



ASSESSFIRST
CONNECTING WITH MEANING

ACCORD DE TRAITEMENT DES DONNÉES PERSONNELLES (DPA) – SERVICE SCAN

Version 1.1 - Date de mise à jour : 29 septembre 2026

1. DÉFINITIONS

Aux fins du présent Accord, les termes ci-dessous ont la signification suivante, qu'ils soient utilisés au singulier ou au pluriel :

« **Candidats** » : désigne les personnes physiques dont les Données à Caractère Personnel sont traitées dans le cadre du Service SCAN pour les besoins de recrutement du Client, et qui constituent des Personnes Concernées au sens du RGPD.

« **Client** » : désigne toute personne physique et/ou morale agissant dans le cadre de son activité professionnelle et ayant signé un Contrat avec AssessFirst.

« **Contrat** » : désigne l'ensemble contractuel liant AssessFirst et le Client pour la fourniture du Service SCAN, comprenant selon les cas un bon de commande accompagné des Conditions Générales de Vente AssessFirst, un contrat spécifique ou tout autre document contractuel accepté par les Parties.

« **Données à Caractère Personnel** » : toute information se rapportant à une personne physique identifiée ou identifiable, au sens du RGPD.

« **Réglementation sur la Protection des Données** » désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le « **RGPD** ») et, plus généralement, toute réglementation applicable en matière de protection des données personnelles.

« **Service** » : désigne le module SCAN auquel le Client a accès via son abonnement à la plateforme AssessFirst.

« **Sous-traitant Ulérieur** » : tout sous-traitant engagé par AssessFirst pour traiter des Données à Caractère Personnel pour le compte du Client dans le cadre du Service SCAN.

« **Violation de données** » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, au sens du RGPD.

« **Responsable de traitement** », « **Sous-traitant** », « **Personne Concernée** » et « **Traitement** » : ont la signification donnée par le RGPD.

2. OBJET ET CHAMP D'APPLICATION

Le présent accord relatif au traitement des données personnelles (ci-après le « DPA ») a pour objet de définir les conditions dans lesquelles AssessFirst traite des Données à Caractère Personnel des Candidats pour le compte du Client dans le cadre du module SCAN.

Le présent DPA est intégré par référence au Contrat et est réputé accepté par le Client lors de la souscription du Service SCAN.

Dans le cadre du Service, le Client agit en qualité de Responsable de traitement et AssessFirst agit en qualité de Sous-traitant.



ASSESSFIRST
CONNECTING WITH MEANING

Le présent DPA s'applique exclusivement au Service SCAN. Il est expressément convenu que les éventuels autres services fournis par AssessFirst au Client sont réalisés en qualité de Responsable de traitement distinct et ne relèvent pas du présent DPA.

AssessFirst se réserve le droit de modifier le présent DPA afin de tenir compte des évolutions légales, réglementaires, jurisprudentielles ou techniques. Toute modification substantielle sera notifiée au Client par tout moyen approprié.

En cas de contradiction entre le présent DPA et le Contrat, le DPA prévaut pour tout ce qui concerne le Traitement des Données à Caractère Personnel par AssessFirst en qualité de Sous-traitant dans le cadre du Service.

3. DESCRIPTION DES TRAITEMENTS

Les caractéristiques du Traitement confié à AssessFirst sont décrites en Annexe 1 du présent DPA, notamment :

- la nature des opérations de Traitement,
- les finalités du Traitement,
- les catégories de Données à Caractère Personnel traitées,
- les catégories de Personnes Concernées,
- la durée du Traitement.

Le Client détermine seul les finalités et les moyens essentiels du Traitement. AssessFirst traite les Données à Caractère Personnel uniquement sur instruction documentée du Client.

Les instructions du Client peuvent notamment être transmises via les paramétrages mis à disposition dans le Service, ou, le cas échéant, par toute instruction écrite du Client, dans les limites des fonctionnalités du Service et du présent DPA.

En cas de divergence, les instructions documentées les plus récentes et conformes à la Réglementation sur la Protection des Données prévalent.

4. OBLIGATIONS DU CLIENT (RESPONSABLE DE TRAITEMENT)

Le Client s'engage à :

- traiter les Données à Caractère Personnel conformément à la Réglementation sur la Protection des Données et, de façon générale, à toute réglementation applicable ;
- disposer d'une base légale valide, appropriée au contexte du recrutement, pour les traitements mis en œuvre dans le cadre du Service ;
- informer les Personnes Concernées conformément aux articles 12 à 14 du RGPD ;
- fournir à AssessFirst des instructions documentées, licites et conformes au RGPD ;
- déterminer la durée de conservation applicable aux Données à Caractère Personnel traitées dans le cadre du Service, adaptée à ses obligations légales et au principe de limitation de la conservation prévu à l'article 5(1) du RGPD ;
- s'assurer que seules les personnes autorisées ont accès au Service et aux comptes utilisateurs.

Le Client demeure seul responsable de la licéité des traitements et des instructions transmises à AssessFirst.

5. DONNÉES SENSIBLES

Le Service SCAN n'est pas destiné, par défaut, au traitement de catégories particulières de données au sens de l'article 9 du RGPD ou de données relatives aux condamnations et infractions (article 10).

A ce titre, le Client s'engage à ne pas inclure, dans les Données à Caractère Personnel traitées dans le cadre du Service, de catégories particulières de Données à Caractère Personnel dites « sensibles » au sens des articles 9

et 10 du RGPD, sauf obligation légale ou instruction spécifique documentée, et à mettre en œuvre les garanties appropriées le cas échéant.

Il est précisé que, dans le cadre de l'utilisation du Service SCAN en mode oral, les données vocales potentiellement traitées ne sont pas utilisées par AssessFirst aux fins d'identifier de manière unique une personne physique et ne constituent donc pas des données biométriques au sens de l'article 4(14) du RGPD, ni des catégories particulières de données au sens de l'article 9 du RGPD.

6. OBLIGATIONS D'ASSESSFIRST (SOUS-TRAITANT)

6.1. OBLIGATIONS GÉNÉRALES

AssessFirst s'engage à :

- traiter les données personnelles uniquement sur instruction documentée du Client, y compris en ce qui concerne les transferts de Données à Caractère Personnel ;
- informer immédiatement le Client si, selon elle, une instruction constitue une violation de la Réglementation sur la Protection des Données ;
- veiller à ce que les personnes autorisées à traiter les Données à Caractère Personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- mettre en œuvre et maintenir les mesures techniques et organisationnelles appropriées afin d'assurer un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD et telles que décrites en Annexe 2 ;
- supprimer ou restituer au Client les Données à Caractère Personnel au terme de la fourniture du Service, conformément à l'article 14 du présent DPA ;
- tenir à disposition du Client les informations nécessaires pour démontrer le respect du présent DPA.

AssessFirst s'engage à ne traiter les Données à Caractère Personnel que pour les besoins de la fourniture du Service, conformément aux instructions documentées du Client.

Le Client est informé qu'AssessFirst peut utiliser, à des fins de recherche, de sécurité, d'amélioration des services et de développement de ses modèles d'intelligence artificielle, des informations ayant fait l'objet d'une anonymisation préalable irréversible, ne permettant plus l'identification directe ou indirecte des Personnes Concernées. Ces informations anonymisées ne constituent plus des Données à Caractère Personnel au sens de la Réglementation sur la Protection des Données, et sont traitées en dehors du champ d'application de celui-ci.

6.2. REGISTRE DES ACTIVITÉS DE TRAITEMENT

AssessFirst tient un registre des catégories d'activités de traitement effectuées pour le compte du Client, comprenant les informations prévues à l'article 30(2) du RGPD :

- le nom et les coordonnées du responsable du traitement, des éventuels sous-traitants ultérieurs et du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte du Client ;
- les éventuels transferts de Données à Caractère Personnel vers un pays tiers ou à une organisation internationale, et l'identification de ce pays tiers ou de cette organisation internationale avec, le cas échéant, les documents attestant de l'existence de garanties appropriées
- une description générale des mesures de sécurité techniques et organisationnelles prises pour assurer la protection des Données à Caractère Personnel.

6.3. ASSISTANCE

AssessFirst assiste le Client, dans la mesure du raisonnable et compte tenu de la nature du traitement et des informations à sa disposition, afin de permettre au Client de respecter ses obligations au titre :

- des demandes d'exercice des droits des Personnes concernées ;
- de la notification des Violations de données ;
- de la réalisation d'analyses d'impact (AIPD) et, le cas échéant, de la consultation préalable ;
- et plus généralement, du respect des obligations prévues par le RGPD.

Cette assistance ne transfère pas à AssessFirst les responsabilités incombant au Client en sa qualité de Responsable de traitement.



ASSESSFIRST
CONNECTING WITH MEANING

6.4. DIVULGATION OBLIGATOIRE

Dans la mesure permise par la loi, AssessFirst informe le Client sans retard indu de toute demande émanant d'une autorité publique ou judiciaire relative aux Données à Caractère Personnel traitées pour le compte du Client dans le cadre du Service.

Si AssessFirst est tenue, en vertu d'une obligation légale applicable, de divulguer des Données à caractère personnel traitées pour le compte du Client, AssessFirst en informe le Client avant toute divulgation, dans la mesure permise par la loi, et lui fournit les informations raisonnablement nécessaires afin de lui permettre de contester ou de demander des mesures visant à limiter la portée de cette divulgation.

Lorsque la loi interdit une telle notification, AssessFirst informe le Client dès que cette interdiction est levée.

Toute divulgation est strictement limitée aux Données à Caractère Personnel exigées par l'obligation légale applicable.

7. SÉCURITÉ DES DONNÉES À CARACTÈRE PERSONNEL

AssessFirst met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD.

Ces mesures tiennent compte :

- de l'état des connaissances,
- des coûts de mise en œuvre,
- de la nature, de la portée, du contexte et des finalités du traitement,
- ainsi que des risques pour les droits et libertés des personnes concernées.

AssessFirst est certifiée ISO/IEC 27001 et maintient un système de management de la sécurité de l'information conforme à cette norme.

Les mesures de sécurité applicables au service SCAN sont décrites en Annexe 2 du présent DPA.

8. CONFIDENTIALITÉ DES DONNÉES À CARACTÈRE PERSONNEL

AssessFirst garantit la confidentialité des Données à Caractère Personnel et veille à ce que seules les personnes habilitées y aient accès, dans la stricte mesure nécessaire à l'exécution du Service. AssessFirst s'engage notamment à :

- ne traiter les Données à Caractère Personnel qu'aux fins d'exécuter le Service, conformément aux instructions documentées du Client ;
- limiter l'accès aux Données à Caractère Personnel aux seules personnes (salariés, prestataires et Sous-traitants ultérieurs) ayant besoin d'en connaître pour l'exécution du Service, et soumises à une obligation de confidentialité appropriée ;
- ne communiquer les Données à Caractère Personnel à aucun tiers, sauf (a) personnel habilité, (b) Sous-traitants ultérieurs conformes au présent DPA, ou (c) obligation légale (dans les conditions de l'article "Divulgation obligatoire") ;
- mettre en œuvre des mesures destinées à prévenir tout accès non autorisé, détourné ou frauduleux aux systèmes traitant les Données à Caractère Personnel ;
- appliquer, dans la mesure applicable, les principes de protection des données dès la conception et par défaut.

Les informations échangées entre les Parties dans le cadre de leurs relations contractuelles peuvent relever du secret des affaires au sens des articles L.151-1 et suivants du Code de commerce. Les Parties mettent en œuvre les moyens nécessaires pour préserver ces informations, conformément aux obligations de confidentialité prévues au Contrat et au présent DPA.



ASSESSFIRST
CONNECTING WITH MEANING

9. RECOURS À DES SOUS-TRAITANTS ULTÉRIEURS

Le Client autorise expressément AssessFirst à engager les Sous-traitants Ultérieurs listés dans la [FAQ en ligne](#) pour traiter les Données à caractère personnel aux fins de fourniture du Service.

AssessFirst s'assure que tout Sous-traitant Ultérieur est soumis, par contrat, à des obligations au moins équivalentes à celles du présent DPA. AssessFirst demeure pleinement responsable envers le Client de l'exécution des obligations du Sous-traitant Ultérieur.

AssessFirst informe le Client de tout ajout ou remplacement de Sous-traitant ultérieur avant que ce changement ne produise ses effets sur le Service. L'information pourra être réalisée par email et/ou via une notification dans le compte Client.

Le Client peut formuler des objections pour des motifs légitimes liés à la protection des données personnelles, dans un délai de 15 jours ouvrés à compter de la notification. En cas d'objection recevable formulée par le Client dans le délai susmentionné, les Parties se rapprocheront de bonne foi afin de rechercher une solution alternative raisonnable permettant de maintenir un niveau de protection des données équivalent.

Lorsque le Sous-traitant Ultérieur concerné réalise une fonction essentielle et non substituable du Service, sans laquelle le Service ne peut être fourni de manière équivalente, et qu'aucune solution raisonnable ne peut être mise en œuvre dans le même délai, le Client pourra résilier l'intégralité du Service concerné, sans pénalité, moyennant un préavis écrit de trente (30) jours.

Jusqu'à la prise d'effet de la résiliation, AssessFirst continue de traiter les Données à Caractère Personnel conformément au présent DPA et aux instructions du Client. Les obligations relatives à la sécurité, à la confidentialité et au sort des données demeurent pleinement applicables.

10. LOCALISATION DES DONNÉES

Les Données à caractère personnel traitées dans le cadre du Service sont hébergées exclusivement au sein de l'Union européenne, via l'infrastructure cloud d'Amazon Web Services (AWS).

Aucun transfert de données personnelles hors de l'Union européenne n'est réalisé dans le cadre du Service.

11. DROITS DES PERSONNES CONCERNÉES

Lorsqu'une demande d'exercice de droits au titre des articles 15 à 22 du RGPD est adressée à AssessFirst, AssessFirst la transmet au Client par courrier électronique à l'adresse communiquée par le Client, accompagnée des informations utiles dont AssessFirst dispose.

Sur demande raisonnable du Client, AssessFirst l'assiste, dans la mesure du possible, afin de faciliter l'exercice des droits des Personnes Concernées prévus par le RGPD (articles 15 à 22), et de permettre au Client de respecter les délais légaux applicables.

AssessFirst ne répond pas directement aux Personnes Concernées, sauf instruction expresse du Client. Lorsque cela est nécessaire, AssessFirst peut aider la personne concernée à identifier le Client en tant que Responsable de traitement et à lui communiquer ses coordonnées.

12. VIOLATIONS DE DONNÉES

AssessFirst notifie au Client toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance et, lorsque cela est possible, dans un délai de quarante-huit (48) heures.

La notification contient, dans la mesure du possible, les informations prévues à l'article 33(3) du RGPD, notamment :



ASSESSFIRST
CONNECTING WITH MEANING

- la nature de la violation ;
- les catégories et le nombre approximatif de Personnes concernées ;
- les catégories et le nombre approximatif d'enregistrements de données concernés ;
- les conséquences probables ;
- les mesures prises ou proposées pour remédier à la violation et en atténuer les effets ;
- le point de contact pour obtenir des informations supplémentaires.

AssessFirst tient un registre documenté des Violations de Données à caractère personnel, incluant les faits, leurs effets et les mesures correctives prises, conformément à l'article 33(5) du RGPD.

AssessFirst coopère de bonne foi avec le Client afin de remédier à la violation et d'en limiter les effets, et d'aider le Client à respecter ses obligations de notification à l'autorité de contrôle et/ou aux Personnes Concernées.

13. ASSISTANCE ET COOPÉRATION RÉGLEMENTAIRE

En complément des dispositions de l'article 6.2 du présent DPA, AssessFirst coopère et assiste le Client, dans la mesure du raisonnable, compte tenu des informations dont elle dispose, et dans les limites de son rôle de Sous-traitant, en cas de demande ou de contrôle d'une autorité de protection des données portant sur les traitements réalisés dans le cadre du Service, dans la mesure permise par la loi.

14. SORT DES DONNÉES EN FIN DE CONTRAT

Sur instruction du Client et dans tous les cas à l'expiration du Contrat, AssessFirst s'engage, dans un délai raisonnable, à :

- supprimer les Données à Caractère Personnel du Client, et/ou
- restituer les Données à Caractère Personnel du Client,

selon le choix exprimé par le Client.

Cette obligation inclut la suppression ou la restitution des Données à Caractère Personnel contenues dans les sauvegardes, sauf obligation légale de conservation ou conservation à des fins probatoires dans le cadre d'un contentieux, auquel cas la suppression intervient à l'issue du délai légal applicable.

Sur demande du Client, AssessFirst fournit une attestation écrite confirmant la suppression des Données à Caractère Personnel.

Les obligations de suppression ou de restitution prévues au présent article ne s'appliquent pas aux informations ayant fait l'objet d'une anonymisation irréversible, lesquelles ne constituent plus des Données à Caractère Personnel et peuvent être conservées et utilisées par AssessFirst conformément au présent DPA à des fins de recherche et d'amélioration de ses services.

15. AUDITS

AssessFirst met à disposition du Client, sur demande écrite et à intervalles raisonnables, les informations nécessaires pour démontrer le respect du présent DPA, notamment sous la forme de certifications et/ou rapports d'audit tiers récents ou documents équivalents (les « Documents d'audit »), lesquels sont confidentiels.

Sauf exigence réglementaire ou incident majeur justifiant un audit additionnel, les audits sont limités à un (1) audit par année contractuelle, et portent exclusivement sur les activités de traitement effectuées par AssessFirst pour le compte du Client dans le cadre du Service.

Les audits sont réalisés prioritairement à distance, sur la base de la documentation, des procédures, des mesures de sécurité mises en œuvre, et des informations relatives aux fournisseurs et infrastructures utilisés par AssessFirst.



ASSESSFIRST
CONNECTING WITH MEANING

Lorsque, à titre exceptionnel, un audit sur site s'avère strictement nécessaire et proportionné au regard des traitements concernés, les Parties conviennent de bonne foi des modalités pratiques applicables, étant précisé qu'AssessFirst ne dispose pas de locaux dédiés au traitement des données personnelles et que les traitements sont réalisés au moyen d'infrastructures cloud et de dispositifs de télétravail sécurisés.

Le Client supporte l'intégralité des coûts d'audit. En cas de non-conformité majeure au présent DPA dûment établie et imputable exclusivement à AssessFirst, les coûts raisonnables de remédiation seront à la charge d'AssessFirst.

Avant tout audit, AssessFirst peut demander au Client (et le cas échéant son auditeur) de signer un engagement de confidentialité couvrant notamment le secret des affaires, la sécurité, et les informations sensibles. AssessFirst peut refuser un auditeur en cas de conflit d'intérêts manifeste ou de risques sérieux pour la confidentialité ou la sécurité.

16. RESPONSABILITÉ

La responsabilité des Parties au titre du présent DPA est régie par le Contrat, sous réserve des dispositions impératives du RGPD, notamment l'article 82.

17. POINT DE CONTACT - DPO

AssessFirst a désigné un DPO auprès de la CNIL.

Pour toute question relative au présent DPA, le Client peut le contacter par courriel à l'adresse privacy@assessfirst.com.

18. DROIT APPLICABLE

Le présent DPA est régi par le droit applicable au Contrat auquel il est intégré par référence.



ANNEXE 1 DPA – DESCRIPTION DU TRAITEMENT

Élément	Description
Personnes Concernées	Candidats du Client
Catégories de données	- Coordonnées : adresse électronique - Données professionnelles et d'évaluation définies par le Client (ex : CV, localisation, type de contrat souhaité, expérience professionnelle) - Résultats générés par le Service consistant en une analyse automatisée de la correspondance entre les réponses du candidat et les critères définis par le Client. - Enregistrements vocaux (optionnel - mode oral uniquement) - Données techniques : adresse IP, journaux d'accès (logs), données de navigation et d'acceptation (clic).
Nature du traitement	Collecte, enregistrement, organisation, structuration, conservation, analyse automatisée, transmission des résultats au Client et suppression.
Finalités du traitement	Préqualification / évaluation des candidats du Client exclusivement pour le compte du Client et selon ses instructions.
Durée du traitement	Déterminée par le Client via les paramétrages du Service. A défaut d'instruction spécifique, les Données sont conservées jusqu'à l'expiration du Contrat.

ANNEXE 2 DPA – MESURES TECHNIQUES ET ORGANISATIONNELLES

AssessFirst met en œuvre les mesures décrites ci-dessous ou des mesures équivalentes permettant d'assurer un niveau de sécurité approprié au sens de l'article 32 du RGPD :

1. MESURES DE SÉCURITÉ TECHNIQUES

- Mesures d'authentification : (i) authentification forte avec 2FA pour les entreprises ; (ii) utilisation d'un identifiant unique par utilisateur, (iii) respect des recommandations de la CNIL pour la gestion des mots de passe.
- Sécurité réseau : (i) transmission entre le serveur et les tiers cryptée en HTTPS de bout en bout, (ii) division fonctionnelle du réseau en sous-réseaux pour garantir la sécurité : séparation des environnements de test et de production, (iii) enregistrement des accès et gestion des incidents, (iv) journalisation des accès, des anomalies et des événements liés à la sécurité, (v) utilisation d'un pare-feu web et logiciel antivirus régulièrement mis à jour, (vi) installation d'outils de détection de vulnérabilités.
- Hébergement et sauvegarde : (i) hébergement fourni par Amazon Web Services dans des serveurs situés dans l'UE, certifiés ISO 27001, (ii) cryptage SSL des sauvegardes lors du transfert, (iii) cryptage des données hébergées et transférées
- Mesures de sécurité physique AWS : (i) contrôle d'accès (badges, portes et armoires verrouillées, conservation de l'accès physique pendant 45 jours), (ii) surveillance vidéo 24/7, (iii) alarme anti-intrusion, (iv) système d'alarme incendie.



2. MESURES DE SÉCURITÉ ORGANISATIONNELLES

- Gestion des employés : (i) vérification des antécédents, (ii) obligations de confidentialité et charte informatique pour le personnel, (iii) gestion des autorisations avec révision annuelle, (iv) sensibilisation du personnel aux risques liés à la vie privée.
- Conformité et gestion des données : (i) nomination d'un délégué à la protection des données (DPO), (ii) registre des activités de traitement régulièrement mis à jour, (iii) sous-traitance uniquement à des sous-traitants offrant des garanties suffisantes, (iv) vérification systématique de la conformité des sous-traitants ultérieurs, (v) création d'un service juridique dédié à la conformité.
- Gestion des incidents : (i) établissement d'une procédure pour les événements de sécurité, (ii) formation du personnel à la procédure, (iii) transmission des événements de sécurité à une équipe d'urgence, (iv) analyse de l'événement par un membre de l'équipe d'urgence, (v) information de toutes les équipes sur les causes et conséquences de l'incident pour prévenir sa récurrence, (vi) examen approfondi par l'équipe de maintenance, les départements concernés et en particulier le service juridique et de communication.
- Participation à des programmes de sécurité : (i) mise en place d'un système de revue sur YesWeHack pour identifier et réduire les risques de sécurité des données via une invitation, (ii) accès contrôlé au programme.

3. CONFORMITÉ OWASP

- A01:2021-Contrôle d'accès défaillant : AssessFirst met en œuvre des politiques strictes de contrôle d'accès, incluant l'authentification à deux facteurs, une gestion appropriée des sessions et des révisions périodiques des accès. Ils disposent également d'une journalisation appropriée pour toutes les actions sensibles et les tentatives d'accès.
- A02:2021-Défaillances Cryptographiques : AssessFirst utilise des connexions sécurisées SSL/TLS et le cryptage des données pour protéger les données en transit et au repos. Ils adhèrent également à des politiques de mot de passe strictes et gèrent de manière sécurisée les clés cryptographiques.
- A03:2021-Injection : les processus de développement de l'entreprise incluent des pratiques de codage sécurisé et des tests de vulnérabilité, ce qui aide à prévenir les vulnérabilités d'injection. Ils suivent également le principe du moindre privilège pour minimiser les dommages potentiels.
- A04:2021-Conception Insecure : AssessFirst conçoit des applications et des processus en tenant compte de la confidentialité et de la sécurité, suivant les principes de protection de la vie privée dès la conception et par défaut.
- A05:2021-Security Misconfiguration: AssessFirst maintient des configurations de sécurité strictes, et les révisé et les met à jour régulièrement. Elle surveille également les modifications non autorisées des paramètres du système.
- A06:2021-Composants vulnérables et obsolètes: AssessFirst s'engage à maintenir les composants logiciels à jour et utilise des solutions de sécurité tierces pour rechercher les vulnérabilités.
- A07:2021 - Défauts d'identification et d'authentification: AssessFirst met en œuvre des mesures d'identification et d'authentification appropriées, telles que des politiques de mots de passe forts, l'authentification à deux facteurs et des examens d'accès réguliers.
- A08:2021-Défaillances du logiciel et de l'intégrité des données: AssessFirst dispose d'un solide plan de sauvegarde et de reprise après sinistre pour protéger et restaurer les logiciels et les données en cas de défaillance.
- A09:2021-Défaillances dans la journalisation et la surveillance de la sécurité : AssessFirst enregistre tous les événements sensibles et s'assure que les informations nécessaires sont présentes dans les entrées du journal. Elle dispose également d'une période de conservation des journaux définie et d'une procédure de réponse aux incidents.
- A10:2021-Falsification des requêtes côté serveur: Les pratiques de sécurité d'AssessFirst, telles que le codage sécurisé et les tests de vulnérabilité réguliers, aident à prévenir les vulnérabilités de falsification de demande côté serveur.