LETZDATA
LUXEMBOURG DATA FACTORY

General Terms and Conditions of the Secure IT Environment (SIE)

These terms and conditions constitute a courtesy translation of the French version "*Conditions générales d'utilisation de l'environnement informatique sécurisé*".

In the event of discrepancies between the two versions, the French version shall prevail.

THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry for Digitalisation

Government commission for data sovereignty

Updated: 30/04/2026

TABLE OF CONTENTS

1. Definitions

In these general terms and conditions (GTC), the following definitions apply:

"**Applicant**": the natural or legal person (including a public authority or public sector body) who submits an Initial Application or Subsequent Application to the CGSD in order to obtain an Authorisation.

"**Application**": an Initial Application or Subsequent Application for an Authorisation.

"**Appropriate Measures**": data anonymisation or data pseudonymisation measures or measures to modify, aggregate, delete or treat data by any other method of disclosure control, which aim to safeguard rights and protected interests, data protection, intellectual property rights, commercial confidentiality, including trade secrets, professional and business secrets, statistical secrecy, rights of third parties and data confidentiality.

"**Authorisation**": any authorisation, particularly the authorisation for re-use of Target Data in accordance with the Regulations, issued by the CGSD following an Initial Application or Subsequent Application.

"**Authorisation Duration**": the period during which the Applicant is authorised to access or use the SPE and the Target Data in accordance with the Authorisation.

"**CGSD**": the Government Commission for data sovereignty within the meaning of the Law of 19 December 2025 establishing the Government Commission for data sovereignty.

"**CTIE**": the Government IT Centre established by the Law of 20 April 2009 establishing the Government IT Centre.

"**Data Holder**": the public sector body that holds PSB Data.

"**DGA**": Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

"**External Data**": all data which do not fall within the scope of the PSB Data and which the Applicant wishes to have made available within the SPE, in addition to or in combination with the PSB Data, as such data may come from third-party, open or private sources.

"**External Technological Solution**": the software, algorithms, artificial intelligence models, systems and tools provided by the Re-User for integration into the SPE.

"**Fee**": the sum owed by the Re-User to the CGSD pursuant to the Authorisation.

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

"**Incident**": any security incident, including personal data breaches within the meaning of the GDPR, as well as any event which is not part of the normal functioning of the SIE and which causes or is likely to cause an interruption, disruption or deterioration of the SIE, including compromising the availability, authenticity, integrity or confidentiality of Target Data, Work Data or results hosted in the SPE,

including, but not limited to, unauthorised access, data loss, alteration, prolonged unavailability, personal data breach, unauthorised re-use and re-identification of a data subject.

"**Initial Application**": an application submitted to the CGSD by an Applicant to obtain an Authorisation.

"**Internal Technological Solution**": the software, algorithms, artificial intelligence models, systems and tools provided as standard solutions in the SPE by the CGSD.

"**IPE**": the intermediate secure processing environment, including the organisational means put in place to ensure compliance with Union and applicable Luxembourg law, within which the External Data and the PSB Data transit and are processed for the purposes of enabling the CGSD to produce the Target Data and to monitor the External Technological Solutions intended to be integrated into the SPE.

"**PSB Data**": data held by a Data Holder.

"**Re-User**": the Applicant who has obtained an Authorisation.

"**Regulations**": the legal and regulatory texts relating to the re-use of Target Data, in particular:

- the Law of 19 December 2025 establishing the Government Commission for data sovereignty and designating the competent bodies and authorities provided for in Articles 7, 13 and 23 of Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) and the single information point provided for in Article 8 of Regulation (EU) 2022/868 and amending the Law of 1 August 2018 on the organisation of the National Commission for Data Protection and the general data protection framework,

- the DGA,

- Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (European Health Data Space Regulation), and

- all other texts with equivalent or similar effect or in the field of artificial intelligence.

"**SIE**": the secure IT environment composed of the SPE and the IPE.

"**SPE**": the secure processing environment foreseen by the DGA, including the organisational means put in place to ensure compliance with Union and Luxembourg law.

"**State**": the State of the Grand Duchy of Luxembourg.

"**Subsequent Application**": an application submitted to the CGSD by a Re-User having obtained an Authorisation, in particular for the extension of the Authorisation Duration, the replacement, addition or removal of a User, the integration of an External Technological Solution, the standby or early closure of the SPE, the export of results or data archiving.

"**Target Data**": PSB Data, and where applicable, External Data, to which Appropriate Measures and possibly additional measures have been applied by the CGSD following an Authorisation and before being made available in the SPE.

"**Technological Solutions**": internal Technological Solutions and, where applicable, External Technological Solutions.

"**Working Data**": data that has been produced in the SPE by the Re-User from the Target Data.

"**User**": any natural person authorised to use the SPE in accordance with the Authorisation.

2. General provisions

2.1. Purpose of the GTC

The GTC establish the framework governing the use of the SIE. The GTC also define the rules applicable to Applications, which constitute a prerequisite for the issuance of any Authorisation.

2.2. Obligation to comply with the GTC

The Re-User undertakes to comply strictly with these GTC. The Re-User further undertakes to impose the same strict compliance on all Users.

The Re-User shall adopt all necessary measures, whether organisational, technical or disciplinary, to ensure full compliance with the obligations set out in the GTC and shall ensure that all Users are subject to the same obligations.

The Re-User acknowledges having read and understood the GTC and having reviewed all related documentation, including the Data Protection Notice set out in Annex 1, and undertakes to communicate all documentation to the Users and to ensure they accept it.

The Re-User shall be liable for any breach of the GTC attributable to the Users, as if it had committed the breach itself.

Without prejudice to any action that may be taken against a User, any breach committed by a User shall be deemed to have been committed by the Re-User.

Where several Re-Users access the same Target Data, such Re-Users shall be held jointly and severally liable for compliance with the GTC.

2.3. Changes to the Terms of Use

The GTC may be amended unilaterally at any time by the CGSD, in particular to take into account legislative or regulatory developments, technical, organisational or operational evolutions of the SIE, or any other adaptation required on grounds of public interest, efficiency or security.

Any amendment to the GTC shall be communicated in advance to the Re-User no later than one (1) month before its entry into force. Such communication shall be made electronically via the Re-User's MyGuichet business eSpace, to the email address of the designated contact point specified in the Initial Application, or by any other durable medium ensuring receipt and storage of the message.

The amendments so communicated shall be deemed accepted by the Re-User unless the Re-User submits a written objection to the CGSD before the date of entry into force specified in the amendment notice.

In the event of an objection, the Re-User shall automatically with immediate effect and without any right of recourse, waive the rights granted under the Authorisation.

Such waiver shall also automatically entail with immediate effect and without any right of recourse, the revocation of all User access to the SPE, and the termination of any right to re-use the Target Data.

The objection—together with its consequences as set out in the preceding paragraphs—shall in no event give rise to any right to compensation.

3. The Application and the assessment thereof by the CGSD

3.1. General provisions

Submitting an Application is a prerequisite for obtaining an Authorisation. Two types of Applications exist, as set out in Clauses 3.2 to 3.3 below.

The Application shall be submitted by the Applicant to the CGSD through the website https://letzdata.public.lu/en.html (the single information point designated in accordance with Article 8(2) of the DGA), which links to the MyGuichet.lu procedure.

The Application must include all information necessary for its assessment. The Applicant undertakes to provide the CGSD with all documents, materials and information requested by the CGSD. The Applicant is responsible for identifying in the Application the resources required to perform the processing operations planned within the SPE, as well as any Technological Solutions the Applicant wishes to have made available in or integrated into the SPE.

The CGSD may refuse an Application:

- on grounds of public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or any other grounds provided for in the Regulations;
- where the integration of an External Technological Solution into the SIE is impossible or would require disproportionate effort, or for any other duly justified reason;
- where any past Incident, or risk of Incident, was attributable to the Re-User, including any risk to the confidentiality of the Target Data, the Working Data or the Technological Solutions, in particular where such risk concerns public policy, national defence secrecy, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or any other grounds provided for in the Regulations;
- where the Re-User's past conduct harmed, or was likely to harm, the integrity, reputation or continuity of the activities of the CGSD or its processors;
- in the event of a negative impact on the SIE;
- where the Re-User previously failed to comply with the GTC or with an Authorisation;
- where the Re-User has previously infringed applicable legal or regulatory provisions, in particular those relating to public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties,

confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the re-use of PSB Data, or any other law applicable to the Re-User or the Users.

The time limit for assessing the Application, as set out in the Regulations, begins only once the CGSD has received all information necessary to determine whether an Authorisation can be granted.

3.2. Initial Application

The purpose of the Initial Application is the re-use of data referred to in Article 3(1) of the DGA. It may also include an application for the integration of an External Technological Solution and an application for archiving.

3.3. Subsequent Application

After obtaining an Authorisation, the Re-User may submit a Subsequent Application.

The Subsequent Application may relate to:

- the extension of the Authorisation Duration;
- the replacement, addition or removal of a User;
- the integration of an additional or alternative External Technological Solution;
- the temporary deactivation of the SPE;
- the export of results;
- archiving (where archiving was not request in the Initial Application) or amending the archival period;
- the early closure of the SPE.

Subsequent Applications must be submitted no later than three (3) months before the expiry of the Authorisation Duration.

3.3.1. Extension of the Authorisation Duration

The Re-User may request the extension of the Authorisation Duration by submitting a Subsequent Application.

Any such extension requires an Authorisation from the CGSD, which shall decide at its full discretion, taking into account technical, organisational and resource constraints.

If no Authorisation is granted, the initial Authorisation Duration remains applicable, and the Re-User shall have no right to an extension.

3.3.2. Replacement, addition or removal of a User

No more than ten (10) Users can be authorised to access the SPE under a single Authorisation.

Any replacement, addition or removal of a User requires a Subsequent Application and the issuance of a corresponding Authorisation.

Each such application must include all necessary supporting documentation, particularly documents that enable the identification of the Users concerned and their entitlement to access the SPE.

The Re-User shall notify the CGSD if a User is no longer entitled to access the SPE upon which the CGSD shall revoke such User's access.

3.3.3. Integration of an additional or alternative External Technological Solution

An application for the integration of an External Technological Solution seeks the integration of that solution into the SPE. The Re-User may, including after a solution has been integrated following the Authorisation of an Initial Application, subsequently request the addition of an External Technological Solution or the replacement of an alternative External Technological Solution through a Subsequent Application, which shall be subject to an Authorisation.

The integration of an External Technological Solution shall be subject to a prior assessment by the CGSD. For this purpose, the CGSD may, at its discretion, require the Applicant to procure, at its own expense, an audit carried out by a third party designated by the CGSD.

The Re-User remains responsible for any External Technological Solutions integrated into the SPE pursuant to the Authorisation.

3.3.4. Temporary deactivation of the SPE at the request of the Re-User

The CGSD may approve an application for temporary deactivation of the SPE for duly justified reasons. The application must indicate:

- the reasons justifying the temporary deactivation;
- the start date of the requested temporary deactivation period;
- the expected end date of that period.

The temporary deactivation requires a Subsequent Application and the issuance of a corresponding Authorisation which will indicate the effective date of temporary deactivation of the SPE.

Neither an application nor an Authorisation for temporary deactivation of the SPE entails the extension of the Authorisation Duration.

Temporary deactivation of the SPE automatically results in:

- the temporary deactivation of all User access to the SPE and the inability to use the SPE; and
- the transfer and storage of Target Data, Work Data and Technological Solutions in the archiving environment of the SIE for the duration of the temporary deactivation, to allow for the secure storage of these items.

Unless the Re-User has requested the early termination of the SPE in accordance with clause 3.3.7, the SPE will only be reactivated following the submission of a Subsequent Application and the subsequent issue of an Authorisation specifying the date of reactivation of the SPE. Upon Authorisation, the CGSD shall proceed to reactivate the SPE and:

- restore User access to the SPE, subject to the terms of the applicable Authorisation;
- restore Target Data, Work Data and Technological Solutions from the archiving environment of the SIE, subject to the terms of the applicable Authorisation.

Upon reactivation of the SPE:

- the Technological Solutions may have become obsolete or unavailable, or may no longer have the same functional, technical or security characteristics as at the time of temporary deactivation;
- Target Data or Work Data may have become obsolete or unavailable, or may no longer have the same functional, technical or security characteristics as at the time of temporary deactivation; and
- CGSD resources initially allocated to the Re-User may have been reallocated and may no longer be available.

Any such unavailability, modification, or obsolescence of Technological Solutions, Target Data, or Work Data shall not give rise to compensation for the Re-User or the Users. The CGSD shall not be liable for any inability to restore the SPE in its original state, or for any loss, alteration, unavailability, or obsolescence of Technological Solutions, Target Data or Work Data, regardless of cause.

The Re-User irrevocably waives all appeals, claims or actions against the CGSD arising out of or in connection with any loss, alteration, unavailability, or inability to restore the SPE, in whole or in part.

Temporary deactivation of the SPE is subject to applicable Fees, as set out in the Fee schedule.

3.3.5. Export of results

Only anonymised results may be exported from the SPE.

Any export of results requires a Subsequent Application and the issuance of a corresponding Authorisation.

Prior to issuing a decision on such application, the CGSD shall assess whether the Re-User has implemented appropriated anonymisation measures for the results proposed for export.

For the purposes of this assessment, the Re-User shall:

- transfer the anonymised results for which export is requested to the designated area within the SPE,
- provide the CGSD with all information and documentation relating to the creation of and anonymisation methods used for the results, in sufficient detail to enable the CGSD to assess, amongst others, the adequacy and effectiveness of the measures applied.

The CGSD shall notify the Re-User of its decision in writing. The CGSD reserves the right to prohibit the use of results containing information jeopardising the rights and interests of third parties. Such protected interests and rights include, but are not limited to, public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or any other rights protected by the Regulations.

Where the CGSD authorises the export of results from the SPE, the CGSD shall make the anonymised results available to the Re-User and provide the necessary instructions for retrieval. The Re-User must

download the results within fifteen (15) days from the date they are made available, after which the results will no longer be available for download.

3.3.6. Archiving

The Re-User may submit a Subsequent Application to request:

- archiving of Target Data, Work Data or Technological Solutions not already covered by an Authorisation, or
- the amendment of the applicable archival period.

Any archiving of Target Data, Work Data or Technological Solutions, including the archival period, is subject to and defined in the applicable Authorisation.

Archiving services are subject to applicable Fees, as set out in the Fee schedule.

3.3.7. Early closure of the SPE at the request of the Re-User

The Re-User may request the early closure of the SPE prior to the end of the Authorisation Duration by submitting a Subsequent Application.

In order for such application to be processed by the requested closure date, the application must be submitted at least one (1) month before the intended effective date. The Re-User is responsible for exporting results in accordance with Clause 3.3.5. and performing any actions necessary for archiving Target Data, Work Data and Technological Solutions deemed necessary in accordance with Clause 3.3.6, prior to the effective date of closure.

Early closure of the SPE shall have the same legal and operational effect as the expiration of the Authorisation Duration.

3.4. New Initial Application

Any substantial amendment of an Authorisation requires the submission of a new Initial Application. It cannot be requested through a Subsequent Application. The CGSD has full discretion to determine whether a requested amendment is substantial. Substantial amendments include, but are not limited:

- the addition of data not covered by the existing Authorisation,
- the addition of categories of data subjects as defined by the GDPR,
- the amendment of authorised purposes or the addition of new purposes not covered by the Authorisation; or
- a change of the Re-User.

4. Communications between the CGSD and the Re-User

All communications between the Re-User and the CGSD, notably those relating to Applications or the use of the SIE, shall be made through the Re-User's *MyGuichet* business eSpace or via the contact email address provided in the Initial Application.

Any information, notification, decision, or other communication made available in the *MyGuichet* business eSpace shall be deemed received by the Re-User on the date it is made available by the CGSD, without any need for any confirmation or acknowledgement of receipt.

The Re-User shall review all communications made available in the *MyGuiche*t business eSpace area.

The CGSD shall not be liable for any consequences resulting the Re-User's failure or delay in consulting such communications.

5. Modalities of operation

5.1. How to connect to the SPE

Access to the SPE is subject to the use of a strong authentication method.

Access to the SPE is personal, confidential, non-transferable, and linked to a named User. Access may be granted subject to the provision of additional documentation, which will be requested from the Re-User and from each User following the issuance of the Authorisation.

The Re-User shall ensure that Users do not disclose or share their access credentials with third parties and do not access the SPE by any means other than those duly authorised by the CGSD. Only Users expressly designated in the applicable Authorisation may access the SPE. Granting any third party not covered by the Authorisation access to the SPE, Target Data or Work Data, or otherwise making such data available to any such third party is strictly prohibited. The Re-User shall ensure compliance with these requirements and shall implement all necessary technical and organisational measures to prevent any unauthorised use of Target Data and Work Data.

The CGSD shall maintain identifiable logs of access to and activities within the SPE for monitoring, auditing and compliance purposes. These records shall be retained by the CGSD for a minimum period of five (5) years.

Any connection to the SPE from a country outside the European Economic Area must comply with the requirements set out in Clause 17.

5.2. Transmissions of External Data and PSB Data to the CGSD after Authorisation

After an Authorisation has been granted and prior to the integration of Target Data into the SPE, External Data and PSB Data must be submitted to the CGSD through the IPE for evaluation and to allow the CGSD to:

- apply the Appropriate Measures;
- test the Appropriate Measures applied; and
- apply additional measures where the Appropriate Measures prove insufficient or inadequate to ensure respect for protected interests and rights, including, but not limited to, intellectual property rights, commercial confidentiality, including trade secrets, professional or business secrets, statistical confidentiality or the proper functioning of the SPE.

To this end, the CGSD shall request the transmission of the relevant PSB Data from the Data Holder and, where appropriate, the relevant External Data from the Re-User through a secure channel designated by the CGSD. The Data Holder and, where applicable, the Re-User shall comply with all obligations set out in Annex 2.

5.3. Integration of Target Data and External Technological Solutions in SPE

Under the Authorisation, the CGSD integrates Target Data and External Technological Solutions into the SPE for access by the Users.

The Authorisation Duration defined in the Authorisation begins on the date on which the first User is granted access to the SPE. From this date, the Re-User shall have one (1) calendar month to review the usability, consistency and accuracy of the Target Data and External Technological Solutions and to report, within the same period and providing sufficient details of the claims, any inconsistences or discrepancies. Upon expiry of this period, the Re-User irrevocably waives any right of action, claim or remedy against the CGSD in connection with the Target Data and External Technological Solutions integrated into the SPE, in particular with respect to their quality, completeness and accuracy.

Target Data may differ from or vary in relation to the data requested. Similarly, certain categories of data may be pseudonymised, anonymised or deleted, in full or in part, when applying additional measures where the Appropriate Measures are not sufficient to ensure compliance with public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or any other applicable law. Such measures do not affect the validity of the Authorisation nor the Re-User's obligation to pay applicable Fees.

Upon expiry of the one (1) calendar month period referred to above, the Target Data and External Technological Solutions in the IPE shall be automatically, irrevocably and definitively destroyed, without prejudice to the possibility that CGSD might retain all or part of the Target Data or the information obtained in the context of the Authorisation. The destruction of Target Data and External Technological Solutions shall not give rise to any right to compensation. The Re-User waives any right of action, claim or remedy against the CGSD arising from or in connection with such destruction.

6. Temporary unavailability of SPE

The CGSD may, at any time and it its sole discretion, modify, develop or maintain the Technological Solutions and the SPE.

The Re-User acknowledges and accepts that such operations may, depending on their nature, result in a planned or unplanned temporary unavailability of the SPE.

Where such unavailability is foreseeable, in particular in the event of scheduled maintenance, updates, technological developments, security requirements or any other operational need, the CGSD may temporarily limit or deactivate User access to the SPE, subject to prior written notice to the Re-User, specifying the reason, the effective date and the estimated duration of the unavailability.

The Re-User acknowledges and accepts that an unplanned temporary unavailability may occur, including due to technical incidents, security constraints, unforeseen malfunctions or any other legitimate reason in order to ensure the proper functioning, integrity or security of the SPE. In this case, the CGSD may intervene without prior notice.

Whether foreseeable or unforeseeable, any temporary unavailability of the SPE shall not entitle the Re-User or the Users to any compensation or extension of the Authorisation Duration, nor to any other remedy whatsoever.

7. Suspension and revocation of SPE use

7.1. Suspension of access to SPE

The CGSD may suspend access to the SPE with immediate effect and without prior notice:

- on grounds of public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or other reasons as provided for in the Regulations;
- where an Incident, or risk of Incident, attributable to the Re-User has occurred, including any risk to the confidentiality, integrity, or security of the Target Data, Work Data, or Technological Solutions, or the SPE (in particular an infringement or risk of infringement of public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or any other rights protected by the Regulations;
- where the conduct of the Re-User harms, or is likely to harm, the integrity, reputation or business continuity of the CGSD or its processor;
- in the event of a negative impact on the SIE;
- in the event of any breach by the Re-User of these GTC or the terms of an Authorisation;
- where Users lack the training, technical competence, or required authority, powers or delegations necessary to use the SPE;
- in the event of non-compliance by the Re-User with applicable legal or regulatory provisions, particular those relating to public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the re-use of PSB Data, or any other legislation applicable to the Re-User or the Users.

The Re-User shall be informed as soon as possible of the reasons for the suspension and, where applicable, of any measures required to remedy the situation.

Any suspension of access to the SPE automatically results in the suspension of access for all Users and the inability to use the SPE.

The CGSD may, at its sole discretion, lift the suspension and restore access to the SPE. The CGSD may also condition the lifting of the suspension on the prior implementation by the Re-User of corrective measures deemed necessary to ensure the continued effectiveness of the Appropriate Measures and, where applicable, any additional measures referred to in Clause 5.2.

Suspension shall not give rise to any right to compensation.

The CGSD reserves the right, at any time, including during a suspension period, to permanently revoke access to the SPE in accordance with Clause 7.2.

7.2. Revocation of access to SPE

The CGSD may revoke Users' access to the SPE in the cases provided for in Clause 7.1. where the relevant event arises after the issuance of the Authorisation, or in the following cases:

- where the non-compliance or the Incident which led to the suspension has not been corrected within the time limit imposed by the CGSD;
- where the nature, gravity or recurrence of the breach renders compliance with one or more of the terms or conditions of the Authorisation impossible; or
- where continued access is likely to compromise security, including of the Target Data, the Work Data, the Internal Technological Solutions or the SPE, regulatory compliance or the rights of third parties.

The revocation decision is notified to the Re-User and automatically results in the revocation of all Users' access to the SPE. Upon revocation, the CGSD may also destroy the SPE, including the Work Data and the External Technological Solutions.

The destruction of the SPE, the revocation of access rights to the SPE or the impossibility for the Re-User or Users to use the SPE shall not give rise to any right to compensation for the Re-User or Users.

7.3. Effects of suspension or revocation

The CGSD shall not be held liable for any direct or indirect, material or non-material, damages suffered by the Re-User or Users arising from or in connection with any suspension or revocation of access to the SPE.

Suspension or revocation does not extend the Authorisation Duration.

All costs associated with restoration of access, remediation, or reactivation of the SPE shall be borne exclusively by the Re-User. Suspension or revocation shall not affect the Re-User's obligation to pay any applicable Fees.

8. Expiry of the Authorisation Duration and the archival period

8.1. Expiry of the Authorisation Duration

Subject to Clause 3.3.1, the Re-User's right to process Target Data and Work Data carried out by Users in the SPE, as well as Users' access to the SPE, shall automatically terminate upon expiry of the Authorisation Duration, without any further notice or formality. Upon such expiry, the CGSD may destroy the SPE, including the Work Data and the External Technological Solutions.

8.2. Expiry of the archival period

Upon expiry of the archival period provided for in the Authorisation, the CGSD may destroy the archived Target Data, Work Data or Technological Solutions, without further notice or formality.

9. Purposes, Re-Users, Privacy, Prohibitions

9.1. General provisions

The Re-User shall ensure that the Target Data is processed within the SPE solely for the purposes and in accordance with the conditions set out in the applicable Authorisation.

The Re-User is solely responsible for ensuring that all Users possess the necessary training, technical knowledge and as the necessary authority, powers and delegations for proper use of the SPE.

Any failure to comply with these instructions may result, at the sole risk of the User and/or the Re-User, in operational issues, including the inability to achieve purposes as set out in the Authorisation and may lead to the in suspension or revocation of access to the SPE.

9.2. Confidentiality obligation

The Re-User is bound by a confidentiality obligation prohibiting the disclosure of any information jeopardising the rights and interests protected by applicable law that the Re-User may have acquired despite the safeguards put in place by the CGSD in accordance with applicable law. The Re-User shall implement appropriate technical and organisational measures to prevent any unauthorised re-identification or re-use of data. Such protected interests and rights include, but are not limited to, public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or any other rights protected by the Regulations.

Without limitation, the Re-User and Users are strictly prohibited from:

- re-identifying or attempting to re-identity any data subject to whom the Target Data or Work Data relate or to infringe the aforementioned rights. The Re-User shall take the necessary technical and operational measures to ensure compliance with these obligations;
- consulting, using or attempting to use the Target Data for purposes other than hose expressly authorised in the Authorisation; and
- copying, extracting or reproducing Target Data or Work Data outside the SPE, or attempting to do so by any means, including by taking screenshots, recordings or photographs of Target Data or Work Data.

This confidentiality obligation shall apply throughout the Authorisation Duration and shall subsist after its termination, whatever the reason for the termination, for an unlimited period, except where expressly required otherwise by law.

9.3. Obligation to communicate any changes affecting the Authorisation

The Re-User shall ensure that all information provided to the CGSD, including information relating to itself, its personnel, Users, subcontractors, and any persons acting on its behalf or at its service, is accurate, complete, and kept up to date.

The Re-User shall notify the CGSD of any changes that may affect such information, including, without limitation:

- any change in its legal status, registered office, corporate purpose, or any other information relevant to the CGSD, and shall provide all necessary supporting documentation; or
- any temporary or permanent departure of a User, in which case the Re-User shall submit a Subsequent Application for the removal of such User in accordance with Clause 3.3.2.

9.4. Use of SPE

The Re-User shall:

- not disable, disrupt, circumvent or attempt to circumvent any technical or organisational elements or measure of or implemented within the SPE;
- use the SPE in compliance with applicable laws and regulations, and generally accepted industry practices, and act in good faith;
- cooperate with the CGSD and any party designated by the CGSD; and
- ensure that its personnel, Users, subcontractors, processors and any other person acting on its behalf or involved in the use of the SPE comply with obligations equivalent in scope and effect to those set out in these GTC.

9.5. Obligation to communicate any Incident or infringement of rights

The Re-User shall, without undue delay, notify the CGSD of any Incident and of any infringement of rights and interests protected by application legislation. Such protected interests and rights include, but are not limited to, public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or any other rights protected by the Regulations.

In the event of a personal data breach, the Re-User shall fully cooperate with the CGSD and provide with all necessary assistance to enable the CGSD to comply with its legal obligations, including those laid down in Articles 33 and 34 of the GDPR.

The Re-User shall employ any means necessary when assisting the CGSD:

- when the Incident is notified to the competent authorities and, if applicable, when communicating it to the data subject; and
- in collecting and providing all information necessary for such notifications, including:
    - the nature of the personal data concerned as well as the categories and approximate number of persons impacted;
    - the likely consequences of the Incident; and
    - the measures taken or proposed to be taken to address the Incident and mitigate its effects.

9.6. Obligation to communicate any re-identification

Without prejudice to the obligations imposed under the GDPR, the Re-User shall immediately notify the CGSD of any re-identification of data subjects within the meaning of the GDPR.

Such notification shall, at a minimum, contain the following elements:

- a description of the nature of the personal data breach, including, where possible, the categories and approximate number of persons affected by the personal data breach and the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point from whom additional information can be obtained;
- a description of the likely consequences of the personal data breach;
- a description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10. Control and audit by the CGSD

10.1. General provisions

The CGSD may, at any time, verify the use of the SPE, the Technological Solutions and the processes, means and any result of the processing of Target Data carried out by the Re-User and Users, including in the event of use of an archiving solution, in particular to ensure compliance with these GTC GCU, applicable law and the rights and interests protected by applicable law. Such protected interests and rights include, but are not limited to, public policy, national defence secrecy, protection of rights and interests safeguarded under international, European or national law, protection of personal data, protection of intellectual property rights, protection of rights of third parties, confidentiality (including trade secrets, professional secrecy, business secrets or statistical confidentiality), cybersecurity, competition law, the proper functioning of the SIE, or any other rights protected by the Regulations.

Upon written request of the CGSD, the Re-User shall allow and contribute to audits of activities carried out in the SPE.

The CGSD may conduct such audit directly or may appoint an auditor of its choice. Audits may also include on-site inspections of the premises or facilities of the Re-User and Users and shall, where appropriate, be conducted subject to reasonable prior notice.

The User shall make available to the CGSD all information necessary to demonstrate compliance with the obligations set out in the GTC and arising directly or indirectly from applicable law.

The CGSD shall make available to the Re-User all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and shall immediately inform the Re-User if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

10.2. Post-Authorisation Audits for External Technological Solutions

The CGSD may at any time verify compliance between the External Technological Solutions and those covered by the Authorisation.

The CGSD may, in the event of a discrepancy between the External Technological Solutions and those authorised in the Authorisation, invite the Re-User to comply with the provisions of that Authorisation.

11. Advertising

The Re-User undertakes to acknowledge the assistance of the CGSD in each publication relating to the results exported from or the related work carried out within the SPE.

The CGSD may use, publish, communicate, disseminate, transmit or otherwise make available to the public any information in connection with the Applications or Authorisations, where it considers such disclosure expedient, in particular in order to respond to a request or query made in accordance with applicable law, including in the context of the exercise of individual rights within the meaning of the GDPR.

Such information may include, but is not limited to:

- the contact details of the Re-User;
- a summary of the Application;
- the Authorisation, as well as any refusal decision adopted by the CGSD;
- the CGSD personal data information notice; and
- a copy of the Re-User's information intended for data subjects in accordance with Articles 12 to 14 of the GDPR, as provided by the Applicant or the Re-User.

12. Exclusion of warranty and support

The SPE is made available to the Re-User on an "as is" and "as available" basis, without any express or implied warranty of any kind. The CGSD does not provide any warranty regarding the performance, continuous availability, error-free operation, security, compatibility or suitability of the SPE for any particular purpose or for the specific needs of the Re-User or Users.

The CGSD does not warrant that the SPE will operate without interruption, nor that the functionalities made available shall meet the expectations of the Re-User or Users or be free from technical defects, vulnerabilities or incompatibilities.

The Re-User shall adopt all necessary measures to secure access by the Users, to protect Target Data, Work Data and Technological Solutions and to ensure that its use of the SPE complies with all applicable legal, regulatory or contractual requirements.

The Re-User is solely responsible for the propre and compliance use of the SPE. The CGSD does not provide support or assistance relating to the use of the SPE and the Re-User shall ensure that it can use of the SPE and that the use is compatible and compliant with its needs and obligations.

13. Responsibility

The obligations of CGSD and the CTIE under the GTC constitute obligations of means only (*obligations de moyens)*, and no specific result or outcome is guaranteed.

For the civil liability of the CGSD or CTIE to be incurred, it must be demonstrated the damage suffered was caused by serious negligence (*négligence grave)* in the choice and application of the means used by the CGSD or CTIE for the performance of their statutory public service tasks.

Any compensation payable to the Re-User shall, in any event, be limited to an amount not exceeding one (1) time the Fee paid under the relevant Authorisation.

14. Fees and invoicing

The use of the SPE shall be subject to the prior payment of the Fee, in accordance with the time limits set out in the Authorisation.

Payment of the Fees shall be made electronically, using the payment methods specified in the Authorisation.

Any delay in payment or failure to pay shall automatically without prior formal notice, result in the application of statutory interest and may, where applicable, lead to the suspension or revocation of access to the SPE, without prejudice to any legal recovery measures available under applicable law.

Any modification of the amount of the Fees shall be communicated to of the Re-User in writing in accordance with Clause 4.

15. Intellectual property

15.1. State intellectual property rights

The Re-User shall not acquire or benefit from any intellectual property rights in the SIE or in any other solution developed or used in the framework of the Regulations, except as expressly provided in Clause 15.2.

Re-Users are strictly prohibited from:

- modifying, altering, falsifying, repairing, copying, reproducing, adapting, distributing, displaying, publishing, reverse engineering, translating, disassembling, decompiling, or attempting to create source code derived from Target Data or Internal Technological Solutions, or otherwise creating derivative products based on Target Data or Internal Technological Solutions, without the State's express prior authorisation;
- assigning, in whole or in part, the licence granted by the State or any rights or obligations arising therefrom to any third party, whether for consideration or free of charge; or
- making the SPE available to any person not expressly authorised.

15.2. Intellectual Property Rights of the Re-User

The Re-User represents and warrants to the CGSD that it:

- holds all the intellectual property rights, exclusive rights or licenses necessary for the External Technological Solutions operated and developed by the Re-User in the SPE;
- has obtained all licenses, consents and authorisations required for the re-use of PSB Data or External Data protected by intellectual property rights; and
- does not infringe the intellectual property rights of the State, of PSB Data Holders, of Data Holders of External Data or of any third parties.

16. Protection of personal data

16.1. The CGSD as controller

In its capacity as the competent body under the applicable legal framework, the CGSD acts as the sole and exclusive controller, within the meaning of the GDPR, for the processing of PSB Data, External Data and Target Data constituting personal data that it carries out in the context of the implementation of the Regulations and the tasks conferred on it by applicable, including, but not limited to:

- processing applications;
- publishing necessary documents, such as the Authorisation;
- implementing Appropriate Measures and additional measures, where required;
- structuring Target Data constituting personal data in accordance with applicable law and the Authorisation; and
- setting up and managing the SIE.

16.2. The Re-User as controller

With regard to Target Data and Work Data constituting personal data, the CGSD acts, in accordance with applicable data protection law and Article 10 of the Law of 19 December 2025 establishing the CGSD, as a processor of the Re-User, who acts as controller.

No processing relationship, whether express or implied, shall be deemed to exist on the part of the CGSD. Any processing activities not expressly referred to in the Authorisation and these GTC must be formalised in a separate agreement compliant with the GDPR, which the CGSD may freely refuse without compensation due for the Re-User.

16.2.1. Key elements of the processing activities by the CGSD: subject matter and duration of processing, nature and purpose of processing, type of personal data and categories of data subjects

The purpose, duration, nature and purpose of the processing activities, the type of personal data and the categories of data subjects are those set out exhaustively in the Authorisation.

16.2.2. Instructions from the Re-User to the CGSD

The CGSD, acting in its capacity as Processor on behalf of the Re-User, processes Target Data and Work Data constituting personal data solely in accordance with the Authorisation or any other agreement concluded between the CGSD and the Re-User.

The CGSD, acting in its capacity as Processor on behalf of the Re-User, processes Target Data and Work Data constituting personal data solely in accordance with the Authorisation or any other agreement concluded between the CGSD and the Re-User.

The CGSD shall promptly inform the Re-User if, in its opinion, any instruction constitutes a breach of the GDPR or other applicable provisions of Union or Luxembourg data protection law.

Where the CGSD is required to carry out additional processing activities on Target Data or Work Data constituting personal data under Union or Luxembourg law, it shall inform the Re-User prior to such processing, unless the relevant legislation prohibits such notification on important grounds of public interest.

The Re-User and the CGSD agree that the Authorisation, read in conjunction with the GTC, constitutes the Re-User's documented instructions to the CGSD for the processing of Target Data and Work Data constituting personal data in the context of the processing relationship.

The CGSD reserves the right to refuse to comply with any instruction from the Re-User that is not covered by the GTC or the Authorisation, or that does not comply with Union or Luxembourg law.

Any instruction not covered by—or contrary to—the Authorisation must be the subject of a prior written agreement between the Re-User and the CGSD. Where the CGSD refuses such an instruction,

the Re-User may request early closure of the SPE in accordance with Clause 3.3.7 of the GTC, without giving rise to any right to compensation.

The CGSD shall assist the Re-User, through appropriate technical and organisational measures and insofar as possible, in complying with its obligation to respond to data subject requests to exercise their rights provided for under Chapter III of the GDPR.

The Re-User instructs the CGSD to delete all Target Data and all Work Data constituting personal data subject within the meaning of the GDPR, processed on the basis of an Authorisation, at the end of the Authorisation Duration, and to destroy all existing copies, unless Union or Luxembourg law requires their retention.

16.2.3. Security of processing of personal data

The staff of the CGSD are subject to statutory confidentiality obligations.

The CGSD implements the necessary measures required under applicable law, including those identified in the general impact assessment performed at the time of adoption of the applicable legislation within the meaning of Article 35(8) GDPR, as well as the Appropriate Measures and, where applicable, additional measures, read in conjunction with the GTC.

Assistance provided by the CGSD to the Re-User in relation to compliance with Articles 32 to 36 of the GDPR shall be provided exclusively upon request of the Re-User.

Upon request, the CGSD shall provide the information necessary to demonstrate compliance with Article 28 of the GDPR, unless such information concerns:

- the implementation by the CTIE of its statutory obligations under the Law of 20 April 2009 establishing the Government IT Centre;
- external relations or State security, including IT infrastructure and systems, or public order;
- the safety of individuals or the protection of privacy;
- the conduct of proceedings before a judicial, extrajudicial or disciplinary authority, or preliminary steps thereto;
- the prevention, investigation or prosecution of criminal offences;
- an intellectual property right;
- secrecy or confidentiality protected by law;
- control, inspection or regulatory missions of a State administration or service, a municipality, a municipal syndicate, a public establishment under State or municipal supervision, or a legal person providing a public service;
- the confidential nature of commercial or industrial information communicated to a public authority;
- the ability of authorities to conduct their economic, financial, fiscal or commercial policy where disclosure would hinder related decision-making processes;
- the confidentiality of deliberations of the Luxembourg Government.

In the event of a disagreement regarding the security measures applied to the SPE by the CGSD in accordance with applicable law, the Re-User may request early closure of the SPE in accordance with Clause 3.3.7, without giving rise to any right to compensation.

16.2.4. Authorised processing

The CGSD may sub-contract to the CTIE all or part of the processing activities relating to Target Data and Work Data constituting personal data. The CTIE may, in turn, engage external service providers whose identity shall not be disclosed to the Re-User.

The Re-User grants the CGSD a general authorisation to use additional processors, without giving rise to any right to compensation, including in the event of opposition by the Re-User.

The CGSD shall ensure that the same data protection obligations as those set out in these GTC are imposed on any processor engaged by the CGSD under a contract or other legal act under Union or Member State law, in particular with regard to offering sufficient guarantees regarding technical and organisational measures to ensure that the processing complies with the GDPR.

The CGSD shall inform the Re-User in writing of any planned change concerning the addition or replacement of the CTIE by another processor.

The Re-User may object to the replacement of the CTIE within one (1) week of being informed accordingly. If no objection is raised within this period, the change is deemed accepted. Any objection shall result in early closure of the SPE in accordance with Clause 3.3.7.

17. International transfers

17.1. Non-personal data

Where the Re-User intends to transfer Target Data or Work Data constituting non-personal data protected for the reasons referred to in Article 3(1)(a) to (c) of the DGA to a third country, the Re-User must inform the CGSD of this intention and of the purpose of the transfer in the Application.

Any transfer of such non-personal data not authorised in the Authorisation is strictly prohibited.

17.2. Personal data

Where Target Data or Work Data constituting personal data is transferred to a third country, the provisions of Annex 3 (Modules 1 and 4) shall apply.

Any transfer of such personal data to a third country or an international organisation shall comply with Chapter V of the GDPR and shall require an Authorisation.

Any transfer of personal data not authorised by an Authorisation is strictly prohibited.

18. Interpretation and nullity

Unless expressly stated otherwise, any reference to Clauses refers to the Clauses of the GTC.

The Annexes form an integral part of the GTC.

The titles of the Clauses of the GTC are for convenience only and shall not affect their interpretation.

Unless the context clearly indicates otherwise, any use of the singular in the GTC shall be deemed to include the plural and vice versa.

Any reference to a law or regulation, or to any of its provisions, shall be construed as a reference to that law, regulation, or provision as amended, recast, re-adopted, or as it may be in the future.

If any Clause of the GTC is held to be illegal, invalid, or unenforceable, in whole or in part, pursuant to a mandatory legal provision or a decision of a competent authority or court, that Clause shall be deemed not to form a part of the GTC, without affecting the legality, validity, or enforceability of the remainder of the GTC.

Any reference in the GTC to the Re-User shall also be deemed to include the Users, unless the context requires otherwise.

19. Applicable law and jurisdiction

The relationship between the CGSD and the Re-User, the GTC, and all Annexes shall be governed exclusively by the laws of the Grand Duchy of Luxembourg, to the exclusion of conflict-of-law rules.

All disputes shall fall under the exclusive jurisdiction of the courts of Luxembourg City.

ANNEX 1 - GDPR INFORMATION NOTICE

Data protection notice for Re-Users, Users and Data Holders regarding processing activities carried out by the Government Commission for data sovereignty

The Regulations allow a Re-User to submit an Application for re-use of data in order to obtain an Authorisation from the CGSD.

The purpose of this data protection notice is to inform the relevant individuals about the processing activities carried out by the CGSD within the context of:

- the management of an Application,
- the management of an Authorisation or refusal decision,
- the collection of PSB Data and External Data following the issuance of an Authorisation,
- the provision of the SPE.

1. Contact details of the CGSD and its data protection officer

The CGSD collects and processes personal data in the course of performing its tasks of public interest and for compliance with its legal obligations.

The contact details of the CGSD, acting as controller, are:

> Government Commission for data sovereigntyAddress: 5, rue Plaetis, L-2338 Luxembourg
> Tel.: +352 247-67700
> E-mail: ald@cgsd.etat.lu

For any question concerning the processing of your data, please contact our data protection officer:

- by e-mail: dpo@cgsd.etat.lu
- by post: 5, rue Plaetis, L-2338 Luxembourg

2. Lawfulness and purposes of processing

2.1. Lawfulness of processing

The CGSD processes your data on the basis of:

- its tasks carried out in the public interest and the legal obligations applicable to the exercise of its activities and missions, in particular the following legislation:
    - the Law of 19 December 2025 establishing the Government Commission for data sovereignty,
    - the DGA,
    - Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (European Health Data Space Regulation),
    - the Law of 1 December 1978 governing non-contentious administrative procedure and the Grand-Ducal Regulation of 8 June 1979 on the procedure to be followed by State and municipal administrations,

- the Law of 17 August 2018 on archiving,
- the GDPR,
- the applicable legislation governing cooperation in the context of parliamentary inquiries and/or with authorities in the context of police, judicial or disciplinary proceedings;

- its legitimate interests or those of third parties in the following contexts:
  - the monitoring and safeguarding of the security of the CGSD's infrastructures and those of its processors,
  - monitoring for investigation, control and prosecution purposes in cases of suspicion, detection and repression of fraud or irregularities,
  - the production of statistics and reports.

Accordingly, the processing activities carried out by the CGSD are lawful pursuant to Article 6(1)(c), (e) and (f), of the GDPR and, where applicable, Article 9(2)(e), (f), (g) and (j), of the GDPR.

2.2. Purposes for processing

Your data is processed for the following purposes:

- management of Applications and Authorisations, and in particular:
  - the pre-filling of Subsequent Applications,
  - the publication of CGSD decisions,
  - the invoicing of Fees,
  - communications between the CGSD and the Applicant/Re-User, as well as other actors who may be involved, such as the Data Holder, the CTIE and the LNDS;

- management of the SIE and the provision of Target Data following the issuance of an Authorisation, and in particular:
  - the receipt of OSP Data and/or External Data transmitted by the Data Holder and/or the Re-User,
  - the application of Appropriate Measures and additional measures,
  - the provision of Target Data in the SPE in accordance with the Authorisation issued by the CGSD,
  - communications between the CGSD and the Re-User, as well as other actors who may be involved, such as the Data Holder and the CTIE;

- performance by the CGSD of its monitoring and supervisory obligations, and in particular:
  - the verification of the processing operations carried out by the Re-User, including those carried out by Users, and the verification of compliance by the Re-User and Users with their legal and regulatory obligations, including those arising from the Regulations and the GTC,
  - the handling of legal files (including disputes, claims, contentious or non-contentious proceedings, amicable procedures, and mediations),
  - compliance management in accordance with applicable regulations, including the management of data breaches and data subject requests under the GDPR,
  - monitoring the information system to verify proper functioning and detect operational anomalies,
  - security, as well as the detection and remediation of Incidents or fraud,

- the identification of irregularities and the conduct of related investigations, monitoring and judicial prosecution,

- ensuring the continuity of the CGSD's activities,
- cooperation with competent authorities,
- the production of statistics and reports,
- records management.

3. Categories of data processed, their sources and recipients

3.1. Categories of data processed

The CGSD processes the following categories of data:

3.1.1. For the Application

- Regarding the Applicant/Re-User:
  - For the contact person: first name(s), last name, role and position, as well as the professional email address. A professional telephone number for the contact person may also be provided;
  - For the persons signing the Application on behalf of the Applicant/Re-User: first name(s), last name(s), position, as well as their signature on the Application;
  - For Users: first name(s), last name, information on their link with the Applicant/Re-User, professional email address, and the country from which the User will access the SPE;
  - When, in the context of an Application, the CGSD requests the Applicant/Re-User to provide an audit for an External Technological Solution: the data contained in the audit report, such as the auditor's first name(s), last name and position;
  - If assistance from the LNDS has been obtained: the professional email address of the LNDS contact person. It is possible to provide the person's first name(s), last name, email address and professional telephone number;

- Regarding the Data Holder:
  - Contact person for a Data Holder: name of the Data Holder, professional email address and telephone number, and, where applicable, the position within the entity. It is possible to provide the contact person's first name(s) and last name;
  - Persons authorised to sign on behalf of the Data Holder: first name(s), last name(s) and position, as well as their signature on the Application.

3.1.2. After the issuance of an Authorisation:

- The personal data of the persons transmitting PSB Data or External Data to the CGSD, at its request via a secure channel, in accordance with Article 5.2. of the GTC:
  - If the Secure Transport ("ST") solution is used:
    - the data necessary to connect to the secure channel for data transmission:
      - ID Token, which may contain the e-mail, last name, first name, and IAM ID or national identification number (13-digit *matricule)* (depending on how clients use the ID Token authentication; see specific terms of use), as well as the organisation's name;

            - where the transfer is carried out between external organizations: IP address and domain name.
        - technical logs.
    - If the OTX solution is used:
        - for accessing the OTX solution:
            - IP addresses;
            - browser information;
            - cookies;
            - user identifier (when the user is logged in);
        - for creating OTX requests:
            - subject;
            - type;
            - subtype;
            - request token;
            - request creation timestamp;
            - request expiry timestamp;
            - user identifier (when the user is logged in);
            - recipients' email addresses;
            - recipients' phone numbers (only for a specific type of request);
            - full name of the request creator;
            - email address of the request creator;
            - IAM ID.
        - for uploading and downloading of files:
            - checksum;
            - content type;
            - original file name;
            - size;
            - file token;
            - token download timestamp;
            - user identifier (when the user is logged in);
        - for logging of file uploads and downloads:
            - IP addresses;
            - file upload/download timestamp;
            - user identifier (when the user is logged in);
        - for email notifications:
            - email address;
            - email address addition timestamp;
            - email address notification timestamp;
            - user token;
            - token creation timestamp;
            - user identifier (when the user is logged in);

- The personal data of Users relating to the access to and use of the SPE, notably:
    - identification data (which may include, depending on the User),
        - IAM ID: a user's identifier;
        - last name;

        - first name;
        - email address;
        - job title;
        - date of birth;
        - national identification number;
        - organisation;
        - location;
        - line manager;
        - mobile phone number;
        - mobile phone type;
    - authentication data,
    - technical data relating to the use of the SPE, such as:
        - technical logs (IP addresses, session information);
        - technical logs of the VPN session (IAM ID, Luxtrust certificate data (organisation, last name, first name, SSN)).

3.1.3. General provisions:

From the beginning of the submission of an Application and until the end of the retention period, the CGSD processes:

- data relating to communications with the Applicant/Re-User, the Data Holder, the CTIE and the LNDS, including communications made via the MyGuichet business eSpace, email addresses, and correspondence linked to an Application, an Authorisation or refusal decision, or the use of the SIE;

- technical data, such as IP addresses, connection logs, and data on the use of technical infrastructures, relating to the management of the MyGuichet business eSpace, an Application, or an Authorisation or refusal decision by the Applicant/Re-User; and

- data relating to natural persons involved in the re-use of public sector data originating from audits or other regulatory controls carried out by the CGSD, in accordance with Article 10.1 of the GTC or other obligations imposed on the CGSD.

3.2. Sources

Categories of data not collected directly from you come from the following types of sources:

- the person who created and completed the certification procedure provided the data to the CGSD;
- the national identification number of the person submitting the Application is collected from the national register of natural persons maintained by the CTIE;
- the person who submitted the Application to the CGSD;
- the contact person of the Applicant/Re-User or the Data Holder;
- the LNDS;
- the CTIE;
- where applicable, lawyers or experts.

3.3. Recipients

In carrying out its tasks of public interest and complying with its legal obligations, the CGSD transmits your data to the CTIE as well as to the following categories of recipients:

- other ministries, administrations, public entities or public-sector bodies, as well as international and European Union entities and agencies, in particular;
- its processors;
- third parties external to the public service who are in relation or in contact with the CGSD, such as lawyers or experts.

Your data may also be transmitted to other recipients strictly to the extent necessary.

4. Collection of data from the data subject: mandatory information and consequences of refusal to provide the data

Mandatory information in an Application is indicated by a flag or an asterisk. Failure to provide the required information will result in the Application being rejected.

Unless otherwise stated, the data collected directly from you is mandatory. Refusal to provide the requested data will make it impossible to provide the requested service.

5. Retention periods

Your data strictly linked to the Application will be retained for the period necessary to carry out all administrative tasks related to the management of the Application and, at a minimum, for the duration required to assess the Application and for the CGSD to issue a decision. Data is retained for thirty (30) years from the notification of the final decision or, where applicable, from the end of the period specified in the granted Authorisation (including any applicable data retention period within the archiving service made available after the end of the SPE's period of use), as amended, if relevant.

The retention periods applicable to data processed within the framework of the SIE are as follows:

- For the transfer of PSB Data and, where applicable, External Data:
    - If the Secure Transport ("ST") solution is used:
        - data in transit during an upload: duration of the data's passage through Secure Transport (receipt, virus scan and deposit in S3 storage);
        - data made available for download: maximum retention period of seven (7) days;
        - authentication: duration of the processing of each call (token verification);
        - technical logs (containing ID Tokens): rotation based on volume (seven (7) days) and centralised storage for five (5) years for security reasons.
        - Backup of the file retention system: no backup.
    - If the OTX solution is used:
        - logs (IP address, actions performed, times of actions, IAM ID): four hundred (400) days;
        - requests' metadata: to be defined for each request;
        - uploaded files: until the expiry date specified in the request;

- retention of uploaded files: thirty (30) days after the source files have been deleted.

- For the SPE:
  - User identification: the data of Users is retained for five (5) years following the end of Authorisation Duration,
  - User use of the SPE: logs are retained for a period of five (5) years.

The retention periods set out above for the entirety of the SIE apply without prejudice to any further processing for compatible purposes, in particular for statistical purposes, scientific research purposes, or for archiving purposes in the public interest (including the transfer and preservation of the data by the National Archives). They also apply without prejudice to any processing necessary for the purpose of lodging an appeal against a decision of the CGSD or in connection with ongoing judicial proceedings.

6. Transfer of your data to a third country

Your data is, in principle, processed within the European Economic Area (EEA). However, the CGSD may be required to transfer your data to a third country (i.e. a country outside the EEA). Any such transfers are carried out in accordance with the conditions laid down in Chapter V of the GDPR, in particular on the basis of an adequacy decision issued by the European Commission, the existence of appropriate safeguards (Article 46 GDPR), the existence of binding corporate rules (Article 47 GDPR), or the application of one of the derogations for specific situations (Article 49 GDPR). Further information regarding any international transfers of your data may be obtained from the CGSD's data protection officer.

7. Rights of the data subject

You have the rights provided for in Articles 12 to 22 of the GDPR. Thus, within the limits of the applicable legislation, you may access your data and obtain a copy of it (Article 15 GDPR), request the rectification of inaccurate or incomplete data (Article 16 GDPR), and request the erasure of such data under the conditions laid down in Article 17 GDPR. You also have, in certain circumstances, the right to the restriction of processing of your data (Article 18 GDPR).

Furthermore, in certain cases, you have the right to object to the processing of your data, subject to the conditions laid down in Article 21 of the GDPR. Where compelling legitimate grounds exist that make the processing of your data necessary and that override your interests, rights, and freedoms, the CGSD may continue to process your data.

It is specified that the data collected by the CGSD during the certification of the business eSpace and reused to prefill an Application cannot be modified within the Application. In the event of any change to the data stored in the certified business eSpace (including a change in the persons with signing authority), the data to be amended must undergo a new certification of the business eSpace by the CGSD.

The processing of your data does not involve automated decision-making producing legal effects concerning you or significantly affecting you in a similar manner.

Any communication relating to a request for information, a complaint, or the exercise of your rights under the GDPR must be addressed to the CGSD's data protection officer.

8. Lodging a complaint with the National Commission for Data Protection (CNPD)

If, after contacting us, you consider that the processing of your personal data by the CGSD constitutes a breach of the GDPR, or that your rights under that Regulation have not been respected, you may lodge a complaint with a data protection supervisory authority, in Luxembourg the National Commission for Data Protection (CNPD) (https://cnpd.public.lu; 15, Boulevard du Jazz, L-4370 Belvaux; Tel.: (+352) 26 10 60-1).

9. Changes to the data protection notice

This privacy notice may be amended to take into account legal, regulatory, or technical developments.

ANNEX 2 – SPECIFIC CONDITIONS FOR IPE

The Data Holder and, where applicable, the Re-user shall transfer to the CGSD, by technical means and in accordance with the standards defined by the CGSD (including, where applicable, pseudonymisation process), the PSB Data and, respectively, the External Data covered by the Authorisation.

The Data Holder, and where applicable the Re-User, shall ensure, insofar as possible and

The Data Holder and, where applicable, the Re-User warrant that:

- PSB Data or External Data transferred to the CGSD are lawful, accurate, up-to-date, and collected in compliance with applicable law (including the GDPR and any relevant sectoral legislation);
- they hold all rights and authorisations necessary to transfer PSB Data or External Data to the CGSD;
- any processing of personal data is lawful within the meaning of Article 6 of the GDPR and, where applicable, Article 9 of the GDPR;
- PSB Data, respectively External Data, transferred to the CGSD respect rights of parties (e.g., copyright, trade secrets) and do not contain any unlawful, defamatory, or discriminatory content.

In all circumstances, the Data Holder and, where applicable, the Re-User shall be liable for any direct or indirect damage resulting from the processing of PSB Data, respectively External Data, that do not comply with the DGA, the GDPR, or any other applicable law.

The Data Holder and, where applicable, the Re-User shall provide the CGSD with a description of the PSB Data, respectively the External Data, covered by the Authorisation, specifying in particular their category, level of sensitivity, and the existence of any rights of third parties (e.g., copyright, trade secrets). The Data Holder and, where applicable, the Re-User shall also identify, to the best of their knowledge, all inherent risks associated with the PSB Data, respectively with the External Data, such as information that directly or indirectly identifies data subjects, rare values, etc. Following the transmission and prior to the integration of Target Data into the SPE, the CGSD shall implement all appropriate technical and organisational measures necessary to ensure the security of PSB Data, and, where applicable, External Data, and to prevent any accidental or unlawful destruction, loss, alteration, disclosure, or unauthorised access.

Where, in the context of Clause 5.2 of the GTC, the CGSD determines that certain PSB Data or External Data must be rectified or deleted before the Target Data can be made available within the SPE, the Data Holder or, where applicable, the Re-User shall make the necessary rectifications or deletions and shall thereafter transmit to the CGSD the modified set of PSB Data or External Data. Based on these modified Data, the CTIE shall perform a new assessment of the Appropriate Measures or of any additional measures deemed necessary.

ANNEX 3 – European Commission Standard Contractual Clauses governing international transfers of personal data

** Disclaimer: Modules 2 and 3 do not apply to the relationship between the CGSD and the Re-User.*

TYPES CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purposes 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.

[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 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, within the meaning of 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 within the meaning of 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.

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

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

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

(e) 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

(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.

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:

(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

[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.

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;

(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.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties 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 subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the

European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

[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.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[5].

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

8.2 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., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter 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.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where

possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6] (in the same country as

[6] 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

the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

---

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 purposes of these Clauses.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data[7], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and 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 data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

[7] This includes whether the transfer and further processing 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.

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(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.[10] 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.

(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

[10] 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.

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.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In

this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[11] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) 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.

(b) 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;

[11] 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.

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

(c) 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.

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

(e) 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

MODULE FOUR: Transfer processor to controller

(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.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-

processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [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.

(b) 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.

<u>SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES</u>

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(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[12];

(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.

[12] 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.

(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.]

(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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

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.

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

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

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

[OPTION 1: 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 _____ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify Member State*).]

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (*specify country*).

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(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 _____ (*specify Member State*).

(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.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of _____ (*specify country*).

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor 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): …

2. …

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): …

2. …

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor 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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: …

Address: …

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …