DATA PROCESSING AGREEMENT (DPA) – SCAN SERVICE

Version 1.3 - Date of update: 27 October 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:

"Candidate" means any natural person using the SCAN Service for the Customer's recruitment purposes.

"Customer" means any natural person and/or legal entity acting within the scope of its professional activity and having signed a Contract with AssessFirst.

"Contract" means the contractual arrangement between AssessFirst and the Customer for the provision of the SCAN Service, comprising, as applicable, a purchase order accompanied by AssessFirst's General Terms and Conditions of Sale, a specific contract or any other contractual document accepted by the Parties.

"Personal Data" means any information relating to an identified or identifiable natural person within the meaning of the GDPR.

"Data Protection Laws" means 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 "**GDPR**") and, more generally, any applicable legislation relating to the protection of personal data.

"Service" means the SCAN module to which the Customer has access through its subscription to the AssessFirst platform.

"Sub-processor" means any processor engaged by AssessFirst to process Personal Data on behalf of the Customer in connection with the SCAN Service.

"Personal Data Breach" means 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.

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

2. Purpose and Scope

This data processing agreement (hereinafter the "DPA") sets out the terms under which AssessFirst processes Candidates' Personal Data on behalf of the Customer within the SCAN module.

This DPA is incorporated by reference into the Contract and is deemed accepted by the Customer upon signature.

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

This DPA applies exclusively to the SCAN Service. It is expressly agreed that any other services provided by AssessFirst to the Customer are performed in AssessFirst's capacity as a separate Controller and are not covered by this DPA.

AssessFirst reserves the right to amend this DPA in order to take into account legal, regulatory, case-law or technical developments.

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

3. Description of the Processing

The characteristics of the Processing entrusted to AssessFirst are set out in Annex 1 to this DPA, including in particular:

- 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 alone determines the purposes and essential means of the Processing. AssessFirst shall process Personal Data only on the documented instructions of the Customer.

The Service does not make any decision based solely on automated Processing within the meaning of Article 22 of the GDPR. Scores, statuses and recommendations are a decision aid for the Customer. Candidates who do not meet the conditions for automatic progression set by the Customer remain visible to the Customer; no rejection or refusal notification is triggered automatically.

Where the Customer connects its applicant tracking system (ATS) to the Service, AssessFirst retrieves, through the application programming interface (API) of that tool and on the Customer's instruction, the CVs of only those Candidates for whom the Customer has triggered an AssessFirst assessment from that tool, and sends back to it, on the Customer's instruction, the pre-qualification status of those Candidates.

The Customer's instructions may in particular be given through the settings made available in the Service or, where applicable, by any written instruction from the Customer, within the limits of the Service's functionalities and of this DPA.
In the event of any discrepancy, the most recent documented instructions that comply with the 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 regulations;
- ensure that it has a valid legal basis, appropriate to the recruitment context, for the Processing carried out through the Service;
- inform Data Subjects in accordance with Articles 12 to 14 of the GDPR, including, where the CV is retrieved from its ATS, about the analysis of that CV by AssessFirst, as Candidates may not access the AssessFirst platform or the information notices displayed on it;
- provide AssessFirst with lawful, documented instructions that comply with the GDPR;
- determine the retention period applicable to the Personal Data processed through the Service, appropriate to its legal obligations and to the storage limitation principle set out in Article 5(1) of the GDPR;
- retain control over the decision on the outcome of each application, and not base a rejection decision solely on the score or status generated by the Service;
- 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 and of the instructions given to AssessFirst.

5. Sensitive Data

By default, the SCAN Service is not intended for the Processing of special categories of data within the meaning of Article 9 of the GDPR or data relating to criminal convictions and offences (Article 10).

Accordingly, the Customer undertakes not to include, in the Personal Data processed through the Service, any special categories of Personal Data, data relating to criminal convictions and offences, or "sensitive" data within the meaning of Articles 9 and 10 of the GDPR and Article 6 of French Law No. 78-17 (the "Informatique et Libertés" Act), nor any other category of personal data subject to a derogatory regime, except where required by law or subject to a specific documented instruction, and to implement appropriate safeguards where applicable.

SCAN Interview: in the context of the use of the SCAN Service in oral mode, any voice data that may be processed are not used by AssessFirst to uniquely identify a natural person and therefore do not constitute biometric data within the meaning of Article 4(14) of the GDPR, nor special categories of data within the meaning of Article 9 of the GDPR.

SCAN CV: the CV submitted by the Candidate may contain information falling within Articles 9 or 10 of the GDPR that the Candidate has mentioned spontaneously. AssessFirst implements measures aimed at limiting the extraction of data from the CV to the categories described in Annex 1 and, for other information, to information directly related to the position only, excluding in particular nationality and origin. Any photograph on the CV is not used for pre-qualification and is not subject to any Processing aimed at uniquely identifying a natural person; it therefore does not constitute biometric data within the meaning of Article 4(14) of the GDPR.

6. AssessFirst's obligations (Processor)

6.1. General obligations

AssessFirst undertakes to:

- process Personal Data only on the documented instructions of the Customer, 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 available to the Customer the information necessary to demonstrate compliance with this DPA.

AssessFirst undertakes to process Personal Data only for the purposes of providing the Service, in accordance with the Customer's documented instructions.

The Customer authorises AssessFirst to anonymise, at the end of the Service, information derived from the Personal Data processed, in order to use it for research, security, service improvement and the development of its artificial intelligence models. For this anonymisation operation, AssessFirst acts as a separate Controller. Information that has been effectively anonymised no longer constitutes Personal Data within the meaning of the Data Protection Laws.

6.2. Record of Processing Activities

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

- the name and contact details of the Controller, of any Sub-processors and of 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 it, in order to enable the Customer to comply with its obligations in respect of:

- requests to exercise the rights of Data Subjects;
- the notification of Personal Data Breaches;
- carrying out data protection impact assessments (DPIAs) and, where applicable, prior consultation;
- and, more generally, compliance with the obligations set out in the GDPR.

This assistance does 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 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, under an applicable legal obligation, to disclose Personal Data processed on behalf of the Customer, AssessFirst shall inform the Customer prior to any disclosure, to the extent permitted by law, and shall provide it with the information reasonably necessary to enable it to challenge or seek to limit the scope of such disclosure.

Where the law prohibits such notification, 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

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

- the state of the art,
- the costs of implementation,
- the nature, scope, context and purposes of the Processing,
- as well as 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 SCAN service are described in Annex 2 to this DPA.

8. Confidentiality of Personal Data

AssessFirst ensures the confidentiality of Personal Data and ensures that only authorised persons have access to it, strictly to the extent necessary for the performance of the Service. In particular, AssessFirst undertakes to:

- process Personal Data only for the purpose of performing the Service, in accordance with the Customer's documented instructions;
- restrict access to Personal Data to those persons (employees, suppliers and Sub-processors) who need to know it for the performance of the Service and who are subject to an appropriate confidentiality obligation;

- not disclose Personal Data to any third party, except (a) authorised personnel, (b) Sub-processors compliant with this DPA, or (c) where required by law (under the conditions of the “Mandatory disclosure” section);
- implement measures designed to prevent any unauthorised, improper or fraudulent access to the systems processing Personal Data;
- apply, where applicable, the principles of data protection by design and by default.

Information exchanged between the Parties in the course of their contractual relationship may constitute trade secrets within the meaning of Articles L.151-1 et seq. of the French Commercial Code. The Parties shall take all necessary measures to protect such 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, for the purpose of Processing Personal Data in connection with the provision of the Service, the Sub-processors listed in the online FAQ accessible at the following link: https://help.assessfirst.com/en/knowledge/client-faq.

AssessFirst shall ensure that each Sub-processor is bound by contract to obligations at least equivalent to those of this DPA. AssessFirst remains 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 via a notification in 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 raised within that period, the Parties shall discuss in good faith in order to find a reasonable alternative solution that maintains 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 solution can be implemented within the same timeframe, the Customer may terminate the entire 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 the fate of the data shall remain fully applicable.

10. Data Location

Personal Data processed in connection with the Service are hosted by AssessFirst exclusively within the European Union, via the Amazon Web Services (AWS) cloud infrastructure.

For Candidates located within the European Union, no transfer of Personal Data outside the European Union is carried out.
For Candidates located outside the European Union, certain Sub-processors may process data from servers located in the geographic region closest to the Candidate; such Processing is subject to appropriate safeguards in accordance with Chapter V of the GDPR (standard contractual clauses or the EU-US Data Privacy Framework).

11. Data Subjects' Rights

Where a request to exercise rights under Articles 15 to 22 of the GDPR is addressed to AssessFirst, AssessFirst shall forward it to the Customer by email, to the address provided by the Customer, together with any relevant information available to AssessFirst.

Upon the Customer's reasonable request, AssessFirst shall assist the Customer, to the extent possible, in facilitating the exercise of Data Subjects' rights under the GDPR (Articles 15 to 22) and in enabling the Customer to comply with the applicable legal deadlines.

AssessFirst shall not respond directly to Data Subjects, unless expressly instructed to do so by the Customer. Where necessary, AssessFirst may help the Data Subject to identify the Customer as the Controller and to obtain its contact details.

12. Personal Data Breaches

AssessFirst shall notify the Customer of any Personal Data Breach as soon as possible after becoming aware of it and, where feasible, within forty-eight (48) hours.

The notification shall contain, to the extent possible, the information provided for in Article 33(3) of the GDPR, in particular:

- the nature of the breach;
- the categories and approximate number of Data Subjects concerned;
- the categories and approximate number of data records concerned;
- the likely consequences;
- the measures taken or proposed to remedy the breach and mitigate its possible adverse effects;
- the contact point from which further information can be obtained.

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

AssessFirst shall cooperate in good faith with the Customer to remedy the breach and limit its effects, and to help the Customer comply with its obligations to notify the supervisory authority and/or Data Subjects.

13. Regulatory assistance and cooperation

In addition to the provisions of Article 6.3 of this DPA, AssessFirst shall cooperate with and assist the Customer, to the extent reasonable, taking into account the information available to it and within the limits of its role as Processor, in the event of a request or an inquiry by a data protection authority concerning Processing carried out under the Service, to the extent permitted by law.

14. Fate of data at the end of the contract

Upon the Customer's instruction and, in any event, upon expiry of the Contract, AssessFirst undertakes, within a reasonable period, to:

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

as chosen by the Customer.

This obligation includes the deletion or return of Personal Data contained in backups, unless retention is required by law or for evidentiary purposes in the context of a dispute, in which case deletion shall take place upon expiry of the applicable legal period.

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

The deletion or return obligations set out in this article do not apply to information anonymised under the conditions set out in Article 6.1, which no longer constitutes Personal Data.

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, in particular in the form of recent third-party certifications and/or audit reports or equivalent documents (the “Audit Documents”), which are confidential.

Unless required by regulation or in the event of a major incident warranting an additional audit, audits are limited to one (1) audit per contractual year and relate exclusively to the Processing activities carried out by AssessFirst on behalf of the Customer under the Service.

Audits are carried out primarily remotely, on the basis of documentation, procedures, the security measures implemented, and information relating to the suppliers and infrastructures used by AssessFirst.

Where, exceptionally, an on-site audit proves strictly necessary and proportionate in view of the Processing concerned, the Parties shall agree in good faith on the practical arrangements, it being specified that AssessFirst does not have premises dedicated to the Processing of Personal Data and that Processing is carried out using cloud infrastructures and secure remote-working arrangements.

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

Prior to any audit, AssessFirst may require the Customer (and, where applicable, its auditor) to sign a confidentiality undertaking covering in particular trade secrets, security and sensitive information. 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 under this DPA is governed by the Contract, subject to the mandatory provisions of the GDPR, in particular Article 82.

17. Contact - DPO

AssessFirst has appointed a DPO, registered with the CNIL (the French supervisory authority).
For any question relating to this DPA, the Customer may contact the DPO by email at privacy@assessfirst.com.

18. Governing law

This DPA is governed by the law applicable to the Contract, into which it is incorporated by reference.

ANNEX 1 DPA – DESCRIPTION OF THE PROCESSING

Element	Description
Data Subjects	Customer's Candidates
Categories of data	Contact details: email address Professional and assessment data defined by the Customer (e.g., CV, location, type of contract sought, professional experience) Technical data: IP address, access logs, browsing and click data. SCAN CV: - CV and data derived from the CV (professional experience; education; skills, tools, languages and estimated language level (CEFR); certifications; other information on the CV directly related to the position; photograph for profile display only); - Pre-qualification status by criterion. SCAN Interview: - Results generated by the Service (automated analysis of the match between the Candidate's responses and the criteria defined by the Customer). - Audio stream of the responses, transcribed in real time and not stored, and transcriptions of the responses (oral mode) - Candidate's written responses (written mode)
Nature of the Processing	Collection, organisation, structuring, storage of the transcription, automated extraction of data from the CV, automated analysis, transmission of results to the Customer, and deletion.
Purposes of the Processing	Pre-qualification 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, the data are retained until the expiry of the Contract. SCAN CV: the CV and the data extracted from it are deleted at the same time as the Candidate's profile. SCAN Interview: the audio stream is not stored.

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 SECURITY 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) logging of accesses and incident management, (iv) logging of accesses, anomalies and security events, (v) use of a web application 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 cabinets, retention of physical access records for 45 days), (ii) 24/7 video surveillance, (iii) intruder alarm, (iv) fire alarm system.

2. Organisational security measures

- Employee management: (i) background checks, (ii) confidentiality obligations and IT charter for staff, (iii) authorisation 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 record of Processing activities, (iii) outsourcing only to Sub-processors offering sufficient guarantees, (iv) systematic verification of the compliance of Sub-processors, (v) creation of a legal department dedicated to compliance.
- Incident management: (i) establishment of a procedure for security events, (ii) training of personnel in the procedure, (iii) transmission of security events to an emergency team, (iv) analysis of the event 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 review by the maintenance team and the departments concerned, in particular the legal and communications departments.
- Participation in security programmes: (i) setting up a review system on YesWeHack to identify and reduce data security risks via an invitation, (ii) controlled access to the programme.

3. OWASP Compliance

- A01:2021-Broken access control: AssessFirst implements strict access control policies, including two-factor authentication, appropriate session management and periodic access reviews. Appropriate logging is also in place 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. It also adheres to strict password policies and manages cryptographic keys securely.
- A03:2021-Injection: the company's development processes include secure coding practices and vulnerability testing, which help prevent injection vulnerabilities. It also follows the principle of least privilege to minimise potential damage.
- A04:2021-Insecure design: 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 unauthorised changes to system settings.
- A06:2021-Vulnerable and outdated 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-Security logging and monitoring failures: 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.