REITLER
REITLER KAILAS & ROSENBLATT LLC

New York
885 Third Avenue, 20th Floor
New York, NY 10022-4834
Tel: 212.209.3050
Fax: 212.371.5500

Princeton
5 Vaughn Drive
Princeton, NJ 08540-6313
Tel: 609.514.1500
Fax: 609.514.1501

October 2018

TO: Interested Parties

RE: Best Practices for Cybersecurity

FROM: Christopher S. Edwards (cedwards@reitlerlaw.com)

Enclosed please find the following materials:

1. Sample Information Security Requirements
2. Sample Business Continuity Plan
3. European Union Model Clauses for Data Processors
4. GDPR Overview

1. INFORMATION SECURITY REQUIREMENTS

1.1. Commitment to information security practices

The Supplier shall set up adequate security measures and operations processes to protect Customer's information and, more specifically, to preserve its confidentiality, integrity and availability, and avoid its disclosure, publication, dissemination and unauthorized alteration. These measures and processes must be applied when using, processing, storing, distributing and destroying the information.

Customer's information must be protected in accordance with information security standards recognized in the financial services industry, such as ISO/IEC 27001:2013.

1.2. Information security policy

The Supplier shall have a documented and approved security policy that is reviewed regularly and communicated to the appropriate resources. The policy must define the topics covered in the main sections of this security appendix.

1.3. Organization of Information Security

The Supplier shall appoint, in writing, an individual to oversee information security for its entire organization. This individual, or another designated person, is responsible for ensuring that all applicable security and compliance requirements are met when providing the Goods and Services specified in the Contract. They will also be the resource person for Customer in matters pertaining to information security. Customer must be notified, in writing, if these individuals are replaced.

1.4. Security Governance

Customer reserves the right to convene one (1) security governance meeting every year with prior notice of fifteen (15) business days to which the Supplier makes a commitment to participate. The main objective of this meeting consists in particular in revalidating the capacity of the Supplier to answer the commitments of security planned by the Contract. Furthermore, comfortingly to this appendix, a rendering of accounts concerning performance indicators in connection with the requirements of security will be made. The security officers of the Supplier, indicated per the requirement 1.3 of the present appendix, must be present on this meeting. The Supplier must answer in writing the questions lifted during the meeting of governance, at the latest ten (10) business days after their reception or according to any other deadline being able to have been suited by mutual agreement between the parties.

Customer also reserves the right to convene without prior notice other punctual meetings of governance according to its needs for conformity, but without limiting itself to it, in the case of a security incident in the market or at the supplier, a case of absolute necessity, etc.

2. OPERATIONS SECURITY

2.1. Security test on applications and operations infrastructure

The Supplier shall, at its own expense, test the security of deliverable and/or infrastructure and/or applications it uses to operate its technological solution and correct detected vulnerabilities. The tests must include vulnerability scanning done on a quarterly basis and intrusion tests on a annual basis, or during major changes to infrastructure or applications used by the Supplier to provide Goods and Services.
Upon request by Customer and at least every year, or in the event of a new version or major change, the Supplier shall provide:

- An executive summary of security tests and their results that must include but not limited to:
    - The scope, the methodology and the length of the test
    - The certifications and work experience of the staff that performed the tests
    - The identified vulnerabilities and their CVE

- Vulnerability corrective action plans and their timelines

3. MANAGEMENT OF INFORMATION SECURITY INCIDENTS

When a major security incident—suspected or confirmed—is reported or detected regarding Customer information or the Goods and Services provided to Customer, the Supplier shall immediately report it to the Customer Security Operations Office by phone at [___] or by email at [___]

4. COMPLIANCE

4.1. Audit rights

Customer reserves the right to audit or have one of their agents audit the Supplier to ensure that the Goods and Services and deliverable are provided in compliance with the provisions of this appendix.
In the event Customer discovers any non-compliance, the Supplier shall make corrections, at its own expense, based on a Customer-approved action plan and timeline.

Upon Customer's request, the Supplier shall provide proof that the corrective plans have been adequately implemented.

4.2. Demonstration of compliance with the security requirements set out in the Contract

The Supplier shall demonstrate its compliance with the security requirements defined in the Contract. To do so, the Supplier shall provide Customer with an annual report **Service Organization Control (SOC) 2 Type II.**

The Supplier shall perform annual SOC 2 (Type 2) audits that include controls that are materially as protective as those used in the SOC 2 (Type 2) executed in 2017.

The Supplier shall report any exceptions or restrictions affecting the delivery of Services provided or systems used as part of the Contract immediately to Customer. The Supplier shall set up corrective action plans and timelines, submit them to Customer and implement them at their own expense. Customer may, at its discretion, request changes to the corrective action plans and timelines.

Upon Customer's request, the Supplier shall provide proof that the corrective action plans have been adequately implemented.

BUSINESS CONTINUITY PLAN

University of [Name]
<department name>

Prepared by: *, Director*
Kevin Borgstedt, Consultant

[Date]

Date of Last Review:
Storage Location:
Primary:
Alternate:

BCP: <department name>

TABLE OF CONTENTS:

BCP: <department name>

Plan Overview

Purpose:

This Business Continuity Plan (BCP) will be updated in response to changes in the business environment. The <department name> will review the plan at least annually.

This document outlines the steps required to operate the <department name> in the event of an unanticipated interruption of normal operations. This document will articulate the triggers for when alternate business processes need to be deployed, the steps to deploy alternate business processes, the methods for verifying that business has been properly restored and ensuring data integrity, and activities for returning to "normal" business processing.

Policy:

This BCP will only be used in situations when it is determined that business impacts and /or business risk requires alternate business processes or locations.

Scope:

This BCP is applicable for the <department name> of the University of [Name].

Assumptions:

The plan will be implemented if systems are unavailable for 48 hours

- Facilities will provide temporary space for critical staff
- UITS will provide technical assistance for temporary location
- Telecommunications will have phone lines available in temporary location
- Equipment can be rented or otherwise acquired as needed
- UITS can restore files from the latest off-site backups

BCP: <department name>

Description of <department name>

Location

University of [Name]

…

…,

Disaster Recovery Strategy

Plan Activation Authorization:

Identify the people that are authorized to activate the various contingency plans.

Primary Name & Title	*Contact Data*	*Alternate Name*	*Contact Data*

Work at Home:

If there are functions that could be performed by staff working from home, describe the approach that would be used to implement the move.

Move to Alternate Location:

If there are functions that could be performed by staff working from an alternate location, describe the approach that would be used to implement the move.

Plan Activation Triggers:

Describe the criteria that would be used to identify the need to activate one of the various contingency plans.

Action	*Trigger Criteria*
	•
	•
	•

BCP: <department name>

Team Roles and Responsibilities

Identify the people responsible for planning, documenting, coordinating, testing, implementing, and maintaining the Business Continuity Plan. If the size of the organization requires creations of multiple specialized teams, describe the teams and identify the members of each team.

Title	*Name*	*Contact Information*

BCP: <department name>

Pre-disaster Activities:

List the tasks that are required on an ongoing basis, to keep the plan current and viable and indicate the person assigned to complete that task.

#	Task	Assignment
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

BCP: <department name>

Emergency Identification and Response:

List the tasks to be performed upon discovery of a possible emergency event or notification that an emergency event has occurred.

#	*Task* (All completed as quickly as possible after notification of disaster. Notification may come from Police, Fire, or Facilities Management, depending on the group that responds first or is designated as "primary" responder. All use the same University contact list.)	*Assignment*
1		
2		
3		
4		
5		
6		

Emergency Damage Assessment / Evaluation:

List the tasks that are required assess the damage caused by an emergency.

#	*Task* (All completed as quickly as possible after authorization to re-enter the damaged structure.)	*Assignment*
1		
2		
3		

BCP: <department name>

Emergency Response Assignments:

List the tasks to be performed in the event that a disaster situation has been declared.

#	Tasks	Assignment	Estimated Completion Time	Date/Time Completed
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Alternative / Manual Processes:

Describe the activities or process steps for each alternative/manual process needed to perform necessary function durin an interruption to normal operations

#	Process Step	Assignment	Estimated Completion Time	Date/Time Completed
1				
2				
3				
4				

Post-Emergency Assignments:

List the activities to be performed after a disaster event or after a recovery exercise. The purpose of these is to incorporate "lessons learned" into the business continuity planning process.

#	Post-Disaster Responsibilities	Assignment	Estimated Completion Time	Date/Time Completed
1				
2				
3				
4				

Communications & Decision-making Protocols:

Describe any communication rules or guidelines that will be used during an emergency.

Communications with news organizations will be channeled through the University's public relations organization.

Returning to Normal Operations:

Authorization:

Identify the people that are authorized to activate plans for returning to normal operations.

Primary Name & Title	*Contact Data*	*Alternate Name*	*Contact Data*

Operating Dependencies:

Identify operational dependencies that impact the return to normal operations. (e.g. applications, servers, or transaction volumes that must be in place before processing can resume)

Steps to Return to Normal Operation:

List the tasks to be performed to return to normal operations.

#	*Task* *(The plan for the return will be developed with Building & Grounds, but will include the general steps shown.)*	*Assignment*
1		
2		
3		
4		
5		
6		
7		
8		

Plan Maintenance Procedures:

Plan Review and Update Process:

Describe the process for keeping the plan current.

Plan Distribution Procedures:

Describe the process for distributing the plan and/or training people to use its content.

Validation Requirements:

Identify frequency and type of testing (tabletop exercises, systems / telephony testing, department recovery tests, functional tests) required for this plan.

Recovery Plan Validation History:

Record the history of review/testing/validation activities for the plan.

Date:	*Type Test / Results:*

Additional Documentation:

Location of Disaster Recovery Documentation for Supporting Systems:

Application	*Document Name*	*Location*

Location of Supporting Documentation:

Document Name	*Location*

Plan Update History:

Date	*Update Session Details*	*Revised By*

BCP: <department name>

Plan Sign Off

This document describes the anticipated activities that will be needed to resume or continue business functions in the event of disruption to normal business activities.

Director/Department Head/Dean	**Date**

ISSN 1725-2555

Official Journal of the European Union

L 39

English edition

Legislation

Volume 53

12 February 2010

Contents

(1) Text with EEA relevance

(Continued overleaf)

Price: EUR 3

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

COMMISSION DECISION

of 5 February 2010

on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

(notified under document C(2010) 593)

(Text with EEA relevance)

(2010/87/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1], and in particular Article 26(4) thereof,

After consulting the European Data Protection Supervisor,

Whereas:

(1) Pursuant to Directive 95/46/EC Member States are required to provide that a transfer of personal data to a third country may only take place if the third country in question ensures an adequate level of data protection and the Member States' laws, which comply with the other provisions of the Directive, are respected prior to the transfer.

(2) However, Article 26(2) of Directive 95/46/EC provides that Member States may authorise, subject to certain safeguards, a transfer or a set of transfers of personal data to third countries which do not ensure an adequate level of protection. Such safeguards may in particular result from appropriate contractual clauses.

(3) Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding the data transfer operation or set of data transfer operations. The Working Party on the protection of individuals with regard to the processing of personal data established under that Directive has issued guidelines to aid with the assessment.

(4) Standard contractual clauses should relate only to data protection. Therefore, the data exporter and the data importer are free to include any other clauses on business related issues which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses.

(5) This Decision should be without prejudice to national authorisations Member States may grant in accordance with national provisions implementing Article 26(2) of Directive 95/46/EC. This Decision should only have the effect of requiring the Member States not to refuse to recognise, as providing adequate safeguards, the standard contractual clauses set out in it and should not therefore have any effect on other contractual clauses.

(6) Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC [2] was adopted in order to facilitate the transfer of personal data from a data controller established in the European Union to a processor established in a third country which does not offer adequate level of protection.

(7) Much experience has been gained since the adoption of Decision 2002/16/EC. In addition, the report on the implementation of Decisions on standard contractual clauses for the transfers of personal data to third countries [3] has shown that there is an increasing interest in promoting the use of the standard contractual clauses for international transfers of personal data to third countries not providing an adequate level of protection. In addition, stakeholders have submitted proposals with a view to updating the standard contractual clauses set out in Decision 2002/16/EC in order to take account of the rapidly expanding scope of data-processing activities in the world and to address some issues that were not covered by that Decision [4].

[1] OJ L 281, 23.11.1995, p. 31.

[2] OJ L 6, 10.1.2002, p. 52.

[3] SEC(2006) 95, 20.1.2006.

[4] The International Chamber of Commerce (ICC), Japan Business Council in Europe (JBCE), EU Committee of the American Chamber of Commerce in Belgium (Amcham), and the Federation of European Direct Marketing Associations (FEDMA).

(8) The scope of this Decision should be limited to establishing that the clauses which it sets out may be used by a data controller established in the European Union in order to adduce adequate safeguards within the meaning of Article 26(2) of Directive 95/46/EC for the transfer of personal data to a processor established in a third country.

(9) This Decision should not apply to the transfer of personal data by controllers established in the European Union to controllers established outside the European Union which fall within the scope of Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC [1].

(10) This Decision should implement the obligation provided for in Article 17(3) of Directive 95/46/EC and should not prejudice the content of the contracts or legal acts established pursuant to that provision. However, some of the standard contractual clauses, in particular as regards the data exporter's obligations, should be included in order to increase clarity as to the provisions which may be contained in a contract between a controller and a processor.

(11) Supervisory authorities of the Member States play a key role in this contractual mechanism in ensuring that personal data are adequately protected after the transfer. In exceptional cases where data exporters refuse or are unable to instruct the data importer properly, with an imminent risk of grave harm to the data subjects, the standard contractual clauses should allow the supervisory authorities to audit data importers and sub-processors and, where appropriate, take decisions which are binding on data importers and sub-processors. The supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject.

(12) Standard contractual clauses should provide for the technical and organisational security measures to be applied by data processors established in a third country not providing adequate protection, in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Parties should make provision in the contract for those technical and organisational measures which, having regard to applicable data protection law, the state of the art and the cost of their implementation, are necessary in order to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access or any other unlawful forms of processing.

(13) In order to facilitate data flows from the European Union, it is desirable for processors providing data-processing services to several data controllers in the European Union to be allowed to apply the same technical and organisational security measures irrespective of the Member State from which the data transfer originates, in particular in those cases where the data importer receives data for further processing from different establishments of the data exporter in the European Union, in which case the law of the designated Member State of establishment should apply.

(14) It is appropriate to lay down the minimum information that the parties should specify in the contract dealing with the transfer. Member States should retain the power to particularise the information the parties are required to provide. The operation of this Decision should be reviewed in the light of experience.

(15) The data importer should process the transferred personal data only on behalf of the data exporter and in accordance with his instructions and the obligations contained in the clauses. In particular the data importer should not disclose the personal data to a third party without the prior written consent of the data exporter. The data exporter should instruct the data importer throughout the duration of the data-processing services to process the data in accordance with his instructions, the applicable data protection laws and the obligations contained in the clauses.

(16) The report on the implementation of Decisions on standard contractual clauses for the transfers of personal data to third countries recommended the establishment of appropriate standard contractual clauses on subsequent onwards transfers from a data processor established in a third country to another data processor (sub-processing), in order to take account of business trends and practices for more and more globalised processing activity.

[1] OJ L 181, 4.7.2001, p. 19.

(17) This Decision should contain specific standard contractual clauses on the sub-processing by a data processor established in a third country (the data importer) of his processing services to other processors (sub-processors) established in third countries. In addition, this Decision should set out the conditions that the sub-processing should fulfil to ensure that the personal data being transferred continue to be protected notwithstanding the subsequent transfer to a sub-processor.

(18) In addition, the sub-processing should only consist of the operations agreed in the contract between the data exporter and the data importer incorporating the standard contractual clauses provided for in this Decision and should not refer to different processing operations or purposes so that the purpose limitation principle set out by Directive 95/46/EC is respected. Moreover, where the sub-processor fails to fulfil his own data-processing obligations under the contract, the data importer should remain liable toward the data exporter. The transfer of personal data to processors established outside the European Union should not prejudice the fact that the processing activities should be governed by the applicable data protection law.

(19) Standard contractual clauses should be enforceable not only by the organisations which are parties to the contract, but also by the data subjects, in particular where the data subjects suffer damage as a consequence of a breach of the contract.

(20) The data subject should be entitled to take action and, where appropriate, receive compensation from the data exporter who is the data controller of the personal data transferred. Exceptionally, the data subject should also be entitled to take action, and, where appropriate, receive compensation from the data importer in those cases, arising out of a breach by the data importer or any sub-processor under it of any of its obligations referred to in the paragraph 2 of Clause 3, where the data exporter has factually disappeared or has ceased to exist in law or has become insolvent. Exceptionally, the data subject should be also entitled to take action, and, where appropriate, receive compensation from a sub-processor in those situations where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent. Such third-party liability of the sub-processor should be limited to its own processing operations under the contractual clauses.

(21) In the event of a dispute between a data subject, who invokes the third-party beneficiary clause, and the data importer, which is not amicably resolved, the data importer should offer the data subject a choice between mediation or litigation. The extent to which the data subject will have an effective choice will depend on the availability of reliable and recognised systems of mediation. Mediation by the data protection supervisory authorities of the Member State in which the data exporter is established should be an option where they provide such a service.

(22) The contract should be governed by the law of the Member State in which the data exporter is established enabling a third-party beneficiary to enforce a contract. Data subjects should be allowed to be represented by associations or other bodies if they so wish and if authorised by national law. The same law should also govern the provisions on data protection of any contract with a sub-processor for the sub-processing of the processing activities of the personal data transferred by the data exporter to the data importer under the contractual clauses.

(23) Since this Decision applies only to subcontracting by a data processor established in a third country of his processing services to a sub-processor established in a third country, it should not apply to the situation by which a processor established in the European Union and performing the processing of personal data on behalf of a controller established in the European Union subcontracts his processing operations to a sub-processor established in a third country. In such situations, Member States are free whether to take account of the fact that the principles and safeguards of the standard contractual clauses set out in this Decision have been used to subcontract to a sub-processor established in a third country with the intention of providing adequate protection for the rights of data subjects whose personal data are being transferred for sub-processing operations.

(24) The Working Party on the protection of individuals with regard to the processing of personal data established under Article 29 of Directive 95/46/EC has delivered an opinion on the level of protection provided under the standard contractual clauses annexed to this Decision, which has been taken into account in the preparation of this Decision.

(25) Decision 2002/16/EC should be repealed.

(26) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31 of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

Article 1

The standard contractual clauses set out in the Annex are considered as offering adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights as required by Article 26(2) of Directive 95/46/EC.

Article 2

This Decision concerns only the adequacy of protection provided by the standard contractual clauses set out in the Annex for the transfer of personal data to processors. It does not affect the application of other national provisions implementing Directive 95/46/EC that pertain to the processing of personal data within the Member States.

This Decision shall apply to the transfer of personal data by controllers established in the European Union to recipients established outside the territory of the European Union who act only as processors.

Article 3

For the purposes of this Decision the following definitions shall apply:

(a) 'special categories of data' means the data referred to in Article 8 of Directive 95/46/EC;

(b) 'supervisory authority' means the authority referred to in Article 28 of Directive 95/46/EC;

(c) 'data exporter' means the controller who transfers the personal data;

(d) 'data importer' means the processor established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(e) 'sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer and who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for the processing activities to be carried out on behalf of the data exporter after the transfer in accordance with the data exporter's instructions, the standard contractual clauses set out in the Annex, and the terms of the written contract for sub-processing;

(f) 'applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(g) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Article 4

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to Chapters II, III, V and VI of Directive 95/46/EC, the competent authorities in the Member States may exercise their existing powers to prohibit or suspend data flows to third countries in order to protect individuals with regard to the processing of their personal data in cases where:

(a) it is established that the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses;

(b) a competent authority has established that the data importer or a sub-processor has not respected the standard contractual clauses in the Annex; or

(c) there is a substantial likelihood that the standard contractual clauses in the Annex are not being or will not be complied with and the continuing transfer would create an imminent risk of grave harm to the data subjects.

2. The prohibition or suspension pursuant to paragraph 1 shall be lifted as soon as the reasons for the suspension or prohibition no longer exist.

3. When Member States adopt measures pursuant to paragraphs 1 and 2, they shall, without delay, inform the Commission which will forward the information to the other Member States.

Article 5

The Commission shall evaluate the operation of this Decision on the basis of available information three years after its adoption. It shall submit a report on the findings to the Committee established under Article 31 of Directive 95/46/EC. It shall include any evidence that could affect the evaluation concerning the adequacy of the standard contractual clauses in the Annex and any evidence that this Decision is being applied in a discriminatory way.

Article 6

This Decision shall apply from 15 May 2010.

Article 7

1. Decision 2002/16/EC is repealed with effect from 15 May 2010.

2. A contract concluded between a data exporter and a data importer pursuant to Decision 2002/16/EC before 15 May 2010 shall remain in force and effect for as long as the transfers and data-processing operations that are the subject matter of the contract remain unchanged and personal data covered by this Decision continue to be transferred between the parties. Where contracting parties decide to make changes in this regard or subcontract the processing operations that are the subject matter of the contract they shall be required to enter into a new contract which shall comply with the standard contractual clauses set out in the Annex.

Article 8

This Decision is addressed to the Member States.

Done at Brussels, 5 February 2010.

For the Commission

Jacques BARROT

Vice-President

ANNEX

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address: .....

Tel. .....; fax .....; e-mail: .....

Other information needed to identify the organisation

.....

(the data **exporter**)

And

Name of the data importing organisation: .....

Address: .....

Tel. .....; fax .....; e-mail: .....

Other information needed to identify the organisation:

.....

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1];

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer [1]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

[1] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely .....

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses [1]. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely .....

[1] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature .....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any):

Signature .....

(stamp of organisation)

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

.....

.....

.....

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

.....

.....

.....

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

.....

.....

.....

Categories of data

The personal data transferred concern the following categories of data (please specify):

.....

.....

.....

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

.....

.....

.....

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

.....

.....

.....

DATA EXPORTER

Name: .....

Authorised Signature .....

DATA IMPORTER

Name: .....

Authorised Signature .....

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

.....

.....

.....

.....

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim [1].

[1] Paragraph on liabilities is optional.

European Commission

Rules for business and organisations

Find out what your organisation must do to comply with EU data protection rules and learn how you can help citizens exercising their rights under the regulation.

Application of the regulation

Who does the data protection law apply to?

Do the rules apply to SMEs?

Do the data protection rules apply to data about a company?

Principles of the GDPR

What data can we process and under which conditions?

Purpose of data processing

How much data can be collected?

For how long can data be kept and is it necessary to update it?

What information must be given to individuals whose data is collected?

Public administrations and data protection

What are the main aspects of the General Data Protection Regulation (GDPR) that a public administration should be aware of?

How should requests from individuals be dealt with?

What if a public administration fails to comply with the data protection rules?

Legal grounds for processing data

Grounds for processing

Sensitive data

Are there any specific safeguards for data about children?

Can data received from a third party be used for marketing?

Obligations

Controller/processor

Are the obligations the same regardless of the amount of data my company/organisation handles?

What does data protection 'by design' and 'by default' mean?

What is a data breach and what do we have to do in case of a data breach?

When is a Data Protection Impact Assessment (DPIA) required?

Data Protection Officers

Dealing with citizens

How should requests from individuals exercising their data protection rights be dealt with?

What personal data and information can an individual access on request?

Do we always have to delete personal data if a person asks?

What happens if someone objects to my company processing their personal data?

Can individuals ask to have their data transferred to another organisation?

What rules apply if my organisation transfers data outside the EU?

How can I demonstrate that my organisation is compliant with the GDPR?

Are there restrictions on the use of automated decision-making?

Enforcement and sanctions

Enforcement

Sanctions

Disclaimer

Library of related documents

European Commission

Who does the data protection law apply to?

Answer

The law applies to:

1. a company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or
2. a company established outside the EU offering goods/services (paid or for free) or monitoring the behaviour of individuals in the EU.

If your company is a small and medium-sized enterprise ('SME') that processes personal data as described above you have to comply with the GDPR. However, if processing personal data isn't a core part of your business and your activity doesn't create risks for individuals, then some obligations of the GDPR will not apply to you (for example the appointment of a Data Protection Officer ('DPO')). Note that 'core activities' should include activities where the processing of data forms an inextricable part of the controller's or processor's activities.

Examples

When the regulation applies

Your company is a small, tertiary education company operating online with an establishment based outside the EU. It targets mainly Spanish and Portuguese language universities in the EU. It offers free advice on a number of university courses and students require a username and a password to access your online material. Your company provides the said username and password once the students fill out an enrolment form.

When the regulation does not apply

Your company is service provider based outside the EU. It provides services to customers outside the EU. Its clients can use its services when they travel to other countries, including within the EU. Provided your company doesn't specifically target its services at individuals in the EU, it is not subject

to the rules of the GDPR.

European Commission

What rules apply if my organisation transfers data outside the EU?

Answer

In today's globalised world, there are large amounts of cross-border transfers of personal data, which are sometimes stored on servers in different countries. The **protection offered by the General Data Protection Regulation (GDPR) travels with the data**, meaning that the rules protecting personal data continue to apply regardless of where the data lands. This also applies when data is transferred to a country which is not a member of the EU (hereinafter referred to as 'third country').

The GDPR provides different tools to frame data transfers from the EU to a third country:

- sometimes, a third country may be declared as offering an adequate level of protection through a European Commission decision ('Adequacy Decision'), meaning that data can be transferred with another company in that third country without the data exporter being required to provide further safeguards or being subject to additional conditions. In other words, the transfers to an 'adequate' third country will be comparable to a transmission of data within the EU.
- in the absence of an Adequacy Decision, a transfer can take place through the provision of appropriate safeguards and on condition that enforceable rights and effective legal remedies are available for individuals. Such appropriate safeguards include:
  - in the case of a group of undertakings, or groups of companies engaged in a joint economic activity, companies can transfer personal data based on so-called binding corporate rules;
  - contractual arrangements with the recipient of the personal data, using, for example, the standard contractual clauses approved by the European Commission;
  - adherence to a code of conduct or certification mechanism together with obtaining binding and enforceable commitments from the recipient to apply the appropriate safeguards to protect the transferred data.
- finally, if a transfer of personal data is envisaged to a third country that isn't the subject of an Adequacy Decision and if appropriate safeguards are absent, a transfer can be made based on a number of

derogations for specific situations for example, where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer.

Example

You're a French company intending to expand its services to South America, notably Argentina, Uruguay and Brazil. The first step would be to check whether those third countries are subject to an Adequacy Decision. In this case, both Argentina and Uruguay have been declared adequate. You'd be able to transfer personal data to those two third countries without any additional safeguards while for transfers to Brazil which is not the subject of Adequacy Decision, you'll have to frame your transfers by providing appropriate safeguards.

References

- Chapter V, Articles 44 to 50) and Recitals (101) to (116) of the GDPR
- Article 29 Working Party's latest Working Documents on International transfers
  - Working Document on Adequacy Referential (update of Chapter One of WP 12), WP 254
  - Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256
  - Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257
- See also for reference the European Commission Communication on Exchanging and Protecting Personal Data in a Globalised World, 10 January 2017