Forbidden

Forbidden Data Processing Appendix (DPA)

Version 2.0

Effective from 13 September 2026

This Data Processing Appendix forms part of the Contract between Forbidden Marketing Limited ("Forbidden", "we", "us" or "our") and the Client.

It applies where Forbidden Processes Personal Data on behalf of the Client in connection with the Services.

1. Purpose and Application

1.1 Application

Where Forbidden Processes Personal Data on behalf of the Client in connection with the Services:

a) the Client acts as Controller; and

b) Forbidden acts as Processor,

in relation to that Processing, except where Applicable Data Protection Law requires or results in a different allocation of roles.

The description of either Party as Controller or Processor under this Appendix applies only to the relevant Processing activity and does not determine that Party's role for every Processing activity carried out under or in connection with the Contract.

Nothing in this Appendix makes a data-protection law applicable to a Party or Processing activity where that law would not otherwise apply.

1.2 Definitions

In this Appendix:

"Applicable Data Protection Law" means the data-protection and privacy legislation applicable to the relevant Party or Processing, including, where applicable:

a) UK Data Protection Law;

b) EU Data Protection Law; and

c) any other applicable data-protection or privacy legislation.

"EEA" means the European Economic Area.

"EU Data Protection Law" means, to the extent applicable to the relevant Processing:

a) Regulation (EU) 2016/679 (the "EU GDPR"), including as applicable within the EEA;

b) applicable national legislation implementing, supplementing or relating to the EU GDPR in an EU or EEA state; and

c) any successor, replacement or amending legislation.

"EU Standard Contractual Clauses" or "EU SCCs" means the standard contractual clauses for international transfers of Personal Data adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, as amended, replaced or superseded from time to time.

“Restricted Transfer” means a transfer of Personal Data that requires an adequacy decision, transfer mechanism, appropriate safeguard, derogation or other legal basis under Applicable Data Protection Law.

“UK Addendum” means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, as amended, replaced or superseded from time to time.

“UK Data Protection Law” means all applicable data-protection and privacy legislation in force from time to time in the United Kingdom, including:

a) the UK GDPR;

b) the Data Protection Act 2018;

c) amendments made by the Data (Use and Access) Act 2025; and

d) any successor, replacement or amending legislation.

“UK IDTA” means the International Data Transfer Agreement issued by the UK Information Commissioner, as amended, replaced or superseded from time to time.

The terms:

“Controller”;

“Processor”;

“Personal Data”;

“Processing”;

“Data Subject”;

“Personal Data Breach”;

“Special Category Data”;

“criminal offence data”; and

“Supervisory Authority”

have the meanings given by Applicable Data Protection Law.

Where relevant, “Supervisory Authority” includes:

a) the UK Information Commissioner; and

b) a competent EU or EEA data-protection supervisory authority.

Capitalised terms not defined in this Appendix have the meanings given in the Forbidden General Terms of Business or other applicable Contract documents.

1.3 Independent Controller Processing

Each Party may separately act as an independent Controller for Personal Data it Processes for its own purposes.

Forbidden may act as an independent Controller in relation to Personal Data Processed for purposes including:

a) business administration;

b) account and client relationship management;

c) invoicing and financial administration;

d) legal and regulatory compliance;

e) information security and fraud prevention;

f) professional record keeping; and

g) internal business management.

Processing carried out by a Party in its capacity as an independent Controller is not governed by the Processor obligations in this Appendix.

Each Party is independently responsible for complying with Applicable Data Protection Law in relation to its own Controller Processing.

2. Processing Details

2.1 Subject Matter

The subject matter of the Processing is the Processing of Personal Data reasonably required for Forbidden to provide the agreed Services.

Depending on the Services purchased, this may include:

a) HubSpot onboarding;

b) configuration;

c) implementation;

d) optimisation;

e) discovery;

f) portal review;

g) Assisted Data Migration;

h) integration work;

i) CMS or website work;

j) training;

k) support;

l) consultancy; and

m) related professional services.

2.2 Duration

The Processing shall continue for:

a) the duration of the relevant Contract or Services;

b) any agreed post-go-live, support or transition period; and

c) any limited period reasonably required afterwards to return, delete or securely dispose of Personal Data in accordance with this Appendix.

2.3 Nature and Purpose

The Processing may include:

a) accessing;

b) reviewing;

c) organising;

d) mapping;

e) importing;

f) migrating;

g) configuring;

h) storing;

i) viewing;

j) testing;

k) troubleshooting;

l) transmitting;

m) supporting; and

n) otherwise Processing Personal Data,

to the extent reasonably required to provide the agreed Services.

2.4 Categories of Data Subjects

Personal Data Processed under the Services may relate to the Client's:

a) employees;

b) workers;

c) contractors;

d) customers;

e) prospective customers;

f) leads;

g) marketing contacts;

h) suppliers;

i) business contacts;

j) website users; and

k) other individuals whose Personal Data is made available to Forbidden in connection with the Services.

2.5 Types of Personal Data

Personal Data may include:

a) names;

b) job titles;

c) business contact information;

d) company information;

e) CRM records;

f) sales records;

g) marketing records;

h) customer-service records;

i) communications;

j) activity history;

k) ticketing and support information;

l) marketing preferences;

m) website interaction information; and

n) other Personal Data contained within the agreed Client systems, data sources or materials.

2.6 Special Category and Criminal Offence Data

The Client shall not intentionally provide Forbidden with Special Category Data or criminal offence data unless:

a) the relevant Processing has been expressly agreed in Writing;

b) the Client has informed Forbidden of the nature of the data;

c) the Processing is necessary for the agreed Services;

d) the Client has established an appropriate lawful basis and any additional condition required by Applicable Data Protection Law; and

e) appropriate additional safeguards have been agreed where required.

Such data is not required for Forbidden's standard Services.

3. Documented Instructions

3.1 Processing Instructions

Forbidden shall Process Personal Data only:

a) on the Client's documented instructions;

b) as reasonably necessary to provide the Services within those instructions; or

c) where required by Applicable Data Protection Law.

The Client's documented instructions include any authorised instruction concerning an international or Restricted Transfer where that transfer forms part of the agreed Services.

3.2 What Constitutes Documented Instructions

The Client's documented instructions include, as applicable:

a) the Contract;

b) applicable Service Terms;

c) the Project Agreement;

d) any Project Schedule or Statement of Work;

e) an approved Blueprint;

f) an approved Final Technical Specification;

g) an Approved Change; and

h) instructions given by an Authorised Representative through an agreed Written project or support channel.

A project task, comment or operational request constitutes a documented instruction only to the extent that it falls within the agreed Services and does not itself expand the commercial scope of the Contract.

3.3 Processing Required by Law

Where Forbidden is required by Applicable Data Protection Law to Process Personal Data other than on the Client's documented instructions, Forbidden shall inform the Client of that legal requirement before carrying out the Processing unless the applicable law prohibits such notification.

3.4 Unlawful Instructions

Forbidden shall immediately inform the Client if, in Forbidden's reasonable opinion, a Client instruction infringes Applicable Data Protection Law.

Forbidden may suspend the affected Processing until the Parties have clarified or amended the instruction where continuing the Processing would create a material legal, regulatory or security risk.

4. Forbidden's Processor Obligations

Forbidden shall:

a) Process Personal Data only in accordance with Section 3;

b) ensure that persons authorised to Process Personal Data have committed themselves to confidentiality or are subject to an appropriate confidentiality obligation;

c) implement appropriate technical and organisational security measures in accordance with Section 6;

d) taking account of the nature of the Processing, provide reasonable assistance to the Client through appropriate technical and organisational measures, insofar as reasonably possible, in responding to requests from Data Subjects exercising their rights under Applicable Data Protection Law;

e) provide reasonable assistance to the Client in relation to security obligations, Personal Data Breaches, data-protection impact assessments and prior consultations with a Supervisory Authority, taking account of the nature of the Processing and the information available to Forbidden;

f) maintain records and information reasonably required to demonstrate compliance with this Appendix and Applicable Data Protection Law applicable to Forbidden as Processor;

g) notify the Client of a Personal Data Breach in accordance with Section 7;

h) comply with the sub-processor requirements in Section 8;

i) comply with the international-transfer requirements in Section 9;

j) return or delete Personal Data in accordance with Section 10; and

k) allow for and contribute to audits and inspections in accordance with Section 11.

Forbidden shall not respond directly to a Data Subject request relating to Client Personal Data unless:

a) instructed by the Client; or

b) required by Applicable Data Protection Law.

Where legally permitted, Forbidden shall inform the Client of a legally required direct response.

Where the Client requests assistance that is unusually extensive, outside the normal scope of the Services, and not required because of Forbidden's breach of this Appendix or Applicable Data Protection Law, any additional Charges must be agreed in advance.

5. Client Obligations

The Client shall:

a) ensure that it has an appropriate lawful basis for the Processing;

b) provide all privacy information and notices required by Applicable Data Protection Law to Data Subjects;

c) ensure that any necessary consents, permissions, rights or other legal requirements are in place;

d) provide lawful, reasonable and sufficiently clear documented instructions;

e) ensure Personal Data supplied to Forbidden is relevant and limited to what is reasonably required for the Services;

f) not intentionally provide Special Category Data or criminal offence data unless agreed in accordance with Section 2.6;

g) determine applicable retention periods;

h) determine marketing permissions and CRM governance requirements;

i) ensure the accuracy and lawfulness of Personal Data it provides;

j) identify any material legal, regulatory, localisation or transfer requirement applying to Client Personal Data that would not reasonably be apparent to Forbidden from the agreed Services; and

k) notify Forbidden promptly of any instruction, requirement or legal issue affecting the Processing.

The Client remains responsible for:

a) determining the purposes and essential means of the Processing;

b) the lawfulness of the Processing;

c) the content and accuracy of Personal Data supplied to Forbidden;

d) determining whether the Client is required to undertake a data-protection impact assessment or prior consultation; and

e) decisions concerning retention, deletion, marketing permissions and regulatory compliance.

6. Security Measures

6.1 Appropriate Measures

Taking account of:

a) the nature, scope, context and purposes of the Processing;

b) the risks to the rights and freedoms of Data Subjects;

c) the state of the art; and

d) the cost of implementation,

Forbidden shall maintain appropriate technical and organisational measures designed to provide a level of security appropriate to the relevant risk.

6.2 Security Objectives and Measures

Where appropriate to the relevant risk, measures maintained by Forbidden may include:

a) pseudonymisation or encryption of Personal Data;

b) access controls;

c) role-based permissions;

d) access limited to authorised persons on a need-to-know basis;

e) password controls;

f) multi-factor authentication where available and appropriate;

g) secure transmission of Personal Data;

h) appropriate storage controls;

i) device security;

j) account security;

k) network-security measures;

l) measures designed to support the ongoing confidentiality, integrity, availability and resilience of systems and services used by Forbidden to Process Personal Data;

m) staff confidentiality obligations;

n) staff data-protection and information-security requirements;

o) backup and recovery arrangements for systems controlled by Forbidden;

p) measures designed to restore availability and access to Personal Data in a timely manner following a relevant physical or technical incident;

q) security update procedures;

r) vulnerability-management procedures;

s) incident identification, response and reporting processes; and

t) appropriate processes for periodically assessing, testing or reviewing the effectiveness of relevant security measures.

The particular measures applied shall depend on the nature of the Processing, the relevant systems and the risks involved.

Forbidden is not responsible for security controls within Client-controlled systems, Client accounts or third-party systems except to the extent Forbidden has expressly agreed responsibility for those controls.

7. Personal Data Breaches

7.1 Notification

Forbidden shall notify the Client of a Personal Data Breach affecting Client Personal Data without undue delay after becoming aware of it.

Where reasonably practicable, Forbidden shall aim to provide an initial notification within twenty-four (24) hours after becoming aware of the Personal Data Breach.

7.2 Information Provided

To the extent reasonably available, Forbidden shall provide information concerning:

a) the nature of the Personal Data Breach;

b) the categories and approximate number of Data Subjects affected;

c) the categories and approximate number of Personal Data records affected;

d) the likely consequences of the Personal Data Breach;

e) measures taken or proposed to address the Personal Data Breach and, where appropriate, mitigate its possible adverse effects; and

f) relevant contact information for follow-up.

Information may be provided in phases where complete information is not immediately available.

7.3 Cooperation

Forbidden shall provide reasonable cooperation to help the Client:

a) investigate the Personal Data Breach;

b) assess applicable notification requirements; and

c) comply with applicable obligations concerning notification to Data Subjects or a Supervisory Authority.

The Client remains responsible for determining whether it is required to notify a Supervisory Authority or Data Subjects unless Applicable Data Protection Law expressly places that obligation on Forbidden.

Notification by Forbidden does not constitute an admission of fault or liability.

8. Sub-processors

8.1 General Authorisation

The Client gives Forbidden general written authorisation to appoint sub-processors where reasonably required to provide the Services, subject to this Section 8.

8.2 Sub-processor List

Forbidden shall maintain a current list of relevant sub-processors that Process Client Personal Data on Forbidden's behalf and make that list available:

a) through the Forbidden Customer Portal, where available; or

b) on reasonable Written request.

8.3 New or Replacement Sub-processors

Forbidden shall give the Client at least fourteen (14) calendar days' prior Written notice of a proposed new or replacement sub-processor that will Process Client Personal Data on Forbidden's behalf.

Unless otherwise stated in this Section 8.3, notices under this Appendix shall be given in accordance with Section 13.8 of the Forbidden General Terms of Business.

For the purposes of notifying the Client of a proposed new or replacement sub-processor only, Forbidden may give notice:

a) by email to an appropriate Client contact;

b) through the Forbidden Customer Portal, where available; or

c) by another Written notification method agreed with the Client.

A notice given in accordance with this Section 8.3 is effective for the purposes of the sub-processor notification requirements in this Appendix.

8.4 Client Objection

The Client may object to the proposed appointment within seven (7) calendar days after receiving notice where it has reasonable data-protection grounds for doing so.

The objection must:

a) be made in Writing;

b) identify the relevant data-protection concern; and

c) provide reasonable supporting details.

8.5 Resolution of Objection

The Parties shall work in good faith to address a valid objection.

Where reasonably possible, Forbidden may:

a) provide further information or safeguards;

b) use a reasonable alternative sub-processor; or

c) adjust the affected Processing.

Where a valid objection cannot reasonably be resolved and Forbidden cannot reasonably provide the affected Services without using the proposed sub-processor, either Party may terminate only the Services materially dependent on that sub-processor.

Any such termination is subject to the applicable Contract provisions concerning Charges and the financial consequences of termination.

Termination under this Section does not affect:

a) Charges that have already become due;

b) Charges for Services already properly performed;

c) approved, unavoidable or non-refundable third-party costs; or

d) any other Charges that the applicable Contract expressly provides remain payable following termination.

The Parties shall act reasonably in determining any Charges attributable to Services that will not be provided as a direct consequence of termination under this Section.

8.6 Sub-processor Obligations

Forbidden shall:

a) enter into a written agreement with each sub-processor imposing the data-protection obligations required by Applicable Data Protection Law for the relevant Processing;

b) require the sub-processor to implement appropriate technical and organisational measures for the relevant Processing; and

c) remain fully responsible to the Client for the performance of the sub-processor's data-protection obligations to the extent required by Applicable Data Protection Law.

9. International Transfers

9.1 General

Forbidden shall not make a Restricted Transfer of Client Personal Data unless:

a) the transfer is authorised by the Client's documented instructions, where such authorisation is required;

b) the transfer is permitted by Applicable Data Protection Law; and

c) an applicable adequacy decision, transfer mechanism, appropriate safeguard, derogation or other lawful basis for the transfer is in place.

The applicable transfer mechanism shall be determined by:

a) the Applicable Data Protection Law governing the relevant transfer;

b) the location and respective roles of the parties to that transfer;

c) the destination of the Personal Data; and

d) whether the relevant importer is itself subject to the applicable data-protection regime.

9.2 Transfers from the EEA to the United Kingdom

Where EU Data Protection Law applies to a transfer of Personal Data from the EEA to Forbidden in the United Kingdom, the Parties may rely on an applicable European Commission adequacy decision covering the United Kingdom for so long as that decision validly applies to the relevant transfer.

Where such an adequacy decision does not apply or ceases to apply to a relevant transfer, the

Parties shall cooperate reasonably to put in place an alternative lawful transfer mechanism where required by EU Data Protection Law.

That mechanism may include, as appropriate:

a) the applicable module or modules of the EU SCCs; or

b) another mechanism permitted by EU Data Protection Law.

Nothing in this Section automatically incorporates the EU SCCs where they are not required for the relevant transfer.

9.3 Restricted Transfers from the United Kingdom

Where UK Data Protection Law applies to a Restricted Transfer, an applicable transfer mechanism may include:

a) applicable UK adequacy regulations;

b) the UK IDTA;

c) the UK Addendum;

d) another appropriate safeguard recognised by UK Data Protection Law; or

e) another lawful transfer mechanism or exception permitted by UK Data Protection Law.

9.4 Onward Transfers

Where Forbidden or a sub-processor makes an onward Restricted Transfer of Client Personal Data, Forbidden shall ensure that an appropriate transfer mechanism or other lawful basis is in place to the extent required by Applicable Data Protection Law.

Where a sub-processor is involved, Forbidden shall require the sub-processor to comply with applicable international-transfer restrictions relating to the relevant Client Personal Data.

9.5 Transfer Assessment and Additional Safeguards

Where Applicable Data Protection Law requires an assessment of the protection afforded to Personal Data in connection with a Restricted Transfer, Forbidden shall carry out, assist with or provide information reasonably required for the applicable assessment to the extent responsibility for that assessment falls on Forbidden.

For a Restricted Transfer governed by UK Data Protection Law, this may include the applicable data protection test or transfer risk assessment required in connection with the relevant transfer mechanism.

Where required by Applicable Data Protection Law, Forbidden shall implement, or require the relevant sub-processor to implement, reasonable supplementary or additional safeguards appropriate to the circumstances of the transfer.

9.6 Transfer Information

On reasonable request, Forbidden shall provide the Client with information reasonably available

to Forbidden and reasonably required to enable the Client to assess a transfer mechanism applicable to Processing carried out by Forbidden or its sub-processors.

Forbidden is not required to disclose:

a) information relating to another client;

b) confidential security information where disclosure would itself create a material security risk; or

c) information that Forbidden is prohibited by law or contractual confidentiality obligations from disclosing,

provided that Forbidden shall use reasonable efforts to provide an appropriate alternative form of information where required to demonstrate compliance.

10. Return and Deletion

10.1 End of Services

At the end of the relevant Services, Forbidden shall, at the Client's choice:

a) return the relevant Personal Data; or

b) securely delete the relevant Personal Data and existing copies,

unless Applicable Data Protection Law requires continued retention.

Where Applicable Data Protection Law requires continued storage, Forbidden shall continue to protect the retained Personal Data and shall not Process it for another purpose except as permitted or required by law.

10.2 Client Choice

The Client shall communicate its choice within thirty (30) calendar days after the relevant Services end.

If the Client does not communicate a choice within that period, Forbidden may securely delete the relevant Personal Data.

10.3 Backup Copies

Personal Data contained in routine backups may remain until deleted through Forbidden's normal secure backup-deletion cycle, provided that:

a) it is not restored or used for ordinary business purposes;

b) access remains appropriately restricted; and

c) it is used only where required for disaster recovery, security, legal or regulatory purposes.

10.4 Independent Controller Records

Nothing in this Section requires Forbidden to delete Personal Data that it lawfully retains in its capacity as an independent Controller, including records required for legal, regulatory, security, insurance or professional record-keeping purposes.

11. Audit and Compliance Information

11.1 Compliance Information

Forbidden shall make available information reasonably required to demonstrate compliance with the Processor obligations applicable to Forbidden under this Appendix and Applicable Data Protection Law.

Where reasonably sufficient, Forbidden may satisfy a request by providing:

a) policies;

b) security information;

c) certifications;

d) independent audit reports;

e) questionnaire responses; or

f) other relevant compliance information.

11.2 Client Audit and Inspection

Where the information provided under Section 11.1 is not reasonably sufficient, the Client may conduct, or appoint an appropriately qualified independent auditor to conduct, an audit or inspection relating to the relevant Processing.

Forbidden shall allow for and reasonably contribute to such an audit or inspection, subject to:

a) reasonable prior Written notice;

b) no more than one audit in any twelve (12) month period unless an additional audit is reasonably required following a Personal Data Breach, material compliance concern or request from a Supervisory Authority;

c) the audit taking place during normal business hours;

d) appropriate confidentiality and security arrangements;

e) reasonable limitations necessary to protect other clients, personnel and systems;

f) no access to information relating to other clients;

g) the auditor not being a direct competitor of Forbidden unless otherwise required by Applicable Data Protection Law or agreed by Forbidden;

h) no vulnerability scanning, penetration testing or intrusive technical testing without Forbidden's prior Written agreement; and

i) the audit not unreasonably disrupting Forbidden's business.

Nothing in this Section prevents an audit, inspection or other access that cannot lawfully be restricted under Applicable Data Protection Law.

11.3 Audit Costs

The Client shall bear its own audit costs.

The Client shall reimburse Forbidden's reasonable costs of supporting an audit where the support required is materially beyond ordinary compliance assistance, provided those costs are reasonable and agreed in advance where practicable.

Forbidden shall not charge the Client for reasonable audit support where the audit identifies a material breach of this Appendix by Forbidden.

11.4 Supervisory Authority

Nothing in this Section limits the rights or powers of a competent Supervisory Authority under Applicable Data Protection Law.

12. Data Protection Impact Assessments and Regulatory Consultation

Where required under Applicable Data Protection Law and taking account of the nature of the Processing and information available to Forbidden, Forbidden shall provide reasonable assistance to the Client with:

a) data-protection impact assessments; and

b) prior consultation with a competent Supervisory Authority.

The Client remains responsible for determining whether a data-protection impact assessment or regulatory consultation is required, except to the extent Applicable Data Protection Law expressly provides otherwise.

Where substantial assistance is required because of circumstances outside Forbidden's breach or ordinary Services, any additional Charges must be agreed in advance.

13. Precedence and Liability

13.1 Precedence

If there is any inconsistency between this Appendix and another Contract document concerning the Processing of Personal Data, this Appendix takes precedence only in relation to that Processing.

For all other matters, the order of precedence in the Forbidden General Terms of Business applies.

Where an applicable mandatory international-transfer mechanism, including the EU SCCs, UK IDTA or UK Addendum, applies to a Restricted Transfer and conflicts with this Appendix, the

mandatory terms of that transfer mechanism prevail to the extent of the conflict in relation to that Restricted Transfer.

13.2 Liability

Each Party's liability arising out of or in connection with this Appendix is subject to the liability provisions in the Forbidden General Terms of Business, including any enhanced liability cap applicable to breach of data-protection obligations.

Nothing in this Appendix excludes or limits liability where such exclusion or limitation is prohibited by Applicable Data Protection Law.

14. Relationship with the Contract and Separate DPAs

14.1 Incorporation

This Appendix forms part of the Contract where Forbidden Processes Personal Data on behalf of the Client.

This Appendix does not:

a) change the Parties' roles for Processing carried out outside the Processor relationship governed by this Appendix;

b) make EU Data Protection Law, UK Data Protection Law or another data-protection regime applicable where it would not otherwise apply; or

c) require the use of a particular international-transfer mechanism where that mechanism is not required by Applicable Data Protection Law.

14.2 Separately Signed Client DPA

Where Forbidden and the Client have entered into a separately signed client-specific data processing agreement or data-processing addendum that expressly applies to the relevant Processing, that signed agreement governs that Processing to the extent stated in it and takes precedence over this Appendix in the event of any inconsistency.

Unless that separately signed agreement expressly provides otherwise:

a) the Forbidden General Terms of Business continue to apply to the Contract;

b) general contractual matters, including Charges, payment, suspension, termination, confidentiality, intellectual property, liability, Force Majeure and formal notices, remain governed by the Forbidden General Terms of Business; and

c) the separately signed data processing agreement does not amend the commercial terms of the Contract merely because it contains data-protection provisions.

Where a separately signed data processing agreement contains its own specific notice, audit, sub-processor, international-transfer or other data-protection procedure, that procedure applies to the relevant data-protection matter to the extent of any inconsistency.

14.3 Notices

Except where this Appendix or a separately signed client-specific data processing agreement expressly provides a specific notification procedure for a particular data-protection matter, formal notices under this Appendix shall be given in accordance with Section 13.8 of the Forbidden General Terms of Business.

Where this Appendix expressly permits a particular notification method, including a sub-processor notification under Section 8.3, that method is sufficient for the relevant notification.

14.4 General Contractual Matters

Except where this Appendix expressly provides otherwise, Charges, payment, suspension, termination, confidentiality, intellectual property, liability, Force Majeure, notices and other general contractual matters are governed by the Forbidden General Terms of Business and other applicable Contract documents.

14.5 Governing Law and Mandatory Transfer Terms

Except to the extent that an applicable mandatory international-transfer mechanism expressly requires otherwise, this Appendix is governed by the governing-law and jurisdiction provisions of the Forbidden General Terms of Business.

Where the EU SCCs, UK IDTA, UK Addendum or another mandatory transfer mechanism applies to a Restricted Transfer, any governing-law, jurisdiction, third-party-beneficiary or Supervisory Authority provisions required by that mechanism apply to the relevant Restricted Transfer to the extent required by its terms.