CONFIDENTIAL

MISSION RGPD

testwe
Security beyond simplicity

Rapport de PIA de la solution de surveillance des examens à distance

Date du document : 27 juillet 2021

I. Rappel du contexte

TestWe propose une plateforme et une application permettant de réaliser des examens en ligne. Ces deux outils sont à destination des établissements d'enseignement secondaire et supérieur, et des professionnels dans le cadre de l'obtention de certifications ou de recrutement du personnel.

Dans le cadre de cette activité, TestWe propose trois catégories de produits différents :

1) ProctorWe : solution de proctoring basée sur l'identification des candidats et la surveillance via webcam.
2) Learning Analytics : fonctionnalité proposant la création de graphiques statistiques basés sur l'analyse des données académiques.
3) Examens TestWe : outil de création d'examens en ligne, comprenant des options de tests dotés d'une correction automatique ou partagée avec les correcteurs et chargés de TD.

L'objectif principal de la plateforme et du logiciel TestWe est de permettre aux établissements d'organiser et d'administrer des sessions d'évaluation dématérialisée en salle ou à distance, dans le cadre d'une formation initiale ou continue.

La solution TestWe est commercialisée dans le monde. Récemment, TestWe a développé un projet à destination du concours SESAME, permettant l'accès à 14 grandes écoles de commerce, et concernant 13 000 candidats par session. Le projet permettra une authentification des candidats en comparant une photographie de référence avec une photographie du candidat prise lors de l'épreuve. TestWe fait ainsi usage d'une technologie de reconnaissance faciale.

En outre, TestWe développe en parallèle l'ajout d'une nouvelle fonctionnalité avec captation du son ambiant couplé avec l'activation de la caméra, afin de sécuriser le déroulement des épreuves.

Pour mener à bien son activité, TestWe fait appel à deux prestataires : AWS pour l'hébergement de ses données en France et SenGrid pour l'envoi de ses emails.

CONFIDENTIAL

En matière de conformité au RGPD, la réalisation d'une analyse d'impact relative à la protection des données personnelles (ci-après « AIPD » ou, en anglais, « PIA » pour Privacy Impact Assessment) est nécessaire.

II. PIA de la solution de surveillance des examens de TestWe

1.1 Vue d'ensemble du traitement

Présentation du traitement considéré :

Description du traitement	La solution développée par TestWe permet de surveiller des examens et des concours d'entrée aux grandes écoles à distance, via le recours à plusieurs technologies (proctoring, captation du son et reconnaissance faciale)
Finalités du traitement	Authentification des étudiants au début de l'examen ; Surveillance des examens et concours d'entrée aux écoles à distance ; Minimisation des risques de fraude lors des examens à distance.
Enjeux du traitement	Le développement et l'utilisation de technologies de reconnaissance faciale, de proctoring et de captation du son pour la surveillance d'examens réalisés par des étudiants, parfois mineurs, doit faire l'objet d'une analyse approfondie.
Responsable de traitement	TestWe (pour le développement de la solution) Les établissements scolaires ou universitaires (pour l'utilisation de la solution)
Sous-traitant(s)	Amazon Web Services, hébergeur des données (serveurs localisés en France).

Recensement des référentiels applicables au traitement :

Référentiels applicables au traitement	Prise en compte
CNIL, « Pour un débat à la hauteur des enjeux », 15 novembre 2019	Lors de la réalisation de l'AIPD

1.2 Données, processus et supports

Description des données, destinataires et durées de conservation :

Données	Destinataires	Durées de conservation
Flux de webcam : photographie de référence des étudiants, photographies de l'environnement de l'étudiant (proctoring), photographies prises dans pendant l'examen	Équipe des développeurs TestWe, corps enseignant de l'établissement utilisateur (surveillants)	**En base active** : 2 mois

Son de l'ordinateur : analyse du volume sonore relevant les séquences au sein desquelles il y a du son dans la pièce de l'étudiant	Équipe des développeurs TestWe, corps enseignant de l'établissement utilisateur (surveillants et managers)	**En base active** : 2 mois

Description des processus et supports :

Processus	Description détaillée du processus	Supports des données concernés
Photographie de référence	Prise d'une photographie de référence de l'étudiant lors du test de la solution avant l'examen	Serveurs TestWe hébergés par AWS en France
Comparaison de la photographie de référence	Comparaison de la photographie de référence avec une photographie prise de l'étudiant au début de l'examen Puis comparaison de la photographie de référence avec le visage apparaissant sur la caméra pendant toute la durée de l'examen afin de vérifier qu'il s'agit bien de l'étudiant	Serveurs TestWe hébergés par AWS en France
Vérification de l'environnement de l'étudiant (proctoring)	Prise de multiples photographies effectuées par secondes pour effectuer un « tour » de l'environnement immédiat de l'étudiant (bureau, pièce, oreilles des étudiants pour vérifier qu'ils n'ont pas d'écouteurs) afin de vérifier qu'aucun élément permettant de frauder l'examen n'est présent	Serveurs TestWe hébergés par AWS en France
Fonctionnalité de captation du son ambiant	Cette fonctionnalité est couplée avec la reconnaissance faciale (sans analyses croisées de données), et permet de détecter si l'étudiant parle à quelqu'un pendant l'examen (analyse du volume sonore sous forme de graphique pour que le surveillant puisse aller écouter les passages au sein desquels il y a du son)	Serveurs TestWe hébergés par AWS en France

	La fonctionnalité est active pendant toute la durée de l'examen	

2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement

Explication et justification des finalités :

Finalités	Légitimité
Les données sont collectées pour vérifier l'identité de l'étudiant au début de l'examen	Exécution du contrat passé avec l'établissement
Les données sont collectées pour minimiser les risques de fraudes pendant toute la durée de l'examen	Exécution du contrat passé avec l'établissement

Explication et justification du fondement :

Critères de licéité	Applicable	Justification
Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.	Oui	Le traitement est nécessaire à l'exécution du contrat de licence d'utilisation conclu avec l'établissement

Explication et justification de la minimisation (adéquates, pertinentes, non excessives) des données :

Détails des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Photographies	Flux des webcams des étudiants	Les données sont nécessaires à l'identification formelle de l'étudiant, à la vérification de son environnement au début de l'examen et à la minimisation des risques de fraudes pendant l'examen	Aucunes vidéos des étudiants ne sont collectées, seulement des photographies, ce qui est moins intrusif de que filmer l'étudiant pendant tout l'examen ; Des « flags » permettent aux surveillants de repérer directement les photographies au

			sein desquelles plusieurs visages ont été détectés, aucun visage ou un visage qui ne serait pas celui de l'étudiant, ce qui permet aux surveillants de ne pas visualiser toutes les photographies
Enregistrements sonores	Son des ordinateurs des étudiants	Les données sont nécessaires à la minimisation des risques de fraudes pendant la durée de l'examen	Des graphiques affichant le niveau sonore des enregistrements permettent aux surveillants de n'écouter que les passages au sein desquels il y a du son autour de l'étudiant

Données exactes et tenues à jour :

Mesures pour la qualité des données	Justification
La photo de référence permet de vérifier l'exactitude des données (identification)	Aucune mise à jour des données n'est nécessaire car elles ne sont conservées que 2 mois après le passage de l'examen

Explication et justification des durées de conservation :

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données courantes	Les données sont conservées pour la durée de l'examen, augmentée de 2 mois à son issue	La conservation des données est nécessaire à la vérification de l'absence de fraude par les surveillants	Purge automatique des systèmes d'information à l'issue du délai de conservation
Données archivées	Aucun archivage n'est effectué	N/A	N/A

Évaluation des mesures :

Mesures garantissant la proportionnalité et la nécessité du traitement	Acceptable / améliorable ?	Mesures correctives
Finalités : déterminées, explicites et légitimes	Acceptable	N/A

Fondement : licéité du traitement, interdiction du détournement de finalité	Améliorable	Le personnel enseignant devrait être sensibilisé sur le fait de ne pas réutiliser ce type de données pour une autre finalité que celle du contrôle de la fraude, via l'affichage de mentions d'informations sur la page ou ces données sont disponibles
Minimisation des données : adéquates, pertinentes et limitées	Améliorable	Seules les photographies « flaguées » et les passages indiquant la présence de sons devraient être collectés, stockés, afin de pouvoir être consultés par les surveillants
Qualités des données : exactes et tenues à jour	Acceptable	N/A
Durées de conservation : limitées	Acceptable	N/A

2.2 Évaluation des mesures protectrices des droits des personnes concernées

Détermination et description des mesures pour l'information des personnes :

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Présence de mentions spécifiques	CGU devant être obligatoirement acceptées après lecture par toutes les étudiantes et tous les étudiants, comportant un renvoi à la politique de confidentialité	L'information des étudiants est réalisée dans ces documents, lors de leur première connexion. Ces documents (politique de confidentialité et CGU) sont ensuite disponibles à tout moment sur l'application et sur le site web
Présence d'une politique de confidentialité sur la plateforme web et l'application locale	Accessible à tous sur le site web	L'information des étudiants est réalisée via la politique de confidentialité, présente sur le site web de TestWe et dont l'existence est précisée au sein des CGU
Présentation des droits de l'étudiant (accès, suppression de données, etc.).	Oui, au sein de la politique de confidentialité	L'information des étudiants est réalisée via la politique de confidentialité, mentionnée au sein des CGU obligatoirement

		acceptées par l'étudiant lors de sa première connexion
Modalités de contact de l'entreprise pour l'exercice des droits des personnes concernées	Par mail, à l'adresse suivante : privacy@testwe.eu (mentionnée au sein de la politique de confidentialité)	L'adresse email est disponible sur le site web de TestWe sein de sa politique de confidentialité

Détermination et description des mesures pour les droits d'accès et à la portabilité :

Mesures pour le droit d'accès	Données internes	Données externes	Justification
Possibilité de demander l'accès aux données	Oui	Oui	Via l'adresse email dédiée : privacy@testwe.eu

Mesures pour le droit à la portabilité	Données internes	Données externes	Justification
Possibilité de récupérer, sous une forme aisément réutilisable, les données personnelles qui ont été fournies par la personne concernée, afin de pouvoir les transférer à un service tiers	Oui	Oui	Exports possibles.

Détermination et description des mesures pour les droits de rectification et d'effacement :

Mesures pour les droits de rectification et d'effacement	Données internes	Données externes	Justification
Possibilité de rectifier les données personnelles	Oui	Oui	Les étudiants peuvent demander l'effacement de leurs données à l'adresse suivante : privacy@testwe.eu
Possibilité de supprimer les données personnelles	Oui	Oui	Les étudiants peuvent demander l'effacement de leurs données à l'adresse suivante : privacy@testwe.eu
Mise en œuvre du droit à l'oubli pour les mineurs	Oui	Oui	Les données sont supprimées à la suite de la demande du mineur

Détermination et description des mesures pour les droits de limitation du traitement et d'opposition : Non applicable (pas de recueil du consentement de l'étudiant par TestWe).

Détermination et description des mesures pour la sous-traitance :

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28
Amazon Web Services (AWS)	Hébergement de la base de données (comprenant les données des étudiants)	Hébergement de l'ensemble des données traitées par TestWe	CGS	Oui (data protection addendum)

Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne : **N/A (aucun transfert de données personnelles hors UE)**.

Évaluation des mesures :

Mesures protectrices des droits des personnes concernées	Acceptable/améliorable ?	Mesures correctives
Information des personnes concernées (traitement loyal et transparent)	Améliorable Les mentions d'information au sein des la politique de confidentialité ne sont pas complètes	**La politique de confidentialité doit être revue et complétée** ; Elle doit également être disponible non seulement sur le site web mais sur l'application et la plateforme
Exercice des droits d'accès et à la portabilité	Acceptable	N/A
Exercice des droits de rectification et d'effacement	Acceptable	N/A
Exercice des droits de limitation du traitement et d'opposition	N/A	N/A
Sous-traitance : identifiée et contractualisée	Acceptable	N/A
Transferts (respect des obligations en matière de transfert de données hors UE)	N/A	N/A

3.1 Évaluation des mesures liées à la sécurité des données

Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données :

Mesures portant spécifiquement sur les données du traitement	Modalités de mise en œuvre ou justification sinon	Acceptable/améliorable ?	Mesures correctives
Chiffrement	Oui par AWS, et les certificats	Acceptable	N/A

	utilisés pour les connexions HTTPS sont gérés avec Let's Encrypt et sont renouvelés périodiquement Pour le proctoring, mise en place d'un cryptage supplémentaire des données avec le protocole OpenPGP		
Anonymisation	Les données de proctoring (photos et audios) et leurs copies sont stockées de façon anonymes dans des systèmes séparés de la base principale qui contient les noms des étudiants	Acceptable	N/A
Cloisonnement des données (par rapport au reste du Système d'Information)	Les données sont stockées dans des systèmes (essentiellement S3 pour les fichiers, MariaDB et MongoDB pour les bases de données) dont les accès sont gérés de façon distincte de ceux des applications	Acceptable	N/A
Contrôle des accès logiques	Les salariés de TestWe ont des accès distincts en fonction de leurs rôles. Ces accès incluent les accès applicatifs à la plateforme TestWe (accès à toutes les écoles ou non etc.) et les accès aux	Acceptable	N/A

	différents systèmes informatiques pour l'équipe technique. Les comptes sur la plateforme TestWe doivent être sécurisés par un mot de passe de 12 caractères minimum. Les accès techniques à droits importants (admin etc.) sur nos plateformes AWS doivent être sécurisés par un mécanisme de double authentification.		
Traçabilité (journalisation)	Oui, conservation des logs de connexion pendant 3 mois.	Acceptable	N/A
Contrôle d'intégrité	Les mécanismes de contrôle de l'intégrité (ex. gestion de la corruption de mémoire) sont gérés par AWS.	Acceptable	N/A
Archivage	N/A (pas d'archivage, seulement des exports pour les établissements qui eux seuls archivent les dossiers des étudiants)	N/A	N/A
Sécurité des documents papier	N/A	N/A	N/A

Description et évaluation des mesures générales de sécurité :

Mesures générales de sécurité du	Modalités de mise en œuvre	Acceptable/améliorable ?	Mesures correctives

système dans lequel le traitement est mis en œuvre	ou justification sinon		
Sécurité de l'exploitation	La maintenance corrective des serveurs est couverte par AWS	Acceptable	N/A
Lutte contre les logiciels malveillants	Antivirus et autres gérés par AWS	Améliorable	Les ordinateurs et autres outils informatiques utilisés par les salariés de TestWe pour accéder aux données des étudiants doivent également être sécurisés (antivirus, chiffrement du disque dur…etc.)
Gestion des postes de travail	Pare-feu et accès aux postes par login-mot de passe	Acceptable	N/A
Sécurité des sites web	Proxy applicatif Sécurité via token Vérification des droits utilisateurs	Acceptable	N/A
Sauvegardes	Les bases de données Mongo et MariaDB utilisées pour les données de TestWe ont toutes les deux des sauvegardes automatiques quotidiennes avec possibilité de restauration pendant plusieurs mois. Ces sauvegardes sont gérées par les fournisseurs (AWS pour MariaDB et	Acceptable.	N/A

	MongoDB cloud pour MongoDB).		
Maintenance	La maintenance corrective et évolutive est couverte par AWS.	Acceptable	N/A
Sécurité des canaux informatiques (réseaux)	Oui, connexion sécurisée en https. Filtrage par IP pour certains services sensibles. Monitoring également des clés utilisées pour accéder aux ressources AWS.	Acceptable	N/A
Surveillance	Différents outils de surveillance sont utilisés pour suivre l'état de la plateforme à différents niveaux, comme FreshPing pour l'accessibilité de la plateforme, AWS CloudFront pour l'état des différents systèmes ou Grafana pour le suivi fonctionnel		
Contrôle d'accès physique	Espace de travail distinct dédié aux développeurs et espace de travail dédié aux équipes support et commerciale	Améliorable	Instaurer des mesures de sécurité physiques supplémentaires (ex. badges individuels)
Sécurité des matériels	Sécurité des datacenters gérée par AWS France Sécurité du matériel informatique du personnel de TestWe	Améliorable La sécurité du matériel informatique du personnel de TestWe doit être prise en considération par la société	Instaurer des mesures de sécurité pour le matériel informatique des équipes de TestWe permettant l'accès aux données des étudiants (filtres de

			confidentialité en cas de télétravail par ex.)
Éloignement des sources de risques	Géré par AWS	Acceptable	N/A
Protection contre les sources de risques non humaines	Géré par AWS	Acceptable	N/A

Les mesures de sécurité physiques mises en place par AWS sont décrites ici.
Les mesures de sécurité techniques mises en place par AWS sont décrites ici.

Description et évaluation des mesures organisationnelles (gouvernance) :

Mesures organisationnelles (gouvernance)	Modalités de mise en œuvre ou justification sinon	Acceptable/améliorable ?	Mesures correctives
Organisation	Une politique de gestion des habilitations est mise en place ; En revanche, concernant les rôles et responsabilités en matière de protection des données, le seul rôle défini est celui de référent RGPD attribué au DG adjoint (risque de conflit d'intérêts), qui est également chargé de la mise en application des lois et règlements touchant à la protection de la vie privée ; Aucun comité de suivi ou équivalent	Améliorable	TestWe pourrait mandater un **DPO** externe, ce qui permettrait d'assurer un suivi de la mise en conformité
Politique (gestion des règles)	Absence de charte informatique ou d'équivalent	Améliorable	Une **charte informatique** devrait être rédigée afin de sensibiliser les équipes de TestWe aux

			bonnes pratiques en matière de protection des données et de bonne utilisation des moyens informatiques
Gestion des incidents et des violations de données	Aucune gestion documentée et testée ; Aucune procédure	Améliorable	Une **procédure interne de gestion des violations de données** personnelles doit être rédigée et mise en place au sein de TestWe
Gestion des personnels	Gestion des habilitations ; Légère sensibilisation des salariés (partage avec les équipes des actions de mise en conformité au RGPD) mais absence de sessions de formation ; Clause de confidentialité dans les contrats de travail.	Améliorable	Une **session de formation / sensibilisation** aux enjeux RGPD devrait être organisée par TestWe pour ses équipes
Relation avec les tiers	Il existe deux types de tiers. Freelance : TestWe recourt ponctuellement au freelance pour des fonctions support (accès aux plateformes utilisateurs concernées) mais aussi de surveillance. Ils ont donc accès à l'ensemble des	Améliorable	Instaurer les mêmes mesures de sécurité aux freelances

	données auxquelles a accès le Surveillant-Manager (soit l'ensemble des photos de l'établissement). Aucune précision n'est donnée sur les mesures de sécurité mises en œuvre pour ces accès. <u>Prestataires</u> (relation contractuelle) : TestWe recourt à des prestataires pour des fonctions support et surveillance. Pour la première, le prestataire n'a accès à rien, excepté la solution de support (la centrale d'appel). Pour la seconde, l'accès aux données est beaucoup plus encadré qu'en freelance. Le prestataire n'a accès qu'aux profils des étudiants assignés, les données sont compartimentées. Chaque membre du personnel du prestataire a un identifiant (login et mot de passe) et ne peut accéder qu'aux données qui leur sont transmises.		
Gestion des projets	Tests des dispositifs réalisés sur des données fictives et des comptes fictifs	Acceptable	N/A

Supervision	Aucun contrôle de l'effectivité et de l'adéquation des mesures touchant à la vie privée ; Aucun audit techniques de la sécurité du système d'information	Améliorable	Un suivi de la mise en conformité au RGPD doit être mis en place et des audits réguliers de sécurité doivent être organisés

3.2 Appréciation des risques : les atteintes potentielles à la vie privée

Analyse et estimation des risques :

Risque	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Accès illégitime à des données	Équipes internes Personnel du client (principalement les surveillants prestataires externes Attaquant	Consultation ou vol des données sur le serveur ou dans les bureaux Usurpation de l'identité	Conséquences d'une communication d'informations potentiellement sensibles (discrimination, menaces, agressions, perte d'emploi, sentiment d'atteinte à la vie privée, etc.)	Conservation limitée des données Contrôle d'accès logique des utilisateurs Sécurité de l'exploitation (authentification) Organisation (habilitations) Traçabilité (logs de connexion) Typologie des droits du personnel du client sur la plateforme (correcteurs et surveillants n'ont accès qu'aux données de	Importante	Limitée

				leurs classes, seul le manager a accès à toutes les données de l'établissement)		
Modification non désirée de données	Équipe interne (Lead Developer) Personnel du client (surveillant) Attaquant	Altération des données sur le serveur Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Absence de validation de l'examen Perte de chance scolaire	Sauvegarde des données par TestWe via ses prestataires Sécurité de l'exploitation (authentification) Contrôle d'accès logique des utilisateurs Organisation (habilitations : seul le Lead Developer chez TestWe peut modifier les données des étudiants) Impossibilité pour le personnel du client de modifier les données des étudiants Traçabilité (logs de connexion)	Importante	Négligeable
Disparition de données	Équipes internes (Lead	Suppression de données	Absence de validation de l'examen	Maintenance et sauvegarde	Importante	Négligeable

	Developer) Personnel du client (manager et professeur) Attaquant Sinistre	Détérioration des serveurs Dégradation physique des postes informatiques	Perte de chance scolaire	assurées par AWS Datacenters AWS sécurisés Contrôle d'accès logique des utilisateurs Organisation (habilitations : seul le Lead Développer peut supprimer les données des étudiants + les données liées à la surveillance ne sont accessible qu'au Lead Developer) Gestion des postes de travail (authentification) Traçabilité (logs de connexion)		

Évaluation des risques :

Risques	Acceptable/améliorable ?	Mesures correctives	Gravité résiduelle	Vraisemblance résiduelle
Accès illégitime à des données	Améliorable Des données pourraient encore être volées au sein des bureaux de TestWe, qui ne sont pas assez sécurisés ; et il existe encore un risque résiduel pour les surveillants	Mettre en place des mesures de sécurité physiques des postes de travail	Importante	Limitée

	(prestataires externes) qui ne sont pas contrôlés	Imposer une acceptation des CGU contenant la politique de confidentialité au personnel du client lors de leur première connexion à la plateforme, y compris pour les surveillants prestataires externes		
Modification non désirée de données	Acceptable	Une politique de gestion des violations de données devrait être rédigée et diffusée Une charte informatique interne devrait être rédigée et diffusée	Limitée	Négligeable
Disparition de données	Acceptable	Une politique de gestion des violations de données devrait être rédigée et diffusée Une charte informatique interne devrait être rédigée et diffusée	Limitée	Négligeable