

DATA PROCESSING AGREEMENT (DPA) - SCAN SERVICE

Version 1.1 - Date of update: 29 September 2026

1. DEFINITIONS

For the purposes of this Data Processing Agreement, the following terms shall have the meanings set out below, whether used in the singular or plural:

“Candidates” refers to the individuals whose Personal Data are processed in connection with the SCAN Service for the Customer’s recruitment purposes and who qualify as Data Subjects within the meaning of the GDPR.

“Customer” refers to any natural and/or legal person acting within the scope of their professional activity and having signed a Contract with AssessFirst.

“Contract”: refers to the contractual agreement between AssessFirst and the Client for the provision of the Service, including, as applicable, a purchase order accompanied by the General Terms and Conditions of Sale, a specific contract or any other contractual document accepted by the Parties.

“Data Protection Laws” refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the “GDPR”), together with any applicable legislation relating to the protection of personal data.

“Personal Data” refers to any information relating to an identified or identifiable natural person within the meaning of the GDPR.

“Personal Data Breach” refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, within the meaning of the GDPR.

“Service”: refers to the SCAN module to which the Customer has access via their subscription to the AssessFirst platform.

“Sub-processor” refers to any third-party engaged by AssessFirst to process Personal Data on behalf of the Customer in connection with the SCAN Service.

“Controller”, “Processor”, “Data Subject” and “Processing” shall have the meanings given to them under the GDPR.

2. PURPOSE AND SCOPE

This Data Processing Agreement (hereafter referred to as the “DPA”) sets out the terms under which AssessFirst processes Candidates’ Personal Data on behalf of the Customer within the SCAN module.

This Data Processing Addendum (DPA) is incorporated by reference into the Contract and is deemed to have been accepted by the Customer upon subscribing to the SCAN Service.

For the purposes of the Service, the Customer acts as Controller and AssessFirst acts as Processor.

This DPA applies exclusively to the SCAN module. Any other services provided by AssessFirst to the Customer are performed in AssessFirst’s capacity as an independent Controller and are not covered by this DPA.

AssessFirst reserves the right to amend this Data Processing Addendum (DPA) in order to take into account legal, regulatory, jurisprudential or technical developments. The Customer will be notified of any substantial amendments by any appropriate means.

In the event of any conflict between this DPA and the Contract, the provisions of this DPA shall prevail with respect to the Processing of Personal Data carried out by AssessFirst as Processor under the Service.

3. DESCRIPTION OF THE PROCESSING

The characteristics of the Processing entrusted to AssessFirst are described in Appendix 1, including the following:

- The nature of the Processing operations;
- The purposes of the Processing;
- The categories of Personal Data processed;
- The categories of Data Subjects;
- The duration of the Processing.

The Customer determines the purposes and essential means of the Processing. AssessFirst shall only process Personal Data in accordance with documented instructions from the Customer.

The Customer's instructions may be transmitted via the settings made available in the Service, or by any written instruction from the Customer where applicable, within the limits of the Service's functionality and this DPA.

In the event of any discrepancy, the most recent documented instructions that comply with Data Protection Laws shall prevail.

4. CUSTOMER'S OBLIGATIONS (CONTROLLER)

The Customer undertakes to:

- process Personal Data in compliance with the Data Protection Laws and, more generally, with any applicable laws and regulations;
- ensure that it has a valid legal basis for the Processing carried out through the Service that is appropriate in the recruitment context;
- provide Data Subjects with the information required under Articles 12 to 14 of the GDPR;
- provide AssessFirst with lawful and GDPR-compliant documented instructions;
- determine the retention period applicable to the Personal Data processed through the Service, ensuring that such retention period is appropriate in light of its legal obligations and the storage limitation principle set out in Article 5(1) of the GDPR;
- ensure that only authorised persons have access to the Service and to user accounts.

The Customer remains solely responsible for the lawfulness of the Processing activities and of the instructions provided to AssessFirst.

5. SENSITIVE DATA

By default, the SCAN Service is not intended to process special categories of data as defined in Article 9 of the GDPR, nor data relating to criminal convictions and offences as defined in Article 10 of the GDPR.

Accordingly, the Customer undertakes not to include, in the Personal Data processed through the Service, any special categories of Personal Data ("sensitive data") within the meaning of Articles 9 and 10 of the GDPR, unless required by law or subject to specific documented instructions, and to implement appropriate safeguards where applicable.

For the avoidance of doubt, in the context of the SCAN Service in spoken mode, any voice data that may be processed is not used by AssessFirst to uniquely identify a natural person and therefore it does not constitute biometric data as defined in Article 4(14) of the GDPR or special categories of data as defined in Article 9 of the GDPR.

6. ASSESSFIRST'S OBLIGATIONS (PROCESSOR)

6.1. GENERAL OBLIGATIONS

AssessFirst undertakes to:

- process Personal Data solely with the Customer's documented instructions, including with regard to transfers of Personal Data;
- inform the Customer immediately if, in its opinion, an instruction infringes the Data Protection Laws;
- ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the GDPR and as described in Annex 2;
- delete or return the Personal Data to the Customer at the end of the provision of the Service, in accordance with Article 14 of this DPA;
- make all necessary information available to the Customer to demonstrate compliance with this DPA.

AssessFirst shall process Personal Data solely for the purpose of providing the Service and in accordance with the Customer's instructions.

The Customer is informed that AssessFirst may use anonymised data, which no longer permits the direct or indirect identification of Data Subjects, for research, security, service improvement and the development of its artificial intelligence models. Such anonymised information no longer constitutes Personal Data within the meaning of the Data Protection Laws and is processed outside their scope.

6.2. RECORD OF PROCESSING ACTIVITIES

AssessFirst shall maintain a record of the categories of Processing activities carried out on behalf of the Customer. This record shall contain the information required under Article 30(2) of the GDPR. This includes:

- the name and contact details of the Controller, AssessFirst as Processor, any Sub-processor, and the Data Protection Officer;
- the categories of Processing carried out on behalf of the Customer;
- where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where applicable, the documentation of suitable safeguards;
- a general description of the technical and organisational security measures implemented to protect the Personal Data.

6.3. ASSISTANCE

AssessFirst shall assist the Customer, to the extent reasonable and taking into account the nature of the Processing and the information available to AssessFirst, in order to enable the Customer to comply with its obligations under the GDPR, in particular with respect to:

- responding to requests from Data Subjects to exercise their rights;
- notification of Personal Data Breaches;
- carrying out Data Protection Impact Assessments (DPIAs) and, where applicable, prior consultations with supervisory authorities;
- more generally, this assistance shall cover compliance with the obligations set out in the GDPR.

However, such assistance shall not transfer to AssessFirst the responsibilities incumbent upon the Customer in its capacity as Controller.

6.4. MANDATORY DISCLOSURE

To the extent permitted by law, AssessFirst shall inform the Customer without undue delay of any request received from a public or judicial authority relating to Personal Data processed on behalf of the Customer in connection with the Service.

If AssessFirst is required, pursuant to applicable law, to disclose Personal Data processed on the Customer's behalf, AssessFirst shall inform the Customer prior to such disclosure, to the extent permitted by law. AssessFirst shall also provide the Customer with any information reasonably necessary to enable them to challenge or seek to limit the scope of such disclosure.

Where such notification is prohibited by law, AssessFirst shall inform the Customer as soon as the prohibition is lifted.

Any disclosure shall be strictly limited to the Personal Data required by the applicable legal obligation.

7. SECURITY OF PERSONAL DATA

In accordance with Article 32 of the GDPR, AssessFirst implements appropriate technical and organisational measures to ensure an adequate level of security. These measures take into account:

- the state of the art;
- the costs of implementation;
- the nature, scope, context and purposes of the Processing; and
- the risks to the rights and freedoms of data subjects.

AssessFirst is ISO/IEC 27001 certified and maintains an information security management system in accordance with this standard.

The security measures applicable to the Service are described in Annex 2 to this DPA.

8. CONFIDENTIALITY OF PERSONAL DATA

AssessFirst ensures the confidentiality of Personal Data and ensures that access is limited strictly to authorised personnel on a need-to-know basis for the performance of the Service. In particular, AssessFirst undertakes to:

- process Personal Data solely for the purpose of providing the Service, in accordance with the Customer's documented instructions;
- restrict access to Personal Data to employees, suppliers and Sub-processors who require access for the performance of the Service and who are subject to appropriate confidentiality obligations;
- not disclose Personal Data to any third party, except (a) authorised personnel, (b) Sub-processors engaged in accordance with this DPA, or (c) where required by law (under the conditions set out in the "Mandatory Disclosure" section);
- implement measures designed to prevent any unauthorised, improper or fraudulent access to systems processing Personal Data;
- where applicable, apply the principles of data protection by design and by default.

Any information exchanged between the Parties in the context of their contractual relationship may be considered confidential business information as defined in Articles L.151-1 et seq. of the French Commercial Code. The Parties must take all necessary measures to protect this information in accordance with the confidentiality obligations set out in the Contract and in this DPA.

9. USE OF SUB-PROCESSORS

The Customer expressly authorises AssessFirst to engage the Sub-processors listed in our [online FAQs](#) for the purpose of Processing Personal Data in connection with the provision of the Service.

AssessFirst shall ensure that any Sub-processor is contractually bound by obligations at least equivalent to those in this DPA. AssessFirst shall remain fully liable to the Customer for the performance of the Sub-processor's obligations.

AssessFirst shall inform the Customer of any intended addition or replacement of a Sub-processor before such change takes effect in relation to the Service. Notification may be provided by email and/or through a notification within the Customer account.

The Customer may object on legitimate data protection grounds within fifteen (15) business days of receiving the notification. In the event of a valid objection, the Parties shall discuss in good faith in order to find a reasonable alternative solution that ensures an equivalent level of data protection.

Where the relevant Sub-processor performs an essential and non-substitutable function of the Service, without which the Service cannot be provided in an equivalent manner, and no reasonable alternative solution can be implemented within the same timeframe, the Customer may terminate the affected Service without penalty upon thirty (30) days' written notice.

Until the termination takes effect, AssessFirst shall continue to process Personal Data in accordance with this DPA and the Customer's instructions. The obligations relating to security, confidentiality and data return or deletion shall remain fully applicable.

10. DATA LOCATION

Any Personal Data processed in connection with the Service is hosted exclusively within the European Union via the Amazon Web Services (AWS) cloud infrastructure.

No transfers of Personal Data outside the European Union are carried out in connection with the Service.

11. DATA SUBJECTS' RIGHTS

If a request to exercise rights under Articles 15 to 22 of the GDPR is made to AssessFirst, it shall forward the request to the Customer by email, using the contact details provided by the Customer. It shall also forward any relevant information available to it.

Upon the Customer's reasonable request, and taking into account the nature of the Processing and the information available to AssessFirst, AssessFirst shall assist the Customer, to the extent possible, in facilitating the exercise of data subjects' rights under Articles 15 to 22 of the GDPR and enabling the Customer to comply with the applicable statutory deadlines.

Unless expressly instructed to do so by the Customer, AssessFirst shall not respond directly to Data Subjects. Where necessary, AssessFirst may assist the Data Subject in identifying the Customer as the Controller and provide the Customer's contact details.

12. PERSONAL DATA BREACHES

AssessFirst shall notify the Customer of any Personal Data Breach without undue delay after becoming aware of it and, where feasible, within forty-eight (48) hours.

This notification will include the information required under Article 33(3) of the GDPR, particularly:

- the nature of the breach;
- the categories and approximate number of Data Subjects concerned;
- the categories and approximate number of Personal Data records affected;
- the likely consequences of the Data Breach;
- the measures taken or proposed to address the Data Breach and mitigate its possible adverse effects;
- a contact point for obtaining further information.

In accordance with Article 33(5) of the GDPR, AssessFirst shall maintain a documented record of Personal Data Breaches, including the facts relating to the breach, its effects and the remedial action taken.

AssessFirst shall cooperate in good faith with the Customer to remedy the breach, mitigate its effects and assist the Customer in complying with its obligations to notify the relevant supervisory authority and/or the affected Data Subjects.

13. REGULATORY ASSISTANCE AND COOPERATION

In addition to the provisions of Article 6.2 of this DPA, AssessFirst shall cooperate with and assist the Customer, to the extent reasonably possible and within the limits of its role as Processor, in the event of any request, inquiry or investigation by a data protection authority relating to Processing carried out under the Service, provided that this is permitted by law.

14. DATA RETURN OR DELETION UPON TERMINATION

Upon the Customer's instruction, and, in any event upon expiration or termination of the Agreement, AssessFirst shall, within a reasonable timeframe:

- delete the Customer's Personal Data, and/or
- return the Customer's Personal Data,

as instructed by the Customer.

This obligation includes the deletion or return of Personal Data contained in backups, unless its retention is required by applicable law or for evidentiary purposes in the context of a dispute. In this case, the data shall be deleted once the applicable statutory retention period has expired.

At the Customer's request, AssessFirst shall provide written confirmation of the deletion of Personal Data.

The deletion and return obligations set out in this section shall not apply to information that has been irreversibly anonymised. This information is no longer considered as Personal Data and may be retained and used by AssessFirst for research and service improvement purposes in accordance with this DPA.

15. AUDITS

Upon written request and at reasonable intervals, AssessFirst shall make available to the Customer the information necessary to demonstrate compliance with this DPA. This information shall be provided in the form of recent certifications and/or third-party audit reports or equivalent documents (the 'Audit Documents'), which shall be treated as confidential.

Unless required by applicable law or in the event of a major incident warranting an additional audit, audits shall be limited to one per contractual year and shall relate exclusively to Processing activities carried out by AssessFirst on behalf of the Customer under the Service.

These audits shall primarily be conducted remotely and shall be based on documentation, policies, implemented security measures and information relating to the suppliers and infrastructures used by AssessFirst.

Where an on-site audit is strictly necessary and proportionate in light of the Processing activities involved, the parties shall agree the applicable practical arrangements in good faith. It should be noted that AssessFirst does not operate dedicated premises for Processing Personal Data, and Processing is carried out through cloud infrastructures and secure remote working arrangements.

The Customer shall bear all audit-related costs. In the event of material non-compliance with this DPA that is duly established and exclusively attributable to AssessFirst, AssessFirst shall bear the reasonable costs of remediation.

Prior to any audit, AssessFirst may require the Customer (and, where applicable, its auditor) to sign a confidentiality undertaking covering trade secrets, security-related information, and other sensitive information in particular. AssessFirst may refuse an auditor in the event of a manifest conflict of interest or serious risks to confidentiality or security.

16. LIABILITY

The liability of the Parties to this DPA shall be governed by the Contract to which this DPA is appended, subject to the mandatory provisions of the GDPR, in particular Article 82.

17. CONTACT - DPO

AssessFirst has appointed a Data Protection Officer (DPO), who is registered with the French supervisory authority (CNIL).

For any questions relating to this DPA, the Customer may contact the DPO by email at: privacy@assessfirst.com.

18. GOVERNING LAW

This DPA shall be governed by the same law as the Contract to which it is appended.

ANNEX 1 DPA – DESCRIPTION OF THE PROCESSING

Element	Description
Data Subjects	Customer's Candidates
Categories of Personal Data	- Contact details: email address - Professional and assessment data defined by the Customer (e.g., CV, location, type of contract sought, professional experience) - Results generated by the Service consisting of an automated analysis of the correspondence between the Candidate's responses and the criteria defined by the Customer - Voice recordings (optional – oral mode only) - Technical data : IP address, access logs, browsing and click data
Nature of the Processing	Collection, recording, organisation, structuring, storage, automated analysis, transmission of results to the Customer, and deletion
Purpose of the Processing	Pre-qualification / assessment of the Customer's Candidates exclusively on behalf of the Customer and in accordance with its instructions
Duration of the Processing	Determined by the Customer through the Service settings. In the absence of specific instructions from the Customer, the Personal Data shall be retained for the duration of the Contract.

ANNEX 2 DPA – TECHNICAL AND ORGANISATIONAL MEASURES

AssessFirst implements the measures described below, or equivalent measures, in order to ensure a level of security appropriate to the risk, within the meaning of Article 32 of the GDPR:

1. TECHNICAL SAFETY MEASURES

- Authentication measures: (i) strong authentication with 2FA for companies; (ii) use of a unique identifier per user, (iii) compliance with CNIL recommendations for password management.
- Network security: (i) end-to-end HTTPS encrypted transmission between the server and third parties, (ii) functional division of the network into sub-networks to guarantee security: separation of test and production environments, (iii) access logging and incident management, (iv) logging of accesses, anomalies and security events, (v) use of a web firewall and regularly updated antivirus software, (vi) installation of vulnerability detection tools.
- Hosting and backup: (i) hosting provided by Amazon Web Services on ISO 27001-certified servers located in the EU, (ii) SSL encryption of backups during transfer, (iii) encryption of hosted and transferred data.
- AWS physical security measures: (i) access control (badges, locked doors and cupboards, retention of physical access for 45 days), (ii) 24/7 video surveillance, (iii) intruder alarm, (iv) fire alarm system.



2. ORGANIZATIONAL SAFETY MEASURES

- Employee management: (i) background checks, (ii) confidentiality obligations and IT charter for staff, (iii) authorization management with annual review, (iv) staff awareness of privacy risks.
- Compliance and data management: (i) appointment of a Data Protection Officer (DPO), (ii) regularly updated register of Processing activities, (iii) outsourcing only to Sub-processors offering sufficient guarantees, (iv) systematic verification of the compliance of subsequent Sub-processors, (v) creation of a legal department dedicated to compliance.
- Incident management: (i) establishment of a procedure for safety events, (ii) training of personnel in the procedure, (iii) transmission of safety events to an emergency team, (iv) event analysis by a member of the emergency team, (v) information to all teams on the causes and consequences of the incident to prevent its recurrence, (vi) in-depth examination by the maintenance team, the departments concerned and in particular the legal and communications departments.
- Participation in security programs: (i) setting up a review system on YesWeHack to identify and reduce data security risks via an invitation, (ii) controlled access to source code.

3. OWASP COMPLIANCE

- A01:2021-Access control failure: AssessFirst implements strict access control policies, including two-factor authentication, appropriate session management and periodic access reviews. They also feature appropriate logging for all sensitive actions and access attempts.
- A02:2021-Cryptographic failures: AssessFirst uses secure SSL/TLS connections and data encryption to protect data in transit and at rest. They also adhere to strict password policies and manage cryptographic keys securely.
- A03:2021-Injection: the company's development processes include secure coding practices and vulnerability testing, which helps prevent injection vulnerabilities. They also follow the principle of least privilege to minimize potential damage.
- A04:2021-Conception Insecure: AssessFirst designs applications and processes with privacy and security in mind, following the principles of privacy by design and by default.
- A05:2021-Security Misconfiguration: AssessFirst maintains strict security configurations and reviews and updates them regularly. It also monitors for unauthorized modifications to system parameters.
- A06:2021-Vulnerable and obsolete components: AssessFirst is committed to keeping software components up-to-date and uses third-party security solutions to scan for vulnerabilities.
- A07:2021 - Identification and authentication failures: AssessFirst implements appropriate identification and authentication measures, such as strong password policies, two-factor authentication and regular access reviews.
- A08:2021-Software and data integrity failures: AssessFirst has a robust backup and disaster recovery plan to protect and restore software and data in the event of failure.
- A09:2021-Deficiencies in security logging and monitoring: AssessFirst logs all sensitive events and ensures that the necessary information is present in the log entries. It also has a defined log retention period and an incident response procedure.
- A10:2021-Server-side request forgery: AssessFirst's security practices, such as secure coding and regular vulnerability testing, help prevent server-side request forgery vulnerabilities.