bics

Standard contractual clauses – Controller to Controller

SECTION I

Clause 1

Purpose and scope

(a) 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)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) 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

(ii) 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").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) 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

(a) 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.

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

---

[1] 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 […].

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) 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

Docking clause

(a) 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.

(b) 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.

(c) 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.

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:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) 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:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) 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.

(b) 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.

(c) 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.

(d) 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

(a) 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.

(b) 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.

(c) 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[2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) 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.

(b) 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.

(c) 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.

---

[2] 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.

(d) 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.

(e) 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.

(f) 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.

(g) 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[3] (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:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) 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 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.

(iii) 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;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) 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

(a) 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.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

Not applicable as per standard EU clauses – module 1.

Clause 10

Data subject rights

(a) 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.[4] 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.

[4] 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.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) 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);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) 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.

(c) 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.

(d) 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:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) 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.

(e) 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.

(f) 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.

(g) 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

(a) 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.

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[5] at no cost to the data subject. It shall inform the data subjects, in the manner set out in

[5] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

(b) 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.

(c) 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:

(i) 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;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) 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.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) 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

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) 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.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) 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.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) 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;

(ii) 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];

(iii) 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.

(c) 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.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) 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). [For Module Three: The data exporter shall forward the notification to the controller.]

---

[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 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.

(f) 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 [for Module Three: , if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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

15.1 Notification

(a) 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:

(i) 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

(ii) 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.

(b) 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.

(c) 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.).

(d) 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.

(e) 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

(a) 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).

(b) 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.

(c) 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

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) 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).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) 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;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) 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 [for Module Three: and the controller] 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.

(d) 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.

(e) 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

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 Belgium

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Brussels, Belgium.

(c) 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.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: BICS

Address: Koning Albert II Laan 27, B-1030 Brussels

Contact person's name, position and contact details: Jan De Cocker, DPO

Activities relevant to the data transferred under these Clauses: For its international data transfers , BICS acts as a wholesale carrier; this includes the transfer of personal data included in voice, mobility and messaging communications exchanged by BICS with the importer in the frame of its core, legacy or value added services ("the Services");

Role (controller/processor): Controller

Data importers:

1. Any operator or carrier that is headquartered outside of the EEA or the equipment of which is located outside of the EEA and to which BICS sends communications traffic, be it voice, messaging, data or signalling one in the context of the BICS General Terms & Conditions for the supply of services agreed between the parties.

Address: as per the agreement entered into between BICS and each concerned operator or carrier

Contact person's name, position and contact details: as per the BICS General Terms & Conditions entered into between BICS and each concerned operator or carrier

Activities relevant to the data transferred under these Clauses: conveyance of international telecommunactions traffic and data

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The end-users in the telecommunications chain.

Categories of personal data transferred

In its role as a Wholesale carrier BICS transfers technical network-related data. Such data contain the phone numbers of the originating and receiving end user, in addition to other information such as the time or duration of the call. BICS' systems generate that information, which is unique to the transit through BICS' network.

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.

Not applicable

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

The transfer happens on a continous basis as long as exporter and importer are parties to the BICS General Terms & Conditions for the supply of services whereby BICS may send traffic to said importer and each time BICS choses to send telecommunication traffic to said importer.

Nature of the processing

As an international wholesale carrier of telecommunications, BICS is transferring the communications it receives from its telecommunications customers to worldwide destinations, for further conveyance of those communications to the destination end user by local operators. In other words, if an end user wants to call someone abroad, in order for that end user to communicate with that person, this end user's telecom network will need to connect the end user call with the network of the operator to which that person is connected. BICS intervenes as part of the chain of conveyance of the call

This is needed in the framework of the contract BICS has entered into with other operators, and amongst others in the communication chain, with the calling end user's mobile phone operator which is the party that needs to inform the end user as a data subject that his/her phone number must be processed to allow international calls to be placed or received.

Purpose(s) of the data transfer and further processing

As explained above, as part of its telecommunications activities and the services it supplies to its customers, BICS may convey telecommunication data towards other parties in the communication chain in order for communications, that BICS receives from other operators, to reach their final destination.

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

12 months

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

N/A

C. COMPETENT SUPERVISORY AUTHORITY

The Belgian Data Protection Authority:

Gegevensbeschermingsautoriteit

Drukpersstraat 35, 1000 Brussel

+32 (0)2 274 48 00

+32 (0)2 274 48 35

contact@apd-gba.be

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

The Importer shall ensure that it has in place and has implemented the following technical and organisation measures for the security of the data:

1. Security policy:

The importer provides its employees with security policies and guidelines to communicate individual

responsibilities with respect to safeguarding the importer' resources. Such security framework in place should be built following ISO/IEC 27001:2022.

All the importer's new hires are required to undertake a series of training sessions, which among other issues address partner and staff responsibilities as they relate to policies and procedures, including Information Security and privacy. Importer's staff is required to complete an individual confirmation of their responsibility for the security of Importer's information to which they are granted access and to take due care to protect the technology equipment assigned to them.

2. Security organisation
    a. Internal security organisation

    Importer must have a formal Corporate Security organization led by a Chief Information Security Officer (CISO) or equivalent, who is responsible for all the security matters in the importer's organization and is assisted by a team of technology and security professionals. The CISO must have the ultimate responsibility for the Importer's security-related decisions and strategies. Certifications and other credentials that attest their proficiency in the field of security held by the CISO's team members is a must.

    b. Confidential agreement

    All Importer' employees (incl. contractors), upon joining the importer's organization and/or during their employment period, as well as certain service providers, are required to sign non-disclosure and confidentiality agreements, demonstrating their commitment to the importer's organization and its information security.

    •

3. Asset management
    a. Asset inventory and classification

    The importer must establish and maintain asset inventory processes for its main physical

    and information assets. Importer's information security policy must define a scheme for

    classifying its main information assets, which would cover at least:

        • Determination of the data classification level of information assets

        • Identification of the information owner

        • Identification of security risk factors

        • Identification of disaster recovery risk factors

    b. Information handling

- Information subject to legislative or regulatory requirements is identified through the asset
- inventory process. Security controls are established to address the relevant requirements.
    •

4. Human resources security

•

- People connecting to the importer's systems and/or network are required to conduct themselves in a manner consistent with the importer's security policies regarding, among other matters, confidentiality, business ethics and

professional standards. The importerr must require that communications via these connections comply with applicable laws and regulations, including those governing:

- • Restrictions on the use of telecommunications technology and encryption
- • Copyrights and license agreement terms and conditions

4.1 Confirmation of Security Responsibilities

All importer's staff (employees and contractors) must participate in regular (at least annual)

regulatory process for Compliance Confirmation, ie providing an individual confirmation of their responsibility for the security of the importer's information to which they have access, and to take due care to protect the technology equipment assigned to them. All staff members sign a personal liability agreement acknowledging their responsibility for the professional equipment and tools received to develop their work, being also responsible for the physical security of these assets.

4.2 Appropriate use

The importer must have in place an the Information Security Policy that addresses the appropriate use of electronic tools and technologies and include sanctions in case of non compliance, up to and including dismissal, depending on the seriousness of the violation.

4.3 Security Awareness Training

Security awareness training must be a component of the importer hiring process. An awareness

program must reinforce periodically the concepts and responsibilities defined in the Information

Security Policy.

4.4 Termination Processes

The importer must establish documented termination processes that define responsibilities for

collection of information assets and removal of access rights for professionals who leave the

importer's organization.

- 5. Physical security
- 5.1 Data Center Security
- If the importer stores data in a data center, the following physical and environmental controls must be incorporated into the design of said data center:
- • Separate protected facilities
- • Badge entrance control
- • Internal and external cameras
- • Temperature and humidity control and monitoring
- • Smoke detection alarm
- • Lightning suppression
- • Transient voltage surge suppression and grounding
- • Redundant power feeds and UPS Systems
- • Physically secured network equipment areas and locked cabinets
- Data center access must be limited to authorized personnel. Visitor access procedures and loading dock security protocols must be established.
- 5.2 Importer's office Security
- Physical access controls must be implemented at all importer's offices. Controls may vary but typically include card-reader access to facilities, on-premises security staff and defined procedures for visitor access control.
- 6. Communications and operations management

- 6.1 Operational Procedures and Responsibilities
-
- The importer's IT organization must establish and maintain controls over standard operating
- procedures, including a repository of procedures, formal review and approval processes, and
- revision management.
- 6.2 Change Control
- The importer's IT organization must establish and maintain a Change Management/Change Control process which includes risk assessment, test and retrieval procedures and review and
- approval components.
- 6.3 Development Environments
- The importer must maintain separate development and production environments. Development
- environments are required to be physically separated from production environments. The
- transfer of an application from development to production must follow the procedures established in the Change Management/Change Control process.
- 6.4 Wireless Networks
- Only IT-managed wireless networks may be permitted on the importer's network, if any. The wireless network must be segmented to ensure only fully managed endpoints are admitted to the corporate network while unmanaged endpoints, are placed on a guest Vlan, and at best with access to internet. Wireless access security controls must include standards for encryption and authentication.
- 6.5 System Backup
- Data center systems must be routinely backed up for disaster recovery purposes. Restoration
- success metrics must be maintained.
- 6.6 Security Software Suite
- The importer must use a combination of technology tools to provide a secure computing environment equipped with antivirus, antispyware, desktop firewall, Secure Remote Access,
- Full disk Hard Drive encryption, SIEM (security information and event management)
- 6.7 Spam Blocking and URL Filtering
- Importer must deploy and regularly update URL filtering software that blocks access to inappropriate web sites from its network. Importer must also establish and maintain e-mail gateway with spam-blocking and anti-virus software
-
  7. Access control
-
- 7.1 Authorization and Authentication Controls
- Importer must follow a formal process to grant or revoke access to its resources. System access
- must be based on the concepts of "least-possible-privilege" and "need-to-know" to ensure that
- authorized access is consistent with defined responsibilities. The importer needs to use a
- combination of user-based, role-based and rule-based access control approaches. Importer needs to establish documented procedures for secure creation and deletion of user accounts,
- including processes to disable and/or delete accounts of employees temporarily away from
- the importer's organization. All importer staff is required to agree to take reasonable precautions to protect the integrity and confidentiality of security credentials.
-
- 7.2 Privileged Access
- Access to authentication servers at administrative, root or system levels is limited to those
- professionals designated by the importer.
-
- 7.3 Password Requirements
- The importer's security policy must establish requirements for password changes, reuse
- and complexity. The importer must require the use of session lock after a period of inactivity through the use of a password.
-
- 7.4 Remote Access
- The importer must use virtual private network (VPN) software to enable secure, internet-based remote access for its professionals. VPN users are required to authenticate using two-factor
- authentication; both a valid user name/password and a corresponding password-protected

- VPN token are required to create a VPN tunnel.
- VPN tunnels must be secured using AES128 or higher encryption. The client software must use
- smart tunneling technology to ensure that communications between the host PC and the
- importer's network are transmitted via an encrypted VPN tunnel. Communications to internet-routed addresses must be conducted outside of the established VPN tunnel. Also, session
- timeout settings must be configured to automatically disconnect the user from a session after
- a period of mouse or keyboard inactivity. Processes must be established to limit third-party
- remote access to the importer's systems. Such access requires approval from the security team and access is limited to those systems required for the third-party to complete the task and is
- monitored on a regular basis.
-
- 7.5 Computer Security
- All importer's desktops and laptops must be protected by hard drive encryption software through
- the 256-bit AES encryption algorithm. The software must enforce password controls and uses
- a dynamic password time-out to prevent brute force password attacks. Additionally, the
- software must be bound to the hard drive, protecting not only the operating system, but also the
- data. The internal policy that regulates the use of laptop must be widely disclosed to the importer's staff.
- Training must be given to new employees of the importer to educate them about theft and to encourage behavior that will help protect laptops against it.
-
- 7.6 Mobile Devices
- Mobile device access must only permitted in accordance with the importer's security policy
- and must require a password to be entered to access the device. The information on the device
- must be erased after ten incorrect access attempts and remote erasure must be made if the device is reported lost or stolen.
-

8. Information systems development cycle

-
- The importer must establish a methodology to manage the acquisition, development and
- maintenance of systems. Key security components related to this methodology include:
- • Business criticality assessment
- • Risk assessment
- • Security team involvement in project reviews and key contracts
- • Utilization of established change control processes to transfer changes from the development to the production environment
- • Penetration testing of a new service/significant change
-
- 8.1 Internal and External Network Scanning
- The importer needs to utilize multiple vulnerability scanning tools to assess its internal and externally facing network environments. These tools are selected and configured to match the requirements of the importer's IT infrastructure, and are updated on an ongoing basis. Processes need to be established to assess and correct the vulnerabilities discovered.
-
- 8.2 Patch Management
- The importer must have patch management processes and tools to assess and deploy operating system and application-specific patches and updates. This process must include steps to evaluate vendor supplied patches to determine servers that require patches and updates, to document procedures for patching and updating servers, and to deploy patches and updates in a timely manner to protect the importer's infrastructure. The importer must continually review patches and updates, as they are released, to determine their criticalities. Patches released on a regularly scheduled basis must be applied following the release; patches released on a regular basis and others determined to be critical must be applied as needed to ensure protection from vulnerabilities.
-

9. Information security incident management

The importer's staff members must be made aware that security incidents must be reported immediately.

The importer must document procedures for the receipt of security incident reports. The importer's security team must have a documented incident response process which includes:

- Escalation process
- Pre-defined roles and responsibilities
- Incident response plan

10. Business continuity and disaster recovery management

The importer must establish a Business Continuity and Disaster Recovery process. To manage this process properly the importer must appoint a Business Continuity Manager and a deputy Business Continuity Manager. The importer must have a BCP strategy approved by its executive management; this strategy must be documented and shared on the internal network of the importer.

Apart from the BCP and DRP documents the importer must also have a Denial of Access Procedure which must allow the importer to continue working in emergency instances.

11. Compliance

11.1 Vulnerability Scanning

The importer must establish processes for performing periodic vulnerability scans of its IT systems. These procedures must specify the use of multiple vulnerability scanning software packages, the creation of vulnerability assessment reports, and the presentation of vulnerability scanning results to the IT organization and IT leadership of the importer. Access to vulnerability scanning tools must be restricted to authorized members of the security team.

11.2 Internal Audit

The importer must be able to rely on internal or external audit organization responsible for assessing internal operations, including the Security and IT teams.

11.3 Ethics & Compliance

The importer must implement procedures to report, either anonymously or not, any misconduct of its professionals or third-parties with respect to the laws and regulations referring to property, secrecy, confidentiality, ethics, business conduct, as well as to internal policies and procedures.

***