FH Vorarlberg
University of Applied Sciences

Transfer of Data to Third Countries

The Status of Implementation of the Modernized Standard Contractual Clauses by Companies in Austria

Master Thesis

Submitted in Fulfillment of the Degree

Master of Arts

University of Applied Sciences Vorarlberg

International Management and Leadership

Submitted to

Mag. Dr. Christian Wirthensohn

Handed in by

Leah Wanjiku Kihuria

Dornbirn, 08.07.2022

Abstract

"Data is the new oil," said British Mathematician and Tesco marketing mastermind Clive Humbly[1]. Data has also been described as the backbone of digital retail enterprises[2] and the currency of the digital age. Whether these statements live up to be true is debatable, but what is certain is the fact that the internet age has contributed to the avalanche of data witnessed today. In a century dominated by predictive analysis and artificial intelligence, it is no surprise that by the end of the last decade, data companies Apple, Amazon and Microsoft closed as the world´s first trillion-dollar companies, with their revenues dwarfing economies of several countries across the globe.[3]

The recognition of the importance of data in today´s economy bears with it the responsibility to protecting its owners. While this intricate balance has long been the subject of legal analysis the General Data Protection Regulation, 2018, is hailed as the world´s most comprehensive and strict data protection regime currently in force. In addition to protecting the personal data of persons from its member countries, the Regulation also seeks to ensure the same protection accompanies any data transferred out of the European Union to other countries.

It is almost 5 years since the Regulation was passed and process of implementation into business operations an important topic of discussion. Of importance to this study are the Modernized Standard Contractual Clauses, a tool of data transfer to countries outside the EU, which replace the three sets of SCCs adopted by the now repealed Data Protection Directive 94/46.

These Standard Contractual Clauses came into effect on 27th September 2021, and companies have until 27th September 2022 to rely on the old set of clauses. With this deadline coming up, how far have the clauses been integrated into operations by businesses in Austria and the EU?

[1] Kershner, M. (2021, June 15). *Data Isn't The New Oil — Time Is*. Forbes. Retrieved December 12, 2021, from https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/

[2] Brown, B. (2021, November 3). Why Source Data Is The New Currency For Retailers. *Forbes*. Retrieved November 24, 2021, from https://www.forbes.com/sites/forbestechcouncil/2021/11/03/why-source-data-is-the-new-currency-for-retailers/

[3] Owens, J. (2019, December 25). The tech giants dominated the decade. But there's still time to rein them in. *The Guardian*. Retrieved November 21, 2021, from https://www.theguardian.com/commentisfree/2019/dec/25/2010s-tech-giants-google-amazon-facebook-regulators

Table of Contents

Contents

List of Figures

List of Tables

Acronyms

“AWS”	Amazon Web Services
“CJEU”	Court of Justice of the European Union
“DPA”	Data Processing Agreement
“EDPB”	European Data Protection Board
“EEA”	European Economic Area
“EU”	European Union
“GDPR”	General Data Protection Regulation
“OECD”	Organisation for Economic Co-operation and Development
“SCCs”	Standard Contractual Clauses

1. Introduction

The centrality of cross-border data trade to modern international trade cannot be understated. So big is data´s role in business that the Organisation for Economic Co-operation and Development ("OECD") acknowledges cross-border trade as one of the foundations upon which international trade is built on even attributing it to the rise of global value chains which account close to three quarters of the value of international trade.[4] In this digital age, data migration has now surpassed that of goods and services. The global economy has become increasingly data-driven thereby consuming data, processing data, and producing more of it.[5] The quantity of data exported as facilitated by digital technologies by now far outnumbers that of traditional trade in goods and services. The following is a practical example of a modern case of cross-border data transfer in the European Union ("EU").

> Consider a market research company based in the EU. This company may sell data on the habits of EU clients to retailers based elsewhere, for example a Japanese car manufacturer interested in designing new electric vehicles tailored to the EU market. Cross-border data sharing also plays a critical role in pharmaceutical and healthcare sectors. For example, there are pharmaceutical companies which carry out their clinical trials in the EU and rely on cross-border data transfers to get authorisation for new treatments from regulatory authorities outside the EU.[6]

One component of the data value chain —personal data— has been subject to increased protection worldwide through legislation. The European Union ("EU") is currently the global leader in data protection, with the passing of Regulation (EU) 2016/679 (General Data Protection Regulation) ("GDPR"). While the Regulations have been hailed for taking a strict stance on data protection, the European Commission ("the Commission") goes a step further by requiring the same level of protection to be accorded on personal data that is transferred outside the Union. It does so by attempting to bring data protection systems in third countries in line with the GDPR standards.[7] The aim is to prevent misuse or violation of the data in the destination country, assuring the data subjects in the destination country the same protection as in the originating country (in the EU).

---

[4] Mine, H., & Dahl, C. B. (2021, July). The value of cross-border data flows to Europe: Risks and opportunities. Frontier Economics. Retrieved April 4, 2022, from https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf

[5] Slaughter, M. J., & McCormick, D. H. (2021, June). Data Is Power. Washington Needs to Craft New Rules for the Digital Age. FOREIGN AFFAIRS. Retrieved March 4, 2022, from https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age

[6] Mine & Dahl, 2021, p. 11 & 12

[7] Hoffman, D. A. (2017, January). *DATA TRANSFERS TO THIRD COUNTRIES* (Policy Brief No. 2017–25). Centrum für Europaische Politik. https://www.cep.eu/fileadmin/user_upload/cep.eu/Analysen/COM_2017_7_Datenuebermittlung/cepPolicyBrief_COM_2017__7_Data_Transfers_to_Third_Countries.pdf

Chapter V (Articles 44-50) of the GDPR lays down requirements for a valid transfer of personal data to a third country (a country outside the European Union("EU") and the European Economic Area ("EEA").[8] It sums them up into 3 categories: adequacy decision, alternative tools of data transfer and derogations for specific situations. Under the alternative tools for data transfer are Standard Contractual Clauses ("SCCs"), the most frequently used mechanism to transfer personal data from the EU and UK abroad, including to the United States.[9] However, the applicability and validity of SCCs recently came under scrutiny in the case of *Data Protection Commissioner vs Facebook Ireland, Maximillian Schrems ("Schrems II")*, leading to an amendment of the previous SCCs to the Modernized Transfer SCCs.

The Modernized SCCs have since come into operation and companies wishing to utilize them are required to follow the laid down requirements to render the SCCs a valid means of protection of third country data transfers.

[8] intersoft consulting. (n.d.). General Data Protection Regulation. https://gdpr-info.eu/
[9] Treacy, B., & Kurth, H. A. (2021, June 24). *Updated SCCs for international data transfers: fir for the future*. Thompson Reuters Practical Law. Retrieved May 2, 2022, from https://uk.practicallaw.thomsonreuters.com/w-031-4820?transitionType=Default&contextData=(sc.Default)&firstPage=true

2. Research Question

This paper recognizes that with the passing of a new law, the actual process of implementation can be an uphill task for most affected by that law. For companies, such a transition often presents several implications such as updating internal legislation and policy to reflect the new law, effecting the changes in the company operations, constant monitoring of any legal developments and the financial requirements to bring the company in line with the legal changes.

For this reason, this paper seeks to find out, since the passing of the modernized SCCs, to what extent have they been fully operationalized by EU companies engaged in data transfer?

This research question will be operationalized by the following research objectives:

- To establish the requirements for implementing SCCs
- To identify how companies have incorporated SCCs into their third country transfers of personal data
- To identify gaps in the implementation process

3. Theoretical background

3.1. Transfer of Data to Third Countries

The following is a scenario that illustrates a data transfer to third countries.

Company A is an automobile company whose Europe regional headquarters are based in Austria. The parent company is in Japan. The head of human resources in Austria periodically uploads all employee data, including personal data of job applicants and former job employees of the European branch to the company´s global human resources information system on servers in Japan. The Japan branch in turn has outsourced the human resource data entry to a subsidiary in India with lower labour costs. Under what circumstances would this transfer of data initially from Europe to its final destination in India be considered an illegal transfer of data?

A basic component of company operations is ascertaining the laws and regulations that govern its operations. In the above scenario, by the fact that one of the automobile company´s branch is in Austria, the GDPR has an overarching jurisdiction on the legality of the personal data transfer to Japan and India. To begin with, the Regulation applies to the processing of personal data wholly or partly by automated means and to the processing of personal data which form part of a filing system or are intended to form part of a filing system during an activity that falls inside the scope of the Union law.[10]

When transferring personal data within the EU, the GDPR imposes no additional requirements related to its direct applicability. However, when personal data is transferred to a country outside the EU (third country transfers), the GDPR lays out guidelines under which the data should be transferred. But before determining which guidelines apply to third country transfers, this research will begin by interrogating these questions:

i) What constitutes a data transfer?
ii) What type of data is protected by the GDPR?
iii) What constitutes a transfer of data to a third country?
iv) What are the requirements for transfer of data to a third country.

3.2. What constitutes a data transfer under the GDPR?

The British supervisory authority, Information Commissioner´s Office (“ICO”), defines a data transfer as an intentional sending of personal data to another party or making the data

[10] Article 2 GDPR

accessible by it, where neither the sender nor recipient is a data subject.[11] For the purposes of establishing what act on personal data is covered by the Regulation, Article 4(2) of the GDPR defines 'processing' as follows:

"…any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction."

The question of data transfer is also dependent on the parties involved in the moving of data, thereby determining who will ultimately be responsible for implementing the Regulation. For a flow of personal data to qualify as a transfer, the data flow must be between a controller and processor.

3.2.1. **Definition of a "Controller"**

While Article 3 refers to controller and processor in defining the territorial jurisdiction of the GDPR, Article 4(7) describes a controller as a natural or legal person, public authority, agency or other which determines the purposes and means of processing personal data while Article 4(8) describes a processor as a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.

The European Data Protection Board ("EDPB") Guidelines 07/2020 on the concepts of controller and processor in the GDPR[12] further break down the definition of controller into five main categories:

- "the natural or legal person, public authority, agency or other body"
- "determines"

[11] Data Privacy Office. (n.d.). *Organization of cross-border data transfer according to GDPR*. https://data-privacy-office.com/en/oformlenie-transgranichnoj-peredachi-dannyh-po-gdpr-chast-1/#f1

[12] *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (Version 2.0). (2021, July). European Data Protection Board. https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

- “alone or jointly with others”
- “the purposes and means”
- “of the processing of personal data”

3.2.1.1. **“the natural or legal person, public authority, agency, or other body.”**

The GDPR regards a controller as “*a natural or legal person, public authority, agency or other body”*. In essence, a controller might be an individual or an organization. However, these Guidelines contend that in practice, the controller is deemed as the organisation instead of the individual, for instance when the CEO of a company orders data processing during the company´s business or when employees process personal data within the activities of the organisation, the controller is the company and not the CEO.

3.2.1.2. **“determines”**

Guidelines 07/2020 define “determines” as the controllers influence over the processing, by virtue of an exercise of decision-making power. A controller is a body that decides on the processing's important parts. A party may declare itself a controller or the duty assigned by legislation based on an examination of the case's facts and circumstances. Two questions are pertinent: "why is this processing taking place?" and "who decided that the processing should take place for a certain purpose?"

These Guidelines further clarify that identifying the controller requires a factual in place of a formal analysis, which in most instances, can be through reference to certain legal and/or factual circumstances from which “influence” can be inferred, unless other elements indicate the contrary. There are two types of control situations: (i) control based on legal provisions, and (ii) control based on factual influence.

i) **control based on legal provisions**

Stems from legal designation of duties by national or Union law. Paragraph 22 of Guidelines 07/2020 refers to Article 4(7) of the GDPR that designates a controller as one to be nominated by the Union or Member State law where the purposes and means of processing are determined by Union or Member State law. For instance, an entity entrusted with certain public tasks such as social security, a task that cannot be fulfilled without gathering at least some personal

data sets in a database or register. In that instance, the law establishes who is the controller, although indirectly. In general, the law may impose a requirement on public or private institutions to keep or provide specific data. These entities would then be regarded controllers in relation to the processing required to carry out this responsibility.

ii) **control stemming from factual influence**

In the absence of control stemming from legal provisions, control is established by analysing the factual circumstances surrounding the processing. This means that the role of controller is not derived from the activities of the controller but rather from the entity´s particular operations in a specific context and from each specific data processing activity.

In practice, certain processing operations are inextricably linked to the role or activities of an entity, resulting in certain data protection duties. This could stem from general legal positions or long-standing legal practice in several fields (civil law, business law, labour law, etc.). In this case, existing traditional roles and professional expertise that normally implies a certain level of responsibility, such as an employer processing personal data about his employees, a publisher processing personal data about its subscribers, or an association processing personal data about its members or contributors, will assist in identifying the controller.

As regards designation of roles in a contract, it may explicitly specify who is the controller or contain enough information to infer who makes decisions about the aims and methods of processing. However, the provisions of a contract are not always binding, as this would merely allow parties to assign liability as they see fit. It is not feasible to become a controller or to avoid controller obligations simply by rewriting the contract in a certain way.

In the factual approach, the controller is the entity that genuinely has a decisive impact on the purposes and means of processing. A processor agreement usually specifies who is the deciding party (controller) and who is the directed party (processor). Even if the processor provides a service that is pre-defined in a specific way, the controller must be given a full description of the service

and must make the final decision to approve or request changes to the way the processing is carried out. What´s more, the processor cannot change the important aspects of the processing without the controller´s agreement.

3.2.1.3. "**Alone or jointly with others"**

Article 4(7) of the GDPR recognises that a controller might be acting alone or jointly with others. Paragraph 31 of Regulations 07/2020 clarify that several different entities may act as controllers for the same processing, with each responsible to maintain the data protection regulations. In addition, an organisation can still be a controller even if it does not make all the decisions as to purposes and means.

These regulations describe a joint controllership relationship to exist where more than one party determine jointly the purpose and means of the processing activity.[13] The assessment of joint controllership should be carried out on a factual, rather than formal analysis of the actual influence on the purposes and means of the processing. The Guidelines give two reasons why a formal criterion would not suffice: i) the formal appointment of a joint contract (by law or in a contract) would be absent; and ii) the formal appointment may fail to reflect the reality of the arrangement, for instance when the role of controller is entrusted to an entity that is not able to "determine" the purposes and means of processing.

However, not all processing relationships give rise to joint controllership. The key elements are that there are two or more entities in the determination of the *purposes* and *means* of a processing. If both or each of these elements are determined by the entities in question, then they qualify to be considered as joint controllers.

The Guidelines assess joint participation to include the form of a common decision taken by two or more entities or result from converging decisions by two or more entities regarding the purposes and essential means,[14] but that will not be covered in this paper.

[13] EDPB (2021, Paragraph 52)
[14] For additional information, see paragraph 54 of Guidelines 07/2020 on Assessment of joint participation.

3.2.1.3.1. **Situations where there is no joint controllership**

Not all processing partnerships, cooperation or collaborations will be considered as joint partnerships. Such qualification necessitates a case-by-case review of each processing at stake and the function of each entity in such processing.

- When similar sets of data are exchanged between two entities without jointly determined purposes or jointly determined means of processing, this is considered as transmission of data between separate controllers.

The Guidelines give an example of transmission of employee data to tax authorities to illustrate this point:

A company collects and processes personal data of its employees with the purpose of managing salaries, health insurance, etc. A law imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control.

In this case, even though both the company and the tax authorities process the same data concerning salaries, but the lack of jointly determined purposes and means of data processing will result in qualifying the two entities as two separate data controllers.

- Joint controllership will also not be assumed in a case where numerous entities use a shared database or infrastructure but each entity sets its own purposes independently. A case example is of marketing operations in a group of companies using a shared database. A group of companies use the same database to manage their clients and prospects, and this database is maintained on the server of the parent company who is the processor of the companies with respect to the storage of data. However, each group business solely inputs and processes the data of its own clients and prospects for its own purposes, determines its own access and retention periods and rectification or deletion of its clients´ and prospects data. Each of these companies cannot in turn see or utilize each other´s information. The fact that these organizations share a group database does not automatically imply joint controllership. As a result, each corporation acts as its own controller in these circumstances.

- Similarly, where various actors successfully process the same personal data in a chain of operations, but each of the actors has an independent purpose and independent means in their part of the chain, in the absence of joint participation in the determination of the purposes and means of the same processing operation, the controllers shall be regarded as successive independent controllers and not joint controllers.

  Case example: Statistical analysis for a task of public interest:
  The legal role of a public authority (Authority A) is to conduct relevant analysis and statistics on how the country's employment rate evolves. To do so, several other government agencies are required by law to provide Authority A with specified information. Authority A decides to process the data using a specified system, which includes data collecting. This also implies that the other units are required to use the system for data disclosure. In this case, Authority A will be the sole controller of the processing for the purpose of analysis and statistics of the employment rate processed in the system, notwithstanding any legal roles attributions, because Authority A determines the purpose of the processing and has decided how the processing will be carried out.[15]

3.2.1.4. **"the purposes and means"**

Guidelines 07/2020 refer to *purposes and means* of data collection as the substantive part of the controller concept, and precisely, what a party should determine to qualify as a controller.[16] The controller answers the questions "why" and "how" of a particular processing and determines why the processing is taking place (i.e. "to what end"; or "what for") and how this target will be achieved, given a particular processing action (i.e. which means shall be employed to attain the objective. The natural or legal person who has such influence over the processing of personal data, thereby participating in the determination of the purposes and means of that processing, fulfils the definition of controller under Article 4(7) of the GDPR.

[15] EDPB (2021, Paragraph 52)
[16] EDPB (2021, Paragraph 32)

The controller decides on both purpose and means of processing but never solely on the purpose. However, there are instances where the controller engages a processor to carry out the processing on its behalf, thereby giving it the right to be able to make certain decisions on its own on how to conduct the processing. For this reason, the EDPB Guidelines[17] provide guidance on the *level of influence* on the "why" and the "how" to differentiate the controller and the extent a processor may make decisions of its own. When one entity determines the purposes and means of processing before entrusting another entity with processing activities that amount to the execution of its detailed instructions, then there is no doubt that the first entity is the controller and the second, the processor.

3.2.1.4.1. Essential vs non-essential means

Whereas the controller is always in charge of determining the purpose of the processing, the challenge sets in when one must differentiate between the between decisions that should be made by the controller and the operating decisions made by the processor. For this reason, a distinction must be made between essential and non-essential means. "Essential means" are determined, and traditionally and inherently reserved to the controller. They are closely linked to the purpose and the scope of the processing such as the type of personal data to be processed, and the categories of data subjects. They are also closely linked to the question of whether the processing is lawful, necessary, and proportionate. "Non-essential means" involve more practical aspects of implementation such as the choice for a particular type of hard or software or the detailed security measures which are left to the discretion of the processor.

To better explain this differentiation, the Guidelines give the following examples:

a) Payroll administration

   Firm A engages Firm B to handle the payment of its employees' salaries. Firm A gives specific instructions on who to pay, how much to pay, when to pay, which bank to pay, how long the data should be kept, and what data should be provided to the tax authority, among other things. In this situation, data is processed for the sole purpose of paying salaries to Firm A's employees, and the payroll administrator is prohibited from using the

[17] EDPB (2021)

data for any other purpose. The way the payroll administrator should do the processing is, in essence, well-defined. Nonetheless, the payroll administrator has the authority to make specific decisions about the processing, such as which software to use and how to do it, how to share access throughout the company, and so on. As long as the administrator does not go against or beyond the instructions supplied by Firm A, it retains its duty as processor.

b) Bank payments

The payroll administration sends information to Bank B as part of Firm A's instructions so that they can make the actual payment to Firm A's employees. This activity comprises Bank B's processing of personal data for the purpose of conducting banking transactions. Within this activity, the bank makes its own decisions about whether data must be processed to deliver the service, how long the data must be held, and so on, independent of Firm A. Firm A has no control over the purpose or methods by which Bank B processes data. As a result, Bank B is to be seen as a controller for this processing, and the communication of personal data from the payroll administration is to be regarded as a transmission of personal data from Firm A to Bank B.

c) Accountants

Firm A also employs Accounting Firm C to conduct bookkeeping audits, and therefore passes financial transaction data (including personal data) to C. Without clear instructions from A, accounting company C processes these data. Accounting firm C determines that the data it collects will only be processed for the purpose of auditing A, in accordance with legal provisions governing the tasks of C's auditing activities, and it determines what data it needs, which categories of persons must be registered, how long the data must be kept, and what technical means to use. In these circumstances, Accounting Firm C should be treated as if it were its own controller while performing auditing services. However, depending on the level of instructions from A, this evaluation may alter. The accounting firm would be working as a processor in a circumstance where the law does not impose explicit requirements on the accounting firm and the client

company offers highly comprehensive instructions on the processing. A contrast could be drawn between a situation where the processing is done as part of the accounting firm's main activity, as defined by the regulations governing this profession, and a situation where the processing is a more limited, auxiliary work carried out as part of the client company's operation.

That said, even if 'non-essential means' decisions can be left to the processor, the controller must nonetheless include some aspects in the processor agreement, such as – in connection to the security requirement, for example – an order to take all measures required pursuant to Article 32 of the GDPR. The processor must also undertake to assist the controller in ensuring compliance with the agreement's terms, for example, Article 32. In any case, the controller is responsible for putting in place necessary technological and organizational measures to ensure that the processing is carried out in compliance with the Regulation and to be able to demonstrate that it is (Article 24). The controller must consider the nature, scope, context, and aims of the processing, as well as the risks to natural person's rights and freedoms. As a result, the controller needs to be thoroughly informed about the methods employed so that it may make an informed decision. It is advisable to document at the very least the essential technological and organizational steps in the contract or other legally binding instrument between the controller and the processor for the controller to be able to establish the lawfulness of the processing.

3.2.1.5. **"of the processing of personal data"**

Article 4(2) GDPR describes processing of personal data as "any operation or set of operations which is performed on personal data or on sets of personal data". Therefore, decisions on the purposes and means (described above) by the controller must relate to processing of personal data.

It is crucial to note that an actor will be considered a "controller" even if it does not intentionally target personal data or has incorrectly assessed that it does not process personal data.

In addition, an actor will also be considered a "controller" even if it does not have access to the data being processed. So long as the actor has determinative influence on the purpose and (essential) means of the processing (e.g., by modifying the specifications

of a service in a way that it determines who´s personal data is processed) regardless of whether the actor outsources the processing activities or not.

The term “controller” might refer to a single processing operation or a group of activities. In practice, the processing of personal data involving multiple actors can be broken down into smaller processing processes, with each actor determining the goal and means on their own. A sequence or set of processing activities involving numerous actors, on the other hand, may occur for the same purpose(s), in which case the processing may comprise one or more joint operations. This means that at “micro-level” the different processing operations of the chain appear as disconnected. It is however important to ensure that at “macro-level”, these processing operations should not be considered as a “set of operations” pursuing a joint purpose using jointly defined means.

3.2.2. **Definition of “Processor”**

Article 4(8) GDPR defines processor as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

The Guidelines further detail the two basic conditions for qualifying as a processor as:

a) being a separate entity from the controller, and
b) processing personal data on the controller´s behalf.

3.2.2.1. **Being a separate entity from the controller**

When the controller decides to delegate all or part of the processing activities to an external organization, it is referred to as a separate entity. For instance, withing a group of companies, one company can be the controller and the other the processor because they are both separate entities. A company's department, on the other hand, cannot act as a processor for another department in the same company because they are the same entity.

3.2.2.2. **Processing personal data on the controller´s behalf**

When a controller processes data using its own resources within its organisation, such as its own employees, it shall not be considered a processor situation. Employees and other individuals acting under the controller’s direct authority,

such temporary employees, are not to be considered processors because they will process data on behalf of the controller´s entity. They are likewise bound by the controller's directives as laid out in Article 29 GDPR.

For the requirement of *processing data on the controller´s behalf* to be fulfilled:

a) Processing personal data on behalf of the controller necessitates a separate entity process personal data on behalf of the controller.
b) The processing must be done on behalf of a controller but otherwise than under its direct authority or control. Nonetheless, the processor is required to implement the controller´s instructions at least regarding the purpose of the processing and the essential elements of the means. In assessing the lawfulness of the processing according to Article 6 and if relevant, Article 9 GDPR, regard will be had to the controller´s activity, and the processor must process the data in accordance with the controller´s instructions. However, as previously discussed, the controller´s instructions may provide the processor with some freedom in terms of how to best serve the controller´s interest, allowing the processor to select the most appropriate technical and organizational means.
c) The processor may not carry out processing for its own purpose(s). A processor violates the Article 28(10) GDPR if it goes beyond the controller's instructions and begins to define its own goals and ways of processing. For that processing, the processor will be deemed a controller, and going beyond the controller's orders may result in fines.

   The Guidelines give an example to illustrate this point.

   Example: Service provider referred to as a data processor but acting as controller

   MarketinZ is a service provider that offers promotional advertising and direct marketing to a variety of businesses. GoodProductZ signs a contract with MarketinZ, under which the latter will provide commercial advertising for GoodProductZ consumers and will operate as a data processor. MarketinZ, on the other hand, decides to use GoodProducts' client database for objectives other than advertising for GoodProducts, such as

expanding their own firm. MarketinZ becomes a data controller for this set of processing activities because of the decision to add an additional purpose to the one for which the personal data were transferred, and their processing for this reason would be in violation of the GDPR.

d) Not all service providers who process personal data while providing a service are considered "processors" under the GDPR. The nature of a processor is derived from its particular activities in a specific environment, not from its nature as a data processor. In other words, a single entity might operate as a controller for some processing processes while also acting as a processor for others, and the qualification as a controller or processor must be evaluated in relation to specific sets of data or actions. The nature of the service will decide whether the processing activity constitutes personal data processing on behalf of the controller as defined by the GDPR.

   In practice, where the offered service is not particularly targeted at processing personal data or where such processing is not a significant aspect of the service, the service provider may be able to identify the objectives and means of processing required to provide the service independently. In that case, the service provider should be considered a distinct controller rather than a processor. However, a case-by-case review is still required to determine the degree of influence each entity has in defining the processing's aims and methods.

   The Guidelines give the following case example to illustrate this point.

   Example: Taxi service

   A taxi service offers an online platform that allows companies to order a cab to transport employees or guests to and from the airport. Company ABC gives the name of the employee to be picked up from the airport when reserving a cab so that the driver may verify the employee´s identify at the time of pick up. In this situation, the taxi service handles the employee´s personal data as part of its service to Company ABC but the processing is not the business´s primary goal. Without any directions from Company ABC, the taxi service creates the online booking platform as part of

establishing its own commercial activity to provide transportation services. In addition, the taxi service also chooses the data categories it collects and for how long it keeps information. Even though the processing occurs in response to a request for service from Company ABC, the taxi service functions as a controller in its own right.

3.3. What type of data is protected under the GDPR?

The GDPR states that "personal data" is the entryway to the application of the GDPR.[18] That means, if a processing of data concerns personal data, then the GDPR applies. Article 4(1) then describes "personal data" as:

> "…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."

The GDPR goes further to state that in practice, this includes all data that is or can be associated with a person in any way. Personal data includes things like a person's phone number, credit card number, or personnel number, as well as account data, license plate number, appearance, client number, and address.

The Regulation suggests that since the definition of "personal data" includes "any information", the term should be accorded a broad interpretation. For instance, considered less explicit information such as recordings of work times which include information about the time when an employee begins and ends his workday, including breaks, and written answers from a candidate during a test and any remarks from the examiner regarding these answers have been considered personal data.[19]

As regards IP addresses, they are classified as personal data if the controller has the legal option of requiring the provider to supply extra information that allows him to identify the user behind the IP address. It's also worth noting that personal data does not have to be objective. Personal data might include subjective information such as opinions, judgments, or estimates or even an

[18] *GDPR*. (n.d.). Intersoft Consulting. Retrieved May 1, 2022, from https://gdpr-info.eu/issues/personal-data/
[19] *GDPR*. (n.d.). (Personal Data)

assessment of a person's creditworthiness or an employer's appraisal of work performance falls. within this category.[20]

According to the Article 4 GDPR, “personal data” applies to the identifiable data of a natural person. It does not apply to information about legal entities such as corporations, foundations, and institutions. The natural person´s data is protected only if the person is alive. The Regulation states the following:

> For natural persons, on the other hand, protection begins and is extinguished with legal capacity. Basically, a person obtains this capacity with his birth, and loses it upon his death. Data must therefore be assignable to identified or identifiable living persons to be considered personal.[21]

Special categories of data

There are categories of personal data that attract a higher level of protection. They are known as special categories or sensitive personal data. The GDPR identifies these data to include genetic (Recital 34), biometric and health data (Recital 35) as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.

Anonymous data

Recital 26 GDPR reiterates that the principles of data protection apply to any information concerning an identified or identifiable natural person. This includes personal data that has been pseudonymised but can still be attributed to a natural person using additional information. However, the principles of data protection do not apply to anonymous information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is no longer identifiable.

To determine whether a natural person is identifiable, all reasonable means reasonably likely to be utilized, such as singling out, by the controller or another person to identify the natural person directly or indirectly should be considered. To determine whether means are reasonably likely to be used to identify the natural person, all objective considerations, such as the costs and time required for identification, should be considered, considering the available technology at the time of processing and technological advancement.

Such personal data should not be processed unless it is allowed in specific cases set out in the Regulation, taking into account that Member States' laws may include specific data protection

[20] *GDPR*. (n.d.). (Personal Data)
[21] *GDPR*. (n.d.). (Personal Data)

provisions in order to tailor the application of this Regulation's rules to comply with a legal obligation, perform a task in the public interest, or exercise official authority vested in the controller. In addition to the specific requirements for such processing, the GDPR requires that the general principles and other rules of the Regulations should apply, in particular, the conditions for legitimate processing. Express derogations from the general prohibition on processing such special categories of personal data should be provided, for example, where the data subject gives his or her explicit consent or in response to specific needs, such as when the processing is carried out in the course of legitimate activities by certain associations or foundations with the goal of allowing the exercise of fundamental freedoms.

3.4. What constitutes a transfer of data to a third country?

The GDPR does not explicitly define “transfer of data to a third country”. However, it impliedly does so by setting out its territorial jurisdiction to include any processing of personal data:

i) by a controller or processor established in the EU whether the processing of data takes place in the EU or not;
ii) of data subjects located in the EU, whether the controller and/or processor is in the Union or not; or
iii) by a controller not established in the Union but in a place where Member State Law applies by virtue of public international law.[22]

The EDPD Guidelines 05/2021 further enumerate three scenarios under which a transfer of personal data shall be considered a “transfer of personal data to a third country or international organisation”:

i) A controller or a processor is subject to the GDPR for the given processing.
ii) This controller or processor (“exporter”) discloses by transmission or otherwise makes personal data subject to this processing, available to another controller, joint controller, or processor (“importer”).
iii) The importer is in a third country or is an international organisation, regardless of whether this importer is subject to the GDPR in respect of the given processing in accordance with the territorial jurisdiction of the GDPR in Article 3.

After ascertaining which transfers would be considered ´third country transfers´, one must then establish the transfers protected under the Regulation. For a flow of personal data to qualify as a

[22] Article 3 GDPR

transfer, the data flow must be between a controller and processor[23]. The definitions of controller and processor have been discussed above.

3.5. Requirements of a transfer of data to a third country

Once the above parameters are established, such a transfer of personal data shall be considered a "transfer of data to third countries", with its validity determined by Articles 44-50 of the GDPR. The GDPR is emphatic on ensuring a similar level of protection of personal data in third countries as in the EU. For this reason, it lays out 3 conditions under which data shall be deemed to have been validly transferred to a third country: adequacy decision, transfers subject to appropriate safeguards and derogations for specific situations.

3.5.1. **Adequacy decision**

To transfer personal data to a third country or an international organisation, the Commission must determine that the third country, a territory or one or more specified sectors within that country, or the international organisation provide adequate protection. Such a transfer shall not require any specific authorisation.[24]

To reach upon an adequacy decision, the Commission shall consider the following:

a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onwards transfer of personal data to another third country or international organisation which are compiled with in that country or international organisation, case-law, as well as effective and enforceable data subject rights for the effective administrative and judicial redress for the data subjects whose personal data are being transferred;
b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

[23] For definitions of ´controller´ and `processor´ refer to section 3.2 above
[24] Article 45 GDPR

c) the international commitments the third country or international organisation concerned has entered, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular the relation to the protection of personal data.

The Commission may declare a country or international organisation to maintain adequate by means of an implementing act. There shall be a periodic review mechanism in the implementing act, at least every four years, which shall consider all relevant developments in the third country of international organisation.[25] Where, especially after this periodic review, a third country, a territory or one or more specified sectors within a third country or an international organisation is found to no longer maintain an adequate level of protection, the Commission shall repeal, amend, or suspend the adequacy decision by means of an implementing act without retro-active effect.[26] However, the Commission shall enter consultations with the third country or international organisation with a view to remedying the situation that led to this suspension.[27] The declaration of a country or international organisation does not ensure adequate protection is without prejudice to transfers of personal data to the third country or the international organisation.[28]

3.5.2. **Transfers subject to appropriate safeguards**

Article 46 of the GDPR states that in the absence of a decision on adequate safeguards, a controller of processor may transfer personal data to a third country or an international organisation if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The protective measures can be put in put in place, without requiring specific authorization from a supervisory authority, by:

a) a legally binding and enforceable instrument between public authorities or bodies;
b) binding corporate rules;
c) standard data protection clauses adopted by the Commission;
d) standard data protection clauses adopted by a supervisory authority and approved by the Commission;
e) an approved code of conduct that is in line with Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the apply the appropriate safeguards, including as regards data subjects´ rights; or

[25] Article 45(3) GDPR
[26] Article 45(5) GDPR
[27] Article 45(6) GDPR
[28] Article 45(7) GDPR

f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects´ rights.

These appropriate safeguards may also be provided for by:

a) contractual clauses between the controller or processor and the controller, processor, or the recipient of the personal data in the third country or international organisation; or
b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

3.5.3. **Binding Corporate Rules**

They are the third means of transfer of personal data to a third country and are approved by the competent supervisory authority. They are available to a group of enterprises engaged in a joint economic activity provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.[29]

3.5.4. **Derogations for specific situations**

Article 49 GDPR provides a leeway to transfer data to third countries in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46. The transfer shall only take place under one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
b) the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request;
c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
d) the transfer is necessary for important reasons of public interest;
e) the transfer is necessary for the establishment, exercise or defence of legal claims;
f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

[29] Recital 110 GDPR

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

When a transfer to a third country or an international organisation cannot be justified by one of the provisions in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to above apply, the transfer may be made only if it is not repetitive, concerns only a small number of data subjects, is required for the purposes of compelling legitimate interests which are not outweighed by the data subject's interests or rights and freedoms, and the controller has assessed all the circumstances surrounding the data transfer and provided appropriate safeguards for the protection of personal data on the basis of that assessment. The controller must report the transfer to the supervisory authority. In addition to the information required by Articles 13 and 14, the controller must inform the data subject of the transfer and on the compelling legitimate interests pursued.

The focus of this paper, however, is on Standard Contractual Clauses (SCCs) as appropriate safeguards for data transfer.

3.6. Standard Contractual Clauses

Standard Contractual Clauses ("SCCs") are standardised and pre-approved model transfer clauses that allow controllers and processors to comply with their obligations under EU data protection law.[30] They were previously described as contractual clauses authorised by Member States for the transfer of personal data to third countries which do not ensure an adequate level of protection and governed by Article 26(2) of Directive 95/46/EC. After the repeal of Directive 95/46/EC by the GDPR[31], the SCCs remain an avenue for transfer of data to third countries, classified under appropriate safeguards and governed by Article 46 of the GDPR.

A survey conducted by the International Association for Analytical Psychology (IAAP) on its subscribers for its "Daily Dashboard" publication revealed that more than 7 in 10 privacy experts working in firms that transfer data from the EU to a third country now use SCCs as the primary legal means for doing so. The research further revealed that other firms also employ "supplementary

[30] *THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS*. (2022, May). European Commission. https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf

[31] Article 95 GDPR

measures" or additional safeguards, either technical (38%), contractual (36%) or policy-based (26%), to complement their use of SCCs.[32]

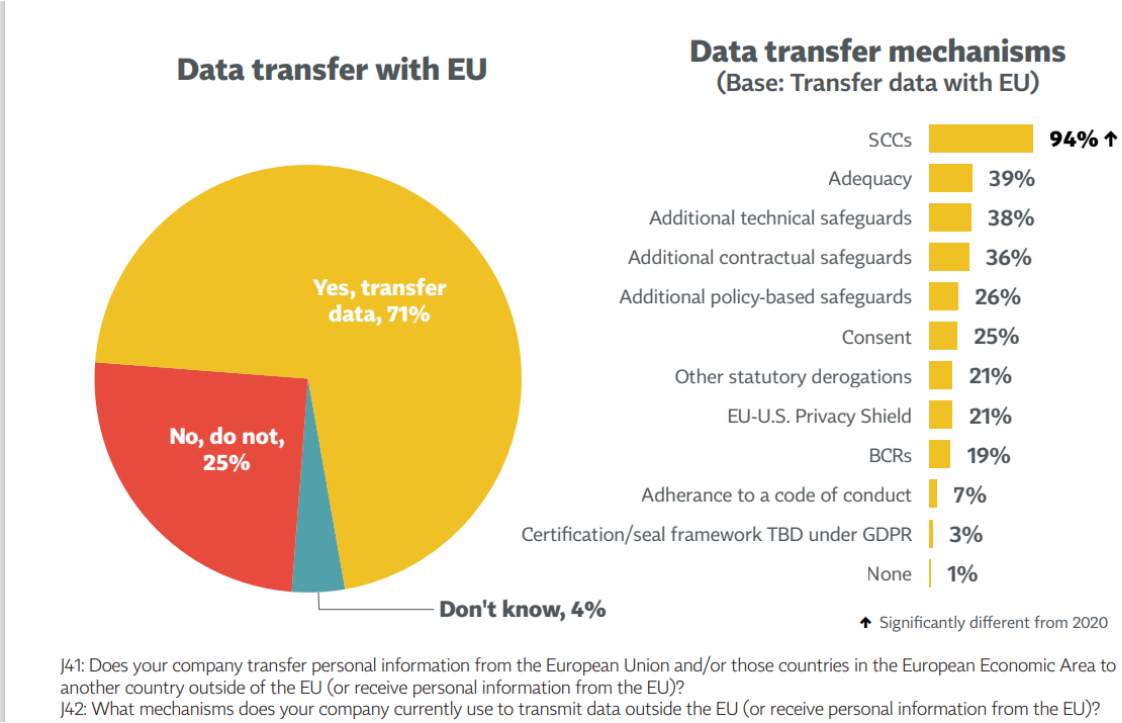


Figure 1: More than 7 in 10 firms transfer data from the EU to a third country; SCC´s are used by nearly 95% of them
Source: IAPP-EY Annual Privacy Governance Report 2021

Despite being considered as the most accessible method of data transfer to third countries,[33] the SCCs came under scrutiny in Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) ("Schrems II")[34] where their capability of ensuring an adequate level of protection of personal data transferred to third countries was questioned given that the standard data protection clauses referred to in the SCC decision do not bind the supervisory authorities of those third countries.

In essence, Article 46(1) of the GDPR dictates that in the absence of an adequacy decision pursuant to Article 45 of the GDPR, the responsibility of providing adequate safeguards rests upon the

[32] Fazlioglu, M. (2021). *IAPP-EY Annual Privacy Governance Report 2021*. https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf
[33] Bradford, L., Abboy, M., & Lidell, K. (2021). Standard contractual clauses for cross-border transfers of health data after Schrems II. Journal of Law and the Biosciences, 8(1). https://doi.org/10.1093/jlb/lsab007
[34] Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems. C-311/18 (Grand Chamber 2020). https://noyb.eu/files/CJEU/judgment.pdf

controller or processor established in the EU. This requirement is reinforced by Recital 108 and 114 GDPR which mandate the controller or processor, in the absence of an adequacy decision to take measures to compensate for the lack of data protection by way of appropriate safeguards and use solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the EU, once the data has been transferred so that they will continue to benefit from fundamental rights and safeguards.[35]

The judgment, however, rendered SCCs as incapable of offering sufficient data protection to users beyond their contractual nature. Even though there is no obligation to use SCCs, they are binding on a controller or processor established in the EU/EEA and the recipient or sender of the transfer of personal data established in a third country where these parties have concluded a contract incorporating those clauses. Nonetheless, they are unable to bind the governments of that third country (privity of contract).[36] As a result, the recipient of such a transfer can only guarantee the necessary protection of the data in accordance with its obligations under the SCCs, but this protection may not be adequate, particularly if the third country's law allows its public authorities to interfere with the rights of the data subjects to whom the data relates.[37]

The judgment went further to add that Articles 44, 46(1) and 46(2) of the GDPR interpreted in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union ("the Charter")[38] require that the level of protection guaranteed by the GDPR is not undermined. For this reason, the controller employing standard data-protection clauses adopted by the Commission is not prevented from adding other clauses or additional safeguards. In fact, the controller is encouraged to provide additional safeguards that supplement standard data protection clauses.[39] It was re-emphasised that the SCC´s adopted by the Commission based on Article 46(2)(c) of the GDPR were solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the Union. It is therefore a responsibility of the controller or processor "to verify…, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data whether the law of the third country… ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."[40]

[35] Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (2020, Paragraph 131)
[36] Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (2020)
[37] Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (2020, Paragraph 132)
[38] Charter of Fundamental Rights of the European Union, 2000/C 364/01 (2000) https://www.europarl.europa.eu/charter/pdf/text_en.pdf
[39] Recital 109 GDPR
[40] Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems (2020, Paragraph 134)

The Commission records two sets of SCCs adopted on June 4, 2021.

i. *SCCs for the relationship between controllers and processors* fulfil the requirements in Article 28(3) of Regulation (EU) 2016/679 (the General Data Protection Regulation) and in Article 29(3) and (4) of Regulation (EU) 2016/679 (the General Data Protection Regulation) applicable to EU institutions, bodies, offices, and agencies ("EUDPR"). Consequently, these SCCs can be used by public and private bodies as well as EU institutions, bodies, offices, and agencies.

ii. *SCCs as a tool for data transfers*, i.e. to comply with the requirements of the GDPR for transferring personal data to countries outside the EEA. They contain specific data protection safeguards to ensure that personal data benefits from a high level of protection when transferred outside the EEA. They can be used by data exporters, without the need to obtain a prior authorisation (for the data transfer if the clauses used) from a data protection authority.[41]

For the purposes of this research, this paper shall only focus on SCCs as a tool for data transfers. These SSCs include modernised clauses for data transfers from controllers or processions in the EU/EEA and controllers or processors outside the EU/EEA[42]. The modernize clauses came into effective as from 27th September 2021 replacing the previous SCCs adopted under Directive (95/46/EC, specifically:

- Commission Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (June 15, 2001) (2001 Clauses) for controller-to-controller transfers.
- Commission Decision 2004/915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (December 27, 2004) (2004 Clauses) for controller-to-controller transfers and amending the 2001 Clauses.
- Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC (February 5, 2010) (2010 Clauses), repealing Commission Decision 2002/16/EC on standard contractual clauses

[41] *THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS*. (2022, May)
[42] *Standard Contractual Clauses (SCC)*(2021, June 4).

for the transfer of personal data to processors established in third countries (December 27, 2001).[43]

The modernized SCCs implement some of the requirements of the Schrems II decision while adapting the provisions to the specifications of the GDPR.[44] However, decisions by a Member State or supervisory authority based under Directive 95/46/EC remain valid until amended, repealed, or replaced by a supervisory authority.[45]

3.1. Requirements for implementing the SCCs

The focus of this paper shall be on Standard Contractual clauses for controllers or processors outside the EU/EEA.

a) As previously stated, SCC´s are limited to providing appropriate safeguards in the absence of an adequacy decision.[46] Therefore, the controller transferring the personal data to a third country and the controller or processor receiving the personal data are free to include the SCC´s in a wider contract and to add other additional safeguards, provided that they do not contradict, directly or indirectly with the SCC´s or prejudice the fundamental rights or freedoms of data subjects.[47]

b) In addition to using the SCCs, the data exporter must fulfil its general responsibilities as controller or processor under Chapter 4 of the GDPR (Articles 24-36) and implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR[48]. These measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.[49] The controller must also fulfil his obligations towards the data subjects (pursuant to Articles 13 and 14 of the GDPR) by, for instance, observing the principles of fair and transparent processing that requires the data subject to

[43] Dumont, D., & Treacy, B. (2021, August 25). *European Commission's International Data Transfer Standard Contractual Clauses: What Businesses Need to Know*. Thompson Reuters. Retrieved January 12, 2022, from https://www.huntonak.com/images/content/7/8/v2/78022/eu-commissions-intl-data-transfer-standard-contractual-clauses.pdf
[44] *EU: Third-party beneficiary rights under revised SCCs*. (2021, July). OneTrust Data Guidance. Retrieved February 12, 2022, from https://www.dataguidance.com/opinion/eu-third-party-beneficiary-rights-under-revised-sccs
[45] Article 46(5) GDPR
[46] Article 46(1)
[47] Recital 109 GDPR
[48] Article 24(1) GDPR
[49] Recital 74 GDPR

be informed of the existence of the processing operation and its purposes[50] and provide the relevant information to the data subject where personal data was not obtained from the data subject for fair and transparent processing of personal data[51]. If the controller intends to transfer personal data to a third country in the absence of an adequacy decision or in the case of transfers subject to Article 47, 47 or Article 49(1) paragraph 2, the controller shall notify the data subject of the method of transfer relied upon and the means to obtain a copy of them or where they have been made available.[52]

c) In case of data transfers from controllers to processors who are outside the territorial scope of the GDPR or from processors subject to the GDPR to sub processors in jurisdictions outside the scope of the GDPR, the SCCs should allow the compliance with Articles 28(3) and (4), binding the processor or sub-processor to data protection obligations under the GDPR.[53]

d) The new SCCs adopt 4 modular approaches:

    a) Controller-to-controller transfers (Module 1)
    b) Controller-to-processor transfers (Module 2)
    c) Processor-to-processor transfers (Module 3)
    d) Processor-to-controller transfers (Module 4)

Controllers and processors should choose the appropriate module for their circumstances to match their SCC requirements to their role and responsibilities regarding the data processing in question. Furthermore, additional controllers and processors should be able to join the SCCs as data exporters or importers at any time during the contract's lifecycle.[54]

e) Data subjects should be given a copy of the standard contractual clauses and should be notified about the types of personal data processed, the right to request a copy of the standard contractual clauses, and any onward transfers. Onward transfers by the data

[50] Recital 60 GDPR
[51] Article 14 GDPR
[52] Article 14(1)(f)
[53] EUR-LEX. (2021). Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union, L:2021:199:TOC*. http://data.europa.eu/eli/dec_impl/2021/914/oj

[54] EUR-LEX. (2021, Paragraph 10)

importer to a third party in another third country should be permitted only if the third party agrees to the standard contractual clauses, if the data subject's protection is otherwise ensured, or in specific circumstances, such as with the data subject's explicit, informed consent.[55]

f) Clause 3 of the SCCs provides for Third-party beneficiaries, whereby data subjects, with some exceptions, may invoke and enforce their rights under the contract against the data exporter and/or data importer without being limited by privity of contract.[56] Standard contractual provisions should oblige the data importer to notify data subjects of a contact point and to respond immediately to any complaints or requests to facilitate individual redress. In the event of a disagreement between a data importer and a data subject who asserts his or her rights as a third-party beneficiary, the data subject shall be allowed to file a complaint with the appropriate regulatory authority or take the matter to the appropriate European courts.[57]

g) Rules on liability between the parties and with respect to data subjects, as well as rules on indemnification between the parties, should be included in standard contractual provisions. The data subject should be entitled to compensation if he or she suffers significant or non-material damage because of a breach of the third-party beneficiary rights under the standard contractual agreements. This, however, should not be construed as an admission of liability under the GDPR.

h) In line with Article 28(3) of the GDPR that requires the processing of data by a processor to be governed by a contract or other act under Union or Member State Law, the data importer shall be required under the SCCs to make all information necessary to establish compliance with the clauses' duties, as well as to allow for and participate in data exporter audits of its processing activities. Should the data importer wish to engage a sub-processor, the SCC´s should include the procedure to obtain specific or general written authorisation of the controller (in accordance to Article 28(2) of the GDPR), as well as the requirement for a written contract with the sub-processor ensuring the same level of protection as the clauses.[58]

[55] EUR-LEX. (2021,Paragraph 11)
[56] EUR-LEX. (2021, Clause 3)
[57] EUR-LEX. (2021, Paragraph 12)
[58] EUR-LEX. (2021Paragraph 15)

i) The SCCs should require the processor to notify the controller if it is unable to carry out the controller's instructions, including if the instructions are in violation of Union data protection law, and the controller to refrain from taking any actions that would prevent the processor from carrying out its obligations under the GDPR. They should also compel the parties to help each other in responding to data subject inquiries and requests under the local law relevant to the data importer or the GDPR for data processing in the Union. In addition, the SCCs should include the requirement to address the laws of the third country (country of destination) that would impact the controller´s compliance with the clauses, for example, binding requests from public authorities in the third country for disclosure of the transferred personal data.[59]

j) Should the laws and practices of the third country of destination prevent the processor from complying with his duties, a transfer of data using the SCCs should not take place. What´s more, before concluding the contract of engagement, the parties should guarantee that they have no cause to suspect that the data importer's laws and practices are not in compliance with these standards at the time they agree to the standard contractual conditions.

[59] EUR-LEX. (2021,Paragraph 17)

4. Research Methodology

Research methodology is the science of studying how research is to be carried out and the procedures by which researchers go about their work of describing, explaining, and predicting phenomena.[60] Its purpose is to lay out the blueprint of the research.

This chapter outlines the research design, laying out the research study from research strategy, data collection and analysis to solutions for the problem being investigated. The first methodological choice this research follows is the qualitative research design.

Ahmad, et al. (2019) define qualitative and quantitative research in the following words:

> Qualitative research… [I]t is an unstructured exploratory research method that studies highly complex phenomena that are impossible to elucidate with quantitative research. Qualitative research is used to gain an in-depth understanding of human behaviour, experience, attitudes, intentions, and motivations, on the basis of observation and interpretation, to find out the way people think and feel. Quantitative research… relies on the methods of natural sciences, which produces numerical data and hard facts. It aims at establishing cause and effect relationship between two variables by using mathematical, computational, and statistical methods.[61]

Lee S.K., (1992) disagrees with this strict definition, adding that such a distinction does not capture the full significance of the different paradigms.[62] He adds that quantitative and qualitative research methods are based upon different ontological and epistemological assumptions which shape the aims of research inquiry, the role of the researcher, and the researcher-respondent relationship. The author illustrates the differences in quantitative and qualitative approaches using the following table.

[60] (PDF) Chapter 3 - Research Methodology and Research Method. Available from: https://www.researchgate.net/publication/333015026_Chapter_3__Research_Methodology_and_Research_Method [accessed Jun 13 2022].
[61] Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A., & Fahreen, Z. (2019). Qualitative v/s Quantitative Research. *Journal of Evidence Based Medicine and Healthcare*, *6*(23), 2828–2832. https://doi.org/10.18410/jebmh/2019/587

Table 1 Differences in quantitative and qualitative approaches

	Quantitative	Qualitative
Ontological Assumption	Objectivity	Subjectivity
Epistemological Assumption	Positivism	Phenomenology
Aims of Inquiry	Universality	Particularity
Role of Researcher	Outsider	Insider
Researcher-Respondent Relationship	Detachment	Involvement
Research Methods	Statistics	Description

The discussion laid forth by the author on the elements that differentiate quantitative and qualitative differences is beyond the scope of this research. Nonetheless, in proceeding to identity its research methodology as qualitative, this paper choses this methodology based on the simple definition by Saunders et al. (2016) that qualitative research is based on non-numeric data such as categorising data while quantitative research is based on numeric data collection method.[63]

4.1. Research strategy

A research strategy is a plan of action to achieve a goal.[64] It indicates the direction the research takes including the process by which the research is conducted. Saunders et al. (2016) links qualitative research to a variety of research strategies. These include:

- Action research (process of inquiry used to develop solutions to real organisational problems through a participative and collaborative approach)
- Case study research (an in-depth inquiry into a topic or phenomenon within a real-life setting)
- Ethnography (studying the culture or social world of a group)
- Grounded Theory (a theory that is grounded in or developed inductively from a set of data), and
- Narrative research (a story/personal account which interprets an event of sequence of events.

To conduct its research, this paper employs case study as its method of data collection. A case study is defined as an in-depth inquiry into a topic or phenomenon within its real-life setting.[65] It is used to probe deeply and intensively to gain insight and understanding of phenomena that is new,

[63]Saunders, M., et al. (2016, Section 5.3)
[64] Travers, M. (2001). *Qualitative Research through Case Studies* (FIRST EDITION). Sage Publishing.
[65] Yin, R. K. (2014). Case Study Research Design and Methods. *Canadian Journal of Program Evaluation*, *5th ed*. https://doi.org/10.3138/cjpe.30.1.108 as cited in Saunders, M., et al. (2016)

not understood, or unexamined.[66] A case study draws attention to the question of what can be specifically learnt about a single case.[67] It is designed to shed light on why a decision or set of decisions were taken, how they were implemented and with what result.[68]

This paper seeks to identify what constitutes a transfer of data from the EU to a third country, the application of SCCs to such transfers, the degree of implementation since the passing of the amended SCCs, and the legal consequences of non-compliance. It especially focuses on cloud storage services, a field rife with personal data transfers across various servers located in multiple locations and jurisdictions. The case studies shall focus on Amazon Web Services ("AWS"), Microsoft Azure("Microsoft") and Oracle Austria ("Oracle"). The case studies conducted take on an in-depth examination of the three Companies' cloud storage services, i.e., the parties involved, the type of data collected and transferred, the destination of the transfers, and the legal mechanisms employed to protect the data transferred. This analysis seeks to shed light on the practical elements of a personal data transfer in a bid to illustrate the mechanisms of the GDPR. It shall also seek to unearth how the Companies have implemented SCCs into their data transfer operations, establish any gaps in the implementation then conclude with a legal opinion on the consequences of non-compliance, if any.

Stake et al., (2005) draws attention to different types of case studies:

> *Intrinsic case study*- a case study undertaken because, first and last, one wants better understanding of this particular case. It is not undertaken primarily because the case represents other cases or because it illustrates a particular trait or problem, but instead because, in all its particularity and ordinariness, the case itself is of interest. The researcher at least temporarily subordinates other curiosities so that the stories of those "living the case" will be teased out. The purpose is not theory building—though at other times the researcher may do just that. Study is taken because of an intrinsic interest in for example, a particular child, clinic, conference, or curriculum.
>
> *Instrumental case study*- a study of a particular case mainly to provide insight into an issue or redraw a generalisation. The case is of secondary interest, it plays a supportive role, and it facilitates our understanding of something else. The case is still looked at in depth, its contexts

[66] Slaughter, M. J., & McCormick, D. H. (2021, June). *Data Is Power. Washington Needs to Craft New Rules for the Digital Age*. FOREIGN AFFAIRS. Retrieved March 4, 2022, from https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age

[67] Stake, R. E., Denzin, N. K., & Lincoln, Y. S. (2005). The SAGE Handbook of Qualitative Research. In *THE SAGE HANDBOOK OF QUALITATIVE RESEARCH* (THIRD EDITION, p. 443). SAGE Publications.

[68] (Schramm, 1971 cited in Yin,7 p. 13) note 7

scrutinized, and its ordinary activities detailed, but all because this helps in pursuing the external interest. The case may be seen as typical of other cases or not. Here the choice of case is made to advance understanding of that other interest.

Multiple/collective case study- where there is even less interest in one particular case, a number of cases may be studied jointly in order to investigate a phenomenon, population, or general condition. It is instrumental case study extended to several case studies. Individual cases in the collection may or may not be known in advance to manifest some common characteristic. They may be similar or dissimilar, with redundancy and variety each important. They are chosen because it is believed that understanding them will lead to a better understanding, and perhaps better theorizing, about a still larger collection of cases.[69]

[69] Pg. 445-449

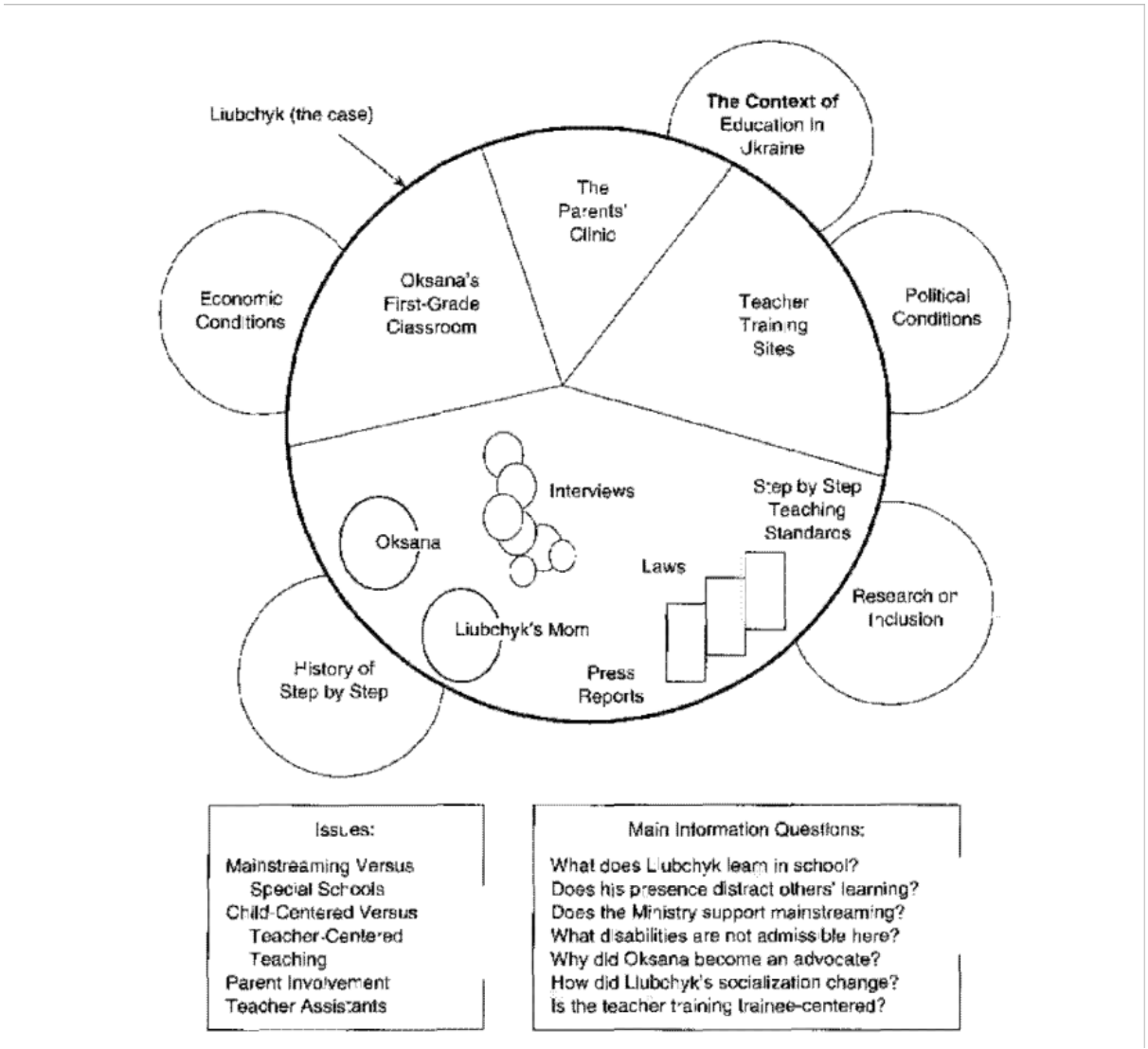


Figure 2 Multiple case study: Plan for the Ukraine case study
Source: Stake et al., (2005, pg.446)

Going by the above descriptions, this research adopts the instrumental case study. While the transfer of data by the three cloud companies in question is looked at in depth, it merely facilitates the role of a practical illustration of the GDPR requirements on the same and eventually shed light on the current state of implementation of the modernized SCCs as a tool of safeguarding the data transferred.

4.2. Cloud Computing: How personal data is transferred to third countries in cloud computing

The aim of this section is to get a practical understanding of a transfer of personal data to third countries and assess the implementation process of standard contractual clauses in such transfers. This study shall focus on the transfer of personal data in cloud computing services, and in particular

storage services. The fluidity of data transfer in cloud computing blurs the element of data location, as the data can be bounced off numerous servers in different locations. Nonetheless, the territorial requirements of the GDPR are clear, and if a controller or processor data transfers were to fall under the realm of Article 3 GDPR, then the transfers must be GDPR compliant.

To illustrate the mechanics of data transfers by cloud companies, this research shall analyse the contents of the privacy policies of the three Companies (also referred to in numerous texts as privacy notice). As they contain detailed descriptions of how these Companies manage and secure their transfers. The case studies shall focus on the three companies mentioned above: Azure, Microsoft´s Cloud Platform ("Microsoft"), Amazon Web Services ("AWS") and Oracle Austria ("Oracle"). The choice of companies is informed by verified peer reviews and ratings conducted by Gantner on the most preferred cloud infrastructure and platform services providers in the world in the last 12 months (from June 2022).[70] In this survey, Amazon´s AWS received 2,791 ratings with 55% rating it at 5 stars. Microsoft Azure came second with 1,763 ratings and 42% 5-star ratings. In third place was Oracle Cloud Infrastructure by Oracle with 135 ratings and 46% 5-star ratings. In Europe, Middle East and Africa, the Companies come in at first, second and fourth places respectively.

4.2.1. Background

The starting point of this discussion is an introduction to cloud computing. Eurostat Statistics Explained (2021) defines cloud computing as:

> …[a]model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Azure (2022) adopts a simpler definition:

> Cloud computing is the delivery of computing services— including servers, storage databases, networking, software, analytics, and intelligence—over the internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

The cost of maintaining an internal information technology infrastructure quick enough to keep up with the speed of business on the one hand, and the era of digital age on the other has ushered in and popularised the use of cloud computing services that provide databases, software, and

[70] Gartner Peer Insights. (2022). *Cloud Infrastructure and Platform Services Reviews and Ratings*. Retrieved February 15, 2019, from https://www.gartner.com/reviews/market/public-cloud-iaas

equipment which are then accessible by companies via the internet. By allowing on-demand access to a shared pool of configurable computing resources, a client only pays for the services without incurring the cost of buying and maintaining the IT infrastructure. The primary benefits of cloud computing include cost savings (pay-as-you-go pricing model allowing customers to acquire only the computing resources they require), scalability (customer-specific processing capacity); and elasticity (rapid response to changes in computing demand).[71] By moving away from traditional on-premises IT infrastructure, cloud computing has vastly improved business efficiency while gradually proving to be the preferred mode of data storage. It is currently estimated that by 2021, 41% of companies in the EU used cloud computing. Of this percentage, 79% used a cloud solution to host their email systems and 66% for storing files. More than half, 59%, used cloud services for security software applications while 61% for used it for office software such as word processing and spreadsheets. [72]

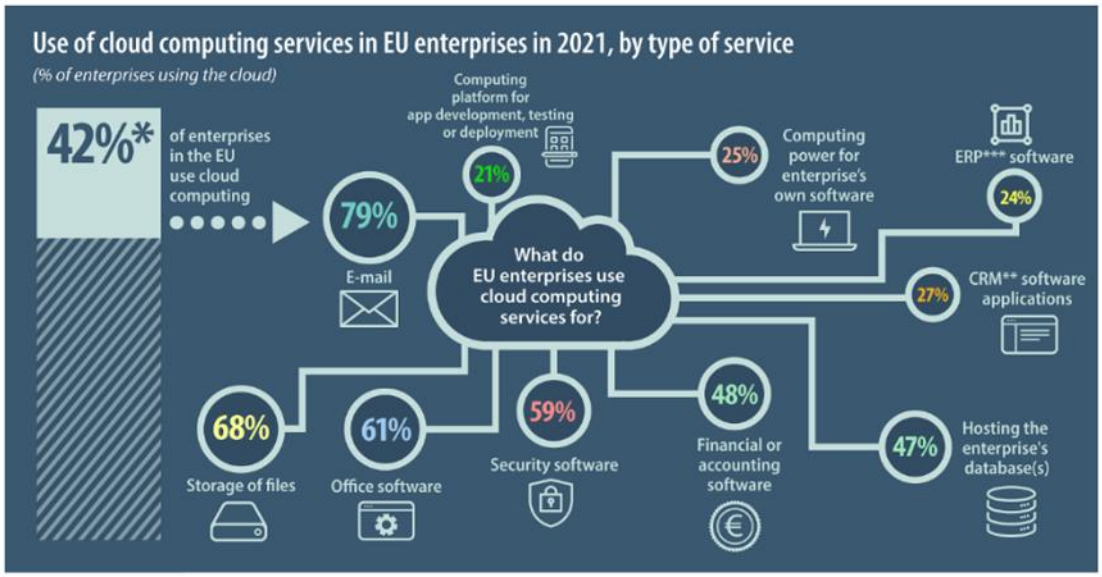


Figure 3: Use of cloud services in EU Enterprises in 2021, by type of service
Source dataset: isoc cicce use

4.2.2. Types of cloud services

Most cloud computing services fall into three broad categories: Infrastructure-as-a-Service ("IaaS"), Platforms-as-a-Service ("PaaS") and Software-as-a-Service ("Saas"). IaaS is the most basic category of computing services that allows clients to rent IT infrastructure (servers and virtual

[71] *13 Key Cloud Computing Benefits for Your Business*. (2018, July 5). GlobalDots. Retrieved December 12, 2021, from https://www.globaldots.com/resources/blog/cloud-computing-benefits-7-key-advantages-for-your-business/
[72] Eurostat. (2021, December 9). *Cloud computing used by 42% of enterprises*. Retrieved March 11, 2022, from https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211209-2

machines, storage, networks, and operating systems) from a cloud provider on a pay-as-you-go basis.[73] PaaS provides customers with the hardware, software, and infrastructure for developing, running, and managing applications without building and maintaining the required infrastructure. SaaS delivers cloud-based applications such as email and office tools over the internet and users access the applications usually with a web browser on the PC, phone, or tablet. providers host and manage the software application and underlying infrastructure, and handle any maintenance, like software upgrades and security patching.

Going into the intricate details of the three categories of cloud services is beyond the scope of this research. This study shall instead focus on the fluidity of data transfer offered under IaaS— storage, backup, and recovery.

With the fluidity of data flow facilitated by cloud services is the elevated concern for privacy, especially because data transcends borders. Cloud providers often use infrastructures spread across multiple locations, seamlessly moving, and replicating data between their servers to take advantage of lightly loaded serves in different time zones, the availability of cheap power (especially fluctuating renewable resources) and to improve performance and resilience.[74]

This fluidity forms the basis of this research. With data stored across multiple locations by cloud companies[75], what safeguards have they employed to protect personal data of EU users and what is the level of their implementation of the said safeguards?

4.2.3. Privacy Policies

The requirements of drafting a privacy policy

As aforementioned, this research shall collect its data from analysing AWS, Microsoft Azure, and Oracle privacy policies.

The GDPR lays out the requirements of drafting one and this outline shall be later used to assess the privacy policies under analysis in this paper.

Most companies outline how they will handle any client, customer, or employee data in their privacy policies. A privacy policy is a public page on a company´s website available to site visitors and the first stop at acquainting oneself with the company´s privacy practices of a company. Even though

[73] Azure (2022)
[74] IBM. (2021, July 14). *Paas (Platform-as-a-Service)*. IBM Cloud. Retrieved May 7, 2022, from https://www.ibm.com/cloud/learn/paas
[75] In this case AWS, Microsoft Azure and Oracle, the companies under review in this research.

the GDPR does not explicitly refer to privacy policies, it does under Articles 12, 13, and 14 lay out guidelines for drafting of one.

To begin with, a privacy policy should be in writing and where appropriate, available electronically. At the request of the data subject, it can also be provided orally after the data subject sufficiently proves its identity[76] to ensure comprehension and to aid the visually impaired. As for the contents of a privacy policy Article 12 GDPR states as follows:

> The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

In essence, the hallmarks of privacy policies are that their information should be:

- concise
- transparent
- intelligible
- easily accessible
- written in a clear plain language that can be easily understood by a child

This way, data subjects can hold controllers and processors accountable over their personal data and can exercise their rights.

The Article 29 Data Protection Working Party (WP 29) published Guidelines that provide practical guidance and interpretive assistance on the above obligations as a requirement for privacy policies under the GDPR. The requirements are explained as follows:

- [8] [c]oncise and transparent manner means that data controllers should present the information/communication effectively and succinctly to avoid information fatigue. …In an online context, the use of a privacy statement/notice will enable a data subject to navigate to the particular section of the privacy statement/notice which they want to

[76] Article 12 GDPR

immediately access rather than have to scroll through large amounts of text searching for particular issues.

- [9] [i]ntelligible means that it should be understood by an average member of the intended audience. Intelligibility is closely linked to the requirement to use clear and plain language.
- [10] [t]ransparency… the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. …[c]ontrollers should also separately spell out in unambiguous language what the most important consequences of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/notice have on a data subject?
- [11] [e]asily accessible means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question.

In addition, these Guidelines suggests that privacy policy language should not use qualifiers such as "may," "might," "some," and "often" because they are intended to be vague. The drafting should also use active voice with sentences and paragraphs being well organized with bullet points to emphasize important details. They should also avoid using overly legalistic or technical language.[77]

As for the contents of a privacy policy, Articles 13 and 14 GDPR differentiate between the requirements of a privacy policy when personal data are collected from the data subject and when personal data are not collected from the data subject respectively. Article 13 states that when personal data are collected from a data subject, the data subject should be provided with the following information:

- The identity and contact details of the controller, and where applicable, its representative and Data Protection Officer
- The purposes of the processing for which it collects personal data and the legal basis
- The legitimate interests of the controller or third party
- The recipients or categories of personal data

[77] *Article 29 Working Party Guidelines on transparency under Regulation 2016/679* (WP260 rev.01). (2018, April). ec.europa.eu. https://ec.europa.eu/newsroom/article29/redirection/document/51025

- The intention to transfer the data to a third country and the safeguards taken
- The period or criteria used to determine the period the personal data will be stored
- The data subject´s access to, rectification or erasure of personal data, or restriction of or objection to processing
- Right to withdraw consent
- Right to lodge a complaint with a supervisory authority
- Whether the collection of personal data is pursuant to a statutory or contractual requirement or obligation and whether the data subject is obligated to provide personal data and the consequences of failing to provide the data
- The existence of automated decision-making and profiling, the logic involved and the consequences of such processing for the data subject.

Where the personal data have not been obtained from the data subject, Article 14 requires the controller to provide similar information as listed above except for:

- Whether the collection of personal data is pursuant to a statutory or contractual requirement or obligation and whether the data subject is obligated to provide personal data and the consequences of failing to provide the data

The controller must additionally include the categories of personal data obtained.

In both instances, the controller should ensure to provide the information:

- Within reasonable time but in the span of one month after obtaining the personal data
- Latest at the time of first communication with the data subject is the personal data was collected for communication
- Latest at the time when the personal data is first disclosed if the data was meant to be disclosed.

4.3. Data collection

Transfer of data in cloud computing services

Following the theoretical outline of the requirements of a transfer of data to third countries in Section 3, this case study shall embark on practical illustrations of the same by the cloud computing companies.

Dates of the last update of the privacy policies

AWS Privacy Notice	https://aws.amazon.com/privacy/	Last updated: June 3, 2022
Microsoft Privacy Statement	https://privacy.microsoft.com/en-us/privacystatement	Last updated: June 2022
Oracle Austria Legal Notice	https://www.oracle.com/at/legal/privacy/	Last updated: 2022

Table 2: Privacy Policies dates of last updates

The section kicks off the discussion by establishing elements that constitute a transfer of data to third countries by interrogating four questions: what constitutes a data transfer; what type of data is protected by the GDPR; what constitutes a transfer of data to a third country; and what are the requirements for data transfer to a third country. These questions are then answered by an in-depth analysis of the GDPR and other supporting legislation and literature.

Similarly, this case study shall study the practical elements of a transfer of data to third countries using the same questions.

i) What constitutes a data transfer?

- The transfer of data

Subject to Article 4(2) of the GDPR, any collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use and disclosure by transmission, dissemination or otherwise making available, alignment, or combination, restriction, erasure, or destruction of personal data by an organisation amounts to an act on personal data controlled by the GDPR. Thus, when an enterprise collects or records personal data[78] then uploads it to a cloud platform owned by another enterprise for storage, it makes the said data available by disclosure to the cloud company, and thus considered to be a data transfer. But to determine whether it's a cross-border transfer of data to a third country, consideration must be made on the transfer chain and eventual destination of the cloud servers.

The AWS, Microsoft Azure, and Oracle´s privacy policies do not explicitly differentiate between personal data they personally collect (data they have control over making them controllers) and that received from clients as part of their cloud storage services (making them processors).

[78] Personal data within the meaning of Article 4(1) of the GDPR which states that 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.

Even so, the Amazon Privacy Statement under the clause—*Location of Personal Information*— states that its clients´ personal information may be stored in or accessed from multiple countries where its affiliated countries are located, including its headquarters in the US. It however accords special treatment to EU customer data, whereby an EU client can choose to store its customer data in any one or more of AWS European regions, and this data is guaranteed to stay in the selected regions[79].

On the Microsoft Privacy Statement on *Reasons we share personal data* Microsoft Azure acknowledges sharing of data among Microsoft-controlled affiliates and subsidiaries or with vendors or agents working on its behalf. Instances when personal data can be shared include transfer of personal data to companies hired by Microsoft, to support or assist in protecting and securing its systems, and thus the data may be shared to perform such functions. In addition, Microsoft may also disclose personal data in the event of a merger or sale of assets.

On storage and processing of personal data, Microsoft states that personal data it collects may be stored and processed in a client´s region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries or service providers operate facilities[80]. The primary storage location is the client´s region or the United States, often with a back up to a data centre in another region. Personal data from the EEA, the United Kingdom and Switzerland is transferred to other countries.

Oracle discloses in its privacy policy under the Section—*Disclosure of Personal Data*— that data stored in its systems may be shared worldwide through its global organisation. Additionally, it may share information with third parties, including:

- Third party service providers such as IT service providers, legal counsel, and auditors to enable the service providers to perform business functions on behalf of Oracle.
- Relevant third parties in upon a reorganization, merger, sale, joint venture, assignment, transfer, or other disposal of all or any portion of its business, assets, or stock, including in connection with any bankruptcy or other process.
- In compliance to a legal obligation, for security reasons and for law enforcement purposes, when Oracle in good faith believes that disclosure is necessary to protect its rights, protect its client´s safety or the safety of others, investigate fraud, or respond to government

[79] The data can be transferred in instances where the transfer is an essential part of the service, or when the transfer is necessary to develop and improve those services.
[80] Microsoft maintains major data centers in Australia, Austria, Brazil, Canada, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom, and the United States

requests, including state and government agencies outside the client´s country of residence, for national security reasons and/or law enforcement purposes.

The transfer of data to servers located in different jurisdictions or to third parties as illustrated above shows the volatility of cross border transfers in cloud storage. Not only is data regularly transferred to different locations but can also reside in multiple locations at the same time. With cloud computing, the relation of data to a geographical location is blurred and even when a cloud company commits to only storing data in a certain location, sometimes the need to beat latency may arise or after a technical or physical event, and the company resorts to moving data to servers in a different jurisdiction for ease of access by its clients. Despite this, physical location is a decisive factor when determining the applicability of the GDPR.

Having illustrated instances of data transfer in the three cloud companies under review, the next issue for consideration is parties involved for the transaction to qualify as a transfer of personal data.

- Parties that can transfer data

Paragraph 3.2 of this paper points out that a transfer is also dependent on the parties involved in the moving of the data. To qualify as a transfer the data flow must be between a **controller** (a *natural or legal person* who *determines alone or jointly with others*, the *purposes and means of processing personal data*)[81] and a **processor** (*natural or legal person*, *public authority*, *agency*, or *other body* that *processes data on behalf of the controller*)[82]. Both parties should not be the data subjects. Under Guidelines 07/2020, a controller exercises control over the purposes and means of data collection whereas a processor acts on the instructions of a controller. Thus, in cloud storage services, the client who contracts cloud companies for data storage is the controller, whereas the cloud services company is the processor.

AWS privacy statement makes no mention of the parties to its cloud services agreement. On the other hand, Microsoft Azure under its *Enterprise Online Services* clause[83] states that it is the processor of personal data and its client the controller. Similarly, Oracle in the description of its data processing terms states that its client is the data controller and Oracle the data processor. In its role as processor, Oracle guarantees to process personal data in accordance with the standard contract for services and any other additional instructions by the client. It further commits to hold its external

[81] Article 4(7) GDPR
[82] Article 4(8) GDPR
[83] Enterprise and Developer Products are Microsoft products and related software offered to and designed primarily for use by organizations and developers.

sub-contractors who are given access to personal data to the same level of data protection and security as Oracle.

This paper finds the assignment of the titles ´controller´ and ´processor´ by Microsoft and Oracle in line with the description accorded by clause 2.1 above.

The next section will illustrate the type of data collected by the three companies that is considered as personal data in the GDPR.

ii) what type of data is protected under the GDPR?

As previously mentioned, the GDPR applies to personal data, which is any piece of information relating to an identifiable natural person. Article 4(1) GDPR lists this data to include; name, an identification number, location data, an online identifier or one or more factors referring to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person.

The following is a list of data collected by the cloud companies in question.

AWS

AWS classifies the personal information it collects into three categories:

- **Information the client gives**. This includes information a client provides when the client searches for, subscribes to or purchases AWS products; creates an AWS account; configures computer settings to grant access permissions to AWS offerings; purchases or uses content, products or services from third-party providers through the AWS marketplace; offers its content, product or services on or through AWS offerings or AWS marketplace; communicates with AWS by phone, email or using any other means; posts on AWS website, subscribes for notifications; completes questionnaire or any other request forms.
- **Automatic information**. AWS automatically collects information from its clients when the client interacts with AWS (visit the site, interact with, or use AWS products), downloads AWS content, opens AWS emails or links or communicates with AWS.
- **Information from other sources**. AWS also collects personal information from third parties in marketing; after sales generation and recruitment information; search results and links including paid listings, and credit history from credit bureaus.

Personal information collected in the above three scenarios include:

- Name, email address, physical address, phone number and other similar contact information.
- Payment information, including credit card and bank account information.
- Location address.
- Information on the client´s organisation and its contacts, such as colleagues and people within the organisation.
- Usernames, aliases, roles and other authentication and security credential information.
- Content of feedback, testimonials, inquiries, support tickets, and any phone conversations, chat sessions, and emails with or to the company.
- The client´s image (still, video or 3D), voice and other identifiers personal to a client when they attend an AWS event or use certain AWS Offerings.
- Identity, including government-issued identification information.
- Corporate and financial information; and
- VAT numbers and other tax identifiers.

Microsoft Azure

Unlike AWS, Microsoft does not have a separate data privacy policy for its software products and its cloud services. It instead redirects its cloud users to the *Enterprise and developer products* subsection under the Microsoft Privacy Statement for an account of how it processes personal data. In a similar fashion to AWS, Microsoft does not distinguish between personal data collected from its customers from that it receives for storage under its cloud services. Nevertheless, the privacy statement details instances when Microsoft collects personal data as: when a client directly interacts with Microsoft and when Microsoft collects data about its clients' interactions, use and experiences with the company´s products.

Personal data collected depends on the privacy settings a client opts for when interacting with Microsoft. However, the company warns that many of the products and features offered require some personal data to which the products and features will not function without. Similarly, when a client enters a contract with Microsoft but declines to submit personal data, Microsoft will decline to enter the said contract or terminate an existing one.

Personal data collected includes:

- Name and contact data: First and last name, email address, mailing address, phone number and any other contact information.
- Credentials: Passwords and password hints, and any other security information used to access the account.
- Demographic data: data on age, gender, and preferred language.
- Payment data: data related to payment information such as credit card number and the card security number.
- Subscription and licencing data: the client´s subscriptions and licences.
- Interactions: data about how the client interacts with Microsoft products including browser history and location data.
- Content: Entails content of files and communications a client uploads, receives, creates, and controls. Additionally, Microsoft also collects files a client stores, retrieves or processes with its cloud services.
- Video or recordings: Microsoft may process images or voice data of clients who attend activities and events at Microsoft buildings, retail spaces and other locations.
- Feedback and ratings when a client reviews or rates Microsoft products.
- Traffic data: Data generated from a client´s use of Microsoft´s communication services.

Oracle

On the Oracle Austria website, Oracle details its privacy terms under its Legal Notice, *Privacy at Oracle*. The Legal Notice is subdivided into six Privacy Policies, all addressing the collection, use, disclosure, and processing of personal information by the various Oracle business units. The privacy policies listed are:

- The **Oracle General Privacy Policy**- applies to information collected in connection to the client´s use of Oracle´s website and mobile applications, and social media pages that link to the General Privacy Policy, and client´s interaction with Oracle, including offline sales and marketing activities.
- The **Services Policy**- details Oracle´s privacy practices and security practices in place for handling i) personal information in connection with Services offered to provide consulting, technical support, cloud, and other services on behalf of its clients, and ii) personal information in system operational data generated by the interaction of end users.

- Oracle´s **Recruitment Privacy Policy**- contains information that Oracle may collect in its online and offline activities.
- The **Oracle Data Cloud Privacy Policy**- addresses the collection and use of marketing and internet-based information to provide interest-based advertising to Oracle Marketing Cloud and Oracle Data Cloud clients.
- The **AddThis Privacy Policy**- contains information about the collection, use, and disclosure of personal information in connection with Oracle´s provision of the AddThis tools and toolbar.
- The **Dyn Internet Performance Tools Privacy Policy**- documents Oracle's collection, use, disclosure, and processing of personal information in conjunction with Dyn's recursive DNS service, updater client, Gauge web browser extension, and RUM beacons.

Of relevance to this study is the Oracle Services Privacy Policy that describes the privacy practices and safeguards that Oracle employs when handling personal information while providing technical support, consulting, cloud, and other services (the “Services”).

Oracle describes personal information as personally identifiable information the client provides that is stored in Oracle servers, customers, or third-party systems and environments that is processed by Oracle to provide the client service. Depending on the service, personal information collected may include:

- Family lifestyle and social information.
- Employment details.
- Financial details.
- Online identifiers such as IP addresses.
- Online behavioural and interest-related information about the client.
- Personal information on the client´s Agents and End-users such as employees, applicants, contractors, colleagues, partners, suppliers, and customers.

It is without doubt that the personal information collected by the three companies falls under the realm of the data protected under the GDPR[84]. Even though all three companies do not explicitly classify the data collected for storage under cloud services as part of the personal data they collect, a run through their cloud services offerings reveals that they do indeed offer cloud storage services

[84] Refer to section 3 above

for clients wishing to outsource storage services. This paper thereby shall proceed to consider their cloud services as avenues for collection of personal data.

In the instances personal data is transferred by an enterprise to a cloud services company, or to different servers in different locations, when is a cross border transfer of data considered to be a transfer to a third county?

iii) What constitutes a transfer of data to a third country?

As previously discussed, three scenarios of data transfer qualify a transfer to be regarded as one to a third country; a transfer whereby: the controller or processor is in the EU or is subject to the GDPR; data subjects are in the EU; or processing of data is by a controller not in the EU but in a location where Member State Law applies by virtue of public international law[85]. Another criterion for establishing whether a transfer is made to a third country is when a controller or processor (´exporter´) discloses by transmission or other means to another controller or processor (´importer´) and this importer is in a third country, regardless of whether this importer is subject to the GDPR or not[86].

AWS under the—*Location of Personal Information*— clause states that Amazon Web Services Incorporation is in the USA and has 84 Availability Zones within 26 geographic zones around the world[87]. it further adds that a client´s personal information may be stored in or accessed from numerous locations, including the USA. It however points out that personal information transfer is conducted in accordance with the AWS Privacy Policy and applicable data protection laws. It also accords special treatment to EU customer data, paying attention to the requirements of data transfer under the GDPR. In addition, a client can choose to store its customer data in any one or more of AWS European regions, and this data is guaranteed to stay in the selected regions.

In a similar fashion, Microsoft Azure maintains a complex set of data centres, the 'Azure Region', designed to offer protection against localized disasters. It makes available zones where data is transferred to offer protection from regional or large geography disasters with disaster recovery by

[85] Article 3 GDPR

[86] *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*. https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en

[87] AWS. (2022). *Why Cloud Infrastructure Matters*. Retrieved May 15, 2022, from https://aws.amazon.com/about-aws/global-infrastructure/#:~:text=AWS%20Global%20Infrastructure%20Map,United%20Arab%20Emirates%20(UAE).

making use of another region.[88] At present, Azure has 4 regions located globally. Below is an illustration of the data availability system set up by Azure.

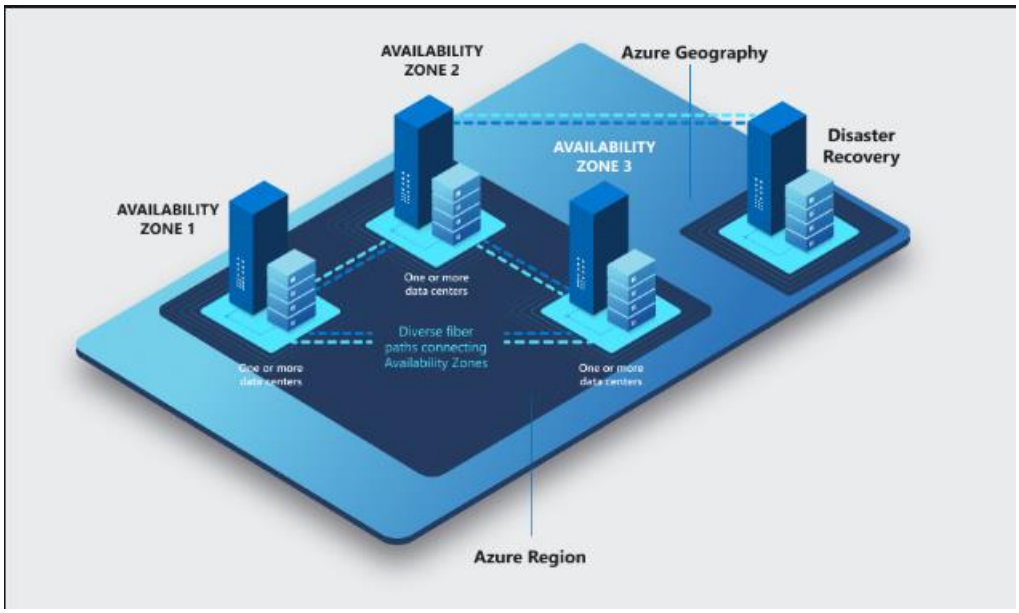


Figure 4 Azure cross-region replication
Source: Microsoft

Americas	Europe	Africa	Asia Pacific
Brazil South	France Central	South Africa North	Australia East
Canada Central	Germany West Central		Central India
Central US	North Europe		Japan East
East US	Norway East		Korea Central
East US 2	UK South		Southeast Asia
South Central US	West Europe		East Asia
US Gov Virginia	Sweden Central		China North 3
West US 2	Switzerland North		
West US 3			

Table 3: Azure regions that support availability zones
Source: Microsoft

[88] Microsoft Azure. (2022, June 22). *Regions and availability zones*. Retrieved June 30, 2022, from https://docs.microsoft.com/en-us/azure/availability-zones/az-overview#regions

As regards Oracle, Clause 7 of its Privacy Policy —*Cross-Border Data Transfers*— states that Oracle may process, transfer, and retain personal information worldwide as necessary to provide its services. Oracle also acknowledges to disclose personal information contained in its systems worldwide throughout its global organization.

In all three instances, this case study illustrates a transfer of data from clients seeking cloud storage services to the cloud companies, and from the cloud companies' different servers located in different jurisdictions. If for instance, both parties, the client and the cloud service provider are in the EU, then the third-country data transfer requirement is not fulfilled. However, the very element of cloud storage cannot be restrained by geographical location. As is illustrated by Azure Data region image above, the intricate system is designed to ensure disaster recovery by transferring data across one or multiple Azure regions, helping its clients access their data regardless of the disaster. This would result to a spider web network of data transfers in the EU and to countries not governed by the GDPR. In addition, the three Companies may on occasion grant access to sub-processors to help them in performing their duties as processors. If in case the sub-processors are located outside the EU/EEA region, that would amount to a transfer of data to a third country.

Having satisfied the three elements of a transfer of data to third countries, this case study shall proceed to identify conditions under which the companies in question validate their transfers.

- **Requirements of a transfer of data to a third country**

A transfer of data subject to the GDPR[89] to a third country shall only be valid if it is conducted in accordance with Sections 44-50 of the GDPR.

AWS, Microsoft Azure, and Oracle briefly mention the data protection mechanisms they employ while conducting cross-border transfers to third countries. Earlier, this research highlighted that the privacy policies only briefly mention the data protection mechanisms they employ, and that detailed information would probably be addressed in Cloud Service Contracts. Nonetheless, the privacy policies are a good start to catch a glimpse of the mechanisms these companies use transfer data to third countries.

AWS in *Location of Personal Information* section states that whenever it transfers personal information to other jurisdictions, it ensures that the transfer is in accordance with its privacy notice

[89] Refer to Chapter 3 of this paper on the description of such transfers

and as permitted by data protection laws. However, the policy makes no mention of a specific method of data protection mechanism it uses when transferring data from EEA to a third country.

Microsoft, in *Security of personal data* clause states that it protects the personal data collected according to its privacy policy and the requirements of applicable law. As regards transfer of personal data from the European Economic Area to other countries which may not have been determined by the European Commission to have an adequate level of protection, Microsoft acknowledges to use a variety of legal mechanisms including contracts such as the standard contractual clauses published by the European Commission under Commission Implementing Decision 2021/914.

In a similar approach, Oracle subjects its cross-border transfers of personal data originating from the EEA to countries outside the EEA (that are not considered to have adequate level of data protection) to appropriate transmission mechanisms which offer an adequate level of protection in accordance with applicable data protection laws such as EU standard contractual clauses.

While Microsoft and Oracle rely on SCC´s for their transfers of personal data to third countries, their privacy policies do not describe in length their choice of safeguards to transfer of personal data. For this reason, this case study extends its research to service contracts provided by the three companies in their websites for a detailed overview of their approach on transfer of data to third countries.

- **AWS GDPR Data Processing Addendum**[90]

The AWS Data Processing Addendum ("AWS DPA") supplements the AWS Customer Agreement and any other agreement that governs AWS and a customer using AWS service offerings when that use of services includes processing personal information governed by the GDPR. It specifically caters to data processing of customer data uploaded to the services under the customer´s AWS accounts and may include data on customer´s customers, employees, suppliers, and End Users.

Clause 12 —*Transfer of Personal Data*— of the AWS DPA states as follows:

12.1 Regions.

> Customer can specify the location(s) where Customer Data will be processed within the AWS Network (each a "Region"), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as

[90] Annex 1

necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.

12.2 Application of Standard Contractual Clauses.

Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a "Data Transfer").

12.2.1 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

12.2.2 When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS will know the identity of Customer's controllers because AWS has no direct relationship with Customer's controllers and therefore, Customer will fulfil AWS's obligations to Customer's controllers under the Processor-to-Processor Clauses.

12.3 Alternative Transfer Mechanism.

The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for lawful Data Transfers.

- **Microsoft Products and Services Data Protection Addendum ("Microsoft DPA")[91]**

The Microsoft DPA governs any services agreement between Microsoft and its customers with regards to processing and security of customer data, professional services data, and personal data.[92] It additionally includes Attachment 1— *The 2010 Standard Contractual Clauses (Processors)*— that regulate the transfer of personal data to processors in third countries which do not ensure an adequate level of data protection. This Attachment is in addition to Microsoft's execution of the 2021 Standard Contractual Clauses.

To the extent that Microsoft processes personal data as processor or sub-processor subject to the GDPR, Attachment 2 —*European Union General Data Protection Terms*— governs the processing.

[91] Annex 2
[92] *Microsoft Products and Services Data Protection Addendum (DPA)*. (2021). Microsoft. Retrieved June 15, 2022, from https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2021

The Attachment then proceeds to adapt references from the Directive 95/46/EC as the relevant and appropriate Articles in the GDPR.

- **Data Processing Agreement for Oracle Services**[93]

Oracle details its data processing terms in its Data Processing Agreement ("Oracle DPA") for Oracle Services[94]. This DPA incorporates a European DPA Addendum which stipulates additional data processing terms for processing personal data originating from and subject to EU/EEA, UK, and Swiss data protection law.

Clause 5 of Oracle´s Data Processing Agreement ("Oracle DPA") *Cross-border transfers* states as follows:

> 5.1 Without prejudice to any applicable regional data centre restrictions for hosted Services specified in Your Services Agreement, Oracle may Process Personal Information globally as necessary to perform the Services.
>
> 5.2 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable Data Protection Law, such transfers shall be subject to (i) for transfers to Oracle Affiliates, the terms of the Oracle Intra-Company Data Transfer and Mandate Agreement, which requires all transfers of Personal Information to be made in compliance with Applicable Data Protection Law and all applicable Oracle security and data privacy policies and standards globally; and (ii) for transfers to Third Party Subprocessors, security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law.

4.4. Results

The purpose of this section is to present the findings of the case studies. Within the framework of the examined privacy policies, the three companies have demonstrated to have operations in the EU with Amazon providing for AWS GDPR Processing Addendum, Microsoft including Attachment 2—*European Union General Data Protection Regulation Terms*— to its Products and Services Data Protection Addendum and Oracle providing Oracle.com Österreich and Oracle.com de websites

[93] Annex 3
[94] *Data Processing Agreement for Oracle Services*. (2019, June 26). Oracle. Retrieved June 15, 2022, from https://www.oracle.com/pl/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

that cater to its operations in Austria and Germany. The three companies also indicate to rely on standard contractual clauses as a means of protection personal data in the event of a transfer to third countries. Nevertheless, an entity wishing to utilize SCCs must meet certain requirements for the SCCs to be considered as validly implemented. These requirements are laid out in Section 3.1. For this reason, this section shall, in addition to analysing whether the three companies adhere to the requirements of validly implementing SCCs, also interrogate the extent they have fully operationalised the clauses.

The results shall focus on three findings:

a) Whether the Companies as data exporters have fulfilled their general responsibilities under Chapter IV (Articles 24-36) GDPR.
b) Whether they have correctly incorporated SCCs to their commercial agreements
c) Whether they have conducted a Transfer Impact Assessment in adopting SCCs as their appropriate tool of safeguarding their transfers of data.

4.5. Findings

i) Inadequate description of the technical and organisational measures

The three Companies, even though they somewhat address the technical and organisational measures they undertake to demonstrate measures they take to ensure security and confidentiality of personal information under their custody, do so very briefly and in general terms.

AWS in describing its organisational and technical measures to secure personal data in its Privacy Policy Section *How We Secure Information* vaguely refers to its security measures as “maintaining a wide variety of compliance systems, use of encryption protocols and software to protect information during transmission and maintenance of physical, electronic and procedural safeguards in the collection, storage and disclosure of personal information”. While it includes a hyperlink that directs its users to the AWS compliance programmes, it neither describes the type of encryption protocols and the software used to protect data during transmission, nor does it provide further details or even direct its customers to a site that addresses these measures. It only attempts to describe the security control measures it takes on data processing which includes supporting an information security program (including the adoption and enforcement of internal policies and procedures to help its customer secure data against loss, disclosure, etc).

Section 4.2.3 above suggests that privacy policy information should be easily accessible, and parties should not have to seek out information. A search through the AWS website and privacy

documents did not reveal any further information on software and encryption protocols, which contradicts the requirement for an easily accessible information on a privacy policy. While it is not necessary to include all data security protocols AWS employs, it would be ideal if the Company inserted a hyperlink directing website users to pages that lay out further details on the same. In addition, the information can also be included in annexes attached to its DPA, and clear information about this highlighted in the privacy policy.

Microsoft on the other hand does not address security measures in its Privacy Policy. Instead, one must resort to its DPA. Earp et al (2005) defines a privacy policy as a description of an organisation´s practices on data collection, use, and disclosure. Through privacy policies, an organisation not only protects itself but also signals integrity and commitment to site users.[95] By leaving out crucial information such as how it addresses security measures, Microsoft not only contravenes the requirements of transparency and accountability in a privacy statement but also signifies little or no commitment to informing its site users on its security measures.

Nonetheless, it addresses the issue in its DPA in the Section —*Data Security*—, under the clauses *Security Practices and Policies, Data Encryption, Data Access*, and *Auditing Compliance*. Additionally, it includes Appendix A that further details its Security Measures. However, in a similar case to AWS, it merely gives a general description of most of its security measures. For example, on *Communication and Operations Management: Operation Policy* it states: "Microsoft maintains security documents describing its security measures…" and no further mention of the said measures is made. Microsoft then goes further to state that the policy will be made available to its customer, along with other information reasonably requested by customer regarding Microsoft security practices and policies. This begs the question of what amounts to a "reasonable" request, and when can a request be accepted or denied. Microsoft does not disclose this criterion.

Oracle under Clause 4—*Security and Confidentiality*— in its Privacy Policy states that its technical and organizational measures designed to protect customer´s personal information conform to the ISO/IEC 27001:2013 standard. ISO/IEC 27000 is a series of international standards that govern all areas of security including physical access, system access, data access, transmission, entry, security monitoring and enforcement.[96] ISO/ICE 27001:2013 specifies the requirements for

[95] Earp, J. B., Anton, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet Privacy Policies Within the Context of User Privacy Values. *IEEE Transactions on Engineering Management*, *52*(2), 227–237. https://doi.org/10.1109/TEM.2005.844927

[96] *ISO/ICE 27000:2018 Information technology- Security techniques- Information security management systems- Overview and vocabulary*. (2018, February). ISO. Retrieved July 1, 2022, from https://www.iso.org/standard/73906.html

establishing, implementing, maintaining, and continually improving an information security management system within the context of the organisation.[97] However a search through the ISO website for these standards reveals that they are not freely accessible but have to be purchased. Oracle on its part does not describe the ISO standards it refers to, but merely refers to them as the guide for its data security measures. Similarly, Microsoft also acknowledges to align its security measures to the requirements set out in ISO 27001, ISO 27002, and ISO 27018. These standards are also only accessible through purchase. It then includes a hyperlink that directs its users to contracts and policies it uses detailing specific security measures for its services. For further details on the security measures, Oracle redirects its users to security practices available at http://www.oracle.com/us/corporate/contracts/cloud-services/index.html. On clicking this link, it opens to a page listing standard contracts and policies that govern the terms, service descriptions and delivers of cloud services, thereby stacking the information under a large list of documents.

It is imperative that the Companies are transparent to their clients on the security measures employed. This way, the controller would have the means of ascertaining that it has contracted a processor who has provided sufficient measures to implement technical and organisational measures to protect data processing and empower the data subject to hold the controller and processor accountable for the processing of its data. When providing further details on these measures, the companies could leave out confidential information or business secrets.

Failure to sufficiently address technical and organisational measures in privacy policies would also hinder a potential controller from sufficiently ascertaining itself on the measures a potential controller has taken. The SCCs require a data exporter to fulfil its responsibilities as controller or processor under Chapter IV GDPR. Article 28(1) in turn requires a controller to only use a processor who provides sufficient technical and organisational guarantees to ensure a processing is conducted in accordance to the GDPR. However, the lack of information by the companies would hinder potential customers to perform due diligence before concluding a cloud services processing contract with the three cloud companies. Article 28 GDPR requires controllers to only use processors who provide sufficient guarantees to implement appropriate technical and organisational measures that meet requirements of the GDPR in a said processing. This requirement calls upon a processor to ascertain the measures a controller uses before entering into a controller-processor agreement.

[97] *ISO/IEC 27001:2013 Information technology- Security techniques- Information security management systems-Requirements*. (2013, October). ISO. Retrieved July 1, 2022, from https://www.iso.org/standard/54534.html

However, the lack of transparency on the security measures the three Companies use would hinder a potential controller from discovering whether the security measures are sufficient to meet the requirements of GDPR for processing. AWS under Section 10 of its DPA—*AWS Certifications and Audits: AWS ISO-Certification and SOC Reports*— pledges, upon customer´s request and provided it has an NDA with the customer to provide the customer with its ISO certifications and its System Organization Controls documentation that describe the controls implemented by AMS. AWS may also provide its customer with a copy of its audit report that details Amazon´s compliance with its obligations.

Microsoft on its part states that it will detail its technical and organisational measures adopted to protect customer data, professional services data and personal data in a Microsoft Security Policy which may be availed to the customer upon a reasonable request.

In both cases, the Companies agree to provide their customer with appropriate documents detailing their security practices, but their definition of customer is an entity that is a signatory of their services agreements. In essence, a potential customer has limited means of verifying the security measures employed by the three companies, and it is only after you are party to the data processing contract that you can ascertain whether the processor (in this case Microsoft and AWS) have implemented sufficient guarantees to implement appropriate technical and organisational measures that meet requirements of the GDPR. It then is possible that customers might enter into contracts with the companies and only realise the insufficiency of security measures in the course of an agreement.

ii) Incorrect application of SCCs

The Modernized SCCs combine four modules that are tailored to various transfer scenarios, with generic terms that apply in all circumstances. To incorporate SCCs into a commercial contract, the SCCs should be applied by filling in the annexes and specifying which modules, options, and specifications they have chosen[98] for their circumstances to match their SCC requirements to their role and responsibilities regarding the data processing in question.

AWS in its DPA Section 12—*Transfers of Personal Data*— states that SCCs will apply to customer data that is transferred directly via onward transfer to any third country. When its customer is acting as the controller the Controller-to-Processor Clauses will apply to a Data Transfer. However, since

[98] THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS (2022, Paragraph 10)

it is unlikely AWS knows the identity of its customer´s controllers as AWS does not have a direct relationship with its customer´s controllers, its customer will fulfil AWS´s obligations to customer´s controllers under the Processor-to-Processor clauses.

Under section 17—*Definitions*— AWS defines "Controller-to-Processor Clauses" as the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 20217914 of 4 June 2021, and currently located at https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf and "Processor-to-Processor Clauses" as the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/915 of 4 June 2021, and currently located at https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf.

Microsoft in its DPA under —*Data Transfers and Location: Data Transfers Section*—states that all transfers of Customer, Data, Professional Services Data, and Personal Data out of the EU or EEA shall be governed by the 2021 Standard Contractual Clauses Implemented by Microsoft. It then commits to abide by the requirements of the EEA regarding the processing of personal data and to subject all transfers of personal data to third countries to appropriate safeguards as described in Article 46 GDPR and thereafter document such transfers according to Article 30(2) GDPR.

Oracle in its DPA under Clause 5— Cross-border transfers— states that cross border transfers shall be subject to (i) for transfers to Oracle Affiliates, the terms of the Oracle Intra-Company Data Transfer and Mandate Agreement, which requires all transfers of Personal Information to be made in compliance with Applicable Data Protection Law and all applicable Oracle security and data privacy policies and standards globally; and (ii) for transfers to Third Party Subprocessors, security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law. It does not explicitly mention which method of data protection for third country transfers it employs, but merely refers to a list of agreements and policies that it adheres to.

AWS is the only company that succinctly describes the Article 46 GDPR transfer tool it employs in its third country data transfers, in this case SCCs and then goes ahead to insert a hyperlink that leads to the clauses. The clauses further state that the annexes are attached to and form part of the AWS GDPR Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf, or other agreement between Customer and AWS governing the processing of Customer Data. Even so, in providing clients with a copy of the SCCs used for the transfer of their personal data, general reference to the SCCs, for example by providing a link to the

Clauses is not sufficient but should instead be a copy of the clauses used in the larger contract for transfer of data.[99]

To enforce SCCs, parties are required to fill in the annexes to the SCCs and sign Annex 1, which forms an integral part of the clauses.[100] As regards fulfilling this requirement, this research finds AWS to be the only company compliant with Article 44 GDPR.

iii) Failure to conduct a Transfer Impact Assessment

In implementing the transfer tools under Article V GDPR, the CJEU in Schrems II requires controllers or processors, acting as exporters to verify on a case-by-case basis in collaboration with the importer in the third country if the law or practice of the third country affects the efficacy of the appropriate safeguards under Article 46 GDPR.[101] The EDPB adopted guidelines that assist controllers and processors assess third countries and determine the appropriate safeguards where necessary. Under the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[102], the EDPB breaks down the recommendations in steps:

- Step 1- **Know your transfers.** A data exporter is required to map out all its transfers by maintaining a record of its processing activities in line with Article 30 GDPR. This record should also include onward transfers. Pursuant to the principle of "data minimisation", the exporter must verify that the data it transfers is adequate, relevant, and limited to what is necessary for the purposes of the transfer.[103]
- Step 2- **Identify the transfer tools you are relying on**. Identify the best suited transfer tool under Article V GDPR.[104]
- Step 3- **Assess the effectiveness of your Article 46 transfer tool against your transfer**. If you choose an Article 46 transfer tool, assess whether it is sufficient for the transfer you are conducting. The Article 46 appropriate safeguard tool should be accompanied with

[99] THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS (2022, Paragraph 32)

[100] THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS (2022, Paragraph 6)
[101]THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS (2022)
[102] *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. (2020, November). EDPB. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
[103] *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. (2020, November, Paragraph 11)
[104] *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. (2020, November, Paragraph 14)

enforceable data subject rights and effective legal remedies.[105] You must determine whether any law or practice of the third country could affect the effectiveness Article 46 GDPR transfer tool you are relying on. When necessary, your data importer should provide you with relevant laws and sources governing the transfer of the nation it Is located.

- Step 4- **Adopt supplementary measures**. Identify and adopt supplementary measures if your research in step 3 reveals that the third country legislation affects the effectiveness of the Article 46 transfer tool. These supplementary measures are meant to bring the level of protection at a similar standard as that in the EU. EDPB recommendations also note that the supplementary measures adopted may be effective in one country and non-effective. In the event the parties find that the supplementary measure is not suitable, they must avoid, suspend or terminate the transfer to avoid compromising the level of protection of the personal data.
- Step 5- **Adopt procedural steps after identifying the relevant supplementary measures**. Adopting procedural steps after identifying effective supplementary measures. After identifying the appropriate supplementary measures to be implemented, you should then follow the procedural guidelines to implementing them. If, for instance, the data exporter has chosen to rely on SCCs, it needs not request authorisation from the supervisory authority on to incorporate these clauses, or additional safeguards, as long as these measures do not contradict with the SCCs. In case the parties have an additional services agreement, its provisions should not contradict the SCCs. If the supplementary measures adopted modify or contradict the SCCs, the parties will not be deemed to be using SCCs and must seek authorisation with the competent supervisory authority.
- Step 6- **Re-evaluate at appropriate intervals**. Re-evaluate the level of protection accorded to the data transferred and monitor any changes in the third country that may affect this protection.

Aside from presenting controllers and processors with a guideline that assists them map out their transfers while ensuring the level of protection envisioned in the GDPR for transferred personal data, the above Recommendations also serves to illustrate that there is no one size fits all method of data transfer. What might work for one transfer may not necessarily be appropriate for another, and with changing legislative frameworks in third countries, constant surveillance must be maintained to ensure the transfer tool remains applicable and that the supplementary measures still afford data subjects their fundamental rights to data protection. These Recommendations call for

[105] Article 46 GDPR

commitment to protecting personal data, commitment that AWS, Microsoft, and Oracle do not illustrate in their Privacy Policies and Data Processing Agreements.

AWS under section 12 of its DPA states that the SCCs will only apply to customer data that is transferred either directly or indirectly to any third country. In addition, the SCCs will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for processors or an alternative recognized compliance standards for lawful data transfers.

Under the Clause *Data Transfers and Location—Data Transfers—* of Microsoft´s DPA, it states that all transfers of Customer Data, Professional Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland shall be governed by the 2021 Standard Contractual Clauses implemented by Microsoft. The Clause goes on to add that Personal Data to a third country or an international organisation will be subject to appropriate safeguards as described in Article 46 of the GDPR.

Oracle under Section 5—*Cross-border data transfers*— subjects its Oracle Affiliate transfers to the terms of the Oracle Intra-company Data Transfer and Mandate Agreement which requires all transfers to comply to applicable data protection laws and all applicable data privacy policies and standards globally; and for transfers to third party processors to security and data requirements consistent with the Oracle Data Processing Agreement and applicable Data Protection Law.

The three Companies do not refer to any mechanism to determine the applicable data transfer tool they will use depending on the country of destination. In addition, in the case of use of SCCs, none of the three Companies mentions continued surveillance in the legislative field of third countries to ensure that the SCCs plus supplementary measures employed still guarantee data subjects their rights to data protection. In the long run, the Companies might be in contravention of Article 32(1) GDDPR which requires the controller and processor to ensure confidentiality, integrity and resilience of processing systems and services.

- Additional findings

iv) Poorly drafted Privacy Policies

Section 4.2.3 of this paper goes into length over the requirements of a privacy policy under the GDPR for a company operating in the EU. It specifically lays emphasis on the need for a privacy policy to contain information that is concise, transparent, intelligible, easily accessible and written in

a clear plain language. It should be such that a data subject can navigate through it with ease, transparent in describing security measures undertaken by the company, and easily accessible.

To begin with, the three Privacy Policies reviewed fail the transparency test. AWS only provides a link describing its compliance systems but fails to detail the encryption protocols and software it uses to protect data during transmission, as well as in the collection, storage, and disclosure of personal information. Azure on the other hand completely leaves out any details of security of data mechanisms in its Privacy Policy. It hence defeats the purpose of a privacy policy when a customer or data subject must conduct an additional search (in this case the Microsoft DPA) to get acquainted with the data protection mechanisms the Company employs. The three Companies also fail the accessibility test, because in all three cases, and for the purposes of this paper, this research had to resort to their DPAs to discover further information on security mechanisms employed by the three that is not available in the Privacy Policies. In line with the requirement for accessibility, the Companies should also have provided the measures they refer to as safeguards or provided a link. In the case of ISO certifications, it would have been sufficient to attach the certifications but conceal any confidential information therein.

Legal Implications

i) Infringement of the right to data protection

Article 8 of the Charter of Fundamental Rights of the European Union[106] guarantees everyone the right to the protection of personal data. It is on this foundation that the GDPR lays down rules for the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data.[107] Technology has aided the rapid movement of data across borders, and it is often that data originating from the EU will find its way into territories with lesser protection mechanisms than that governing the EU. While this is commonplace, the GDPR is in place to ensure that the same protection personal data enjoys within the borders of the EU is the same or almost of a similar standard when it is transferred to third countries. For this reason, entities engaged in collection and storage of data or any other kind of processing, and its eventual transfer ought to view data beyond a modern age business component but also as an essential part of individuals that should be strictly guarded.

[106] (2000/C 364/01)
[107] Article 1 GDPR

This paper has emphasised the importance of a privacy policy; that it is a declaration of a company´s commitment on its security practices. A data processing services agreement further spells out the duties and responsibilities that accrue to the signatory parties. The gaps in implementation and generality of terms as illustrated above not only shows a lack of commitment to data protection but also a non-willingness to protect the most crucial information of entrusted to them and a continuous breach of data protection laws. Even when the privacy policies did not address an issue important to this research, it resorted to the data processing agreements, and as has been illustrated, most often the gap is not resolved. The failure to aptly address issues can be construed not only as non-compliance to the GDPR but also as violation of the fundamental right of data protection.

ii) Erroneous application of Chapter V GDPR Transfer Tools.

According to the findings of this research, it is prudent that a data exporter conducts an analysis of its data transfer to determine the most appropriate tool of data transfer. As has been illustrated, the three Companies make no mention of such an analysis but merely mention the Tool of Transfer, without giving reasons as to why it's the most appropriate tool. If these Companies were to apply a blanket one-size-fits-all approach to transfer of data to third countries, then chances are high that in some cases, the wrong approach might be used, thereby defeating the purpose of Chapter V GDPR. In addition, the lack of mention of continued surveillance on third country legislation illustrates a lack of commitment to keep up to date with the changing legislative and business environment and in no time, these Companies may eventually transfer data to a third country by not only using a wrong transfer tool but also conduct an illegal transfer.

iii) Failure to discharge controller/processor duties

A controller that continues to use the services of a processor that does not fulfil its duties not only puts its clients´ data at risk but also is in violation of its controller duties as well. As has been pointed out in the findings above, when a processor conceals or makes it difficult for a controller to ascertain the former´s security measures in place to protect transfers, the controller not only fails to discharge its respective exporter rights but also their duties towards their clients.

iv) Legal suits for non-compliance

It goes without saying that this repeated non-compliance of data protection rules by companies will soon lead to massive suits against companies by clients for breach of their responsibilities. The Austrian Data Protection Authority found Google Analytics to be in violation of the GDPR in the wake

of Schrems II decision[108]. Similarly, a successful suit against a company not found to be complaint with the GDPR might cause a domino effect of similar suits against companies.

[108] *Austrian DSB: Use of Google Analytics violates "Schrems II" decision by CJEU.* (2022, January 13). Noyb. Retrieved July 8, 2022, from https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal

5. Limitations and Future Research

Even though this research has presented an analysis of privacy policies to demonstrate the current state of implementation of the modernised SCCs, it is no way a reflection of the overall current state of implementation in Austria. While this research focussed on three international companies with operations in Austria, a further study on local Austrian companies is required for a better analysis.

In addition, even though privacy policies and data processing agreements are a great source of information, it would also be helpful to include interview relevant stakeholders in companies for their input on the implementation procedures followed in their Companies that might not be captured in their websites. Unfortunately, this would only re-emphasise the outlying theme of this research which is lack of transparency on their public sites. Interviews nonetheless would unearth the challenges faced by companies in implementation of the GDPR.

6. Conclusion

The need for companies to discharge their rights and responsibilities for data protection transcends merely attempting to be compliant with relevant rules and regulations but also signifies their commitment to the safety of their customer. In the wake of digital hacks and data leaks, this responsibility only grows much higher.

To be compliant with data protection rules, and particularly the GDPR calls for much more than an acknowledgment or passive compliance, and data exporters must design their operations to adopt an active and continuous approach to data protection.

In addition, companies must also keep up with surveillance of the legal and business field because as the technology changes, so do the data protection needs, and what might work today might be obsolete tomorrow.

References

13 Key Cloud Computing Benefits for Your Business. (2018, July 5). GlobalDots. Retrieved December 12, 2021, from https://www.globaldots.com/resources/blog/cloud-computing-benefits-7-key-advantages-for-your-business/

Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A., & Fahreen, Z. (2019). Qualitative v/s Quantitative Research. *Journal of Evidence Based Medicine and Healthcare*, *6*(23), 2828–2832. https://doi.org/10.18410/jebmh/2019/587

Article 29 Working Party Guidelines on transparency under Regulation 2016/679 (WP260 rev.01). (2018, April). ec.europa.eu. https://ec.europa.eu/newsroom/article29/redirection/document/51025

Austrian DSB: Use of Google Analytics violates "Schrems II" decision by CJEU. (2022, January 13). Noyb. Retrieved July 8, 2022, from https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal

AWS. (2022). *Why Cloud Infrastructure Matters*. Retrieved May 15, 2022, from https://aws.amazon.com/about-aws/global-infrastructure/#:~:text=AWS%20Global%20Infrastructure%20Map,United%20Arab%20Emirates%20(UAE).

Azure. (2022). *What is cloud computing?* Retrieved May 5, 2022, from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-cloud-computing/#benefits

Bradford, L., Abboy, M., & Lidell, K. (2021). Standard contractual clauses for cross-border transfers of health data after Schrems II. *Journal of Law and the Biosciences*, *8*(1). https://doi.org/10.1093/jlb/lsab007

Brown, B. (2021, November 3). Why Source Data Is The New Currency For Retailers. *Forbes*. Retrieved November 24, 2021, from

https://www.forbes.com/sites/forbestechcouncil/2021/11/03/why-source-data-is-the-new-currency-for-retailers/

Data Privacy Office. (n.d.). *Organization of cross-border data transfer according to GDPR*. https://data-privacy-office.com/en/oformlenie-transgranichnoj-peredachi-dannyh-po-gdpr-chast-1/#f1

Data Processing Agreement for Oracle Services. (2019, June 26). Oracle. Retrieved June 15, 2022, from https://www.oracle.com/pl/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

Dumont, D., & Treacy, B. (2021, August 25). *European Commission's International Data Transfer Standard Contractual Clauses: What Businesses Need to Know*. Thompson Reuters. Retrieved January 12, 2022, from https://www.huntonak.com/images/content/7/8/v2/78022/eu-commissions-intl-data-transfer-standard-contractual-clauses.pdf

Earp, J. B., Anton, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet Privacy Policies Within the Context of User Privacy Values. *IEEE Transactions on Engineering Management*, *52*(2), 227–237. https://doi.org/10.1109/TEM.2005.844927

EU: Third-party beneficiary rights under revised SCCs. (2021, July). OneTrust Data Guidance. Retrieved February 12, 2022, from https://www.dataguidance.com/opinion/eu-third-party-beneficiary-rights-under-revised-sccs

EUR-LEX. (2021). Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union, L:2021:199:TOC*. http://data.europa.eu/eli/dec_impl/2021/914/oj

Eurostat. (2021, December 9). *Cloud computing used by 42% of enterprises*. Retrieved March 11, 2022, from https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211209-2

Eurostat Statistics Explained. (2021, January 19). *Cloud Computing*. Retrieved April 15, 2022, from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Cloud_computing

Fazlioglu, M. (2021). *IAPP-EY Annual Privacy Governance Report 2021*. https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

Gartner Peer Insights. (2022). *Cloud Infrastructure and Platform Services Reviews and Ratings*. Retrieved February 15, 2019, from https://www.gartner.com/reviews/market/public-cloud-iaas

GDPR. (n.d.). Intersoft Consulting. Retrieved May 1, 2022, from https://gdpr-info.eu/issues/personal-data/

Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.0). (2021, July). European Data Protection Board. https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

Hoffman, D. A. (2017, January). *DATA TRANSFERS TO THIRD COUNTRIES* (Policy Brief No. 2017–25). Centrum für Europaische Politik. https://www.cep.eu/fileadmin/user_upload/cep.eu/Analysen/COM_2017_7_Datenuebermittlung/cepPolicyBrief_COM_2017__7_Data_Transfers_to_Third_Countries.pdf

IBM. (2021, July 14). *Paas (Platform-as-a-Service)*. IBM Cloud. Retrieved May 7, 2022, from https://www.ibm.com/cloud/learn/paas

intersoft consulting. (n.d.). *General Data Protection Regulation*. https://gdpr-info.eu/

ISO/ICE 27000:2018 Information technology- Security techniques- Information security management systems- Overview and vocabulary. (2018, February). ISO. Retrieved July 1, 2022, from https://www.iso.org/standard/73906.html

ISO/IEC 27001:2013 Information technology- Security techniques- Information security management systems- Requirements. (2013, October). ISO. Retrieved July 1, 2022, from https://www.iso.org/standard/54534.html

Kershner, M. (2021, June 15). *Data Isn't The New Oil — Time Is*. Forbes. Retrieved December 12, 2021, from https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/

Lee S.K, J. (1992). Quantitative versus qualitative research methods — Two approaches to organisation studies. *Asia Pacific Journal of Management*, *9*, 87–94. https://doi.org/10.1007/BF01732039

Microsoft Azure. (2022, June 22). *Regions and availability zones*. Retrieved June 30, 2022, from https://docs.microsoft.com/en-us/azure/availability-zones/az-overview#regions

Microsoft Products and Services Data Protection Addendum (DPA). (2021). Microsoft. Retrieved June 15, 2022, from https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?year=2021

Mine, H., & Dahl, C. B. (2021, July). *The value of cross-border data flows to Europe: Risks and opportunities*. Frontier Economics. Retrieved April 4, 2022, from https://www.digitaleurope.org/wp/wp-content/uploads/2021/06/Frontier-DIGITALEUROPE_The-value-of-cross-border-data-flows-to-Europe_Risks-and-opportunities.pdf

THE NEW STANDARD CONTRACTUAL CLAUSES – QUESTIONS AND ANSWERS. (2022, May). European Commission. https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf

Owens, J. (2019, December 25). The tech giants dominated the decade. But there's still time to rein them in. *The Guardian*. Retrieved November 21, 2021, from https://www.theguardian.com/commentisfree/2019/dec/25/2010s-tech-giants-google-amazon-facebook-regulators

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. (2020, November). EDPB. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Saunders, M., Lewis, P., & Thornhill, A. (2016). *RESEARCH METHODS FOR BUSINESS STUDENTS* (Seventh edition). Pearson.

Slaughter, M. J., & McCormick, D. H. (2021, June). *Data Is Power. Washington Needs to Craft New Rules for the Digital Age*. FOREIGN AFFAIRS. Retrieved March 4, 2022, from https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age

Stake, R. E., Denzin, N. K., & Lincoln, Y. S. (2005). The SAGE Handbook of Qualitative Research. In *THE SAGE HANDBOOK OF QUALITATIVE RESEARCH* (THIRD EDITION, p. 443). SAGE Publications.

Standard Contractual Clauses (SCC). (2021, June 4). European Commission. Retrieved April 6, 2021, from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Travers, M. (2001). *Qualitative Research through Case Studies* (FIRST EDITION). Sage Publishing. https://uk.sagepub.com/en-gb/eur/qualitative-research-through-case-studies/book210591#:~:text=Qualitative%20Research%20through%20Case%20Studies%20will%20help%20students%20improve%20the,approaches%20such%20as%20critical%20discourse

Treacy, B., & Kurth, H. A. (2021, June 24). *Updated SCCs for international data transfers: fir for the future*. Thompson Reuters Practical Law. Retrieved May 2, 2022, from https://uk.practicallaw.thomsonreuters.com/w-031-4820?transitionType=Default&contextData=(sc.Default)&firstPage=true

Yin, R. K. (2014). Case Study Research Design and Methods. *Canadian Journal of Program Evaluation*, *5th ed*. https://doi.org/10.3138/cjpe.30.1.108

Appendixes

Appendix 1: AWS GDPR Data Processing Addendum

Appendix 2: Microsoft Products and Services Data Protection Addendum

Appendix 3: Data Processing Agreement for Oracle Services

Appendix 1: AWS GDPR Data Processing Addendum

AWS GDPR DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the AWS Customer Agreement available at http://aws.amazon.com/agreement, as updated from time to time between Customer and AWS, or other agreement between Customer and AWS governing Customer's use of the Service Offerings (the "**Agreement**") when the GDPR applies to your use of the AWS Services to process Customer Data. This DPA is an agreement between you and the entity you represent ("**Customer**", "**you**" or "**your**") and Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties (as applicable) under the Agreement (together "**AWS**"). Unless otherwise defined in this DPA or in the Agreement, all capitalised terms used in this DPA will have the meanings given to them in Section 17 of this DPA.

1. Data Processing.

1.1 **Scope and Roles.** This DPA applies when Customer Data is processed by AWS. In this context, AWS will act as processor to Customer, who can act either as controller or processor of Customer Data.

1.2 **Customer Controls.** Customer can use the Service Controls to assist it with its obligations under the GDPR, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if AWS becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. AWS will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.

1.3 **Details of Data Processing.**

1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer Data.

1.3.2 **Duration.** As between AWS and Customer, the duration of the data processing under this DPA is determined by Customer.

1.3.3 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

1.3.4 **Nature of the processing.** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.

1.3.5 **Type of Customer Data.** Customer Data uploaded to the Services under Customer's AWS accounts.

1.3.6 **Categories of data subjects.** The data subjects could include Customer's customers, employees, suppliers and End Users.

1.4 **Compliance with Laws**. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2. **Customer Instructions.** The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the AWS management console and APIs made available by AWS for the Services) constitute Customer's documented instructions regarding AWS's processing of Customer Data ("**Documented Instructions**"). AWS will process Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between AWS and Customer, including agreement on any additional fees payable by Customer to AWS for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if AWS declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the processing, Customer agrees that it is unlikely AWS can form an opinion on whether Documented Instructions infringe the GDPR. If AWS forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

3. **Confidentiality of Customer Data.** AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.

4. **Confidentiality Obligations of AWS Personnel.** AWS restricts its personnel from processing Customer Data without authorisation by AWS as described in the AWS Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. **Security of Data Processing**

5.1 AWS has implemented and will maintain the technical and organisational measures for the AWS Network as described in the AWS Security Standards and this Section. In particular, AWS has implemented and will maintain the following technical and organisational measures:

(a) security of the AWS Network as set out in Section 1.1 of the AWS Security Standards;

(b) physical security of the facilities as set out in Section 1.2 of the AWS Security Standards;

(c) measures to control access rights for AWS employees and contractors to the AWS Network as set out in Section 1.1 of the AWS Security Standards; and

(d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by AWS as described in Section 2 of the AWS Security Standards.

5.2 Customer can elect to implement technical and organisational measures to protect Customer Data. Such technical and organisational measures include the following which

can be obtained by Customer from AWS as described in the Documentation, or directly from a third party supplier:

(a) pseudonymisation and encryption to ensure an appropriate level of security;

(b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer; measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

(c) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by Customer.

6. Sub-processing.

6.1 **Authorised Sub-processors.** Customer provides general authorisation to AWS's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The AWS website (currently posted at https://aws.amazon.com/compliance/sub-processors/) lists Sub-processors that are currently engaged by AWS. At least 30 days before AWS engages a Sub-processor, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which AWS has engaged the Sub-processor; or (iii) move the relevant Customer Data to another AWS Region where AWS has not engaged the Sub-processor.

6.2 **Sub-processor Obligations.** Where AWS authorises a Sub-processor as described in Section 6.1:

(i) AWS will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Customer Data for any other purpose;

(ii) AWS will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by AWS under this DPA, AWS will impose on the Sub-processor the same contractual obligations that AWS has under this DPA; and

(iii) AWS will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause AWS to breach any of AWS's obligations under this DPA.

7. AWS Assistance with Data Subject Requests. Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which AWS will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the GDPR. If a data subject makes a request to AWS, AWS will promptly forward such request to Customer once AWS has identified that the request is from a data subject for whom Customer is responsible. Customer authorises on its behalf, and on behalf of its controllers when Customer is acting as a processor, AWS to respond to any data subject who makes a request to AWS, to confirm that AWS has forwarded the request to Customer. The parties agree that Customer's use of the

Service Controls and AWS forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

8. Optional Security Features. AWS makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and

(d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorised access and measures to control access rights to Customer Data. **9. Security Incident Notification.**

9.1 **Security Incident.** AWS will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

9.2 **AWS Assistance.** To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), AWS will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the Security Incident as AWS is able to disclose to Customer, taking into account the nature of the processing, the information available to AWS, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

9.3 **Unsuccessful Security Incidents.** Customer agrees that:

(i) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorised access to Customer Data or to any of AWS's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and

(ii) AWS's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by AWS of any fault or liability of AWS with respect to the Security Incident.

9.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means AWS selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the AWS management console and secure transmission at all times.

10. AWS Certifications and Audits.

10.1 **AWS ISO-Certification and SOC Reports.** In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:

(i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and

(ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

10.2 **AWS Audits.** AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be AWS's Confidential Information.

10.3 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this DPA.

10.4 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the processing and the information available to AWS, AWS will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information AWS makes available under this Section 10.

11. Customer Audits. Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under the GDPR or the Standard Contractual Clauses, by instructing AWS to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending AWS written notice as provided for in the Agreement. If AWS declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.

12. Transfers of Personal Data.

12.1 **Regions.** Customer can specify the location(s) where Customer Data will be processed within the AWS Network (each a "**Region**"), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.

12.2 **Application of Standard Contractual Clauses.** Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a "**Data Transfer**").

12.2.1 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

12.2.2 When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS will know the identity of Customer's controllers because AWS has no direct relationship with Customer's controllers and therefore, Customer will fulfil AWS's obligations to Customer's controllers under the Processor-to-Processor Clauses.

12.3 **Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognised compliance standard for lawful Data Transfers.

13. **Termination of the DPA.** This DPA will continue in force until the termination of the Agreement (the "**Termination Date**").

14. **Return or Deletion of Customer Data**. At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Data.

15. **Duties to Inform.** Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by AWS, AWS will inform Customer without undue delay. AWS will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

16. **Entire Agreement; Conflict**. This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses.

17. **Definitions.** Unless otherwise defined in the Agreement, all capitalised terms used in this DPA will have the meanings given to them below:

"**AWS Network**" means AWS's data center facilities, servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS's control and are used to provide the Services.

"**AWS Security Standards**" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Annex 1.

"**controller**" has the meaning given to it in the GDPR.

"**Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing

Decision (EU) 2021/914 of 4 June 2021, and currently located at https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf.

"**Customer Data**" means the "personal data" (as defined in the GDPR) that is uploaded to the Services under Customer's AWS accounts.

"**EEA**" means the European Economic Area.

"**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"**processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

"**processor**" has the meaning given to it in the GDPR.

"Processor-to-Processor Clauses" means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf.

"Security Incident" means a breach of AWS's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Service Controls" means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

"Standard Contractual Clauses" means (i) the Controller-to-Processor Clauses, or (ii) the Processorto-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.

"Third Country" means a country outside the EEA not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

Annex 1 AWS Security Standards

Capitalised terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the AWS Network, and (c) minimise security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (for example, card access systems, etc.) or validation by human security personnel (for example, contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (for example, primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2. **Continued Evaluation**. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Appendix 2: Microsoft Products and Services Data Protection Addendum

Volume Licensing

Microsoft Products and Services Data Protection Addendum

Last updated September 15, 2021

Published in English on September 15, 2021. Translations will be published by Microsoft when available. These commitments are binding on Microsoft as of September 15, 2021.

Table of Contents

Introduction

The parties agree that this Microsoft Products and Services Data Protection Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data, Professional Services Data, and Personal Data in connection with the Products and Services. The DPA is incorporated by reference into the Product Terms and other Microsoft agreements. The parties also agree that, unless a separate Professional Services agreement exists, this DPA governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in Customer's volume licensing agreement, the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Professional Services Data, or Personal Data, as defined herein. For clarity, consistent with Clause 10 of the 2010 Standard Contractual Clauses in Attachment 1, when the 2010 Standard Contractual Clauses are applicable, the 2010 Standard Contractual Clauses prevail over any other term of the DPA Terms.

Microsoft makes the commitments in this DPA to all customers with volume license agreements. These commitments are binding on Microsoft with regard to Customer regardless of (1) the Product Terms that are otherwise applicable to any given Product subscription or license, or (2) any other agreement that references the Product Terms.

Applicable DPA Terms and Updates

Limits on Updates

When Customer renews or purchases a new subscription to a Product or enters into a work order for a Professional Service, the then-current DPA Terms will apply and will not change during Customer's subscription for that Product or term for that Professional Service. When Customer obtains a perpetual license to Software, the then-current DPA Terms will apply (following the same provision for determining the applicable then-current Product Terms for that Software in Customer's volume licensing) and will not change during Customer's license for that Software.

New Features, Supplements, or Related Software

Notwithstanding the foregoing limits on updates, when Microsoft introduces features, offerings, supplements or related software that are new (i.e., that were not previously included with the Products or Services), Microsoft may provide terms or make updates to the DPA that apply to Customer's use of those new features, offerings, supplements or related software. If those terms include any material adverse changes to the DPA Terms, Microsoft will provide Customer a choice to use the new features, offerings, supplements, or related software, without loss of existing functionality of a generally available Product or Professional Service. If Customer does not install or use the new features, offerings, supplements, or related software, the corresponding new terms will not apply.

Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, Microsoft may modify or terminate a Product or Professional Service in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects Microsoft to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for Microsoft to continue operating the Product or offering the Professional Service without modification, and/or (3) causes Microsoft to believe the DPA Terms or the Product or Professional Service may conflict with any such requirement or obligation.

Electronic Notices

Microsoft may provide Customer with information and notices about Products and Services electronically, including via email, through the portal for an Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

Prior Versions

The DPA Terms provide terms for Products and Services that are currently available. For earlier versions of the DPA Terms, Customer may refer to https://aka.ms/licensingdocs or contact its reseller or Microsoft Account Manager.

Table of Contents / General Terms

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the volume license agreement. The following defined terms are used in this DPA:

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data.

"Data Protection Requirements" means the GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"DPA Terms" means the terms in the DPA and any Product-specific terms in the Product Terms that specifically supplement or modify the privacy and security terms in the DPA for a specific Product (or feature of a Product). In the event of any conflict or inconsistency between the DPA and such Product-specific terms, the Product-specific terms shall prevail as to the applicable Product (or feature of that Product).

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

"Local EU/EEA Data Protection Laws" means any subordinate legislation and regulation implementing the GDPR.

"GDPR Terms" means the terms in Attachment 2, under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

"Personal Data" means any information relating to an identified or identifiable natural person. 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.

"Product" has the meaning provided in the volume license agreement. For ease of reference, "Product" includes Online Services and Software, each as defined in the volume license agreement.

"Products and Services" means Products and Professional Services. Product and Professional Service availability may vary by region and applicability of this DPA to specific Products and Professional Services is subject to the limitations in the Scope section in this DPA.

"Professional Services" means the following services: (a) Microsoft's consulting services, consisting of planning, advice, guidance, data migration, deployment and solution/software development services provided under a Microsoft Enterprise Services Work Order that incorporates this DPA by reference; and (b) technical support services provided by Microsoft that help customers identify and resolve issues affecting Products, including technical support provided as part of Microsoft Unified Support or Premier Support Services (as described in the Services Consulting and Support Description or the Description of Services, respectively), and any other technical support services. The Professional Services do not include the Products or, for purposes of the DPA, Supplemental Professional Services.

"Professional Services Data" means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from a Product) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services.

"2010 Standard Contractual Clauses" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010. The 2010 Standard Contractual Clauses are in Attachment 1.

"2021 Standard Contractual Clauses" means the standard data protection clauses (processor-to-processor module) between Microsoft Ireland Operations Limited and Microsoft Corporation for the transfer of personal data from processors in the EEA to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission in decision 2021/914/EC, dated 4 June 2021.

"Subprocessor" means other processors used by Microsoft to process Customer Data, Professional Services Data, and Personal Data, as described in Article 28 of the GDPR.

"Supplemental Professional Services" means support requests escalated from support to a Product engineering team for resolution and other consulting and support from Microsoft provided in connection with Products or a volume license agreement that are not included in the definition of Professional Services.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies.

General Terms

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its providing the Products and Services, including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer's data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Products and Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Products and Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Products and Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of Products and Services, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Data Protection Terms

This section of the DPA includes the following subsections:

- Scope
- Nature of Data Processing; Ownership
- Disclosure of Processed Data
- Processing of Personal Data; GDPR
- Data Security
- Security Incident Notification
- Data Transfers and Location
- Data Retention and Deletion
- Processor Confidentiality Commitment
- Notice and Controls on use of Subprocessors
- Educational Institutions
- CJIS Customer Agreement
- HIPAA Business Associate
- California Consumer Privacy Act (CCPA)
- Biometric Data
- Supplemental Professional Services
- How to Contact Microsoft
- Appendix A – Security Measures
- Appendix B – Data Subjects and Categories of Personal Data
- Appendix C – Additional Safeguards Addendum.

Scope

The DPA Terms apply to all Products and Services except as described in this section.

The DPA Terms will not apply to any Products specifically identified as excluded, or to the extent identified as excluded, in the Product Terms, which are governed by the privacy and security terms in the applicable Product-specific terms.

For clarity, the DPA Terms apply only to the processing of data in environments controlled by Microsoft and Microsoft's subprocessors. This includes data sent to Microsoft by Products and Services but does not include data that remains on Customer's premises or in any Customer selected third party operating environments.

For Supplemental Professional Services, Microsoft only makes the commitments in the Supplemental Professional Services section below.

Previews may employ lesser or different privacy and security measures than those typically present in the Products and Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. For Products, the following terms in this DPA do not apply to Previews: Processing of Personal Data; GDPR, Data Security, and HIPAA Business Associate. For Professional Services, offerings designated as Previews or Limited Release only meet the terms of the Supplemental Professional Services.

Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data, Professional Services Data, and Personal Data only as described and subject to the limitations provided below (a) to provide Customer the Products and Services in accordance with Customer's documented instructions, and (b) for business operations incident to providing the Products and Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data and Professional Services Data. Microsoft acquires no rights in Customer Data or Professional Services Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Products and Services

For purposes of this DPA, "to provide" a Product consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, quality, and security).

For purposes of this DPA, "to provide" Professional Services consists of:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and
- Ongoing improvement (improving delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including installing the latest updates and fixing software defects).

When providing Products and Services, Microsoft will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.

Processing for Business Operations

For purposes of this DPA, "business operations" consist of the following, each as incident to delivery of the Products and Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure of Processed Data outlined below).

When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section.

Disclosure of Processed Data

Microsoft will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Professional Services Data; (c) Personal Data; and (d) any other data processed by Microsoft in connection with the Products and Services that is Customer's confidential information under the volume license agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under the volume license agreement.

Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

Processing of Personal Data; GDPR

All Personal Data processed by Microsoft in connection with providing the Products and Services is obtained as part of either (a) Customer Data, (b) Professional Services Data, or (c) data generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed software. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Professional Services is also Professional Services Data. Pseudonymized identifiers may be included in data processed by Microsoft in connection with providing the Products and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in Attachment 2 govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Product-specific terms or this DPA. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its volume licensing agreement (including the DPA Terms and any applicable updates), along with the product documentation and Customer's use and configuration of features in the Products, are Customer's complete documented instructions to Microsoft for the processing of Personal Data, or the Professional Services documentation and Customer's use of the Professional Services. Information on use and configuration of the Products can be found at https://docs.microsoft.com/en-us/ (or a successor location) or other agreement incorporating this DPA. Any additional or alternate instructions must be agreed to according to the process for amending Customer's agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for business operations incident to providing the Products and Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use. Microsoft is accepting the added responsibilities of a data "controller" under GDPR for processing in connection with its business operations to: (a) act consistent with regulatory requirements, to the extent required under GDPR; and (b) provide increased transparency to Customers and confirm Microsoft's accountability for such processing. Microsoft employs safeguards to protect Customer Data, Professional Services Data, and Personal Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR. With respect to processing of Personal Data under this paragraph, Microsoft makes the commitments set forth in the Additional Safeguards section; for those purposes, (i) any Microsoft disclosure of Personal Data, as described in the Additional Safeguards section, that has been transferred in connection with business operations is deemed a "Relevant Disclosure" and (ii) the commitments in the Additional Safeguards section apply to such Personal Data.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled "Nature of Data Processing; Ownership" above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Products and Services pursuant to Customer's volume licensing agreement and for business operations incident to providing the Products and Services to Customer (as further described in the section of this DPA entitled "Nature of Data Processing; Ownership" above).
- **Categories of Data.** The types of Personal Data processed by Microsoft when providing the Products and Services include: (i) Personal Data that Customer elects to include in Customer Data and Professional Services Data; and (ii) those expressly identified in Article 4 of the GDPR that may be generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed software. The types of Personal Data that Customer elects to include in Customer Data and Professional Services Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix B.
- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix B.

Data Subject Rights; Assistance with Requests

Microsoft will make available to Customer, in a manner consistent with the functionality of the Products and Services and Microsoft's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Microsoft receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with the Products and Services for which Microsoft is a data processor or subprocessor, Microsoft will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Products and Services. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data, Professional Services Data, and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. A description of the security controls for these requirements is available to Customers.

Each Core Online Service also complies with the control standards and frameworks shown in the table in the Product Terms. Each Core Online Service and Professional Service implements and maintains the security measures set forth in Appendix A for the protection of Customer Data and Professional Services Data.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate ISO 27001, ISO 27002, ISO 27018 or any standard or framework in the table for Core Online Services in the Product Terms, unless it is no longer used in the industry and it is replaced with a successor (if any).

Data Encryption

Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.

Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. In the case of Online Services on which Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties.

Data Access

Microsoft employs least privilege access mechanisms to control access to Customer Data and Professional Services Data (including any Personal Data therein). Role-based access controls are employed to ensure that access to Customer Data and Professional Services Data required for service operations is for an appropriate purpose and approved with management oversight. For Core Online Services and Professional Services, Microsoft maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix A. For Core Online Services, there is no standing access by Microsoft personnel to Customer Data and any required access is for a limited time.

Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Products and Services meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Microsoft provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application).

Auditing Compliance

Microsoft will conduct audits of the security of the computers, computing environment, and physical data centers that it uses in processing Customer Data, Professional Service Data, and Personal Data, as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

To the extent Customer's audit requirements under the 2010 Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will

promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data, Professional Services Data, and Personal Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Microsoft's other customers or to Microsoft systems or facilities not involved in providing the applicable Products and Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.

If the 2010 Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the 2010 Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the 2010 Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the 2010 Standard Contractual Clauses or Data Protection Requirements. Microsoft Corporation is an intended third-party beneficiary of this section.

Security Incident Notification

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, Professional Services Data, or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to Customer by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information with Microsoft for each applicable Product and Professional Service. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft's notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Products and Services.

Data Transfers and Location

Data Transfers

Customer Data, Professional Services Data, and Personal Data that Microsoft processes on Customer's behalf may not be transferred to, or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section. Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms.

All transfers of Customer Data, Professional Services Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Products and Services shall be governed by the 2021 Standard Contractual Clauses implemented by Microsoft. In addition, transfers from the United Kingdom and Switzerland shall be governed by the 2010 Standard Contractual Clauses. In the case of any inconsistency between the 2021 Standard Contractual Clauses and the 2010 Standard Contractual Clauses, the inconsistency shall be resolved so as to provide an adequate level of data protection for the Customer Data, Professional Services Data, and Personal Data under applicable law. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail, although Microsoft does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18. Microsoft agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

Location of Customer Data at Rest

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in the Product Terms.

Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

Data Retention and Deletion

At all times during the term of Customer's subscription or the applicable Professional Services engagement, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service and Professional Services Data.

Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA to retain such data.

For Personal Data in connection with the Software and for Professional Services Data, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon Customer's request, unless authorized under this DPA to retain such data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data, Professional Services Data, or Personal Data as described in this section.

Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Customer Data, Professional Services Data, and Personal Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data, Professional Services Data, and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

Microsoft may hire Subprocessors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Microsoft of the processing of Customer Data, Professional Services Data, and Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft makes available information about Subprocessors on a Microsoft website. When engaging any Subprocessor, Microsoft will ensure via a written contract that the Subprocessor may access and use Customer Data, Professional Services Data, or Personal Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Customer Data, Professional Services Data, or Personal Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 6 months in advance of providing that Subprocessor with access to Customer Data. Additionally, Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 30 days in advance of providing that Subprocessor with access to Professional Services Data or Personal Data other than that which is contained in Customer Data. If Microsoft engages a new Subprocessor for a new Product or Professional Service that processes Customer Data, Professional Services Data, or Personal Data, Microsoft will give Customer notice prior to availability of that Product or Professional Service.

If Customer does not approve of a new Subprocessor for an Online Service or Professional Services, then Customer may terminate any subscription for the affected Online Service or the applicable Statements of Service for the applicable Professional Service, respectively, without penalty or termination fee by providing, before the end of the relevant notice period, written notice of termination. If Customer does not approve of a new Subprocessor for Software, and Customer cannot reasonably avoid use of the Subprocessor by restricting Microsoft from processing data as set forth in the documentation or this DPA, then Customer may terminate any license for the affected software product without penalty by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns. If the affected Product is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for any subscriptions or other applicable unpaid work for the terminated Products or Services from subsequent invoices to Customer or its reseller.

Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Microsoft acknowledges that for the purposes of the DPA, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data and Professional Services Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Products and Services that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data and Professional Services Data in Microsoft's possession as may be required under applicable law.

CJIS Customer Agreement

Microsoft provides certain government cloud services ("Covered Services") in accordance with the FBI Criminal Justice Information Services ("CJIS") Security Policy ("CJIS Policy"). The CJIS Policy governs the use and transmission of criminal justice information. All Microsoft CJIS Covered Services shall be governed by the terms and conditions in the CJIS Customer Agreement located here: http://aka.ms/CJISCustomerAgreement.

HIPAA Business Associate

If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data or Professional Services Data, as those terms are defined under the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations promulgated thereunder (collectively, "HIPAA"), execution of Customer's volume licensing agreement includes execution of the HIPAA Business Associate Agreement ("BAA").The full text of the BAA identifies the Online Services or Professional Services to which it applies and is available at http://aka.ms/BAA. Customer may opt out of the BAA by sending the following information to Microsoft in a written notice (under the terms of the Customer's volume licensing agreement):

- the full legal name of the Customer and any Affiliate that is opting out; and
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the opt out applies.

California Consumer Privacy Act (CCPA)

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Customer Data, Professional Services Data, and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale" exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA Terms, Product Terms, or other agreement between Microsoft and Customer.

Biometric Data

If Customer uses Products and Services to process Biometric Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to retention periods and destruction; (ii) obtaining consent from data subjects; and (iii) deleting the Biometric Data, all as appropriate and required under applicable Data Protection Requirements. Microsoft will process that Biometric Data following Customer's documented instructions (as described in the "Processor and Controller Roles and Responsibilities" section above) and protect that Biometric Data in accordance with the data security and protection terms under this DPA. For purposes of this section, "Biometric Data" will have the meaning set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements.

Supplemental Professional Services

When used in the sections listed below, the defined term "Professional Services" includes Supplemental Professional Services, and the defined term "Professional Services Data" includes data obtained for Supplemental Professional Services.

For Supplemental Professional Services, the following sections of the DPA apply in the same manner as they apply to Professional Services: "Introduction", "Compliance with Laws", "Nature of Processing; Ownership", "Disclosure of Processed Data", "Processing of Personal Data; GDPR", the first paragraph of "Security Practices and Policies", "Customer Responsibilities", "Security Incident Notification", "Data Transfer" (including the terms regarding the 2010 Standard Contractual Clauses and 2021 Standard Contractual Clauses), the third paragraph of "Data Retention and Deletion", "Processor Confidentiality Commitment", "Notice and Controls on use of Subprocessors", "HIPAA Business Associate" (to the extent applicable in the BAA), "California Consumer Privacy Act (CCPA)", "Biometric Data", "How to Contact Microsoft", "Appendix B – Data Subjects and Categories of Personal Data", and "Appendix C – Additional Safeguards Addendum".

How to Contact Microsoft

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form, located at http://go.microsoft.com/?linkid=9846224. Microsoft's mailing address is:

Microsoft Enterprise Service Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited can be reached at the following address:

Microsoft Ireland Operations, Ltd.
Attn: Data Protection
One Microsoft Place
South County Business Park
Leopardstown
Dublin 18, D18 P521, Ireland

Appendix A – Security Measures

Microsoft has implemented and will maintain for Customer Data in the Core Online Services and Professional Services Data the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership**. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. Microsoft personnel with access to Customer Data or Professional Services Data are subject to confidentiality obligations. **Risk Management Program**. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service and before processing Professional Service Data or launching the Professional Services. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory**. Microsoft maintains an inventory of all media on which Customer Data or Professional Services Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** - Microsoft classifies Customer Data and Professional Services Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and Professional Services Data and has procedures for disposing of printed materials that contain such data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data or Professional Services Data on portable devices, remotely accessing such data, or processing such data outside Microsoft's facilities.
Human Resources Security	**Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. Microsoft limits access to facilities where information systems that process Customer Data or Professional Services Data are located to identified authorized individuals. **Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data or Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain. **Protection from Disruptions**. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Microsoft uses industry standard processes to delete Customer Data and Professional Services Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data or Professional Services Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered. - Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located. - Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional Services and for Azure Government Services, which are reviewed every twelve months.

Domain	Practices
	- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data and Professional Services Data, including malicious software originating from public networks. **Data Beyond Boundaries** - Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that is transmitted over public networks. - Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities. **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data or Professional Services Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data or Professional Services Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data or Professional Services Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data and Professional Services Data when needed. - Microsoft restricts access to Customer Data and Professional Services Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data or Professional Services Data they are not authorized to access.

Domain	Practices
Information Security Incident Management	**Incident Response Process** - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data and Professional Services Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data or Professional Services Data are located. - Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.

Appendix B – Data Subjects and Categories of Personal Data

Data subjects: Data subjects include the Customer's representatives and end-users including employees, contractors, collaborators, and customers of the Customer. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by Microsoft. Microsoft acknowledges that, depending on Customer's use of the Products and Services, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of data: The personal data that is included in e-mail, documents and other data in an electronic form in the context of the Products and Services. Microsoft acknowledges that, depending on Customer's use of the Products and Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);

- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

Appendix C – Additional Safeguards Addendum

By this Additional Safeguards Addendum to the DPA (this "Addendum"), Microsoft provides additional safeguards to Customer for the processing of personal data, within the scope of the GDPR, by Microsoft on behalf of Customer and additional redress to the data subjects to whom that personal data relates.

This Addendum supplements and is made part of, but is not in variation or modification of, the DPA.

1. **Challenges to Orders**. In the event Microsoft receives an order from any third party for compelled disclosure of any personal data processed under this DPA, Microsoft shall:

   a. use every reasonable effort to redirect the third party to request data directly from Customer;

   b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and

   c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law of the European Union or applicable Member State law.

If, after the steps described in a. through c. above, Microsoft or any of its affiliates remains compelled to disclose personal data, Microsoft will disclose only the minimum amount of that data necessary to satisfy the order for compelled disclosure.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. **Indemnification of Data Subjects**. Subject to Sections 3 and 4, Microsoft shall indemnify a data subject for any material or non-material damage to the data subject caused by Microsoft's disclosure of personal data of the data subject that has been transferred in response to an order from a non-EU/EEA government body or law enforcement agency in violation of Microsoft's obligations under Chapter V of the GDPR (a "Relevant Disclosure"). Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from Microsoft or otherwise.

3. **Conditions of Indemnification**. Indemnification under Section 2 is conditional upon the data subject establishing, to Microsoft's reasonable satisfaction, that:

   a. Microsoft engaged in a Relevant Disclosure;

   b. the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and

   c. the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. though c.

Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under Section 2 if Microsoft establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

4. **Scope of Damages**. Indemnification under Section 2 is limited to material and non material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Microsoft's infringement of the GDPR.

5. **Exercise of Rights**. Rights granted to data subjects under this Addendum may be enforced by the data subject against Microsoft irrespective of any restriction in Clauses 3 or 6 of the Standard Contractual Clauses. The data subject may only bring a claim under this Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Addendum are personal to the data subject and may not be assigned.

6. **Notice of Change**. Microsoft agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the data exporter and its obligations under this Addendum, the 2010 Standard Contractual Clauses, or the 2021 Standard Contractual Clauses 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 this Addendum or the Standard Contractual Clauses, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

7. **Termination**. This Addendum shall automatically terminate if the European Commission, a competent Member State supervisory authority, or an EU or competent Member State court approves a different lawful transfer mechanism that would be applicable to the personal data in the Customer Data, Professional Services Data, or other Personal Data that is processed under the DPA (and if such mechanism applies only to some of that data, this Addendum will terminate only with respect to that data) and that does not require the additional safeguards set forth in this Addendum.

Attachment 1 – The 2010 Standard Contractual Clauses (Processors)

Execution of the volume licensing agreement by Customer includes execution of this Attachment 1, which is countersigned by Microsoft Corporation. This Attachment 1 is in addition to Microsoft's execution of the 2021 Standard Contractual Clauses. In the case of any inconsistency between this Attachment 1 and the 2021 Standard Contractual Clauses, the inconsistency shall be resolved so as to provide an adequate level of data protection for the Customer Data, Professional Services Data, and Personal Data under applicable law. In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

Beginning May 25, 2018, and thereafter, references to various Articles from the Directive 95/46/EC in the Standard Contractual Clauses below will be treated as references to the relevant and appropriate Articles in the GDPR.

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, Customer (as data exporter) and Microsoft Corporation (as data importer, whose signature appears below), each a "party," together "the parties," have agreed on the following Contractual Clauses (the "Clauses" or "Standard Contractual 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

(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;

(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;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 below 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 subprocessor 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 subprocessor 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 below;

(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 subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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

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;

(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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

(j) to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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.

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: Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing 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.

4. The data exporter shall keep a list of subprocessing 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 subprocessor 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 subprocessor 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.

Appendix 1 to the Standard Contractual Clauses

Data exporter: Customer is the data exporter. The data exporter is a user of Products or Professional Services as defined in the DPA and Product Terms.

Data importer: The data importer is MICROSOFT CORPORATION, a global producer of software and services.

Data subjects: Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter as detailed in Appendix B to the DPA.

Categories of data: The personal data transferred that is included in e-mail, documents, and other data in an electronic form in the context of the Products or Professional Services. Microsoft acknowledges that, depending on Customer's use of the Products or Professional Services, Customer may elect to include personal data from any of the categories detailed in Appendix B to the DPA.

Processing operations: The personal data transferred will be subject to the following basic processing activities:

a. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the applicable volume licensing agreement between data exporter and the Microsoft entity to which these Standard Contractual Clauses are annexed ("Microsoft"). The objective of the data processing is the performance of Products and Services.

b. Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the "Processing of Personal Data; GDPR" section of the DPA. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities in accordance with the "Security Practices and Policies" section of the DPA.

c. Customer Data and Personal Data Access. For the term designated under the applicable volume licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data and personal data, or (2) make such corrections, deletions, or blockages on its behalf.

d. Data Exporter's Instructions. For Products and Services, data importer will only act upon data exporter's instructions as conveyed by Microsoft.

e. Customer Data and Personal Data Deletion or Return. Upon expiration or termination of data exporter's use of Products or Professional Services, it may extract Customer Data and personal data and data importer will delete Customer Data and personal data, each in accordance with the DPA Terms applicable to the agreement.

Subcontractors: In accordance with the DPA, the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data and personal data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data and personal data for any other purpose.

Appendix 2 to the Standard Contractual Clauses

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

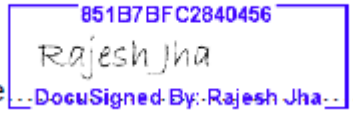
1. **Personnel**. Data importer's personnel will not process Customer Data or personal data without authorization. Personnel are obligated to maintain the confidentiality of any such Customer Data and personal data and this obligation continues even after their engagement ends.

2. **Data Privacy Contact.** The data privacy officer of the data importer can be reached at the following address:

Microsoft Corporation
Attn: Chief Privacy Officer
1 Microsoft Way
Redmond, WA 98052 USA

3. **Technical and Organization Measures.** The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data and personal data, as defined in the Security Practices and Policies section of the DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the Security Practices and Policies section of the DPA are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signing the Standard Contractual Clauses, Appendix 1, and Appendix 2 on behalf of the data importer:

Signature 

Rajesh Jha, Executive Vice President

Microsoft Corporation

One Microsoft Way, Redmond WA, USA 98052

Attachment 2 – European Union General Data Protection Regulation Terms

Microsoft makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Microsoft with regard to Customer regardless of (1) the version of the Product Terms and DPA that is otherwise applicable to any given Product subscription or license, or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer. These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Product Terms or other agreement between Microsoft and Customer. These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

Relevant GDPR Obligations: Articles 28, 32, and 33

1. Microsoft shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Microsoft shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))

2. Processing by Microsoft shall be governed by these GDPR Terms under European Union (hereafter "Union") or Member State law and are binding on Microsoft with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer's licensing agreement, including these GDPR Terms. In particular, Microsoft shall:

(a) process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Microsoft is subject; in such a case, Microsoft shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) take all measures required pursuant to Article 32 of the GDPR;

(d) respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;

(e) taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

(f) assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Microsoft;

(g) at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;

(h) make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Microsoft shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

3. Where Microsoft engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Microsoft shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))

4. 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, Customer and Microsoft shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

5. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))

6. Customer and Microsoft shall take steps to ensure that any natural person acting under the authority of Customer or Microsoft who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))

7. Microsoft shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Microsoft.

Data Processing Agreement for Oracle Services

("Data Processing Agreement")

Version June 26, 2019

1. Scope and Applicability

1.1 This Data Processing Agreement applies to Oracle's Processing of Personal Information on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. Unless otherwise expressly stated in Your Services Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of Your Services Agreement.

1.2 In addition, any Processing of Personal Information subject to Applicable European Data Protection Law is subject to the additional terms of the European DPA Addendum set out in Exhibit 1 and the Oracle Processor Code referenced therein.

2. Responsibility for Processing of Personal Information and Your instructions

2.1 You are a Controller and Oracle is a Processor for the Processing of Personal Information as part of the provision of the Services. Each party is responsible for compliance with its respective obligations under Applicable Data Protection Law.

2.2 Oracle will Process Personal Information solely for the purpose of providing the Services in accordance with the Services Agreement and this Data Processing Agreement.

2.3 In addition to Your instructions incorporated into the Services Agreement, You may provide additional instructions in writing to Oracle with regard to Processing of Personal Information in accordance with Applicable Data Protection Law. Oracle will promptly comply with all such instructions to the extent necessary for Oracle to (i) comply with its Processor obligations under Applicable Data Protection Law; or (ii) assist You to comply with Your Controller obligations under Applicable Data Protection Law relevant to Your use of the Services.

2.4 Oracle will follow Your instructions at no additional cost to You and within the timeframes reasonably necessary for You to comply with your obligations under Applicable Data Protection Law. To the extent Oracle expects to incur additional charges or fees not covered by the fees for Services payable under the Services Agreement, such as additional license or third party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to Oracle's obligation to comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees.

2.5 Unless otherwise specified in the Services Agreement, You may not provide Oracle with any sensitive or special Personal Information that imposes specific data security or data protection obligations on Oracle in addition to or different from those specified in the Data Processing Agreement or Services Agreement.

3. Privacy Inquiries and Requests from Individuals

3.1 If You receive a request or inquiry from an Individual related to Personal Information processed by Oracle for the provision of Services, You can either (i) securely access Your Services environment that holds Personal Information to address the request, or (ii) to the extent such access is not available to You, submit a "service request" via My Oracle Support (or other applicable primary support tool or support contact provided for the Services, such as Your project manager) with detailed written instructions to Oracle on how to assist You with such request.

3.2 If Oracle directly receives any requests or inquiries from Individuals that have identified You as the Controller, it will promptly pass on such requests to You without responding to the Individual. Otherwise, Oracle will advise the Individual to identify and contact the relevant controller(s).

4. Oracle Affiliates and Third Party Subprocessors

4.1 To the extent Oracle engages Third Party Subprocessors and/or Oracle Affiliates to Process Personal Information, such entities shall be subject to the same level of data protection and security as Oracle under the terms of the Services Agreement. Oracle is responsible for the performance of the Oracle Affiliates' and Third Party Subprocessors' obligations in compliance with the terms of this Data Processing Agreement and Applicable Data Protection Law.

5. Cross-border data transfers

5.1 Without prejudice to any applicable regional data center restrictions for hosted Services specified in Your Services Agreement, Oracle may Process Personal Information globally as necessary to perform the Services.

5.2 To the extent such global access involves a transfer of Personal Information subject to cross-border transfer restrictions under Applicable Data Protection Law, such transfers shall be subject to (i) for transfers to Oracle Affiliates, the terms of the Oracle Intra-Company Data Transfer and Mandate Agreement, which requires all transfers of Personal Information to be made in compliance with Applicable Data Protection Law and all applicable Oracle security and data privacy policies and standards globally; and (ii) for transfers to Third Party Subprocessors, security and data privacy requirements consistent with the relevant requirements of this Data Processing Agreement and Applicable Data Protection Law.

6. Security and Confidentiality

6.1 Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of Personal Information designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures. Additional details regarding the specific security measures that apply to the Services You have ordered are set out in the relevant security practices for these Services:

- For **Cloud Services**: Oracle's Hosting & Delivery Policies, available at http://www.oracle.com/us/corporate/contracts/cloud-services/index.html;
- For **NetSuite (NSGBU) Services**: NetSuite's Terms of Service, available at: http://www.netsuite.com/portal/resource/terms-of-service.shtml;
- For **Global Customer Support Services**: Oracle's Global Customer Support Security Practices available at: https://www.oracle.com/support/policies.html;
- For **Consulting and Advanced Customer Support (ACS) Services**: Oracle's Consulting and ACS Security Practices available at: http://www.oracle.com/us/corporate/contracts/consultingservices/index.html.

6.2 All Oracle and Oracle Affiliates employees, as well as any Third Party Subprocessors that Process Personal Information, are subject to appropriate written confidentiality arrangements, including confidentiality agreements, regular training on information protection, and compliance with Oracle policies concerning protection of confidential information.

7. Audit Rights

7.1 You may audit Oracle's compliance with its obligations under this Data Processing Agreement up to once per year. In addition, to the extent required by Applicable Data Protection Law, You or Your Regulator may perform more frequent audits.

7.2 If a third party is to conduct the audit, the third party must be mutually agreed to by You and Oracle (except if such third party is a Regulator). Oracle will not unreasonably withhold its consent to a third party auditor requested by You. The third party must execute a written confidentiality agreement acceptable to Oracle or otherwise be bound by a statutory or legal confidentiality obligation.

7.3 To request an audit, You must submit a detailed proposed audit plan to Oracle at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Oracle will review the proposed audit plan and provide You with any concerns or questions. Oracle will work cooperatively with You to agree on a final audit plan.

7.4 The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Oracle's health and safety or other relevant policies, and may not unreasonably interfere with Oracle business activities.

7.5 Upon completion of the audit, You will provide Oracle with a copy of the audit report, which is subject to the confidentiality terms of Your Services Agreement. You may use the audit reports only for the purposes of meeting Your regulatory audit requirements and/or confirming compliance with the requirements of this Data Processing Agreement.

7.6 Each party will bear its own costs in relation to the audit, unless Oracle promptly informs you upon reviewing Your audit plan that it expects to incur additional charges or fees in the performance of the audit that are not covered by the fees payable under Your Services Agreement, such as additional license or third party contractor fees. The parties will negotiate in good faith with respect to any such charges or fees.

7.7 Without prejudice to the rights granted in Section 7.1 above, if the requested audit scope is addressed in a SOC, ISO, NIST, PCI DSS, HIPAA or similar audit report issued by a qualified third party auditor within the prior twelve months and Oracle provides such report to You confirming there are no known material changes in the controls audited, You agree to accept the findings presented in the third party audit report in lieu of requesting an audit of the same controls covered by the report.

8. Incident Management and Breach Notification

8.1 Oracle has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Personal Information transmitted, stored or otherwise Processed. Oracle will promptly define escalation paths to investigate such incidents in order to confirm if a Personal Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Personal Information Breach, mitigate any possible adverse effects and prevent a recurrence.

8.2 Oracle will notify you of a confirmed Personal Information Breach without undue delay but at the latest within 24 hours. As information regarding the Personal Information Breach is collected or otherwise reasonably becomes available to Oracle, Oracle will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Personal Information Breach; (ii) the measures taken to mitigate any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of Personal Information that were the subject of the Personal Information Breach. You agree to coordinate with Oracle on the content of Your intended public statements or required notices for the affected Individuals and/or notices to the relevant Regulators regarding the Personal Information Breach.

9. Return and Deletion of Personal Information

9.1 Upon termination of the Services, Oracle will promptly return, including by providing available data retrieval functionality, or delete any remaining copies of Personal Information on Oracle systems or Services environments, except as otherwise stated in the Services Agreement.

9.2 For Personal Information held on Your systems or environments, or for Services for which no data retrieval functionality is provided by Oracle as part of the Services, You are advised to take appropriate action to back up or otherwise store separately any Personal Information while the production Services environment is still active prior to termination.

10. Legal Requirements

10.1 Oracle may be required by law to provide access to Personal Information, such as to comply with a subpoena or other legal process, or to respond to government requests, including public and government authorities for national security and/or law enforcement purposes.

10.2 Oracle will promptly inform You of requests to provide access to Personal Information, unless otherwise required by law.

11. Definitions

"**Applicable Data Protection Law**" means all data privacy or data protection laws or regulations globally that apply to the Processing of Personal Information under this Data Processing Agreement, which may include Applicable European Data Protection Law.

"**Applicable European Data Protection Law**" means (i) the EU General Data Protection Regulation EU/2016/679, as supplemented by applicable EU Member State law and as incorporated into the EEA Agreement; (ii) the Swiss Federal Act of 19 June 1992 on Data Protection, as amended; and (iii) the UK Data Protection Act 2018.

"**Europe"** means for the purposes of this Data Processing Agreement (i) the European Economic Area, consisting of the EU Member States, Iceland, Lichtenstein and Norway; (ii) Switzerland and (iii) the UK after it withdraws from the EU.

"**Individual"** shall have the same meaning as the term "data subject" or the equivalent term under Applicable Data Protection Law.

"**Process/Processing**", "**Controller**", "**Processor**" and "**Binding Corporate Rules**" (or the equivalent terms) have the meaning set forth under Applicable Data Protection Law.

"**Oracle Affiliate(s)**" means the subsidiar(y)(ies) of Oracle Corporation that may Process Personal Information as set forth in Section 4.

"**Oracle Intra-Company Data Transfer and Mandate Agreement"** means the Oracle Intra-Company Data Transfer and Mandate Agreement for Customer Services Personal Information entered into between Oracle Corporation and the Oracle Affiliates.

"**Oracle Processor Code**" means Oracle's Privacy Code for Processing Personal Information of Customer Individuals referenced in the European DPA Addendum.

"**Oracle**" means the Oracle Affiliate that has executed the Services Agreement.

"**Personal Information**" shall have the same meaning as the term "personal data", "personally identifiable information (PII)" or the equivalent term under Applicable Data Protection Law.

"**Personal Information Breach"** means a breach of security leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed

on Oracle systems or the Services environment that compromises the security, confidentiality or integrity of such Personal Information.

"**Regulator**" shall have the same meaning as the term "supervisory authority", "data protection authority" or the equivalent term under Applicable Data Protection Law.

"**Services**" or the equivalent terms "Service Offerings" or "services" means the Cloud, Advanced Customer Support, Consulting, or Global Technical Support services specified in the Services Agreement.

"**Services Agreement**" means (i) the applicable order for the Services you have purchased from Oracle; (ii) the applicable master agreement referenced in the applicable order, and (iii) the Service Specifications.

"**Third Party Subprocessor**" means a third party, other than an Oracle Affiliate, which Oracle subcontracts with and which may Process Personal Information as set forth in Section 4.

"**You**" means the customer entity that has executed the Services Agreement.

Other capitalized terms have the definitions provided for them in the Services Agreement.

Exhibit 1: European Data Processing Addendum for Oracle Services

("European DPA Addendum")

This European DPA Addendum supplements the Data Processing Agreement to include additional Processor terms applicable to the Processing of Personal Information subject to Applicable European Data Protection Law.

Except as expressly stated otherwise in the Data Processing Agreement, the Services Agreement, this European DPA Addendum or the Oracle Processor Code, in the event of any conflict between these documents, the following order of precedence applies (in descending order): (i) the Oracle Processor Code; (ii) this European DPA Addendum; (iii) the body of the Data Processing Agreement; and (iv) the Services Agreement.

1. Cross-Border Data Transfers – Oracle Processor Code

1.1 The Oracle Processor Code (Binding Corporate Rules for Processors) applies to the Processing of Personal Information by Oracle on Your behalf in its role as a Processor as part of the provision of Services under the Services Agreement and this European DPA Addendum, where such Personal Information is: (i) subject to any data transfer restrictions under Applicable European Data Protection Law; and (ii) processed by Oracle or an Oracle Affiliate in a country outside Europe.

1.2 The most current version of the Oracle Processor Code is available on https://www.oracle.com/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf, and is incorporated by reference into the Services Agreement and this European DPA Addendum. Oracle has obtained EEA authorization for its Processor Code and will maintain such authorization for the duration of the Services Agreement.

1.3 Transfers to Third Party Subprocessors shall be subject to security and data privacy requirements consistent with the Oracle Processor Code, the Data Processing Agreement and the Services Agreement.

2. Description of Processing

2.1 *Duration of processing activities*. Oracle may Process Personal Information during the term of the Services Agreement and to perform its obligations under Section 9 of the Data Processing Agreement, unless otherwise required by applicable law.

2.2 *Processing activities.* Oracle may Process Personal Information as necessary to perform the Services, including where applicable for hosting and storage; backup and disaster recovery; service change management; issue resolution; applying new product or system versions, patches, updates and upgrades; monitoring and testing system use and performance; IT security purposes including incident management; maintenance and performance of technical support systems and IT infrastructure; and migration, implementation, configuration and performance testing.

2.3 *Categories of Personal Information.* In order to perform the Services and depending on the Services You have ordered, Oracle may Process some or all of the following categories of Personal Information: personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, and business contact details; financial details; goods and services provided; unique IDs collected from mobile devices, network carriers or data providers; IP addresses and online behavior and interest data.

2.4 *Categories of Data Subjects.* Categories of Data Subjects whose Personal Information may be Processed in order to perform the Services may include, among others, Your

representatives and end users, such as Your employees, job applicants, contractors, collaborators, partners, suppliers, customers and clients.

2.5 Additional or more specific descriptions of Processing activities, categories of Personal Information and Data Subjects may be described in the Services Agreement.

3. Your Instructions

3.1 Your right to provide instructions to Oracle as specified in Section 2 of the Data Processing Agreement encompasses instructions regarding (i) data transfers as set forth in Section 1 of this European DPA Addendum; and (ii) assistance with Data Subject requests to access, delete or erase, restrict, rectify, receive and transmit (data portability), block access to or object to Processing of specific Personal Information or sets of Personal Information as described in Section 3 of the Data Processing Agreement.

3.2 To the extent required by the Applicable EEA Data Protection Law, Oracle will immediately inform You if, in its opinion, Your instruction infringes Applicable European Data Protection Law. You acknowledge and agree that Oracle is not responsible for performing legal research and/or for providing legal advice to You.

4. Notice and Objection Right to New Oracle Affiliates and Third Party Subprocessors

4.1 Subject to the terms and restrictions specified in this Section 4 of the European DPA Addendum and Section 4 of the Data Processing Agreement, You provide Oracle general written authorization to engage Oracle Affiliates and Third Party Subprocessors to assist in the performance of the Services.

4.2 Oracle maintains lists of Oracle Affiliates and Third Party Subprocessors that may Process Personal Information. These lists are available via My Oracle Support, Document ID 2121811.1 (or other applicable primary support tool, user interface or contact provided for the Services, such as the NetSuite Support Portal or Your Oracle project manager). If You would like to receive notice of any intended changes to these lists of Oracle Affiliates and Third Party Subprocessors, You can (i) sign up per the instructions on My Oracle Support, Document ID 2288528.1; or (ii) Oracle will provide you notice of intended changes where a sign up mechanism is not available. For ACS and Consulting Services, any additional Third Party Subprocessors that Oracle intends to use will be listed in Your order for ACS or Consulting Services, or in a subsequent "Oracle Subprocessor Notice", which Oracle will send to you by e-mail as necessary.

4.3 Within fourteen (14) calendar days of Oracle providing such notice to You under Section 4.2 above, You may object to the intended involvement of a Third Party Subprocessor or Oracle Affiliate in the performance of the Services, providing objective justifiable grounds related to the ability of such Third Party Subprocessor or Oracle Affiliate to adequately protect Personal Information in accordance with the Data

Processing Agreement or Applicable European Data Protection Law in writing by submitting a "service request" via (i) My Oracle Support (or other applicable primary support tool) or (ii) for ACS and Consulting Services, the project manager for the Services. You and Oracle will work together in good faith to find a mutually acceptable resolution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Subprocessor's or Oracle Affiliate's compliance with the Data Processing Agreement or Applicable European Data Protection Law, or delivering the Services without the involvement of such Third Party Subprocessor. To the extent You and Oracle do not reach a mutually acceptable resolution within a reasonable timeframe, You shall have the right to terminate the relevant Services (i) upon serving thirty (30) days prior notice; (ii) without liability to You or Oracle and (iii) without relieving You from Your payment obligations under the Services Agreement up to the date of termination. If the termination in accordance with this Section 4.3 only pertains to a portion of Services under an order, You will enter into an amendment or replacement order to reflect such partial termination.

5. Information and Assistance

5.1 For hosted Services, Your audit rights under Section 7 of the Data Processing Agreement include the right to conduct inspections of the applicable Services data center facility that hosts Personal Information.

5.2 In addition, You may request that Oracle audit a Third Party Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist You in obtaining a third-party audit report concerning the Third Party Subprocessor's operations) to verify compliance with the Third Party Subprocessor's obligations. You will also be entitled, upon written request, to receive copies of the relevant privacy and security terms of Oracle's agreement with any Third Party Subprocessors and Oracle Affiliates that may Process Personal Information.

5.3 Oracle provides You with information and assistance reasonable necessary for You to conduct Your data protection impact assessments or consult with Your Regulator(s), by granting You electronic access to a record of Processing activities and any available privacy & security functionality guides for the Services. This information is available via (i) My Oracle Support, Document ID 111.1 or other applicable primary support tool provided for the Services, such as the NetSuite Support Portal, or (ii) upon request, if such access to My Oracle Support (or other primary support tool) is not available to You.

6. Data Protection Officer

6.1 Oracle has appointed a Global Data Protection Officer and, in some European countries, a local Data Protection Officer. Further details on how to contact Oracle's Global Data Protection Officer and, where applicable, the local Data Protection Officer, are available here.

6.2 If You have appointed a Data Protection Officer, You may request Oracle to include the contact details of Your Data Protection Officer in the relevant Services order.

Statutory Declaration

I hereby declare on oath that I have prepared this master´s thesis independently and without the use of other that the specified aids. The positions taken directly or indirectly from external sources are identified as such. The work has not yet been submitted in the same way or a similar form to another examination authority and has not yet been published.

Dornbirn 8th August, 2022 Leah W. Kihuria