



IRIS Software Limited - Customer Data Processing Terms

+ Version and Document Control

Version:	V.DPA-FY25
Published:	29/07/2024
Effective:	29/07/2024
Change Control Comments:	Addition of clause 4.4

+ Table of Contents

	Definitions
	Specific interpretive provision(s)
Section 1	Data processing provisions
Section 2	Instructions and details of processing
Section 3	Technical and organisational measures
Section 4	Using staff and other processors
Section 5	Assistance with the Customer's compliance and Data Subject rights
Section 6	International data transfers
Section 7	Records, information, and audit
Section 8	Breach notification
Section 9	End of Processing
Section 10	Liability, indemnities, and compensation claims
Section 11	Survival of data protection provisions
	SCHEDULE 1
	DATA PROCESSING DETAILS

+ Definitions

Definitions

(Any other capitalised terms not contained in this section will be as defined in the IRIS Software Group General Terms & Conditions ('Terms & Conditions'))

Applicable Law means as applicable and binding on the Customer, the Supplier and/or the Services:

- (a) any law, statute, regulation, byelaw or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that the Services are provided to or in respect of;
- (b) the common law and laws of equity as applicable to the parties from time to time;
- (c) any binding court order, judgment or decree; or
- (d) any applicable direction, policy, rule or order that is binding on a party and that is made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business;

Appropriate Safeguards means such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time including the Standard Contractual Clauses annexed to Commission Implementing Decision (2021/914/EU) of 4 June 2021 on standard contractual clauses for the transfer of personal data to processors established in third countries;

Data Controller has the meaning given to that term (or to the term 'controller') in Data Protection Laws;

Data Processor has the meaning given to that term (or to the term 'processor') in Data Protection Laws;

Data Protection Laws means as applicable and binding on the Customer, the Supplier and/or the [Services]:

- (a) in the United Kingdom:
 - (i) the Data Protection Act 2018; and/or
- (b) "UK-GDPR"; in member states of the European Union: the GDPR, and all relevant member state laws or regulations giving effect to or corresponding with the GDPR; and
- (c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;

Data Protection Losses means any and all liabilities, including all:

- (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and
- (b) to the extent permitted by Applicable Law:
 - (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;
 - (ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and
 - (iii) the reasonable costs of compliance with investigations by a Supervisory Authority;

Data Subject has the meaning given to that term in Data Protection Laws;

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

GDPR	means the General Data Protection Regulation (EU) 2016/679;
International Organisation	means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
International Recipient	has the meaning given to that term in clause 6.1;
Personal Data	has the meaning given to that term in Data Protection Laws;
Personal Data Breach	means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data transmitted, stored or otherwise processed;
Processing	has the meanings given to that term in Data Protection Laws (and related terms such as process and processed have corresponding meanings);
Processing Instructions	
Protected Data	means Personal Data received by the Supplier from or on behalf of the Customer in connection with the performance of the Supplier's obligations under this Agreement and in the provision of the Services;
Sub-Processor	means another Data Processor engaged by the Supplier for carrying out processing activities in respect of the Protected Data on behalf of the Customer under the terms of this Agreement; and
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.
UK-GDPR	means the EU General Data Protection Regulation 2016/679 as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

+ Specific interpretive provision(s)

In clauses 1 to 11 (inclusive):

(a) a reference to any Applicable Laws (including to the Data Protection Laws and each of them) and to terms defined in such Applicable Laws shall be replaced with or incorporate (as the case may be) references to any Applicable Laws replacing, amending, extending, re-enacting or consolidating such Applicable Law (including the GDPR and any new Data Protection Laws from time to time) and the equivalent terms defined in such Applicable Laws, once in force and applicable;

(b) a reference to a law includes all subordinate legislation made under that law;

(c) references to a law of the European Union include a reference to that law as incorporated into the laws of the United Kingdom at any time after the United Kingdom ceases to be a Member State of the European Union.

+ Data processing provisions

1 Data Processor and Data Controller

- 1.1 The parties agree that, for the Protected Data, the Customer shall be the Data Controller and the Supplier shall be the Data Processor.
- 1.2 The Supplier shall process Protected Data in compliance with:
 - 1.2.1 the obligations of Data Processors under Data Protection Laws in respect of the performance of its obligations under this Agreement; and
 - 1.2.2 the terms of this Agreement.
- 1.3 The Customer shall comply with:
 - 1.3.1 all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under this Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and
 - 1.3.2 the terms of this Agreement.
- 1.4 The Customer warrants, represents and undertakes, that:
 - 1.4.1 all data sourced by the Customer for use in connection with the Services, prior to such data being provided to or accessed by the Supplier for the performance of the Services under this Agreement, shall comply in all respects, including in terms of its collection, storage and processing (which shall include the Customer providing all of the required fair processing information to, and obtaining all necessary consents from, Data Subjects), with Data Protection Laws;
 - 1.4.2 all instructions given by it to the Supplier in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and
 - 1.4.3 [it has undertaken due diligence in relation to the Supplier's processing operations, and it is satisfied that:
 - (a) the Supplier's processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Supplier to process the Protected Data; and
 - (b) the Supplier has sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.
- 1.5 The Customer shall not withhold, delay or condition its agreement to any change requested by the Supplier in order to ensure the Services and the Supplier (and each Sub-Processor) can comply with Data Protection Laws.

+ Instructions and details of processing

2 Instructions and details of processing

- 2.1 Insofar as the Supplier processes Protected Data on behalf of the Customer, the Supplier:
 - 2.1.1 unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with this Agreement and the Customer's documented instructions as set out in this clause 2 and Schedule 1 (Data processing details) (**Processing Instructions**);
 - 2.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing

the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

2.1.3 shall without undue delay inform the Customer if the Supplier becomes aware of a Processing

Instruction that, in the Supplier's opinion, infringes Data Protection Laws, provided that:

- (a) this shall be without prejudice to clauses 1.3 and 1.4;
- (b) to the maximum extent permitted by Applicable Law, the Supplier shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Customer's Processing Instructions following the Customer's receipt of that information;

2.2 The processing of Protected Data to be carried out by the Supplier under this Agreement shall comprise the processing set out in Schedule 1 (Data processing details).

+

Technical and organisational measures

3 Technical and organisational measures

3.1 The Supplier shall implement and maintain, at its cost and expense, appropriate technical and organisational measures (details of which can be provided upon request):

3.1.1 in relation to the processing of Protected Data by the Supplier; and taking into account the nature of the processing, to assist the Customer insofar as is possible in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data.

+

Using staff and other processors

4 Using staff and other processors

4.1 The Customer authorises the appointment of any of the Sub-Processors listed in the applicable Services description or related document provided with an Order. Any proposed changes to such pre-listed Sub-Processors will be notified to Customers in writing, thereby giving the Customer the opportunity to reasonably object to such changes (grounds for objection being non-compliance of Data Protection Laws).

4.2 The Supplier shall:

4.2.1 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing equivalent obligations as under clauses 1 to 11 (inclusive) that is enforceable by the Supplier;

4.2.2 ensure each such Sub-Processor complies with all such obligations; and

4.2.3 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

4.3 The Supplier shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify the Customer of any such requirement before such disclosure).

4.4 IRIS Employee Verification

- 4.4.1 The Customer provides general authorisation to the Supplier to appoint Supplier-authorised third parties for the purposes of providing the Services or additional services, which may involve the disclosure of Customer Data to those third parties. The Supplier agrees to remain transparent where Supplier transfers Data to a third party and how Customer can opt out of such services / functionality.
- 4.4.2 For transparency, some products or Services may permit the transfer of Data to an Employment Data Connector (“EDC”) to provide additional over the top services by income/credit verification services, employment verification services, salary benchmarking services and other financial services providers (“EDC Providers”) to Customers and their employees (Data Subjects). The Supplier confirms that access by Customer (and Data Subjects’ access) to such services shall remain optional at all times and may be opted out of. Should service/functionality remain active, the legal basis of such Data Subjects Data transfers to EDC Providers may either be on the basis of consent or legitimate interest. The Customer accepts that the Supplier does not accept liability for the use of or processing by such third party EDC Providers.
- 4.4.3 Further information can be found at: <https://www.iris.co.uk/products/iris-employee-verification/>
-

+ Assistance with the Customer’s compliance and Data Subject rights

5 Assistance with the Customer’s compliance and Data Subject rights

- 5.1 The Supplier shall refer all Data Subject Requests it receives to the Customer within a reasonable period of time from receipt of the request., If such Data Subject Requests is deemed manifestly unfounded or excessive the Customer shall pay the Supplier’s Charges at the Supplier’s then standard rates, for recording and referring the Data Subject Requests in accordance with this clause 5.1.
- 5.2 The Supplier shall provide such reasonable assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to the Customer in ensuring compliance with the Customer’s obligations under Data Protection Laws with respect to:
- 5.2.1 security of processing;
- 5.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);
- 5.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and
- 5.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach, provided the Customer shall pay the Supplier’s Charges for providing the assistance in this clause 5.2,
-

+ International data transfers

6 International data transfers

- 6.1 Subject to the Supplier's prior notification to the customer whether such a transfer is relevant to the service provision, the Customer agrees that the Supplier may transfer Protected Data to countries outside the European Economic Area (EEA) or to any International Organisation(s) (an **International Recipient**) where the Supplier or its Sub-Processors operate, provided all transfers by the Supplier of Protected Data to an International Recipient (and any onward transfer) shall (to the extent required under Data Protection Laws) be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The provisions of this Agreement shall constitute the Customer’s instructions with respect to transfers in accordance with clause 2.1.

+

Records, information and audit

7 Records, information and audit

7.1 The Supplier shall maintain, in accordance with Data Protection Laws binding on the Supplier, written records of all categories of processing activities carried out on behalf of the Customer.

7.2 The Supplier shall, in accordance with Data Protection Laws, make available to the Customer such information as is reasonably necessary to demonstrate the Supplier's compliance with its obligations under Article 28 of the GDPR (and under any Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose, subject to the Customer:

7.2.1 giving the Supplier reasonable prior notice of such information request, audit and/or inspection being required by the Customer;

7.2.2 ensuring that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to the Supervisory Authority or as otherwise required by Applicable Law);

- 7.2.3 ensuring that such audit or inspection is undertaken during normal business hours not more than once in any 12-month period (unless there is reasonable cause), with minimal disruption to the Supplier's business, the Sub-Processors' business and the business of other customers of the Supplier; and
 - 7.2.4 paying the Supplier's reasonable costs for assisting with the provision of information and allowing for and contributing to inspections and audits.
-

+ Breach notification

8 Breach notification

- 8.1 In respect of any Personal Data Breach involving Protected Data, the Supplier shall, without undue delay:
 - 8.1.1 notify the Customer of the Personal Data Breach; and
 - 8.1.2 provide the Customer with details of the Personal Data Breach Deletion or return of Protected Data and copies.
-

+ End of Processing

9 End of Processing

- 9.1 The Supplier shall, at the Customer's written request, either delete or return all the Protected Data to the Customer in such form as the Customer reasonably requests within a reasonable time after the earlier of:
 - 9.1.1 the end of the provision of the relevant Services related to processing; or
 - 9.1.2 once processing by the Supplier of any Protected Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under this Agreement, and delete existing copies (unless storage of any data is required by Applicable Law and, if so, the Supplier shall inform the Customer of any such requirement). In the absence of any such request to return the personal data, the supplier will delete all protected data after a reasonable period following the end of the provision of services.
-

+ Liability, indemnities and compensation claims

10 Liability, indemnities and compensation claims

- 10.1 The Customer shall indemnify and keep indemnified the Supplier in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Supplier and any Sub-Processor arising from or in connection with any:
 - 10.1.1 non-compliance by the Customer with the Data Protection Laws;
 - 10.1.2 processing carried out by the Supplier or any Sub-Processor pursuant to any Processing Instruction that infringes any Data Protection Law; or
 - 10.1.3 breach by the Customer of any of its obligations under clauses 1 to 11 (inclusive), except to the extent the Supplier is liable under clause 10.2.
- 10.2 Subject to S.2 clause 10 of the Terms and Conditions, the Supplier shall be liable for any losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with this Agreement:

- 10.2.1 only to the extent caused by the processing of Protected Data under this Agreement and directly resulting from the Supplier's breach of clauses 1 to 11 (inclusive); and
- 10.2.2 in no circumstances to the extent that any losses are contributed to or caused by any breach of this Agreement by the Customer (including in accordance with clause 2.1.3(b)).
- 10.3 If a party receives a compensation claim from a person relating to processing of Protected Data, it shall promptly provide the other party with written notice and full details of such claim. The party with conduct of the action shall:
- 10.3.1 make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed); and
- 10.3.2 consult fully with the other party in relation to any such action, but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under this Agreement for paying the compensation.
- 10.4 The parties agree that the Customer shall not be entitled to claim back from the Supplier any part of any compensation paid by the Customer in respect of such damage to the extent that the Customer is liable to indemnify the Supplier in accordance with clause 10.1.
- 10.5 This clause 10 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:
- 10.5.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and
- 10.5.2 that it does not affect the liability of either party to any Data Subject.
-

+ Survival of data protection provisions

11 Survival of data protection provisions

- 11.1 Clauses 1 to 11 (inclusive) shall survive termination (for any reason) or expiry of this Agreement and continue:
- 11.1.1 indefinitely in the case of clauses 9 to 11 (inclusive); and
- 11.1.2 until 12 months following the earlier of the termination or expiry of this Agreement in the case clauses 1 to 8 (inclusive), provided always that any termination or expiry of clauses 1 to 8 (inclusive) shall be without prejudice to any accrued rights or remedies of either party under any such clauses at the time of such termination or expiry.
-

+ SCHEDULE 1 DATA PROCESSING DETAILS

SCHEDULE 1 DATA PROCESSING DETAILS

1 Subject-matter of processing:

The provision of services by the Supplier to the Customer as outlined in any Order and/or associated documentation.

2 Duration of the processing:

For the duration of any Order/Agreement.

3 Nature and purpose of the processing:

Processing activities, such as storage and data transfer will be undertaken by the Supplier and Personal Data will be processed to provide the services to the Customer as outlined in an Order and/or associated documentation.

4 Type of Personal Data:

Types of Personal Data as may be supplied by the Customer including name, address, email address, phone numbers.

5 Categories of Data Subjects:

Data subjects include the Customer's representatives and personnel, such as employees, contractors and collaborators and other categories of data subjects as may be supplied by the Customer.

6 Processing Instructions

As may be agreed in an Order or reasonably provided by the Customer.