

***Template***

**DATA PROCESSING AGREEMENT**

|  |  |
| --- | --- |
| Code Document  | 29e-BM/SG/HDCV/FSOFT |
| Version | 1.3 |
| Effective date |  01.11.2022 |

Table of content

[1 INTRODUCTION 5](#_Toc104984171)

[1.1 Definitions 5](#_Toc104984172)

[2 PROCESSING OF PERSONAL DATA 7](#_Toc104984173)

[2.1 Processor/Importer Obligations 7](#_Toc104984174)

[2.2 Controller’ Obligation 7](#_Toc104984175)

[3. PROCESSOR PERSONAL 8](#_Toc104984176)

[4. TECHNICAL AND ORGANIZATION SECURITY MEASURES 9](#_Toc104984177)

[5. SUB–PROCESSING 10](#_Toc104984178)

[6. DATA SUBJECT RIGHTS 11](#_Toc104984179)

[7. PERSONAL DATA BREACH 12](#_Toc104984180)

[8. DATA PROTECTION IMPACT ASSESSMENT (DPIA) 14](#_Toc104984181)

[9. TRANSFER IMPACT ASSESSMENT (TIA) 15](#_Toc104984182)

[10. AUDIT 16](#_Toc104984183)

[11. INTERNATIONAL TRANSFER 17](#_Toc104984184)

[12. GENERAL TERMS 18](#_Toc104984185)

[12.1 Order of precedence 18](#_Toc104984186)

[12.2 Changes in Data Protection Laws or Regulations 18](#_Toc104984187)

[12.3 Severance 18](#_Toc104984188)

[13. MISCELLANEOUS 19](#_Toc104984189)

[14. SIGNATURE 20](#_Toc104984190)

[APPENDIX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA 21](#_Toc104984191)

[APPENDIX 2: STANDARD CONTRACTUAL CLAUSES (PROCESSORS) 22](#_Toc104984192)

RECORD OF CHANGE

| No | Effective Date | Version | Change Description | Reason | Reviewer | Final Reviewer | Approver |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01.05.2021 | 1.0 | Newly issued | Legal requirement | TrangNN4 | Michael Hering | HoanNK |
| 2 | 01.10.2021 | 1.1 | New version of SCC came in force 06/2021, reference Template\_Standard Contractual Clauses\_v2.0 | Legal requirement | TrangNN4 | Michael Hering | HoanNK |
| 3 | 01.04.2022 | 1.2 | Appendix 2 changed to: Template\_Standard Contractual Clauses\_v2.2, Template\_GDPR Example To Measures\_v1.1 | Biannually revision | LinhDTD1 | Michael Hering | HoanNK |
| 4 | 01.11.2022 | 1.3 | Added: 9 Transfer Impact Assessment TIA | Biannually revision | LinhDTD1 | Michael Hering | HoanNK |

**DATA PROCESSING AGREEMENT**

Contract concerning the collection, processing, or use of personal data in commission pursuant to the European Union General Data Protection Regulation Article 28, APPI, PDPA or other national Personal Data Protection Regulations and the national laws for cross-border data transmission, including in countries that do not yet have adequate data protection laws.

Between

**Company name**

Address

Phone number:

E-mail:

Corporate ID:

Registered in the Commercial register of …I District Court, Section: … No...,
represented by …, Managing director/CEO

 **As data** **exporter/controller**

And

**Company name**

Address

Phone number:

E-mail:

Corporate ID:

Registered in the Commercial register of …I District Court, Section: … No...,
represented by …, Managing director/CEO

**As data** **importer/processor**

# INTRODUCTION

For the purpose of this Agreement, the terms “Controller”, “Processor”, “Data Subjects”, “Personal Data”, “Processing”, “Personal Data Breach”, “Binding Corporate Rules”, “Supervisory Authority” shall have the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing General Data Protection Regulation or GDPR.

## Definitions

In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

**Applicable Laws** means any applicable constitution, treaty, statute, rule, regulation, ordinance, order, directive, code, interpretation, judgment, decree, injunction, writ, determination, award, permit, license, authorization, requirement or decision of or agreement with or by any legislative, administrative, judicial or other governmental authority relating in any way to the privacy, confidentiality, security or protection of Personal Data or Personal Information, as they may be amended from time to time, in any jurisdiction, including without limitation EU General Data Protection Regulation (EU) 2016/679 (“GDPR”), and national laws implementing the GDPR, as amended from time to time, Canada’s Personal Information Protection and Electronics Documents Act; Canada’s Anti-Spam Legislation; the California Consumer Privacy Act of 2018, Cal. Civil Code section 1798.100 et seq., (“CCPA”); Act on the Protection of Personal Information, Japan, 30 May 2017 (APPI); Personal Data Protection Act 2012, Singapore (PDPA); Personal Data (Privacy) Ordinance, Hongkong, 2012 (PDPO); South Korea’s substantial Personal Information Protection Act (PIPA) was enacted on Sept. 30, 2011; applicable laws regulating the Internet and unsolicited email communications; applicable laws relating to security breach notification; applicable laws imposing minimum security requirements; applicable laws requiring the secure disposal of records containing certain personal information.

**Company Affiliate** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

**Company Group Member** means Company or any Company subsidiary or legal entity.

**Personal Data** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Company Personal Data** means any Personal Data processed by a Processor on behalf of a Company Group Member.

**Data Protection Laws** means EU Data Protection Laws GDPR, its UK specific derogations and, to the extent applicable, the data protection or privacy laws of any other country like APPI, PDPA, PDPO, PIPA, PIPEDA., CCPA.

**EEA** means the European Economic Area.

**Transfer** means transfers of personal data by any business in the European Economic Area (“EEA”) to outside the EEA e.g., where data is to be held on servers abroad, or emails or attachments containing personal data are sent to recipients abroad, are unlawful unless within narrow exceptions. “Transfers” in this context also include remote screen access in the US to data held on servers in the EEA.

Restricted Transfer means:

A transfer of Company Personal Data from any Company Group Member to a Group Member (Processor) or an onward transfer of Company Personal Data from a Group member (Processor) to a Group Member (Processor), means data transfer between Group members.

In each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established below.

**Standard Contractual Clauses** (SCCs) are standard sets of contractual terms and conditions which the sender and the receiver of personal data both sign up to, aimed at protecting personal data leaving the European Economic Area (EEA) through contractual obligations in compliance with the GDPR's requirements.

**Security/Personal Data Breach**, means the occurrence of any actual breach of security which will likely lead to, leads to or that may have led to, accidental or unlawful destruction, loss, alteration, compromise, disclosure of, or unauthorized access to Personal Data, stored, transmitted, or otherwise processed.

A breach is therefore a type of security incident and there are three different types of breach that may occur:

Confidentiality breach – an accidental or unauthorized disclosure of, or access to, personal data.

Availability breach – an accidental or unauthorized loss of access to, or destruction of, personal data.

Integrity breach – an accidental or unauthorized alteration of personal data.

A breach can concern confidentiality, availability, and integrity of personal data at the same time, as well as any combination of these.

**Sub-processor** means any natural or legal person, public authority, agency, or anybody other than the data subject, controller, processor, and persons who under direct authority of controller or processor, are authorized to process personal data (including any third party and any Processor Affiliate).

# PROCESSING OF PERSONAL DATA

## 2.1 Processor/Importer Obligations

Processor must be complied with all applicable Data Protection Laws in the processing personal data of its legal entities and subsidiaries.

The Processor has not to process company name controller personal data other than on the relevant documented instructions unless processing is required by applicable laws to which the relevant contracted Processor (processor) is subject, in which case Processor or the relevant Processor affiliate shall to the extent permitted by applicable laws inform the relevant company name controller of that legal requirement before the relevant processing of that personal data.

It is hereby clarified and implied for the purposes of this Data Protection Agreement, that the controller has obtained sufficient authorization, legitimate interest and/or written consent from its Data Subjects for the personal data provided to the Processor entered into Processor’s systems/software, SAP, Peoplesoft, Service Now, etc.

***2.2 Controller’ Obligation***

Company name controller must give instructions to Processor and each Processor Affiliate how to process company name controller Personal Data; and in particular, transfer company name controller Personal Data to any country or territory as reasonably necessary for the purpose of the processing, warrants and represents that it is and will be at all relevant times remain duly and effectively authorized as to the given instruction.

Annex 1 to this Agreement sets out certain information regarding the contracted Processor(processor) processing of company name controller Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other local Data Protection Laws). company name controller may make reasonable amendments to Annex 1 by written notice to Partner from time to time as company name controller reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section) confers any right or imposes any obligation on any party to this agreement.

**3. PROCESSOR PERSONAL**

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any contracted processor who may have access to the company name controller Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant company name controller Personal Data, as strictly necessary for the purposes of the processing, and to comply with Applicable Laws in the context of that individual's duties to the contracted processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality. Processor shall train every employee involved in data processing regarding personal data protection principle and regulations.

**4. TECHNICAL AND ORGANIZATION SECURITY MEASURES**

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 natural persons, Processor shall in relation to company name controller Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk.

In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by processing, in particular from a Personal Data Breach.

The Processor shall take appropriate technical and organizational security measures to protect Personal Data against accidental loss or damage and unauthorized access, use, disclosure, alteration or destruction and to ensure the confidentiality, security, integrity, and availability of Personal Data.

Measures to be undertaken by the Processor shall include:

* The measures to securely dispose of Personal Data taking into account available technology so that such information cannot be practicably read or reconstructed
* Limiting access to Personal Data to Processor personnel: Processor has taken reasonable steps to ensure the reliability of Processor personnel who are granted the minimum access level(s) to the Personal Data that are necessary to carry out their job role in performance of Processor’s obligations; have been trained in the proper handling of Personal Data; are subject to written obligations of confidentiality in respect of Personal Data and only process Personal Data in accordance with the given instructions
* Implementing logging and auditing techniques for access to the personal data Processor processes on behalf of the company name controller
* Encryption of all personal Data processed on behalf of the company name controller where such processing takes place using laptops or other electronic portable devices
* Use of encryption of personal data as appropriate taking into account the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss alteration, unauthorized disclosure of, or access to personal data.

The processor must have policies and procedures based on the ISO27001 framework.

Processor shall regularly test, assess and evaluate the effectiveness of the technical and organizational security measures Processor has implemented. Upon company name controller written request, Processor shall provide company name controller with the results of the test, assessment and evaluation of the effectiveness of the technical and organization measures Processor has implemented including details of these measures which are sufficient to demonstrate compliance with Data Protection Laws.

**5. SUB–PROCESSING**

Processor is not allowed to disclose, assign, lease or communicate Personal Data to any sub-contractor, without informing and obtaining the specific prior written consent of company name controller.

Processor shall impose on its authorized sub-contractor by way of a contract or other legal act, the same legal requirements as the Processor undertakes in this agreement, in particular the obligation to provide sufficient guarantees to the processing by implementing appropriate technical and organizational measures. Where the authorized sub-contractor fails to fulfil its data protection obligations, Processor shall remain fully liable to the data controller for the performance of that sub-contractor’s obligation.

Processor should ensure that all obligations set out in this agreement are fully and entirely reflected in its own agreements with sub-contractors, as if the latter were a party hereto, including without limitation that: the same level of protection should be granted to the Sub-Processing of Personal Data as per the terms of this agreement and in accordance with the GDPR, Privacy Shield, APPI, PDPA and/or other Data Protection Regulation and; any sub-contractor may only engage additional sub-contractors of its own for the Sub-Processing of the Personal Data after the data controller has been notified thereof, has given its written approval to the additional engagement and only if the terms of such sub-contractor’s agreement with its own sub-contractor reflect the terms of this agreement as if the latter were a party hereto.

Processor acknowledges that, for the purposes of its compliance with this agreement, any engagement of a sub-contractor for any reason other than the sub-processing of the Personal Data that may incidentally, directly or indirectly entail the exposure or accessibility of the Personal Data to such sub-contractor shall be subject to all requirements of this agreement applicable to company name controller own processing of the Personal Data.

Processor shall upon data controller' request at any time, provide a copy of any sub-processing agreement it concludes relating to the sub-processing of Personal Data, save that the Data Processor should have the right to exclude confidential and commercially sensitive information not relating to the processing of the Personal Data that may be contained in such agreement. Any agreement or arrangement between the Processor and its sub-contractor(s) that relate directly or indirectly to the Personal Data shall be fully documented in writing.

Processor has to ensure that the arrangement between on the one hand processor or the relevant Processor affiliate and on the other hand the sub-processor, is governed by a written contract including terms which offer at least the same level of protection for company name controller personal data as those set out in this agreement and meet the requirements of article 28(3) of the GDPR or other local data protection laws.

If the arrangement involves a Restricted Transfer, Processor has to ensure that a Standard Contractual Clauses SCC are at all relevant times incorporated into the agreement between on the one hand Processor, or the relevant Processor affiliate and on the other hand the sub-processor or before the sub-processor first processes company name controller’ Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses.

**6. DATA SUBJECT RIGHTS**

Taking into account the nature of the processing, Processor and each Processor affiliate shall assist each company name controller group member by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the company name controller's obligations, as reasonably understood by company name controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

The Processor shall:

* Promptly notify company name controller if it receives a request from a Data Subject under any Data Protection Law in respect of company name controller Personal Data
* Ensure that it does not respond to that request except on the documented instructions of company name controller or as required by Applicable Laws to which the it is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform company name controller of that legal requirement before the contracted processor responds to the request.

**7. PERSONAL DATA BREACH**

Processor shall notify company name controller without undue delay upon Processor or any sub-processor becoming aware of a Personal Data Breach affecting personal data processed in behalf of company name controller, providing company name controller with sufficient information to allow each company name controller group member to meet any obligations to report or inform Data Subjects and/or supervisory authorities of the Personal Data Breach under the Data Protection Laws.

Processor shall co-operate with company name controller and each company name controller member and take such reasonable commercial steps as are directed by company name controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

Processor shall promptly notify company name controller and in all cases such notice should be made no later than 72 hours after becoming aware of a Security Breach of Personal Data.

The notification must at least include:

* Time, date and location of the Security Breach of Personal Data
* A description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records
* The name and contact details of Processor CEO or the Board member responsible for Data Protection
* The name and contact details of Processor Data Protection Officer or data protection representative
* A description of the likely consequences of the breach
* A description of the measures taken, or to be taken, by the Processor to address the breach and mitigate its possible adverse effects.

If a Security Breach occurs the Processor shall also:

* Promptly provide all other information and assistance reasonably requested by company name controller in order to comply with the company name controller’s legal entities/subsidiaries obligations related to a Security Breach under applicable law (including Data Protection Laws) (e.g., in reporting to the supervisory authority)
* Keep company name controller apprised of any additional information related to the Security Breach that may become available to the Processor after the initial notification
* Not inform any third party of such Security Breach without the company name controller prior written consent, unless the Processor is compelled by applicable law. In case the Processor is compelled by applicable law, then the Processor shall notify the company name controller regarding the content of such disclosure to minimize the adverse impact to the company name controller
* If requested by company name controller, perform a root cause analysis of the Security Breach and promptly inform company name controller of the results of the root cause analysis
* Determine whether the Security Breach may be repeated or is ongoing
* Undertake immediate action to prevent a repeated occurrence of the Security Breach

The obligations in this clause are without prejudice to any obligations that Processor has under applicable law.

**8. DATA PROTECTION IMPACT ASSESSMENT (DPIA)**

A DPIA is a way to analyze personal data processing and helps to identify and minimize data protection risks systematically and comprehensively.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm –- to individuals or to society at large, whether it is physical, material, or non- material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to eradicate the risks altogether but should help to minimize risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

The Processor and each Processor affiliate shall provide reasonable assistance to each company name controller group member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which company name controller reasonably considers to be required of any company name controller member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to processing of company name controller Personal Data by, and taking into account the nature of the processing and information available to, the contracted processors.

# 9. Transfer Impact Assessment (TIA)

A Transfer Impact Assessment (TIA) is a type of risk assessment that enables organisations like FPT Software (i.e. ‘data exporter’) to determine if the SCCs or other mechanism under Article 46 of the GDPR, that they intend using for transferring personal data outside the EEA provides an adequate level of protection in the specific circumstances of that transfer.

The TIA must evaluate whether the laws and practices in the country outside the EEA (i.e. third country) where the personal data is being transferred to or accessed from, provides ‘essentially equivalent’ protection and does not impinge on the effectiveness of the SCCs or other mechanism under Article 46 of the GDPR used to facilitate the data transfer.

If the outcome of the TIA is that the laws and practices in the third country impinge on the effectiveness of the GDPR Article 46 mechanism, then FPT Software (i.e. ‘data exporter) must identify and adopt supplementary measures to bring the level of protection for the transferred personal data up to the EU level of protection.

A TIA is only required when transferring personal data to a third country outside the EEA not covered by an European Commission adequacy decision. An adequacy decision is a decision adopted by the European Commission where it has decided that a third country, a territory, one or more specified sectors (e.g. public or private) within a third country or an international organisation including its subordinate bodies (such as the United Nations and the World Health Organisation) ensures an adequate level of protection of personal data. Where adequacy decisions are relied upon, no other GDPR transfer mechanism, such as appropriate safeguards under Article 46 noted above or a TIA, are required.

The TIA must be undertaken by FPT Software subsidiary or legal entity who are intending to transfer personal data to countries outside the EEA not covered by an EU adequacy decision. Whilst undertaking the TIA, FPT Software subsidiary or legal entity will need the assistance of the organisation (i.e.‘data importer’) in the country outside the EEA where the personal data is being transferred to and the Global Data Protection Officer GDPO. The TIA must be made available to a supervisory authority, such as the Data Protection Commission, upon request.

**10. AUDIT**

The company name controller should be entitled to conduct Personal Data protection audit under the terms and conditions of this agreement or to have such audit conducted by an independent and recognized expert chosen by the data controller. Such audit must allow an analysis of compliance with the Data Protection Laws and Regulations in force, in particular the verification of all the technical, logical and organizational security measures implemented by the Service Processor, the verification of the Service Processor data server locations where are hosted Personal Data, and of its copying and deletion logs, and an analysis of the measures implemented to delete the Personal Data and to prevent any unauthorized disclosure of such Personal Data.

The Processor should fully cooperate and make available to the data controller (and/or where applicable the data controller’s audit representatives or external auditors) any documents relating to the security of the processed Personal Data including, in particular, the necessary technical documentation, the risk analyses produced, and a detailed list of the security measures implemented.

The Processor and each Processor affiliate shall make available to each company name controller on request all information necessary to demonstrate compliance with this agreement, and shall allow for and contribute to audits, including inspections, by any company name controller or an auditor mandated by any company name controller in relation to the processing of the company name controller Personal Data.

The audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

company name controller undertaking an audit shall give the Processor reasonable notice of any audit or inspection to be conducted under this chapter and shall make (and ensure that each of its mandated auditors makes) reasonable endeavors to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Processor premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. Processor need not give access to its premises for the purposes of such an audit or inspection:

* To any individual unless he or she produces reasonable evidence of identity and authority.
* Outside standard business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and company name controller undertaking an audit has given notice to the Processor or the relevant Processor affiliate that this is the case before attendance outside those hours begins.
* For the purposes of more than [one] audit or inspection in any [calendar year], except for any additional audits or inspections which:
* Company name controller undertaking an audit reasonably considers necessary because of genuine concerns as to the Processor or the relevant Processor affiliate’s compliance with this agreement
* Company name controller is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory

**11. INTERNATIONAL TRANSFER**

The Parties hereby acknowledge and agree that the Standard Contractual Clauses with DPIA or TIA (Transfer Impact Assessment) shall apply to any Restricted Transfers made in connection this agreement.

The Processor represents, warrants, and covenants that no Authorized Subcontractor will be permitted to undertake or receive a Restricted Transfer before executing the Standard Contractual Clauses.

The Processor represents and warrants that every Restricted Transfer made by Sub-Processor, or any Authorized Sub-contractor shall be undertaken in accordance with the Standard Contractual Clauses.

The Processor represents, warrants, and covenants that every transfer of Personal Data by Sub-processor from the European Economic Area or Switzerland to the United States shall be made pursuant to the Privacy Shield Framework and Principles, and further represents and warrants that it self-certifies to, and complies with, the Privacy Shield Framework and Principles, and shall maintain such self- certification and compliance for the duration of the MSA.

The Processor represents and warrants that every Authorized Sub-contractor that transfers Personal Data from the European Economic Area or Switzerland to the United States adheres to the Privacy Shield Principles.

Company name controller (as "data exporter") and each contracted processor, as appropriate, (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that company name controller to processor.

The Standard Contractual Clauses shall come into effect under this chapter on the later of:

* The data exporter becoming a party to them
* The data importer becoming a party to them
* Commencement of the relevant Restricted Transfer

This chapter shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

The Processor warrants and represents that, before the commencement of any Restricted Transfer to a sub-processor which is not a Processor affiliate entry into the Standard Contractual Clauses under this chapter, and agreement to variations to those Standard Contractual Clauses, as agent for and on behalf of that sub-processor will have been duly and effectively authorized.

**12. GENERAL TERMS**

The parties to this agreement hereby submit to the choice of jurisdiction stipulated in this agreement with respect to any disputes or claims howsoever arising under this agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity.

This agreement and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in this agreement.

***12.1 Order of precedence***

In the event of any conflict or inconsistency between this agreement and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

With regard to the subject matter of this agreement, in the event of inconsistencies between the provisions of this amendment and any other agreements between the parties, the provisions of this agreement shall prevail.

***12.2 Changes in Data Protection Laws or Regulations***

Company name controller may:

* By at least 30 (thirty) calendar days written notice to Processor from time to time make any variations to the Standard Contractual Clauses, as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law
* Propose any other variations to this agreement which company name controller reasonably considers to be necessary to address the requirements of any Data Protection Law.

If company name controller give notice:

* Processor shall promptly co-operate (and ensure that any affected sub-processors promptly co-operate) to ensure that equivalent variations are made to any agreement
* Processor shall not unreasonably withhold or delay to any consequential variations to this agreement.

If company name controller gives notice, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in company name controller notice as soon as is reasonably practicable.

***12.3 Severance***

Should any provision of this agreement be invalid or unenforceable, then the remainder of this agreement shall remain valid and in force. The invalid or unenforceable provision shall be either amended as necessary to ensure its validity and enforceability, while preserving the parties’ intentions as closely as possible or, if this is not possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

**13. MISCELLANEOUS**

This agreement and the Standard Contractual Clauses will terminate simultaneously and automatically with a change of control.

This agreement may be amended or modified only by a writing signed by both Parties. Processor acknowledges and agrees that whether it is acting as a controller or a processor on behalf of another controller may disclose this agreement to third parties (including other controllers, data subjects and regulators) for purposes of demonstrating compliance with Applicable Laws.

The Parties hereby acknowledge and agree that any remedies arising from any Personal Data Breach or any breach by sub-processor or any Authorized Person of the terms of this agreement are not and shall not be subject to any limitation of liability provision that applies to sub-processor.

**14. SIGNATURE**

IN WITNESS WHEREOF, this agreement becomes binding with effect from the date first set out above.

**COMPANY NAME CONTROLLER**

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**COMPANY NAME PROCESSOR**

Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# APPENDIX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

Appendix 1 includes certain details of the processing of company name controller Personal Data as required by Article 28(3) GDPR.

**Categories of Personal Data**

The Personal Data concern the following categories of Personal Data:

Please, describe.

**Categories of data subjects**

The Personal Data concern the following categories of Individuals:

Please, describe.

**Purposes of the data processing**

The Personal Data will be processed for the following purposes:

Please, describe.

**Processing activities**

The Personal Data will be subject to the following processing activities:

Processor will perform its Processing obligations under this Data Processing Agreement in datacenter servers or cloud environment that comply with appendix 2 of this Data Processing Agreement. The specific Processing activities will be pursuant to the Agreement or otherwise pursuant to specific work order, project or otherwise written instructions provided to Processor.

**Recipients of the Personal Data**

The Personal Data may only be disclosed to the following recipients:

Please, describe.

**Retention periods**

The Personal Data may only be retained for the duration of this Data Processing Agreement. Company may instruct Processor to delete and/or return Personal Data at any time during the duration of this Data Processing Agreement.

Please, describe.

# APPENDIX 2: STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

Please use Template\_Standard Contractual Clauses\_v2.3 came in force June 2021 by EU commission decision.

Example for technical and organizational measures see Template\_GDPR\_example\_TO measures\_V1.2

Example Transfer Impact Assessment TIA see Template\_Risk Management TIA\_v1.1