)

Appendix I.b – Security Measures

Processor shall maintain and enforce various policies, standards and processes designed to secure personal data and other data to which Processor employees are provided access, and updates such policies, standards and processes from time to time consistent with industry standards. Without prejudice to the rules contained within Clause 6 (Security Measures) of the Agreement, the Processor shall implement appropriate technical and organizational measures to ensure a level of security adequate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of the data subjects. These measures shall ensure full compliance with Article 32 of the GDPR. Following is a description of some of the core technical and organizational security measures implemented by Processor as of the date of signature:

1. General Security Procedures

1.1. Processor shall be responsible for establishing and maintaining an information security program that is designed to: (i) protect the security and confidentiality of Personal Data; (ii) protect against anticipated threats or hazards to the security or integrity of the Personal Data; (iii) protect against unauthorized access to or use of the Personal Data; (iv) ensure the proper disposal of Personal Data, as further defined herein; and, (v) ensure that all employees and subcontractors of Processor, if any, comply with all of the foregoing. Processor will designate an individual to be responsible for the information security program. Such individual shall respond to Controller inquiries regarding computer security and to be responsible for notifying Controller-designated contact(s) if a breach or an incident occurs, as further described herein.

1.2. Processor shall conduct formal privacy and security awareness training for all personnel and contractors as soon as reasonably practicable after the time of hiring and/or prior to being appointed to work on Personal Data and annually recertified thereafter. Documentation of security awareness training shall be retained by Processor, confirming that this training and subsequent annual recertification process have been completed.

1.3. Controller shall have the right to review an overview of Processor's information security program prior to the commencement of Service and annually thereafter upon Controller request.

1.4. In the event of any apparent or actual theft, unauthorized use or disclosure of any Personal Data, Processor shall immediately commence all reasonable efforts to investigate and correct the causes and remediate the results thereof, and within 2 business days following confirmation of any such event, provide Controller notice thereof, and such further information and assistance as may be reasonably requested. Upon Controller's request, remediation actions and reasonable assurance of resolution of discovered issues shall be provided to Controller.

1.5. Processor will not transmit any unencrypted Personal Data over the internet or any unsecured network, and will not store any Personal Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing

device is protected by industry-standard encryption software. Processor shall encrypt Personal Data in transit into and out of the Services over public networks using industry standard protocols.

2. Network and Communications Security

2.1. All Processor connectivity to Controller computing systems and/or networks and all attempts at same shall be only through Controller's security gateways/firewalls and only through Controller-approved security procedures.

2.2. Processor will not access, and will endeavor its best efforts to prevent unauthorized persons or entities to access, Controller computing systems and/or networks without Controller's express written authorization and any such actual or attempted access shall be consistent with any such authorization.

2.3. Processor will take appropriate measures to ensure that Processor's systems connecting to Controller's systems and anything provided to Controller through such systems does not contain any computer code, programs, mechanisms or programming devices designed to, or that would enable, the disruption, modification, deletion, damage, deactivation, disabling, harm or otherwise be an impediment, in any manner, to the operation of Controller's systems.

2.4. Processor will maintain technical and organizational measures for data protection including: (i) firewalls and threat detections systems to identify malicious connection attempts, to block spam, viruses and unauthorized intrusion; (ii) physical networking technology designed to resist attacks by malicious users or malicious code; and (iii) encrypted data in transit over public networks using industry standard protocols.

3. Personal Data Handling Procedures

3.1. Disposal of Personal Data on paper shall be done in a secure manner, to include shredders or secure shredding bins within Processor space from which Personal Data is handled or accessed ("Controller Work Area"). Shredding must take place within the Controller Work Area before disposal or transit outside of the Controller Work Area or be performed offsite by a reputable third party under contract with Processor.

3.2. Erasure of Information and Destruction of Electronic Storage Media. All electronic storage media containing Personal Data must be wiped or degaussed for physical destruction or disposal, in a manner meeting forensic industry standards such as the NIST SP800-88 Guidelines for Media Sanitization, prior to departing Controller Work Area(s), with the exception of encrypted Personal Data residing on portable media for the express purpose of providing service to the Controller. Processor shall maintain commercially reasonable documented evidence of data erasure and destruction for infrastructure level resources. This evidence must be available for review at the request of Controller.

3.3. Processor shall maintain authorization and authentication technologies and processes to ensure that only authorized persons access Personal Data, including: (i) granting access rights on the basis of the need-to-know-principle; (ii) reviewing and maintaining records of employees who have been authorized or who can grant, alter or cancel authorized access to systems; (iii) requiring personalized, individual access accounts to use passwords that meet complexity,

length and duration requirements; (iv) storing passwords in a manner that makes them undecipherable if used incorrectly or recovered in isolation; (v) encrypting, logging and auditing all access sessions to systems containing Personal Data; and (vi) instructing employees on safe administration methods when computers may be unattended such as use of password protected screen savers and session time limits.

3.4. Processor shall maintain logical controls to segregate Personal Data from other data, including the data of other customers.

3.5. Processor shall maintain measures to provide for separate processing of data for different purposes including: (i) provisioning Controller within its own application-level security domain, which creates logical separation and isolation of security principles between customers; and (ii) isolating test or development environments from live or production environments.

4. Physical Security

4.1. All backup and archival media containing Personal Data must be contained in secure, environmentally controlled storage areas owned, operated, or contracted for by Processor. All backup and archival media containing Personal Data must be encrypted.

4.2. Technical and organizational measures to control access to data center premises and facilities are in place and include: (i) staffed reception desks or security officers to restrict access to identified, authorized individuals; (ii) visitor screening on arrival to verify identity; (iii) all access doors, including equipment cages, secured with automatic door locking systems with access control systems that record and retain access histories; (iv) monitoring and recording of all areas using CCTV digital camera coverage, motion detecting alarm systems and detailed surveillance and audit logs; (v) intruder alarms present on all external emergency doors with one-way internal exit doors; and (vi) segregation of shipping and receiving areas with equipment checks upon arrival.

4.3. Processor shall maintain measures to protect against accidental destruction or loss of Personal Data including: (i) fire detection and suppression, including a multi-zoned, dry-pipe, double-interlock, pre-action fire suppression system and a Very Early Smoke Detection and Alarm (VESDA); (ii) redundant on-site electricity generators with adequate supply of generator fuel and contracts with multiple fuel providers; (iii) heating, ventilation, and air conditioning (HVAC) systems that provide stable airflow, temperature and humidity, with minimum N+1 redundancy for all major equipment and N+2 redundancy for chillers and thermal energy storage; and (iv) physical systems used for the storage and transport of data utilizing fault tolerant designs with multiple levels of redundancy.

5. Security Testing

During the performance of services under the Agreement, Processor shall engage periodically a Third-Party (“Testing Company”) to perform penetration and vulnerability testing (“Security Tests”) with respect to Processor’s systems containing and/or storing Personal Data.

The objective of such Security Tests shall be to identify design and/or functionality issues in applications or infrastructure of the Processor systems containing and/or storing

Personal Data, which could expose Controller's assets to risks from malicious activities. Security Tests shall probe for weaknesses in applications, network perimeters or other infrastructure elements as well as weaknesses in process or technical countermeasures relating to the Processor systems containing and/or storing Personal Data that could be exploited by a malicious party.

Security Tests shall identify, at a minimum, the following security vulnerabilities: invalidated or un-sanitized input; broken or excessive access controls; broken authentication and session management; cross-site scripting (XSS) flaws; buffer overflows; injection flaws; improper error handling; insecure storage; common denial of service vulnerabilities; insecure or inconsistent configuration management; improper use of SSL/TLS; proper use of encryption; and anti-virus reliability and testing.

Within a reasonable period after the Security Test has been performed, Processor shall notify Controller in writing of any critical security issues that were revealed during such Security Test which have not been remediated. To the extent that critical security issues were revealed during a particular Security Test, Processor shall subsequently engage, at its own expense, the Testing Company to perform an additional Security Test to ensure resolution of identified security issues. Results thereof shall be made available to the Controller upon request.

6. Security Audit

Processor, and all subcontracted entities (as appropriate) will perform whenever convenient detailed security and vulnerability tests and assessments against all systems processing Personal Data conducted by independent third-party security experts that include a thorough code analysis and a comprehensive security audit, and shall perform regular (i.e. at least bi-annually) penetration tests (for exploits including, but not limited to, XSS, SQL injection, access controls, and CSRF) against any Internet-facing systems used in connection with the Services. Processor further agrees to perform regular risk assessments of the physical and logical security measures and safeguards it maintains applicable to its protection of Personal Data. Processor will provide Controller, upon request, a summary report of such tests and assessments, including a description of any significant (i.e., moderate or greater) risks identified and an overview of the remediation effort(s) undertaken to address such risks, and attest to Controller the date of the most recent security and vulnerability assessment at Controller reasonable request.

7. Anonymization and Pseudonymization of personal data

7.1. When possible, the Processor should ensure that data is anonymized or pseudonymized before data processing operations.

7.2. When pseudonymizing data, the key for reverting the process should be protected and stored in an adequate manner and according to industry standards.

7.3. Anonymization should be preferred to pseudonymization.

7.4. The Processor should guarantee the anonymization is not reversible, in accordance with the technological state of the art.

8. Other technical and organizational measures

8.1. A Data Protection Officer should be appointed when the applicable legislation or good practices requires it.

8.2. When available for the Processor's industry, the Processor should acquire/adhere to Codes of Conduct and/or independent Certification regarding the processing of Personal Data and in accordance with the GDPR.

8.3. The Processor should keep itself updated of any developments to legislation, case-law or opinions from supervisory authorities regarding subjects that are relevant for the provision of services and inform the Controller if it considers that any of the above may have an impact on the services the Processor provides.

(**Version:** October 2021)

stratio

Appendix I.c – General Authorization for Sub-processing

Sub-Processor	**Purpose**	**Entity Country**	**Appropriate safeguards** *(Only applicable to transfers of data outside the EEA)*	**Onward Transfers** *(Y/N)*
AWS	Cloud services for storage and software hosting	Ireland	[…]	No

(**Version:** October 2021)