Pearson
TalentLens

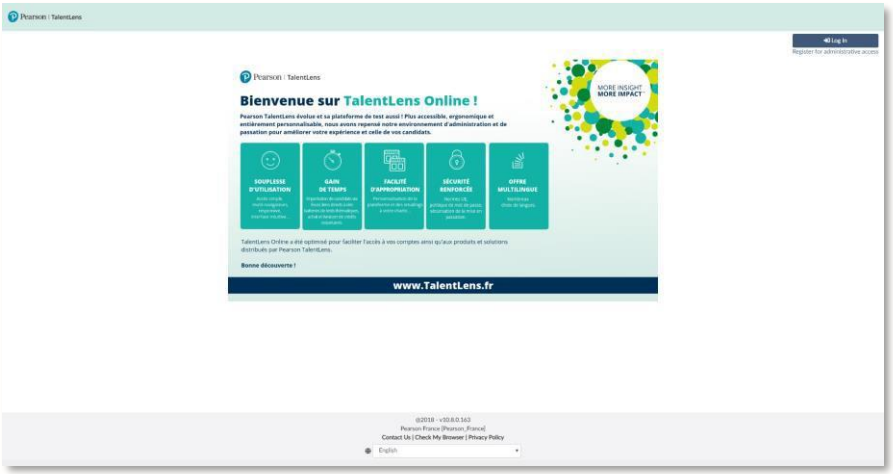
TALENTLENS ONLINE

Foire Aux Questions

FOIRE AUX QUESTIONS
INFORMATION SUR L'APPLICATION

TalentLens Online est une plateforme globale en ligne destinée à la conduite d'évaluations RH comme les Aptitudes, la Personnalité et le Développement Professionnel. Le client utilise la plateforme pour gérer les candidats/employés en en termes de planification des évaluations, de calcul des scores et de résultats sous forme de rapports téléchargeables.
Le candidat/employé administre l'évaluation en ligne en utilisant un navigateur web situé, sur site ou à distance.

ACCESSIBILITÉ



Une fois votre inscription terminée et validée, vous pouvez accéder à votre environnement en ligne TalentLens Online en cliquant sur le lien dans votre « e-mail de bienvenue » ou simplement en tapant votre URL dans la barre d'adresse de votre navigateur.
Entrez ensuite votre identifiant et votre mot de passe.
N'oubliez pas de mettre en signet votre URL unique.

Quels sont les systèmes d'exploitation compatibles ?

Afin d'optimiser l'expérience des utilisateurs et de vos candidats, nous vous invitons à utiliser l'un des navigateurs compatibles suivants :

- Internet Explorer 8.0 ou plus récent.
- Microsoft Edge.
- Firefox (dernière version qui doit disposer des mises à jour automatiques).
- Chrome (dernière version qui doit disposer des mises à jour automatiques).
- Safari (Mac 5.0 ou plus récent).

Qui utilisera l'application ?

L'administrateur des tests, l'administrateur du compte et le candidat/employé.

Pearson TalentLens

TYPE DE DONNÉES DE L'APPLICATION

Quel type de données personnelles sera traité par cette application ?

- **Administrateur des tests et du compte**
  - Prénom
  - Adresse e-mail professionnelle
  - Numéro de téléphone
  - Adresse professionnelle
  - Qualifications professionnelles

- **Candidats**
  - Prénom
  - Adresse e-mail
  - Scores d'évaluation bruts et étalonnés

- **Pour certains tests seulement**
  - Date de naissance
  - Niveau d'éducation / qualifications professionnelles
  - Sexe
  - Langue maternelle
  - Pays de résidence

- **Général**
  - Informations de connexion
  - Cookies de session
  - Langue de l'interface

Aucune information sur la carte de paiement, financière, de propriété intellectuelle et de données de recherche ne sera traité par la plateforme.

Où ces données seront-elles hébergées ?

Dublin, Irlande

Qui aura accès à ces données ?

Les clients ont accès à leurs propres données. Seul un petit nombre d'administrateurs de la plateforme Pearson et TalentLens ont accès aux données des clients ou des candidats.

Comment accéder à ces données ?

TalentLens Online est accessible via Internet à l'aide d'un navigateur Web standard.

Cette application ou ce système utilise-t-il des services cloud ?

Oui, PSI PAN (le sous-traitant de Pearson) utilise Microsoft Azure dans la région de l'UE, hébergé en Irlande.

Les utilisateurs du système peuvent-ils télécharger/extraire des données sur leurs machines locales ?

Oui.

Les utilisateurs du système peuvent-ils télécharger/extraire des données sur leurs machines locales ?

Oui.

Existe-t-il des exigences d'intégration qui nécessitent l'échange de données avec les systèmes clients existants ?

Non, mais des intégrations facultatives peuvent être fournies.

AUTHENTIFICATION, AUTORISATION ET GESTION DES ACCÈS

Existe-t-il des exigences d'intégration pour l'authentification et/ou l'autorisation ?

Non.

Quels sont les mécanismes de contrôle d'accès utilisateur fournis par le système/application (par exemple, accès basé sur les rôles) ?

TalentLens Online utilise un accès basé sur les rôles. Les utilisateurs ont besoin d'un nom d'utilisateur et de mots de passe uniques pour accéder à l'application.

Quels comptes sont requis pour gérer le système et/ou l'application ?

Le propriétaire du compte est configuré par Pearson TalentLens en tant qu'administrateur pour permettre la gestion des utilisateurs dans ce compte client.

Qui est responsable de l'accès des utilisateurs au système et à l'application (c.-à-d. Ajouter, modifier et supprimer l'accès) ?

Le propriétaire du compte ou un autre administrateur désigné du compte au sein de l'organisation du client est responsable de l'accès utilisateur.

Comment votre organisation gère-t-elle la comptabilité des comptes génériques et des identifiants fonctionnels ?

Les comptes génériques ne sont pas autorisés. Chaque utilisateur a un nom d'utilisateur et un mot de passe uniques.

Quels contrôles de sécurité avez-vous pour vous assurer que d'autres clients ou des tiers ne pourraient pas accéder sans autorisation aux données du client dans ce système / cette application ?

Les données client sont logiquement séparées dans la base de données.

Quelle méthode d'authentification est utilisée pour authentifier les utilisateurs de l'application système ?

TalentLens Online gère l'authentification au sein de l'application avec des noms d'utilisateur, des mots de passe, des rôles et des autorisations uniques.

Pearson
TalentLens

GESTION DES COMPTES ET DES MOTS DE PASSE

Le système/l'application empêche-t-il la réutilisation des 6 derniers mots de passe ?

Non.

Le système/l'application nécessite-t-il un changement de mot de passe initial après la première connexion de l'utilisateur ?

Oui.

Le système/l'application est-il configuré avec les normes de sécurité de compte suivantes ?

Verrouillage du compte après plus de 5 tentatives de connexion infructueuses : Oui

Durée de verrouillage d'au moins 30 minutes ou jusqu'à ce que l'administrateur réinitialise le compte : l'administrateur doit déverrouiller le compte.

Durée d'expiration de l'expiration de l'inactivité de la session utilisateur ? 30 minutes.

Votre système/application est-il configuré pour appliquer les paramètres de mot de passe suivants :

Au moins 8 caractères : 8 caractères minimum

Contenir au moins une majuscule, une minuscule, un caractère alphanumérique et un caractère spécial : Partiellement : Au moins une minuscule et au moins une majuscule.

Expire le mot de passe après 90 jours ? Non.

Pearson
TalentLens

ACCÈS AU RÉSEAU ET PROTECTION DES DONNÉES

Les certificats numériques de votre organisation sont-ils signés par un tiers de confiance ?

Oui, DigiCert SHA2.

Veuillez lister les protocoles réseau ou les ports requis pour ce système/cette application.

Port 443 (HTTPS).

Comment votre système sécurise-t-il les données en transit ?

Oui, en utilisant TLS.

L'accès à cette application sera-t-il limité aux réseaux identifiés par le client ?

Non.

Votre organisation utilise-t-elle le chiffrement pour sécuriser les données au repos ? Qui est le fournisseur de cryptage et quel algorithme de cryptage est implémenté ? Le module de cryptage FIPS 140-2 est-il validé ?

Oui, norme de l'industrie, FIPS 140-2 validée, fournisseur non divulgué.

Les bandes de sauvegarde sont-elles cryptées ?

Oui.

Comment les historiques sont-ils protégés contre la falsification ?

Les historiques sont cryptés et l'accès à ceux-ci est contrôlé.

Votre organisation applique-t-elle le chiffrement sur les appareils portables contenant des données sensibles (par exemple, bandes de sauvegarde, clés USB, CD/DVD, ordinateurs portables, smartphones) ? Qui est le fournisseur de cryptage et quel algorithme de cryptage est implémenté ? Le cryptage du module FIPS 140-2 est-il validé ?

Oui, conformément à notre politique globale, le chiffrement est appliqué sur tous les appareils mobiles et supports de stockage.

Si vous fournissez une assistance à distance, veuillez décrire comment vous vous connecterez à l'environnement informatique du client.

En général, le support à distance n'est pas nécessaire. Toutefois, si nécessaire et approuvé par le client, l'équipe d'assistance technique Pearson peut fournir un support à distance. Le support technique de Pearson ne se fera pas à distance dans le compte client mais utilisera un compte de test si nécessaire.

La base de données de l'application est-elle dans un environnement partagé ?

Non, la base de données est hébergée dans un groupe virtuel protégé et séparé.

Pearson TalentLens

Si votre entreprise autorise l'accès aux serveurs et aux données de votre réseau sans fil, comment cet accès est-il sécurisé ?

Protocole de sécurité WPA2 Enterprise.

Quels systèmes peuvent être connectés directement à la (aux) base(s) de données ?

Seuls les serveurs d'applications spécifiques peuvent se connecter au serveur de données.

Comment l'accès administratif aux serveurs est-il restreint (par utilisateur, par rôle, par appareil ou une combinaison de ceux-ci) ?

Par utilisateur.

Existe-t-il des systèmes permettant d'éviter que les données ne soient filtrées via le réseau ou un périphérique physique (par exemple une clé USB) ?

Non.

Existe-t-il des cas où l'application ou le système est requis pour utiliser un service non sécurisé (par exemple, telnet, rsh, ftp, etc.) ou sinon stocker ou transmettre des mots de passe en texte clair ?

Non.

AUDIT, HISTORIQUES ET SURVEILLANCE

Le système/l'application est-il configuré pour consigner l'accès au compte privilégié (par exemple, super-user, administrateur et administrateur racine), y compris les accès, les mises à jour, les créations et les suppressions ?

Oui.

Le système/l'application conserve-t-il un rapport d'analyse sécurisé chaque fois qu'un utilisateur accède, met à jour, recueille et supprime des informations ?

Oui.

Si oui, le rapport d'analyse contient-il au moins les informations suivantes ?

Identifiant unique de l'utilisateur : Oui

Identifiant unique de données (par exemple patient) : Oui

La fonction effectuée par l'utilisateur : Oui

L'heure et la date auxquelles la fonction a été effectuée : Oui

Combien de temps les historiques sont-ils conservés et le client peut-il les obtenir sur demande ?

Les historiques sont conservés pendant 2 ans. Oui, ils peuvent être fournis sur demande écrite.

Surveillez-vous votre système pour une activité suspecte ? À quelle fréquence examinez-vous les historiques ?

Oui, tous les jours.

VULNÉRABILITÉ ET GESTION DES MENACES

Qui sera responsable de la maintenance des mises à jour du système avec les correctifs de sécurité ou correctifs ?

Le PSI-PAN gère cela, régi par l'accord de sécurité formel Pearson-PAN.

Comment vos systèmes et applications sont-ils protégés contre les virus et les logiciels malveillants ?

Le PSI-PAN gère cela, régi par l'accord de sécurité formel Pearson-PAN.

Votre organisation effectue-t-elle régulièrement des analyses de vulnérabilité de sécurité ?

Oui, le PSI-PAN gère cela, régi par l'accord de sécurité formel Pearson-PAN.

Votre organisation a-t-elle effectué un test de pénétration de la sécurité sur votre environnement ?

Oui, le PSI-PAN gère cela, régi par l'accord de sécurité formel Pearson-PAN.

Utilisez-vous des outils pour tester spécifiquement la sécurité des applications Web que vous développez ?

Oui, le PSI-PAN gère cela, régi par l'accord de sécurité formel Pearson-PAN.

Pearson
TalentLens

DISPONIBILITÉ, SAUVEGARDE ET RÉCUPÉRATION

Quels mécanismes sont en place pour traiter la tolérance aux pannes et la haute disponibilité de ce système ?

Oui, le PSI-PAN gère cela, régi par l'accord de sécurité formel Pearson-PAN.

Qui sera responsable du processus de sauvegarde et de récupération ?

Le PSI-PAN gère cela, régi par l'accord de sécurité formel Pearson-PAN.

Quel est le temps de récupération prévu en cas de panne imprévue ?

TalentLens Online est conçu pour une disponibilité 24h/24, 7j/7 et 365 j/an.
En cas de panne, l'objectif est d'aborder le problème dès que possible techniquement et de rétablir le service.

GESTION DU CHANGEMENT

Veuillez fournir un résumé de votre processus standard de gestion du changement.

Si des modifications sont nécessaires pour les environnements de pré-production ou de production, des tickets de modification formels sont saisis avec les informations de modification et les notifications appropriées. Toute modification à la pré-production et à la production doit être examinée et approuvée par un « Conseil Consultatif sur le Changement ». Une fois examiné et approuvé, le ticket peut être mis en œuvre par l'équipe de gestion du changement. La mise en œuvre des changements suit un cycle de développement de 6 semaines.

Comment les changements de personnel sont-ils traités ? En particulier, y a-t-il un processus de changement pour supprimer l'accès du personnel lorsqu'ils partent ?

Oui, il existe un processus pour ajouter et supprimer l'accès pour les utilisateurs.

Avez-vous un environnement séparé pour le développement, le test d'acceptation des utilisateurs (UAT) et la production ?

Oui.

Quelle est votre méthode de notification des clients et du personnel lorsqu'un changement de système ou de demande doit être mis en œuvre ?

Un système de création de tickets est utilisé pour les modifications et des notifications par e-mail sont également utilisées.

CONFIRMITÉ

Votre organisation exige-t-elle que les employés suivent chaque année une formation à la sécurité et à la protection de la vie privée ?

Pour Pearson, oui. PSI PAN est régi par la convention de sécurité formelle Pearson-PAN.

Quels processus votre organisation a-t-elle mis en place pour se conformer aux lois, aux règlements et aux normes de l'industrie applicables ?

Pearson et PSI PAN emploient de nombreuses mesures de protection administratives, physiques et techniques pour se conformer aux lois applicables, aux règlements et aux normes de l'industrie.

Avez-vous un plan de réponse aux incidents et un processus de notification de violation ?

Oui.

Pouvez-vous fournir une documentation détaillant le fonctionnement, l'architecture et l'administration du système ou de l'application ?

Uniquement disponible sous supervision et en ayant une NDA en place.

OPÉRATIONS INTERNATIONALES

Votre organisation effectue-t-elle des opérations internationales ?

Oui, Pearson a des bureaux dans le monde entier.

Votre organisation s'associe-t-elle avec des fournisseurs ou des sous-traitants ayant des activités internationales ?

Oui. En ce qui concerne la plateforme TalentLens Online avec PSI-PAN.

Dans quels pays vos employés, fournisseurs ou donneurs d'ordre internationaux ont- ils des activités ?

Pearson est une société internationale qui possède des filiales, des fournisseurs et des bureaux dans de nombreux pays du monde.

L'un de vos employés, sous-traitants ou fournisseurs internationaux aura-t-il accès aux systèmes, applications ou données du client ?

Seul un petit nombre d'administrateurs de plates-formes Pearson et PSI-PAN en Europe ont accès aux données des clients.

Veuillez décrire les systèmes clients, les applications et les données auxquels vos employés, fournisseurs ou donneurs d'ordre internationaux auront accès.

TalentLens Online est hébergé sur un environnement de cloud sécurisé situé à Dublin, en Irlande. Seul un petit nombre d'administrateurs de bases de données Pearson et PSI-PAN en Europe ont accès aux données des clients.

Comment vos employés, fournisseurs ou donneurs d'ordre internationaux accèderont-ils aux systèmes, aux applications et aux données des clients ?

Seul un petit nombre d'administrateurs de bases de données Pearson et PSI-PAN en Europe ont accès aux données des clients.

Quels contrôles de sécurité informatique sont mis en œuvre pour garantir que les données sont transmises de manière sécurisée à vos employés, fournisseurs ou entrepreneurs internationaux ?

Toutes les données en mouvement sont cryptées en utilisant TLS.

Quels contrôles de sécurité informatique sont mis en œuvre pour garantir que les données sont stockées de manière sécurisée chez vos employés, vos fournisseurs ou vos donneurs d'ordre internationaux ?

Les données sont uniquement stockées cryptées dans la base de données TalentLens Online et sont accessibles à un petit nombre d'administrateurs de plates-formes Pearson et PSI-PAN en Europe.

Veuillez fournir les noms des fournisseurs, les noms de produits et les versions des logiciels antivirus et de chiffrement de poste de travail utilisés par vos loyers, fournisseurs ou fournisseurs internationaux.

Concernant Pearson, Symantec Endpoint Protection est utilisé. PSI-PAN, est régi par l'accord de garantie formel Pearson-PAN.

Pearson
TalentLens

DOCUMENTATION REQUISE

Veuillez fournir une documentation sur l'architecture du système qui comprend un diagramme de réseau décrivant le système et les connexions externes. Notez que les informations IP et les informations sensibles peuvent être omises.

Cette information est la propriété de Pearson et/ou de PSI-PAN et n'est divulguée que sous réserve d'une NDA.

Veuillez fournir un résumé de votre dernier test de pénétration de sécurité.

Cette information est la propriété de Pearson et/ou du PSI-PAN, régie par l'accord de garantie formelle Pearson-PAN, et est seulement divulguée sous surveillance avec une NDA.

Veuillez fournir un rapport de synthèse de votre dernière analyse de vulnérabilité.

Cette information est la propriété de Pearson et/ou du PSI-PAN, régie par l'accord de garantie formel Pearson-PAN, et est seulement divulguée sous surveillance avec une NDA.

Veuillez fournir des résumés du programme de sécurité de l'information, des plans de continuité des activités, des méthodes de gestion des risques et des pratiques d'embauche de l'organisation.

La stratégie de gestion de la sécurité de l'information de Pearson repose sur le cadre ISO27001. À l'heure actuelle, Pearson a fait l'objet d'audits SOC2 externes et/ou de sécurité interne à l'égard des pratiques exemplaires en matière de sécurité et des Critères communs de SOC2 dans diverses parties de l'entreprise. Malheureusement, les résultats de ces audits sont considérés comme confidentiels et exclusifs et ne peuvent être partagés hors de l'entreprise.

Veuillez fournir les rapports d'audit indépendants et les certifications disponibles (par exemple: HITRUST, P CI DSS, SSAE 16 Type, II etc.).

Cette information est la propriété de Pearson et/ou du PSI-PAN, régie par l'accord de garantie formel Pearson-PAN, et n'est pas divulguée.