TERMS AND CONDITIONS

**Online Services Agreement**

1. SCOPE
   1. Subject to the terms and conditions set forth herein and in the Order Page (hereinafter jointly referred to as the "Contract"), CRIF S.p.A., a company registered in Italy and located at with registered office at Via della Beverara 21, 40131 Bologna, VAT no. 02083271201, (hereinafter “CRIF”) provides its services exclusively to entities lawfully conducting business activity, (e.g. individual entrepreneurs or commercial companies), who buy such services in relation to their business activity and accept the terms and conditions expressed in this Contract as well as other relevant documents (hereinafter “CUSTOMER”). The service provided by CRIF referred herein as the "Skyminder Service" gives access, within the limits allowed by law and for the period covered by this Contract, to business information including reports (hereinafter “Business Information Report”) and commercial information on companies and enterprises in different countries, and compliance check reports (hereinafter “Compliance Check Reports”) meaning reports that can be requested on both companies and persons and verifies worldwide information, like Sanctions List, Enforcement data, PEP (political exposed persons), Adverse Media, SOE data (state owned companies), Registrations category. CRIF and the CUSTOMER are also hereinafter jointly referred to as the “Parties”. “Order Page” means an online ordering web page available on the Website, where the CUSTOMER will select the information and services requested by the CUSTOMER as well as the method of payment and the applicable fees.
   2. Detailed information on the Skyminder Service is contained on the website www.skyminder.com ("Website") and in the Order Page which is an integral part of the Contract.
   3. The CUSTOMER declares from this time forth that the Skyminder Service is suitable for the specific use the CUSTOMER intends to make of it and assumes all relevant risk.
2. METHOD OF PROVIDING THE SKYMINDER SERVICE
   1. Within a reasonable time, upon completion of the online registration, including the acceptance of this Contract, CRIF will activate the identification code (username) and the access key (password) defined by the CUSTOMER for using the Skyminder Service through the Website (hereinafter “Account”).
   2. CRIF reserves the right not to activate the Account if it has reason to believe, at its sole discretion, that any irregularity occurred in the registration process.
   3. The CUSTOMER shall use the Account to access the Website and make requests for the reports of interest, as available within the Skyminder. It will be possible to view the requests and the results on the Website.
   4. CRIF will not be responsible for any defect, discontinuity or impossibility in accessing and/or using the Skyminder Service resulting from circumstances that are not under the control of CRIF (such as, for example, any defect in the equipment used by the CUSTOMER for accessing the Skyminder Service, problems in the Internet network, force majeure or unforeseeable events). CRIF does not warrant that the Website will be uninterrupted, error-free or accessible, that defects will be corrected, that the Website will be secure or operate without error or that this Website or services will meet client’s requirements.
   5. The Parties expressly stipulate that, should it become necessary for CRIF to perform maintenance operations on the Skyminder Service, as to ensure correct access and continuity in supplying the service, CRIF may proceed, by means of online communication on the Website, to temporarily suspend the access to the Skyminder.
   6. The Skyminder Service is subject to the availability of the data and information as provided by the competent public authorities and the third party providers that are specialized in processing information from public archives and/or other sources.
   7. The CUSTOMER shall use the Skyminder Service and the content received by CRIF only for internal business purposes. The CUSTOMER shall not copy, reproduce in any form, resell and/or provide to third parties the reports and information obtained from the Skyminder Service, either individually or in aggregate (including within the same group of companies of the CUSTOMER). Any other utilization without the prior written consent of CRIF shall be deemed to constitute an abuse.
   8. The CUSTOMER has been made aware and accepts that the activation of the Skyminder Service allows the CUSTOMER to purchase only the information specified in the Order Page.
   9. Without prejudice to the provisions of point 4.4 below, any changes to the contents, the available information and reports, to the functionality, the features and to the cost of the service will be displayed on the Order Page; these changes will be considered to be governed by this Contract and its integral and substantial parts.
   10. The object of the performances rendered by CRIF shall under no circumstances constitute any possible assignment of proprietary rights. CRIF shall be comprehensively and exclusively entitled to all rights (incl. copyrights and other intellectual property) related to the works and materials provided to CUSTOMER within the Skyminder Service. The ideas, concepts, methods, techniques and know-how used by CRIF for the contractual fulfilment can also be used by CRIF for other purposes at its complete discretion.
3. EFFECTIVE DATE OF THE SKYMINDER SERVICE

3.1 Subject to section 2.4 and 2.5, the Skyminder Service will be available as of the date of activation of the Account.

1. DATA MANAGEMENT
   1. CRIF undertakes to use the best practices for managing the Skyminder Service data and information. Furthermore, the CUSTOMER has been made aware that CRIF receives, among other things, the information and data specified in this Contract from third-party providers and will not be held responsible under any circumstances for any incompleteness and/or errors and/or defects that are not attributable to CRIF itself in providing this Skyminder Service.
   2. The Skyminder Service is provided by CRIF on an “as is” basis and without warranties of any kind either express or implied. To the fullest extent permissible pursuant to applicable law, CRIF disclaims all warranties, express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose or any implied warranties arising from course of dealing or usage of trade.
   3. Any obstacles to the collection of the data and information caused by the non-availability of the public sources or third party providers to provide such data, will not be attributed to CRIF.
   4. The CUSTOMER is aware that the organization and structure of the information within the Skyminder Service are subject to applicable laws and regulations and, therefore, are subject to possible modification and restructuring in case of relevant changes in such laws and regulations. Furthermore, CRIF is authorized to make any changes of a technical nature and/or in the content and/or in the type of information included in the Skyminder Service, that should become necessary for technical reasons, organizational reasons, or for reasons not attributable to CRIF.
2. PAYMENT
   1. For accessing the Skyminder Service the CUSTOMER is required to pay the amounts specified in the Order Page, according to the CRIF current fees, which the CUSTOMER declares to know and accept, and in accordance with the methods of payment selected by the CUSTOMER on the Order Page. The amounts are considered to exclude VAT (if applicable) and other duties and expenses related to the provision of the Skyminder Service, with the exception of anything expressly indicated in the Order Page and subsequent amendments pursuant to section 2.9.
   2. For each payment made by the CUSTOMER, CRIF will issue an invoice which will be sent to the CUSTOMER via electronic means at the e-mail address provided by the CUSTOMER on the registration form filled out at the time of acceptance of this Contract.
   3. CRIF reserves the right to change the rates defined in the Order Page whenever the costs for performing the Skyminder Service increase for any reason. In the latter case, CRIF will publish the new current rates in the Order Page. The new prices will be automatically applied after such publication.
3. TERM OF CONTRACT
   1. This Contract will be effective as of the date of online registration and completion by the CUSTOMER of the acceptance procedure on the Website ("Effective Date") and shall continue until it is terminated according to section 10. Upon expiration of the abovementioned term, if the CUSTOMER wishes to reactivate its Account in order to restart to use the Skyminder Service, it shall send a written request to CRIF to the following email address: activations@skyminder.com and shall sign the new contract that will be sent to it by CRIF. At the end of this procedure, CRIF shall reactivate the CUSTOMER’s Account within a reasonable time. It is understood between the Parties that CRIF reserves the right to refuse, at its sole discretion, the CUSTOMER's request for reactivation.
4. OBLIGATIONS AND RESPONSIBILITIES OF CRIF
   1. CRIF will be able to make any changes deemed necessary or appropriate to the structure of the reports information provided, without any objection being opposed by the CUSTOMER.
   2. CRIF will not be held responsible for damages of any kind and for any reason that is incurred by the CUSTOMER or third parties in relation to this Contract or to the services described herein, due to unforeseeable events, force majeure, incorrect functioning of the national and international data and telephone networks and/or the incorrect functioning of the equipment used by the CUSTOMER.
   3. CRIF, which receives information originating from public archives and/or other sources processed by specialized third party providers, will not be held responsible under any circumstances for any errors, incompleteness, or any other defects in connection with the information and data provided. Specifically, CRIF will not be held responsible, either directly or indirectly, with regard to the content of the information or for any damage resulting from such errors, incompleteness or defects or, in any case, for reasons beyond its control. Without prejudice to the provisions of this section, CRIF shall be considered responsible solely for direct damages (excluding indirect, incidental or consequential damages such as, without limitation, loss of profit) caused to the CUSTOMER as a result of malicious intentions or gross negligence of CRIF in the performance of the Skyminder Service.
   4. CRIF is exempt from all responsibility following the use by the CUSTOMER and/or by their successors in title of the information and data provided within the Skyminder Service, specifically, but without any exclusion whatsoever, in case of use that does not conform with the laws in force and/or the methods and/or the terms and conditions specified in this Contract; specifically, it will not be held responsible in any manner for any decisions and/or evaluations made by the CUSTOMER on the basis of the information and data from the Skyminder Service.
   5. CRIF does not assume any obligation or give any guarantee not expressly included in this Contract.
5. OBLIGATIONS AND RESPONSIBILITIES OF THE CUSTOMER
   1. The CUSTOMER guarantees (i) that it is an entity lawfully conducting business activity, such as a company or an individual entrepreneur, who uses the Skyminder Service exclusively in the context of his business or professional activities; (ii) that the data provided for the stipulation of the Contract are truthful, correct, and up-to-date; the violation of this guarantee constitutes cause for the immediate termination of this Contract and gives CRIF the right to definitively retain the price paid as a penalty, without prejudice to the right to demand further damages.
   2. Any changes to the data provided, that is, the postal address and the e-mail address, must be promptly reported to CRIF to allow them to update said data; if the CUSTOMER does not promptly report such changes, any claim and/or responsibility could be opposed by CRIF.
   3. The CUSTOMER undertakes to use the information and the data from the Skyminder Service diligently and not to transfer for any reason, reuse, resell, and/or make available to third parties the information from the Skyminder Service. The CUSTOMER is not authorized to disclose the information from the Skyminder Service, releasing CRIF from any improper or non-compliant use of said information by the CUSTOMER.
   4. The CUSTOMER may order and use the Compliance Check Reports solely for the purposes of meeting regulatory compliance requirements regarding anti-money laundering, counter-terrorism financing, fraud risk management and anti-bribery or corruption. It being understood that CUSTOMER’s use of the Compliance Check Reports shall be for only lawful and legitimate business purposes, including those specified above in connection with a specific information request, relating to its business. The CUSTOMER shall not use the Compliance Check Reports for marketing or employment screening purposes, nor shall the CUSTOMER use any information contained in the Compliance Check Reports for a purpose not otherwise authorized in this Contract.
   5. The CUSTOMER undertakes to keep, in a safe and confidential manner, the identification code and the access key provided by CRIF; the violation of this obligation may result in the automatic termination of this Contract, without prejudice to the right of CRIF to definitively retain the amounts already paid by the CUSTOMER as a penalty, without prejudice to the right to demand further damages.
   6. Should the confidentiality of the access key be compromised for any reason (theft, loss, etc.), the CUSTOMER is required to: i) immediately change the access key through the Website and ii) immediately inform CRIF of this situation by any means as soon as they get informed, and then confirm this notification by sending a certified electronic mail (or equivalent method with acknowledgement of receipt) within 24 hours. It is understood that the CUSTOMER is considered responsible for any purchase made until 10:00 a.m. of the first working day after CRIF receives the certified electronic mail. If the CUSTOMER is unable to change the access key as per section 8.6.i) above and at its request within the abovementioned certified electronic mail, CRIF undertakes to deactivate the access key as soon as possible. In addition, the CUSTOMER may be required to comply with additional terms and conditions set forth by the information providers for the access to certain contents, as displayed and notified to the CUSTOMER in the personal account from time to time. Such additional terms and conditions shall be deemed to be part of this Contract.
   7. The Client hereby agrees not to use the Skyminder Service or related communication services to:

a) send or forward messages or communications which are abusive, offensive, obscene, or of such nature to give intentionally offence to any recipient;

b) send or forward messages which promote, sell or advertise any product or service to any recipients; and/or

c) send or forward files or other material which is affected by viruses or similar threats;

* 1. The CUSTOMER is responsible for any damage resulting if:
* it uses the data and information from the Skyminder Service to upset, abuse, limit, or, in any case, violate the rights of interested third parties and/or, in any case, not in line with the purpose of the Skyminder Service and not in compliance with the current regulations regarding the protection of personal data;
* it uses brands, names, and/or logos belonging to CRIF;
* it allows unauthorized people to use the identification code and the access key;
* it introduces and/or uses files or other material containing incorrect data and/or viruses;
* it violates the contractual provisions for which it is responsible.
  1. The CUSTOMER further agrees to indemnify, defend and hold harmless CRIF and the information providers from any and all claims, damages, liabilities, costs, charges, and expenses, including attorneys’ fees, arising out of any breach of this Contract by the CUSTOMER, including any use of the business information and/or of the reports and/or of any other content which is not expressly authorized under this Contract, including without limitation any violation of copyrights belonging to third parties.
  2. It is also agreed between the Parties that any evaluations resulting from the consultation of the data and information from the Skyminder Service are undertaken by the CUSTOMER, and/or by their successors in title, with complete autonomy and under their own sole and direct responsibility.

1. ASSIGNMENT
   1. The Contract and the rights and obligations arising from it cannot be transferred by the CUSTOMER to third parties, in whole or in part, without the prior written consent of CRIF.
   2. The CUSTOMER expressly authorizes CRIF to transfer this Contract to other companies that are subsidiaries, parent companies, affiliated companies, or associated companies of CRIF.
2. TERMINATION CLAUSE
   1. CRIF has the right to unilaterally and immediately terminate this Contract at any time, in such case CRIF shall deactivate the CUSTOMER’s Account without any notice to the CUSTOMER.
   2. The CUSTOMER has the right to unilaterally terminate this Contract at any time, in such case the CUSTOMER will send a written request to CRIF at the following e-mail address: [activations@skyminder.com](mailto:activations@skyminder.com); CRIF within reasonable time shall deactivate the CUSTOMER’s Account.
   3. It is understood between the Parties that:
3. in case of termination for convenience of this Contract by CRIF, CRIF shall reimburse the Customer the amount already paid by the CUSTOMER for Business Information Reports and/or Compliance Check Reports not yet delivered by CRIF;

b) in case of termination for convenience of this Contract by the CUSTOMER, CRIF shall withhold any amount already paid by the CUSTOMER for Business Information Reports and/or Compliance Check Reports not yet delivered by CRIF without any obligation to deliver such reports.

10.4 Notwithstanding the foregoing, if the termination by CRIF is due for the following breaches of Contract by CUSTOMER:

- violation of section 2.7;

- violation of sections 8.1, 8.3 and 8.5;

- violation of section 9;

- violation of section 13;

CRIF shall withhold any amount already paid by the CUSTOMER for Business Information Reports and/or Compliance Check Reports not yet delivered by CRIF without any obligation to deliver such report.

1. EXCLUSIVE JURISDICTION AND APPLICABLE LAW

11.1 The Parties expressly stipulate that for any dispute arising from the Contract and, in any case, for any dispute relating to or in connection with said Contract, the court of competent jurisdiction is exclusively the court of Bologna, Italy. This Contract is governed by the laws of Italy.

1. RIGHT OF INSPECTION
   1. During the validity of this Contract CRIF or its authorized representatives shall be entitled to audit the CUSTOMER’s compliance with its obligations under this Contract on reasonable notice.
   2. During the course of any audit carried out by CRIF, if required at its sole discretion, also in CUSTOMER’s premises, the CUSTOMER will use its best endeavours to provide all reasonable assistance to CRIF and make available one or more of its managers or senior officials with the appropriate level of expertise and authority to answer any reasonable enquiries of CRIF. The CUSTOMER will use its best endeavours to provide CRIF with any information it reasonably requests and/or to evidence the CUSTOMER's compliance with this Contract.
   3. The scope of any such audit shall be limited to those files, books, records, accounts, procedures and quality control policies that are reasonably and directly relevant to the CUSTOMER’s compliance to this Contract. CRIF shall take all reasonable steps to minimise disruption to the CUSTOMER’s business during such audits, which shall be carried out during normal business hours. CRIF shall bear all costs for the above-mentioned audits.

13. DATA PROTECTION

13.1 In the execution of the Agreement, the Parties will process data as independent controllers. The Parties undertake to comply with the data processing provisions set out by EU Regulation 679/2016 (“GDPR”) and by any other applicable legislation in force, and to use systems and procedures for data processing operations in compliance with the provisions of article 32 of the GDPR.

13.2 Whether the CUSTOMER is stablished outside of the European Union, the transfer of personal data shall be carried out, without specific authorizations, if the third country guarantees an adequate level of data protection according to the European Commission. In the absence of the aforementioned adequacy decision adopted by the European Commission, such transfer to third countries may be carried out by adopting the Standard Contractual Clauses (Schedule B). In such case the CUSTOMER undertakes to provide information required by “Transfer Impact Assessment” (Schedule A) as per the recommendation 01/2020 of the European Data Protection Board, prior signing the Standard Contractual Clauses.

13.3 Should the CUSTOMER breach the terms stated in this article, CRIF shall be entitled to automatically terminate the Agreement.

Annexes:

- Schedule A Transfer Impact Assessment

- Schedule B Standard Contractual Clauses

**SCHEDULE A**

**TRANSFER IMPACT ASSESSMENT:**

Request for information (based on EDPB Recommendations 1 and 2 of 2020) and minimum contractual requirements as this document is meant to be a substantial part of the SCC.

EXPLANATORY NOTE:

As regards the impact of Data Importer’s laws and practices on compliance with the standard contractual clauses and with the data subjects fundamental rights, different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer.

Therefore, please provide us with the relevant answers to following questions:

1. enumerate the laws and regulations in the destination country applicable to the importer or its (sub) processors that would permit access by public authorities to the personal data that are subject to the transfer, in particular in the areas of intelligence, law enforcement, administrative and regulatory supervision applicable to the transferred data;

|  |
| --- |
|  |

1. in the absence of laws governing the public authorities’ access to data, provide information and statistics based on the importer’s experience or reports from various sources (e.g. partners, open sources, national case law and decisions from oversight bodies) on access by public authorities to personal data in situations of the kind of the data transfer at hand (i.e. in the specific regulatory area; regarding the type of entities to which the data importer belongs;…);

|  |
| --- |
|  |

(3) indicate which (technical/organizational/contractual) measures are taken to prevent the access to transferred data (if any) in the relevant Annex II;

(4) provide sufficiently detailed information on all requests of access to personal data by public authorities which the importer has received over the last 24 months, in particular in the areas mentioned under (1) above and comprising information about the requests received, the data requested, the requesting body and the legal basis for disclosure and to what extent the importer has disclosed the data request;

|  |
| --- |
|  |

(5) specify whether and to what extent the importer is legally prohibited to provide the information mentioned under (1) – (5) above.

|  |
| --- |
|  |

(6) In the light of the answers under (1) – (5) above, advice:

a) if the processing is based on clear, precise and accessible rules under article 8(2) of the EU Charter of Fundamental Rights and, as the case may be, on the jurisprudence of the European Court of Human Rights related to article 8 of the European Convention on Human Rights (“ECHR”) dealing with surveillance issues in States party to the ECHR;

b) if the necessity and proportionality under article 52(1) and 7 of the EU Charter of Fundamental Rights with regard to the legitimate objectives pursued by the law/practice/public authority request could be demonstrated[[1]](#footnote-1);

c) if an independent oversight mechanism on such kind of data subjects’ rights exists;

d) if the country of the importer grants effective remedies for the possible violations of the individuals’ fundamental rights as enshrined in Article 47 of the Charter of Fundamental Rights;

(7) In the light of the above, the importer also grants that:

a) it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data;

b) it will not purposefully create or change its business processes in a manner that facilitates access to personal data or systems,

c) that national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key;

d) it shall inform the public authority which requests access to the data of the incompatibility of the order with the safeguards contained in the Article 46 GDPR transfer tool and the resulting conflict of obligations for the importer and the importer shall notify simultaneously and as soon as possible the exporter and/or the competent supervisory authority from the EEA, insofar as possible under the third country legal order;

e) it shall keep a record of requests for access received from public authorities and the response provided, alongside the legal reasoning and the actors involved (e.g. if the exporter has been notified and its reply, the assessment of the team in charge of dealing with such requests, etc.). These records should be made available to the data exporter, who should in turn provide them to the data subjects concerned where required.

(8) specify whether the data importer engages (also through its processor/sub-processor and further sub-processor) in any onward transfer of the personal data within the same or other third countries without an equivalent level of protection of the personal data to that afforded within the EU.

|  |
| --- |
|  |

**ANNEX I**

**EXPLANATORY NOTE:**

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

**A. LIST OF PARTIES**

**MODULE ONE: Transfer controller to controller**

**Data exporter(s):** [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name:

Address:

Contact person’s name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (controller/processor):



**Data importer(s):** [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Name:

Address:

Contact person’s name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role (controller/processor):



**B. DESCRIPTION OF TRANSFER**

**MODULE ONE: Transfer controller to controller**

Categories of data subjects whose personal data is transferred      ………………………..

Categories of personal data transferred

………………………..

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

     ………………………..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

     …………………………

Nature of the processing

     …………………………

Purpose(s) of the data transfer and further processing

     ………………………..

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

     ……………………..

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

     ……………………..

**C. COMPETENT SUPERVISORY AUTHORITY**

**MODULE ONE: Transfer controller to controller**

Identify the competent supervisory authority/ies in accordance with Clause 13 of the relevant Standard Contractual Clauses:

ITALY

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

**MODULE ONE**: **Transfer controller to controller**

**EXPLANATORY NOTE:**

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

SCC, data exporter contractual audit rights, reporting obligations under point (7) lett. d) above; importer’s record of access requests as per the following point (7) lett. e) above, Appointment letter as authorized subject under art. 29 of the GDPR based on a strict need-to-know principle;       \_\_\_\_\_

[Examples of other possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

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

**ANNEX III – LIST OF SUB-PROCESSORS**

**SCHEDULE B**

EUROPEAN

COMMISSION

Brussels, 4.6.2021

C(2021) 3972 final

*STANDARD CONTRACTUAL CLAUSES*

*Adopted by the European Commission according to the COMMISSION IMPLEMENTING DECISION*

*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*

**SECTION I**

*Clause 1*

***Purpose and scope***

1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[[2]](#footnote-2) for the transfer of personal data to a third country.
2. The Parties:
   1. the natural or legal person(s), public authority/ies, agency/ies or other body/ies

(hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and

* 1. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

1. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

***Effect and invariability of the Clauses***

1. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to

select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

1. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

*Clause 3*

***Third-party beneficiaries***

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   2. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b);
   3. Clause 12 - Module One: Clause 12(a) and (d);
   4. Clause 13;
   5. Clause 15.1(c), (d) and (e);
   6. Clause 16(e);
   7. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b);
2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

***Interpretation***

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

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

*Clause 6*

***Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7 - Optional*

***Docking clause***

1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
2. Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
3. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES**

*Clause 8*

***Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**MODULE ONE: Transfer controller to controller**

**8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

1. where it has obtained the data subject’s prior consent;
2. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
3. where necessary in order to protect the vital interests of the data subject or of another natural person.

**8.2 Transparency**

1. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
   1. of its identity and contact details;
   2. of the categories of personal data processed;
   3. of the right to obtain a copy of these Clauses;
   4. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
2. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
3. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
4. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.3 Accuracy and data minimisation**

1. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
2. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
3. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

**8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[[3]](#footnote-3) of the data and all back-ups at the end of the retention period.

**8.5 Security of processing**

1. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
2. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
3. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
4. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
5. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
6. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
7. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

**8.6 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter “sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

**8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union[[4]](#footnote-4) (in the same country as the data importer or in another third country, hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

1. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
2. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
3. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
4. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
5. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
6. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

**8.9 Documentation and compliance**

1. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
2. The data importer shall make such documentation available to the competent supervisory authority on request.

*Clause 9*

***Use of sub-processors***

***(DELETED: NOT APPLICABLE IN CASE OF TRANSFER CONTROLLER TO CONTROLLER)***

*Clause 10*

***Data subject rights***

**MODULE ONE: Transfer controller to controller**

1. The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[[5]](#footnote-5) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
2. In particular, upon request by the data subject the data importer shall, free of charge :
   1. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
   2. rectify inaccurate or incomplete data concerning the data subject;
   3. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
3. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
4. The data importer shall not make a decision based solely on the automated

processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

* 1. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  2. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

1. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
2. The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
3. If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

*Clause 11*

***Redress***

1. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

**MODULE ONE: Transfer controller to controller**

1. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
2. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
   1. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
   2. refer the dispute to the competent courts within the meaning of Clause 18.
3. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
4. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
5. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

*Clause 12*

***Liability***

**MODULE ONE: Transfer controller to controller**

1. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
2. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
3. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
4. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
5. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

*Clause 13*

***Supervision***

**MODULE ONE: Transfer controller to controller**

1. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

1. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries,

submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

**SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY**

**PUBLIC AUTHORITIES**

*Clause 14*

***Local laws and practices affecting compliance with the Clauses***

**MODULE ONE: Transfer controller to controller**

1. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   1. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[6]](#footnote-6);
   3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

***Obligations of the data importer in case of access by public authorities***

**MODULE ONE: Transfer controller to controller**

other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

**15.1 Notification**

1. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
   1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
   2. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
2. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
3. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
4. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
5. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

*Clause 16*

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

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   1. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   2. the data importer is in substantial or persistent breach of these Clauses; or
   3. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

1. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
2. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

*Clause 17*

***Governing law***

**MODULE ONE: Transfer controller to controller**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of ITALY.

*Clause 18*

***Choice of forum and jurisdiction***

**MODULE ONE: Transfer controller to controller**

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. The Parties agree that those shall be the courts of Bologna (Italy).
3. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
4. The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

**ANNEX I**

**A. LIST OF PARTIES**

**MODULE ONE: Transfer controller to controller**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

1. …

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: …

Address: …

Contact person’s name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

1. …

**B. DESCRIPTION OF TRANSFER**

**MODULE ONE: Transfer controller to controller**

*Categories of data subjects whose personal data is transferred*

*………………………..*

*Categories of personal data transferred*

*………………………..*

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

*………………………..*

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

*…………………………*

*Nature of the processing*

*…………………………*

*Purpose(s) of the data transfer and further processing*

*………………………..*

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

*……………………..*

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

*……………………..*

**C. COMPETENT SUPERVISORY AUTHORITY**

**MODULE ONE: Transfer controller to controller**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

*………………………….*

**ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

**MODULE ONE: Transfer controller to controller**

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*

*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

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

1. See article 23.1 GDPR, and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations022020-european-essential\_en . [↑](#footnote-ref-1)
2. Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […]. [↑](#footnote-ref-2)
3. This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible. [↑](#footnote-ref-3)
4. The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

   [↑](#footnote-ref-4)
5. That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension. [↑](#footnote-ref-5)
6. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or [↑](#footnote-ref-6)