

Recruit Genie Data Processing Agreement (EXAMPLE)

Version 4.8



This document is provided as a standard template for review purposes only. The applicable version will be the version incorporated into or executed with the relevant customer agreement. This publication does not create contractual obligations and may be updated periodically.

Parties

1. Recruit Genie (Europe) Ltd a company incorporated in England and Wales under No. 11891133 whose registered office is at 33 Park Place, LS1 2RY, England (**Data Processor**).
2. **#CLIENTNAME#** a company registered in **England** and Wales under No. **#CLIENTCOMPANYNUMBER#** whose registered office is at **#CLIENTREGISTEREDADDRESS#** (**Customer / Data Controller**).

Each a “party” and together the “parties”.

Background

3. The Data Processor is a provider of cloud-based HR recruitment solutions (**Services**).
4. The parties entered into an agreement for the provision of services on **#AGREEMENTDATE#** (**Agreement**).
5. The parties have agreed to enter into this Data Processing Agreement (**DPA**) in relation to the processing of personal data by the Data Processor on behalf of the Customer in the course of providing the Services. The terms of this DPA are intended to apply in addition to and not in substitution of the terms of the Agreement.

AGREEMENT

Meanings

1. In this DPA, the following words are defined:

Affiliate	any entity that directly or indirectly controls, or is controlled by, or is under common control with the subject entity. ‘Control’ for the purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
-----------	--

Customer Personal Data	The Personal Data identified in Schedule 1.
Data Protection Law	a. all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom applicable to the Processing of Personal Data under the Agreement, including, but not limited to the GDPR and the UK GDPR; and b. to the extent applicable, the data protection or privacy laws of any other country.
GDPR	a. 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 (the EU GDPR); and b. the EU GDPR as implemented or adopted under the laws of the United Kingdom (UK GDPR).
Personnel	in relation to a party, those of its employees, workers, agents, consultants, contractors, sub-contractors, representatives or other persons employed or engaged by that party on whatever terms.
Sub-processor	any entity (whether or not an Affiliate of the Data Processor, but excluding the Data Processor's Personnel) appointed by or on behalf of the Data Processor to process Personal Data on behalf of the Data Controller under this DPA.
Working Day	any day, other than a Saturday, Sunday, or public holiday in England and Wales.

2. Terms such as "Data Subject", "Processing", "Personal Data", "Controller", and "Processor", "Supervisory Authority" and "Personal Data Breach" shall have the same meaning as ascribed to them in the Data Protection Law.
3. In this DPA unless the context requires a different interpretation:
 - a. the singular includes the plural and vice versa;
 - b. references to sub-clauses, clauses, schedules or appendices are to sub-clauses, clauses, schedules or appendices of this DPA;
 - c. a reference to a person includes firms, companies, government entities, trusts and partnerships;
 - d. 'including' is understood to mean 'including without limitation';
 - e. reference to any statutory provision includes any modification or amendment of it;
 - f. the headings and sub-headings do not form part of this DPA; and
 - g. 'writing' or 'written' will include email unless otherwise stated.

Processing customer personal data

4. For the purpose of Data Protection Law, the **Customer** shall be the **Data Controller** and **Recruit Genie** will be the **Data Processor** of the Customer Personal Data.
5.
 - a) The Data Processor shall process, store, and use the Customer Personal Data only to the extent necessary to provide the Services, to fulfil the Data Controller's prior written instructions (including this DPA, the Agreement, and any applicable addendum), or as otherwise as agreed by the parties in writing, and for no other purposes whatsoever unless it is otherwise required to do so under Data Protection Law, in which case the Data Processor shall notify the Data Controller in writing before the processing (save where it is prohibited from doing so by law).
 - b) The Data Processor shall notify Data Controller immediately if, in its opinion, an instruction infringes Data Protection Law.
 - c) Upon termination of the provision of Services by the Data Processor, the Data Processor shall, at the choice of the Data Controller, permanently delete or return to the Data Controller the personal data (unless storage is required by law) in accordance with Clauses 20 to 23.
 - d) The Data Controller represents and warrants that it has all necessary rights to provide the personal data to the Data Processor for the processing to be performed in connection with the Services. To the extent required by Data Protection Laws, the Data Controller is responsible for providing all necessary privacy notices to data subjects and ensuring that it has the appropriate legal basis under Data Protection Laws for the processing required under the Agreement, including the transfer of Customer Personal Data to the Data Processor pursuant to this DPA.
 - e) Artificial Intelligence Processing

Where the Services include AI-assisted functionality, the processing of Personal Data shall also be subject to the AI Processing Addendum attached to and incorporated into this DPA. The Client acknowledges that Recruit Genie may engage approved AI-related subprocessors identified in the AI Processing Addendum and the Subprocessor Schedule.

The AI Processing Addendum forms part of this DPA and sets out additional terms relating to the nature, scope, and safeguards applicable to such Processing.

The Data Processor shall process Customer Personal Data using such AI-assisted features only in accordance with:

- (i) this DPA;
- (ii) the Agreement; and
- (iii) the AI Processing Addendum.

In the event of any conflict between the AI Processing Addendum and this DPA, the AI Processing Addendum shall prevail solely in respect of AI-related Processing.

For the avoidance of doubt, the AI-assisted features do not constitute automated decision-making under Article 22 of Data Protection Law, and do not produce decisions with legal or similarly significant effects without human involvement.

6.

a) The Data Processor and each Affiliate shall take reasonable steps to ensure the reliability of Personnel who have access to the Customer Personal Data, and shall ensure in each case that such Personnel is subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they Process the Customer Personal Data in compliance with all applicable law (including Data Protection Law) and only in accordance with clause 5(a) of this DPA.

b) Confidentiality: The Data Processor shall treat all Customer Personal Data confidentially and (without prejudice to its other obligations under this DPA) will take steps to protect Customer Personal Data that are substantially similar to those it takes to protect its own Personal Data (but not less than reasonable care) to prevent its unauthorised disclosure. The Data Processor shall inform all its employees, agents and approved sub-processors engaged in Processing the Customer Personal Data of its confidential nature. The Data Processor shall cause all such persons or parties to sign agreements with confidentiality obligations no less restrictive in the use and protection of the Customer Personal Data than those Data Processor has to Data Controller.

Security

7. The Data Processor will maintain information and data security measures in relation to the Processing of Customer Personal Data under this DPA. The measures to be maintained must provide a level of security for the Customer Personal Data appropriate to the risk concerning confidentiality, integrity, and availability of the Customer Personal and the resilience of the Data Processors systems processing the Customer Personal Data. The state of the art, implementation costs, the nature, scope and purposes of the Processing, as well as the probability of occurrence and the severity of the risk to the rights and freedoms of the Data Subjects must be taken into account. Such measures may include, as appropriate:
 - a. the pseudonymisation and encryption of Personal Data;
 - b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - c. the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and
 - d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.
8. In assessing the appropriate level of security, the Data Processor shall take into account any risks that are presented by the Processing, in particular, from a Personal Data Breach.
9. Without prejudice to the obligations in clauses 7 and 8, the Data Processor shall maintain and provide the technical and organisational measures described in Schedule 2 of this DPA. To meet its obligations in clauses 7 and 8, the Processor may from time to time implement alternative measures, subject to prior written notification to the Data Controller.

Sub-processors and transfers to third countries

10. The Data Controller authorises the Data Processor and each Affiliate to appoint the Sub-processors listed in Schedule 3.

11. With respect to each Sub-processor, the Data Processor, or the Affiliate shall:
 - a. carry out appropriate due diligence prior to the Processing by such Sub-processor to ensure that the Sub-processor is capable of providing the level of protection for Customer Personal Data required by the terms of the Agreement and this DPA;
 - b. enter into a written agreement with the Sub-processor incorporating terms which are substantially similar (and no less onerous) than those set out in this DPA and which meet the requirements of Article 28(3) of the EU GDPR; and
 - c. remain fully liable to the Customer for all acts or omissions of such Sub-processor as though they were its own.
12. The Data Processor (and each Sub-processor) is not permitted to transfer Customer Personal Data to any third country (**transfer**) unless such transfer is on the basis of an adequacy decision pursuant to Article 45 of the EU GDPR or is subject to appropriate safeguards in accordance with the requirements of Article 46 of the EU GDPR. No transfer of Customer Personal Data is in any event permitted unless such transfer is notified to the Data Controller pursuant to the mechanism in Clause 13, and such notification shall be subject to the rights granted the Data Controller in Clause 14.
13. The Data Processor may continue to use Sub-processors already engaged by the Data Processor as at the date of this DPA subject to the Data Processor meeting the obligations set forth in the preceding clause as soon as reasonably practicable.
13. The Data Processor shall give the Data Controller prior written notice of the appointment of any new Sub-processor, including the name of the Sub-processor it seeks to appoint, the Processing activity to be undertaken by the Sub-processor and the other details set forth in Schedule 3.
14. If within 30 days of receipt of notice under the preceding clause, the Data Controller notifies the Data Processor in writing of any objections to the proposed appointment:
 - a. the parties will work in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of the proposed Sub-processor without unreasonably burdening the Customer; and
 - b. where such a change cannot be made within 30 days of the Data Processor's receipt of the Data Controller's notice, the Data Controller may, notwithstanding the terms of the Agreement, serve written notice on the Data Processor to terminate the Agreement.

The Data Controller's agreement to a transfer or appointment of a Sub-processor, or failure to raise an objection pursuant to clause 14, is without prejudice to the Data Processor's obligations hereunder and its liability to the Data Controller.

Data subject rights

15. Taking into account the nature of the Processing, the Data Processor and each Affiliate shall assist the Data Controller in implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising Data Subjects' rights under the Data Protection Law.
16. The Data Processor shall:
 - a. promptly (and in any event, within 24 hours) notify the Data Controller if it (or any of its Sub-processors) receives a request from a Data Subject; and

- b. fully cooperate with and assist the Data Controller in relation to any request made by a Data Subject,

under the Data Protection Law in respect of Customer Personal Data Processed by the Data Processor under the terms of the Agreement or this DPA.

Personal data breaches

- 17. The Data Processor shall:
 - a. notify the Data Controller without undue delay (in any event, no later than 24 hours) upon becoming aware of any Personal Data Breach affecting the Customer Personal Data Processed by the Data Processor under this DPA;
 - b. provide sufficient information to enable the Data Controller to evaluate the impact of such Personal Data Breach and to meet any obligations on the Data Controller to report the Personal Data Breach to a Supervisory Authority and/or notify the affected Data Subjects in accordance with the Data Protection Law;
 - c. provide the Data Controller with such assistance as the Data Controller may reasonably request; and
 - d. cooperate with the Data Controller and take such reasonable steps (as directed by the Data Controller) to assist in the evaluation, investigation, mitigation and remediation of each such Personal Data Breach.

Data Protection Impact Assessment and Prior Consultation

- 18. The Data Processor and each Affiliate shall provide reasonable assistance to the Data Controller with any data protection impact assessments and prior consultations with Supervisory Authorities or other competent authorities which the Data Controller considers necessary pursuant to Articles 35 and 36 of the EU GDPR.
- 19. Such assistance from the Data Processor shall be limited, in each case, to the scope of Processing of Customer Personal Data under this DPA.

Return and deletion of personal data

- 20. Subject to the subsequent clause, the Data Processor and each Affiliate shall promptly and in any event, within 30 days of the expiry or termination of the Agreement, delete or return (as directed by the Data Controller) all copies of Customer Personal Data Processed by the Data Processor and/or its Sub-processors on behalf of the Data Controller by such means as the parties shall agree in writing.
- 21. The Data Processor (and its Sub-processors) may retain Personal Data Processed under this DPA to the extent required by any applicable law to which the Data Processor (or any Sub-processor) is subject and only to the extent and for such period as required by applicable law. Where applicable, the Data Processor shall notify the Data Controller of any such requirement and ensure the confidentiality of such Personal Data. Any Personal Data Processed under this

DPA and retained by the Data Processor (or any Sub-processor) in accordance with this clause shall be not Processed for any other purpose other than the purpose specified in the applicable laws.

22. The Data Controller may require the Data Processor to provide written certification confirming that it has complied in full with its obligations under this section entitled 'Return and deletion of personal data.'

Audits

23. The Data Processor shall make available to the Data Controller on request all information necessary to demonstrate compliance with this DPA.
24. The Data Processor shall allow for and contribute to audits, including inspections, by the Data Controller (or any other auditor mandated by the Data Controller) in relation to the Processing of Personal Data under this DPA.
25. The Data Controller (or any other auditor mandated by the Data Controller) shall give the Data Processor or Affiliate reasonable notice of any audit or inspection, and shall make all reasonable endeavours to avoid causing any damage, injury or disruption to the Data Processor or Affiliate's premises, equipment, personnel and business in the course of the audit or inspection.
26. Such audit rights may be exercised only once in any calendar year during the term of the Agreement and, in addition, after any Personal Data Breach.

Liability

27. Nothing in this DPA limits or excludes either party's liability for death or personal injury caused by its negligence, or fraud or fraudulent misrepresentation.
28. Subject to the preceding clause, the total liability of either party to the other for any non-compliance with this DPA shall be subject to any limitation regarding monetary damages set forth in the Agreement.

General terms

29. Except in respect of any provision of this DPA that expressly or by implication is intended to come into or continue in force on or after the expiry or termination of the Agreement, this DPA shall be coterminous with the Agreement.
30. No party may assign, transfer or sub-contract to any third party the benefit and/or burden of the DPA without the prior written consent (not to be unreasonably withheld) of the other party.
31. No variation of the DPA will be valid or binding unless it is recorded in writing and signed by or on behalf of both parties.
34. Unless otherwise agreed, no delay, act or omission by a party in exercising any right or remedy will be deemed a waiver of that, or any other, right or remedy.

35. If any court or competent authority finds that any provision (or part) of the DPA is invalid, illegal or unenforceable, that provision or part-provision will, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of the DPA will not be affected.
36. Any notice (other than in legal proceedings) to be delivered under the DPA must be in writing and delivered by recorded post to or left by hand delivery at the other party's registered address or place of business.
37. The parties submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.
38. This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.
39. Nothing in this DPA reduces the Data Processor's obligations under the Agreement in relation to the protection of Personal Data or permits the Data Processor to process (or permit the processing of) personal data in a manner which is prohibited by the Agreement.
40. In the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

Schedule 1 – Data Collection & Processing activities

This Schedule 1 includes certain details of the data Collection & Processing of Customer Personal Data as required by Article 28(3) EU GDPR. The subject matter and duration of the Processing of the Personal Data are set out in the Agreement and this DPA.

Customer Personal Data

All Personal Data relating to the categories of data subjects identified below and which is processed by the Data Processor in connection with the Services.

Purpose of Processing

The Customer Personal Data shall be processed on behalf of the Data Controller only for the purposes of, and to the extent required, for providing the Services, as more particularly identified in the Data Processor's Record of Processing Activity supplied to the Data Controller and detailed in the table below.

Including (where enabled by the Customer) AI-assisted candidate matching, scoring, and insight generation as further described in the AI Processing Addendum.

Personal Data being processed

As more particularly identified in the Data Processor's Record of Processing Activity supplied to the Data Controller and detailed in the table below.

Sensitive or special categories of personal data to be processed (where applicable)

As more particularly identified in the Data Processor's Record of Processing Activity supplied to the Data Controller and detailed in the table below.

Purpose of processing	Categories of individuals	Categories of personal data
Application Processing	Candidates	Contact Details Online Identifier Location Data Education Qualifications Document CV Employment History Video / Audio Recordings (Interview)
Onboarding	Offered Candidate	Contact Details Financial Details Online Identifier Location Data Education Qualifications Next of Kin Identifier Information Right to work Identifier Document ID Referee Details
System Users	Client Employee	Contact Details

		Online Identifier
--	--	-------------------

Schedule 2 - Technical and organisational measures

1) Specific Security requirements.

a) The Data Processor and Sub-processors shall implement the following measures and documents with respect to Customer Personal Data:

- i) The data security programme and associated physical, technical, organisational and security measures shall be documented in writing by the Data Processor and shall comply in all material respects with the Information Security Management System (ISMS) family of standards as published by the Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), also known as the ISO/IEC 27000 series, may be modified or replaced from time to time.
- ii) Provide a secondary authentication (two-factor authentication (2FA)) like a security token or biometric factor, as well as a password.
- iii) **Isolation of Personal Data.** The principle of least privilege shall be implemented and enforced (i.e., authorised Data Processor personnel should only be granted the minimal data-access privileges required to complete their job functions or responsibilities). Data Processor or Sub-processor shall permit only authorised Data Processor personnel, Data Controller employees or third parties designated by Data Controller to have access to data locations. Controls such as scrambling, anonymisation, and pseudonymisation shall be implemented and maintained, as well as strong credentials, secure tokens, multi-factor authentication and other authentication solutions. Customer Personal Data shall be physically segregated from other clients' data, or strong logical controls shall be implemented and maintained to prevent other clients from accessing the Customer Personal Data. Production data must never be stored in a non-production environment (i.e., development, test, pre-production). Access to the system that hosts Customer Personal Data must be restricted to the required Ips and ports of other systems only.
- iv) **Sent Personal Data.** Checksums must be used while transferring Customer Personal Data to ensure data integrity. Personal Data sent by Data Processor or Sub-processor to Data Controller, or on behalf of Data Controller, shall be free of malware.

b) Viruses.

- i) use reasonable, good faith and diligent efforts to implement industry best practices at all times to identify, screen, prevent and otherwise ensure that no viruses are coded or introduced into any Data Controller systems or Data Processor's systems, or any Data Processor technology used to provide the Services to Data Controller;

- ii) ensure that, without the prior written consent of Data Controller, no software directly or indirectly provided to Data Controller contains any code which could have the effect of disabling or otherwise rendering ineffective all or any portion of the Services;
- iii) if a virus or such disabling code is found in any such systems or software:
 - 1. promptly notify Data Controller;
 - 2. at no additional charge, provide reasonable, good faith and diligent efforts to assist Data Controller in reducing and/or eliminating the effects of the virus or disabling code without causing a loss of operating efficiency or Customer Personal Data or interruption in the provision of the services; and
 - 3. if the virus or disabling code causes a loss of operational efficiency or loss of Customer Personal Data, assist Data Controller to the same extent to mitigate and restore such losses; and
 - 4. perform a code scan before deploying any Data Processor software or applications into production. Any vulnerabilities found by the code scan must be remediated before deploying it into production. If a vulnerability cannot be remediated, then Data Processor must obtain Data Controller's approval before deploying it into production.

c) **Backdoors.**

- i) Data Processor certifies that (a) it has not purposefully created any backdoors that could be used to access the Customer Personal Data or systems, and (b) it has not purposefully created or changed its business processes in a manner that facilitates access to Customer Personal Data or systems.

d) **Event Logs.**

- i) Complete and accurate logs of all events on systems and networks used to perform the Services or otherwise Process Customer Personal Data (**Event Logs**), including information such as date, time, user ID, device accessed, and port used. Data Processor shall maintain such Event Logs for a minimum of 12 months and Data Processor shall periodically analyse the Event Logs for security related events, unusual activities, and other issues, such as unsuccessful attempts to create backup copies of Personal Data. Access to the log data must be restricted to only authorised Data Processor personnel, or approved by Data Controller, or a person designated by Data Controller via a traceable ticket system. Periodic reviews of user access must be performed to ensure access to the Event Log data is still relevant and needed.

e) **Restoring Data.**

- i) the restoration of any destroyed, lost or altered Customer Personal Data shall be performed by the party that has operational responsibility for maintaining the system on which such Personal Data resides and for creating and maintaining backup copies of

such Personal Data. Data Processor shall bear the cost of restoring such data to the extent:

1. Data Processor is operationally responsible for inputting such data; or
2. such destruction, loss or alteration is attributable to the failure of Data Processor or Data Processor personnel to comply with Data Processor's obligations under this DPA.

f) **Encryption.**

- i) encrypt all Customer Personal Data at rest, and in transit, and in storage; and
- ii) encrypt all Personal Data on portable devices;
using a FIPS-140-2 compliance encryption algorithm.

h) **Penetration Test.**

- i) Data Processor shall annually test, assess, and evaluate the effectiveness of its security measures by conducting a penetration test based on industry accepted penetration testing approaches on its systems used to store or Process Customer Personal Data. Data Processor will provide a summary of the results of each penetration test to Data Controller, which summary shall include the number of issues identified during the test, how Data Processor will resolve the identified issues and a proposed timeline for, and commitment to, issue resolution.

j) **Contingency Planning.**

- i) Upon the occurrence of any event that constitutes a disaster under the applicable disaster recovery/business continuity plan (**Disaster Event**), Data Processor shall promptly implement, as appropriate, such disaster recovery/business continuity plan and provide disaster recovery and business continuity services as described in such plan. The occurrence of a Disaster Event shall not relieve Data Processor of its obligation to implement the applicable disaster recovery/business continuity plan and provide disaster recovery and business continuity services. Data Processor shall test, assess, and evaluate such plan at least annually.

k) **Backup of Data.**

- i) **Backup Copies.** As part of Data Processor's implementation of the disaster recovery/business continuity plan described above, Data Processor shall generate and maintain backup copies of all Personal Data residing on its systems. Such backup copies shall be considered "Customer Personal Data" as used in this DPA, and all Data Processor's obligations in this DPA, including those related to data security and privacy, shall apply to such backup copies to the same extent such obligations apply to other Customer Personal Data. Data Processor shall perform backup restoration testing at least annually to ensure the integrity and accuracy of backup copies of Customer Personal Data.

2) Assistance with responding to data subject requests

- a) Data Processor and Sub-processors that Process Customer Personal Data shall implement all technical and organisational measures required to enable Data Controller to update, erase, isolate, obtain and disclose Personal Data relating to a specific data subject which shall include the following:
- i) **Updates and modifications.** Ensure all updates or modifications to Customer Personal Data are approved by authorised Data Processor Personnel, and logged, monitored, and reviewed periodically. Ensure data integrity controls are implemented and used to prevent the unauthorised modification or destruction of the Customer Personal Data. Ensure backups are maintained to be able to roll-back any modifications or destructions.
 - ii) **Erasure and/or deletion.** Ensure Customer Personal Data erased and/or deleted is approved by an authorised Data Processor personnel and/or by Data Controller and done in a secure way. For erasure and/or deletion in a cloud environment, crypto-shredding must be used to ensure the Customer Personal Data is unusable. All erasures and/or deletions must be logged and monitored. All original files, back-ups and replications must be erased and/or deleted as well.

Schedule 3 - Sub-processors

COMPANY	PURPOSE	COMPANY LOCATION	SERVER LOCATION	TYPES OF PERSONAL DATA	SAFEGUARDS FOR THE TRANSFER OF PERSONAL DATA
Microsoft Corporation (Cloud infrastructure / Azure)	Cloud infrastructure (Azure), productivity tools (e.g., email, file storage)	Ireland	UK	All	EU Law (ISO 27001 Certified)
Microsoft Corporation (Azure AI Foundry)	AI-assisted candidate matching, recruitment analysis, scoring and insight generation.	Ireland	UK	Candidate information, CV/resume content, employment history, qualifications, skills data, job descriptions and related recruitment information submitted for analysis.	Microsoft Products and Services Data Protection Addendum; processing within Microsoft's Azure environment; customer prompts, completions and training data are not made available to model providers and are not used to train foundation models without customer permission; subject to Azure security and compliance controls.
Amazon Web Services	S3 Data Storage (Optional)	EU	UK	Candidate Interview Videos	EU Law (ISO 27001 Certified)
Rchilli	CV/Resume parsing and enrichment	USA	EU	Resume content, name, email, job history	EU Law (ISO 27001 Certified)
Google	Analytics (Optional)	USA	USA	Basic website browsing info such as pageviews and visit data such as device type, operating system, and browser type	Standard Contractual Clauses and data encryption (ISO 27001 Certified)
HA	Hosting	UK	UK	All	EU Law (ISO 27001 Certified)
CameraTag	Video recording & processing for applications or interview (Optional Service)	USA	EU	Candidate Interview Videos	Standard Contractual Clauses and data encryption
Weglot	Language Translation (Optional Service)	EU	EU	NA (no personal data)	EU Law (SOC 2 Type II certified)

Sinch Sweden AB (SINCH)	SMS and messaging services	EU	EU	Phone number, message content	EU Law (ISO 27001 Certified)
Twilio SendGrid	Transactional Email	USA	USA	Names, emails, content	Standard Contractual Clauses and data encryption (ISO 27001 Certified)
Mailjet	Transactional Email	EU	EU	Names, emails, content	EU Law (ISO 27001 Certified)
Freshdesk	Customer support and helpdesk system	EU	EU	Names, emails, support messages	EU Law (ISO 27001 Certified)

AI Processing Note: Recruit Genie uses Microsoft Azure AI Foundry models for AI-assisted services. Personal data submitted to these services is processed by Microsoft within Azure. AI-generated outputs retained by Recruit Genie form part of the customer's data held within Recruit Genie and are retained in accordance with the customer's applicable retention policies. Microsoft may perform limited temporary processing, caching and abuse-monitoring activities necessary to provide and secure the service.

For the most up to date version of this Sub-processors list please visit <https://recruitgenie.co.uk/legal-sub-processors/>