## SECTION I

**CLAUSE 1:** Purpose and scope
Purpose to ensure compliance with the GDPR; statement that can agree extra provisions so long as these do not contradict the clauses or prejudice rights of DSs; inclusion of third-party beneficiary rights; definitions in the GDPR apply; in the event of a conflict between the clauses and other agreements the clauses shall prevail; Annex 1B specifies the applicable transfers; optional accession mechanism.

## SECTION II: OBLIGATIONS OF THE PARTIES

**CLAUSE 1:** Data protection safeguards (= data protection principles)

<table>
<thead>
<tr>
<th>C2C</th>
<th>C2P</th>
<th>P2P</th>
<th>P2C</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Instructions: Importer to process only on documented instructions of exporter. Must immediately advise exporter if cannot follow instructions.
- Exporter to inform importer that it acts under instructions of controllers; identity of controllers and details of instructions to be provided. Importer to process only on documented instructions from controller as supplemented by non-conflicting instructions from exporter. Importer must advise if cannot follow instructions and exporter must notify controller.
- Exporter to process data only on instructions from the controller importer.
- Exporter to notify importer if it is unable to follow instructions. Importer to refrain from any action that would prevent the data exporter from fulfilling its obligations under the GDPR – e.g., as regards cooperation with SAs.

- Purpose limitation: Importer not to process personal data for any purposes incompatible with those in Annex 1.B, without DS’s prior consent.
- Importer only to process data for specific purposes of transfer as per Annex 1.B.
- N/A.

- Transparency: Data importer must inform DSs, directly or indirectly, if its identity and contact details; any change in purpose; if data disclosed to any third party, the identity of the third party and purpose of disclosure. Exemption where DS already has the information or where notice would be impossible or involve disproportionate effort. In this case, must post a publicly available privacy notice with the information.
- Parties to provide copy of clauses to DS on request.
- N/A.

- Ongoing data accuracy commitment on parties; notification of inaccuracy to each other; data minimization obligation on importer.
- Parties to notify each other if aware of inaccuracy. Importer to cooperate to rectify. For P2P, must also notify and cooperate with controller.
- N/A.
<table>
<thead>
<tr>
<th>C2C</th>
<th>C2P</th>
<th>P2P</th>
<th>P2C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage limitation obligation on importer.</td>
<td>Storage limitation obligation on importer at end of which must return or delete data — notwithstanding any requirements under local law that prohibit this. In that case, must guarantee continued protection and only process as required by such local law.</td>
<td>N/A.</td>
<td>Parties to ensure security of data during transmission.</td>
</tr>
<tr>
<td>Security obligation — on both parties during transmission and on importer once received. Importer to ensure personnel under obligation of confidentiality. Personal data breach reporting obligation on importer if data breach likely to result in significant adverse effects. Notice to data exporter and competent SA and to DSs, if necessary in conjunction with data exporter (exemption for disproportionate effort). Importer must document breaches and remediation.</td>
<td>Security obligation as per C2C but if pseudonymisation is used, additional information to identify — where possible — to remain under exclusive control of exporter. Importer to implement toms specified in Annex II. Importer only to allow access to personal data to personnel where &quot;strictly necessary&quot; for contract and subject to appropriate confidentiality. Personal data breach obligations in line with the GDPR. For P2P, importer to notify controller where appropriate; assistance obligations to enable exporter to meet its obligations to assist the controller under the GDPR.</td>
<td>N/A.</td>
<td>N/A.</td>
</tr>
<tr>
<td>Special categories of personal data — importer to apply specific restrictions.</td>
<td>Special categories — importer to apply specific restrictions listed in Annex 1.B.</td>
<td>N/A.</td>
<td>N/A.</td>
</tr>
<tr>
<td>Onward transfers: Permissible if third party is bound by these clauses; or adequate safeguards provided per Articles 45 through 47 of the GDPR; or third party and data exporter enter into new agreement providing same level of protection as the clauses and importer provides a copy of this to exporter, or explicit consent of DS plus notice to data exporter.</td>
<td>Onward transfers only per instructions of the exporter (or for P2P, of the controller). If in a third country only if per Articles 45 through 47 of the GDPR or if third party agrees to be bound by these clauses.</td>
<td>N/A.</td>
<td>N/A.</td>
</tr>
<tr>
<td>Processing to be under authority of importer.</td>
<td>N/A.</td>
<td>N/A.</td>
<td>N/A.</td>
</tr>
<tr>
<td>Accountability: Parties to be able to demonstrate compliance. Importer to make documentation available to competent SA on request.</td>
<td>Importer to deal with queries from exporter (or for P2P, exporter or controller). Parties to be able to demonstrate compliance — in particular, importer to have documentation on processing carried out on behalf of the exporter. Importer to make available information necessary to demonstrate compliance and to agree to audit or to rely on an independent audit organized by and at the cost of the importer — to include on premise inspection on reasonable notice. Audit results and other information to be available to SA on request. For P2P accountability, etcetera, obligations owed to exporter and controller.</td>
<td>Parties to be able to demonstrate compliance.</td>
<td>N/A.</td>
</tr>
</tbody>
</table>
### CLAUSE 2: Local laws affecting compliance with the clauses

Warranty from parties — no reason to believe laws in third country, including relating to access by public authorities would prevent importer from fulfilling its obligations. Carveout for laws in the third country that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate to safeguard an objective per Article 23(1) of the GDPR (restrictions, i.e. exemptions). Parties state that warranty is given taking due account of:

- Circumstances of the transfer, i.e., content and duration of contract; scale and regularity of transfers; length of processing chain and transmission channel used; type of recipient; purpose; nature of data; relevant practical experience of public authority requests (or lack thereof) for the type of data transferred.
- Laws of third country.
- Any safeguards in addition to the clauses, including t.o.ms applied during transmission and at destination.

Importer to make best efforts to provide relevant information for assessment and to continue to cooperate in ensuring compliance; also to notify exporter if reason to believe subject to laws not in line with above obligations, including as a result of change in law.

Assessment above to be documented and to be available to SA on request.

Exporter that receives an importer's conflict of laws alert or otherwise concludes importer can no longer comply, must promptly identify appropriate t.o.ms to address the situation. If exporter is a processor, this must be in consultation with the controller. If exporter concludes that it can implement appropriate safeguarding measures and will continue transfer on this basis, it must notify SA, along with applicable documentation. If exporter concludes it cannot provide additional safeguards, must cease transfer. If importer is sub-processor, must suspend transfer if controller instructs it to do so.

### CLAUSE 3: Obligations of importer in case of government access requests

Importer to notify exporter and DS where possible and if necessary with help of exporter, if it receives a legally binding request for disclosure of personal data by a public authority in the third country or if it becomes aware of direct access by public authorities in the third country to personal data transferred pursuant to the clauses. Processor exporter must forward the notification to the controller.

If local law prohibits notification to exporter/DS, importer agrees to use best efforts to obtain a waiver of the prohibition and to communicate as much as possible. Importer to document its best efforts so it can demonstrate them on request of exporter.

Importer to provide exporter, at regular intervals, with the greatest possible amount of relevant information on requests received — e.g., number of requests, type of data requested and requesting authority, if challenged and outcome. All to be as permissible under law of third country. Exporter processor to forward above to the controller.

Importer to preserve records of the above and to make available to competent SA on request.

Importer must comply with these provisions irrespective of any notice to exporter advising it that it cannot comply (yes, really).

Importer to assess requests for data to confirm legality under law of third country; if there are grounds to challenge under third country law, importer to exhaust all such available remedies.

Importer to seek interim measures to suspend effects of the request until court has decided on the merits. Importer not to disclose personal data until required to do so under applicable procedural rules. Importer to provide minimum amount of information permissible in response to a request. Importer to document legal assessment and challenge and — to extent permissible under third country law — to make available to exporter and to competent SA on request. (There seems to be a drafting error here — a note requiring a processor exporter to forward above to the controller is needed.)

<table>
<thead>
<tr>
<th>C2C</th>
<th>C2P</th>
<th>P2P</th>
<th>P2C</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLAUSE 2: Local laws affecting compliance with the clauses</td>
<td>CLAUSE 3: Obligations of importer in case of government access requests</td>
<td>N/A if processor merely processes data received from controller. If processor combines this with this personal data collected by processor in the EU then provisions do apply.</td>
<td></td>
</tr>
</tbody>
</table>
**CLAUSE 4: Use of sub-processors**

<table>
<thead>
<tr>
<th>C2C</th>
<th>C2P</th>
<th>P2P</th>
<th>P2C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>N/A.</strong></td>
<td>Restrictions on sub-contracting without authority of exporter. Options included for specific prior authorization or general written authorization, on the basis of notice given in sufficient time to allow the exporter a right of objection, and based on attached list of sub-processors (in Annex III). Importer to provide copy of sub-processor agreement on request. Importer to be responsible for acts of sub-processor. Sub-processing clause to have third-party beneficiary clause whereby exporter is third-party beneficiary to contract in event of bankruptcy of importer — including a right to require deletion or return of data.</td>
<td>N/A.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In P2P clauses, authorization has to be given by the controller. Third-party rights in the event of bankruptcy of importer are to be exercizable by the data exporter.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CLAUSE 5: Data subject rights**

<table>
<thead>
<tr>
<th>C2C</th>
<th>C2P</th>
<th>P2P</th>
<th>P2C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Importer to deal with and to facilitate exercise of DS rights. Obligation to provide information in intelligible and easily accessible form, using clear and plain language. DS rights correspond to rights of transparency and access (including to information in Annex I), rectification and erasure under the GDPR and rights to object to processing for direct marketing purposes. There is no obligation to support portability or restriction or to allow a general right to object to processing based on legitimate interest or performance of a task in the public interest. There are restrictions on use of automated individual decision making, which are not as extensive as those under the GDPR and are akin to those under Directive 95/46. There are derogations for requests that are excessive or where refusal is allowed under the laws of the third country and in line with Article 23 of the GDPR restrictions (i.e., derogations). Data exporter must inform DS if it refuses a request.</td>
<td>Obligation for importer to notify exporter of request it receives directly from DS. Obligation for importer to assist exporter, in line with Article 28 of the GDPR. For P2P, importer must notify controller where appropriate and must assist controller.</td>
<td>Further assurance provision.</td>
<td></td>
</tr>
</tbody>
</table>
### C2C

**CLAUSE 6: Redress**

Importer to provide contact point for complaints (either by direct notice or website). Complaints to be handled promptly. Optional provision for importer to agree that complaints can be lodged with independent dispute resolution body.

**CLAUSE 7:** Liability

**CLAUSE 8:** Indemnification

Each party liable for damage caused. Liability limited to actual damage and punitive damages excluded.

Each party liable to DS for damage it causes. For C2P and P2P transfers, data exporter also liable to DS for damage caused by data exporter or data importer. If more than one party is responsible for damage, then parties are jointly and severally liable to DS.

Importer cannot avoid liability by blaming actions of a sub-processor.

Exporter’s liability under the GDPR not affected by above provisions. Where transfer is P2P, controller’s ultimate liability to DS also not affected by this.

If one party is held liable for a breach caused by another, it can claim back liability corresponding to the party's part of responsibility. Indemnification is contingent on prompt notification and cooperation and assistance.

### C2P

**CLAUSE 9:** Supervision

Data importer to agree to submit to jurisdiction of competent SA and to respond to inquiries, submit to audits by and comply with measures adopted by the SA, including remedial and compensatory measures.

The competent SA will be the SA that is competent in relation to the data exporter. If the data exporter is not established in a member state, but the GDPR is applicable on an extraterritorial basis by virtue of Article 3(2), then the SA of the member state where DSs are, whose data is transferred shall be competent.

This section may benefit from some drafting edits to make clear that there could be multiple SAs.

### P2P

**SECTION III FINAL PROVISIONS**

**CLAUSE 1 (NONCOMPLIANCE AND TERMINATION):** Importer to inform exporter if unable to comply with the clauses. If importer is in breach or unable to comply, exporter shall suspend transfer or terminate contract. Exporter entitled to terminate if suspension continues for more than one month, for substantial or persistent breach by importer, or failure by importer to comply with binding decision of court or competent SA. Exporter must inform competent SA of any such noncompliance.

In event of termination, data to be deleted or returned. (For P2C, deleted not returned.) If importer has to keep data to meet third country law, it will continue to ensure protection for personal data and only process for so long as required under local law. Party(ies) can revoke agreement to be bound by clauses if an adequacy decision is adopted or if the GDPR becomes part of the legal framework of the third country.

**CLAUSE 2 (GOVERNING LAW):** Clauses to be governed by law of one of the member states, provided that law allows for third-party beneficiary rights. Parties to specify the member state. For C2P or P2P only, parties may select for clauses to be governed by law of the member state where the data exporter is established, provided this allows for third-party beneficiary rights. (Note the requirement that the member state law must allow for third-party beneficiary rights may mean that Irish law cannot be selected, where there is uncertainty over third party rights.)

**CLAUSE 3 (FORUM AND JURISDICTION):** Disputes to be resolved by courts of an EU member state. Parties to specify which member state this is. DS may also bring proceedings in courts of member state where the DS has their habitual residence. Parties agree to submit themselves to jurisdiction of courts of EU member states.
## ANNEX 1

### A: LIST OF PARTIES
- Name, address, contact details, signature.
- Description of activity relevant to the transfer.
- For exporter to include details of DPO and/or EU representative.
- For P2P transfers, to include identity and contact details of controller.

### B: DESCRIPTION OF TRANSFER
- Categories of data subjects and personal data.
- Details of any special category data.
- Purposes of transfer and further processing.
- Maximum retention periods (if any).
- For transfers to (sub)processors, annex to reflect instructions from the controller and the subject matter, nature and duration of processing.

## ANNEX II TECHNICAL AND ORGANIZATIONAL MEASURES, INCLUDING TO ENSURE SECURITY
For transfers to (sub)processors, this annex sets out the instructions from the controller(s) and the measures to provide assistance to the controller.

## ANNEX III LIST OF SUB-PROCESSORS