RGPD –
Ce qu'il faut savoir

SHL.

1 Introduction

En tant que premier fournisseur mondial de solutions d'évaluation de talents, nous prenons très au sérieux notre obligation d'assurer le plus haut niveau de protection aux données personnelles que vous nous confiez. Le maintien de la conformité avec la législation applicable en matière de protection des données est une priorité commerciale essentielle.

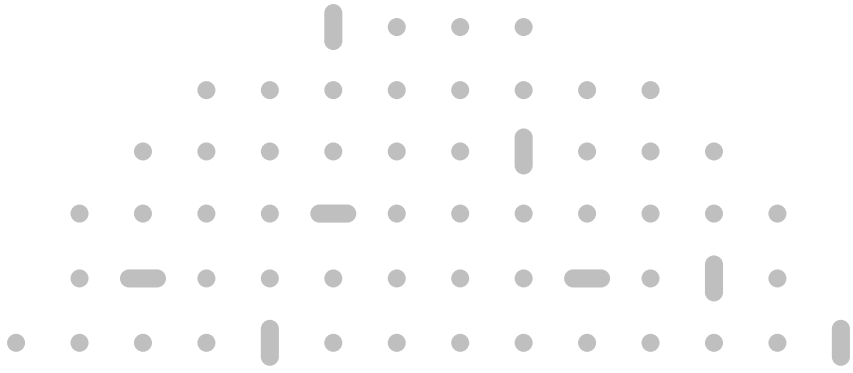
Cette déclaration vous fournit des informations sur la façon dont nous nous conformons au Règlement Général sur la Protection des Données (RGPD) entré en vigueur le 25 mai 2018, ainsi que sur nos programmes pour soutenir votre conformité au RGPD. En qualité de sous-traitant, nous bénéficions d'une expérience éprouvée en matière de sécurité des données et de bonnes pratiques.

Nous nous engageons à respecter les dispositions du RGPD, telles que détaillées à la Section 3, dans une optique d'amélioration continue.

2 Qu'est-ce que le RGPD et en quoi vous concerne-t-il ?

Le RGPD et la réforme de la loi n°78-17 en date du 6 janvier 1978 relative à l'informatique aux fichiers électroniques et aux libertés intervenue suite au RGPD constituent des changements importants en matière de protection des données au sein de l'UE et de la France, avec plusieurs changements clés ayant eu un impact sur nos services et nos clients :

- **Responsabilité:** le nouveau principe de responsabilité dans le cadre du RGPD oblige les organisations à démontrer plus explicitement leur conformité avec les principes du RGPD.
- **Droits individuels étendus:** droits individuels (droits d'accès, de rectification, d'opposition au traitement des données et de limitation du traitement) avec ajout du droit à l'effacement et du droit à la portabilité des données pour chaque personne concernée.
- **Cadre de gouvernance:** en lien avec le principe de responsabilité, il s'agit de l'obligation pour les responsables du traitement et les sous-traitants de mettre en oeuvre des mesures techniques et organisationnelles adaptées, et de démontrer que tout traitement de données personnelles est conforme au RGPD.
- **Amendes:** en cas de violations du RGPD, les Autorités de Contrôle des États Membres de l'UE et la CNIL en France (qui sont responsables de l'application du RGPD) peuvent infliger des amendes allant jusqu'à 4 % du chiffre d'affaires global ou 20 000 000 euros, en fonction du montant le plus élevé.



3 Pourquoi travailler avec nous ?

Nous accordons la priorité à la sécurité des données: nous comprenons nos obligations en matière de sécurité, et nous les avons toujours pris au sérieux, et ce bien avant l'établissement du RGPD. Notre engagement en matière de sécurité est démontré par nos actuels programmes de certification, en place depuis de nombreuses années. En particulier, nous avons développé et mis en oeuvre un système de gestion de la sécurité de l'information certifié ISO 27001 depuis plus de 10 ans. De plus, nous avons obtenu la certification ISO 22301 pour nos Pratiques de Continuité des Activités et nous disposons de certifications ISO 20000 pour notre capacité à maintenir, soutenir et gérer professionnellement nos services informatiques en appliquant les meilleures pratiques.

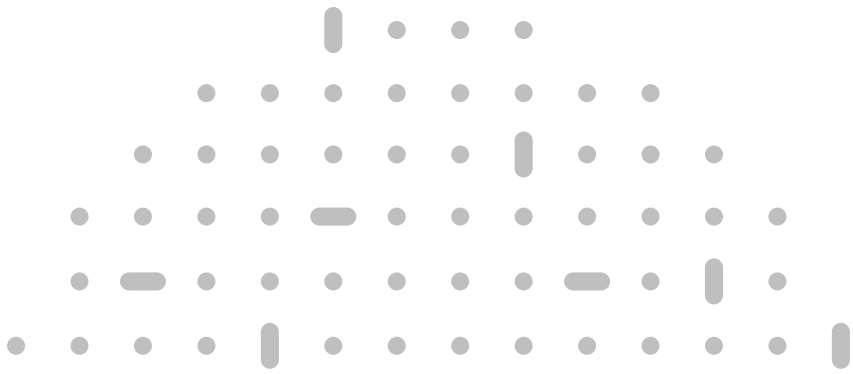
Nous avons pris toutes les mesures nécessaires. Pour améliorer encore davantage nos solides systèmes de protection des données dans le but de nous conformer au RGPD, nous avons pris les mesures suivantes.

- **Politiques et procédures mises à niveau:** dans le cadre de notre stratégie de conformité au RGPD, nous avons examiné et mis à niveau les politiques et procédures existantes afin de garantir cette conformité. Notre personnel et les personnes revêtant des rôles clés sont continuellement formés sur ces politiques de conformité ainsi que pour vous fournir une assistance dans vos propres efforts de conformité.
- **Avis de protection des données mis à jour:** l'avis de protection des données présenté aux candidats lorsqu'ils passent une évaluation est conforme aux exigences du RGPD.
- **Accords de traitement de données mis à jour:** nous avons mis à jour nos accords de traitement de données avec nos clients afin d'inclure les dispositions visant à nous conformer aux exigences du RGPD.
- **Protection des données dès la conception et par défaut:** nous nous engageons à faciliter la stratégie de gouvernance de la protection des données de nos clients, incluant les nouvelles obligations sur le respect de la protection des données dès la conception et par défaut conception et par défaut. La protection de des

données dès la conception conception exige que les organisations prennent des mesures appropriées pour intégrer les principes de protection des données du RGPD dans leurs opérations, tout en tenant compte des coûts, du contexte et des risques. La protection des données par défaut oblige les organisations à prendre, par défaut, des mesures techniques et organisationnelles appropriées pour minimiser l'utilisation des données pour toutes les finalités pour lesquelles elles sont collectées.

- **Notification de violation des données personnelles:** en application du GDPR, vous avez l'obligation d'informer l'autorité de contrôle sans retard excessif et, si possible, au plus tard 72 heures après avoir eu connaissance d'une violation de données à caractère personnel. Dans le cas où nous aurions connaissance d'une violation affectant vos données personnelles, nous vous en informerons sans retard indu dans un délai maximum de 48 heures, et vous aiderons à vous conformer à vos obligations en vertu du RGPD en vous fournissant, en temps opportun, les informations requises liées à la violation de données personnelles.
- **Analyses d'impact relative à la protection des données:** nous faciliterons votre respect des obligations du RGPD en vous aidant à réaliser des analyses d'impact relatives à la protection des données afin d'identifier et de minimiser le risque de non-conformité.
- **Surveillance de la conformité au RGPD:** nous continuerons d'examiner et d'auditer régulièrement la sécurité de nos services ainsi que notre conformité à nos politiques et procédures en vertu du RGPD.
- **Formation:** en poursuivant notre programme de formation de longue date sur la protection des données, nous continuerons à former notre personnel à l'échelle mondiale sur les critères applicables en matière de protection des données incluant le RGPD, dans le cadre de notre certification ISO 27001. De plus, nous dispensons une formation approfondie aux personnes revêtant des rôles clés, conformément au RGPD.
- **Tenir des registres de traitement:** comme l'exige le RGPD, dans notre rôle de sous-traitant, nous tenons un registre de nos activités de traitement pour chaque type de traitement de données effectué.
- **Évaluation des droits individuels:** en vertu du RGPD, vous êtes tenu(e), en tant que responsable du traitement, de faciliter l'exercice des droits de chaque personne concernée. En tant que sous-traitant, nous avons exposé ci-dessous les moyens par lesquels nos systèmes et processus peuvent vous aider à respecter vos obligations envers les personnes concernées:

Article du RGPD	Conformité
Article 13 **Le droit à l'information**	Notre plateforme d'évaluation comprend un avis de protection des données présenté aux individus avant de passer l'évaluation. Cet avis fournit à l'individu en question des informations sur la collecte et le traitement que nous effectuons, conformément à la législation applicable en matière de protection des données. Dans la mesure où l'évaluation fait partie d'un processus de recrutement global (et que l'évaluation n'est généralement pas votre premier point de collecte de données sur les candidats), les exigences de notification de l'Article 13 peuvent également devoir être satisfaites avant d'accéder à notre plateforme d'évaluation. Vous pouvez utiliser plusieurs méthodes différentes, telles que votre site Web de carrières, un formulaire de candidature en ligne ou un système de suivi des candidats pour recevoir les candidatures initiales, et pour collecter d'autres informations personnelles, par exemple des informations de CV ou une adresse de résidence, etc. Pour chacun de ces systèmes, un avis de protection des données traitant du cycle complet de recrutement serait nécessaire au moment de la collecte des données. Vous devez demander un avis juridique indépendant afin de connaître vos obligations de conformité en vertu de l'Article 13 du RGPD.



Article du RGPD	Conformité
Article 15 - 18 **Le droit** **• d'accès** **• à la rectification** **• à l'effacement** **• à la limitation du traitement**	La demande d'un candidat d'accéder, de corriger, de supprimer ou de limiter le traitement de ses propres données doit vous être adressée, en tant que responsable du traitement des données. Nous recevons occasionnellement des demandes de suppression d'informations ou d'accès à leurs résultats directement de la part des candidats. Nous redirigeons ces demandes vers le responsable du traitement des données. Nous vous fournissons ensuite le soutien et les informations dont vous avez besoin pour remplir vos obligations envers le candidat. Si nous recevons une demande de ce type directement de votre part en tant que client, nous avons déjà mis en place des processus permettant de répondre à votre demande, qu'il s'agisse d'une réponse rapide de demande d'accès ou de suppression de données d'une personne concernée. Les clients demandent souvent « pendant combien de temps conservez-vous les données ? » En tant que sous-traitant, nous conservons les données conformément aux contrats passés avec nos clients, ce qui signifie que nous supprimons les données suite à une demande émanant de vous, nos clients. Dans le cadre de notre stratégie de conformité au RGPD, nous avons apporté des améliorations à notre plateforme afin d'intégrer une automatisation et une efficacité accrues dans nos processus de suppression des données.

Article du RGPD	Conformité
Article 20 **Le droit à la portabilité des données**	Le droit à la portabilité des données s'applique uniquement : • aux données personnelles qu'un individu (c'est-à-dire un candidat) a fournies à nos clients en leur qualité de responsable du traitement ; • lorsque le traitement est fondé sur le consentement de l'individu ou sur les besoins de l'exécution d'un contrat ; et • lorsque le traitement est effectué avec des moyens automatisés (il ne s'applique pas aux enregistrements papier). Compte tenu du contexte des produits et services que nous proposons, nous considérons ce droit comme étant étroitement lié au droit d'accès comme indiqué ci-dessus. Par conséquent, nous vous enverrons ces demandes en tant que responsable du traitement des données, et nous vous assisterons dans vos décisions en termes de conformité. Les informations collectées directement auprès de l'individu sont limitées et, par conséquent, les fournir dans un « format structuré, couramment utilisé, lisible par machine et interopérable » peut être facilement effectué au cas par cas. Il vous appartient, en tant que responsable du traitement, de déterminer l'étendue des informations que vous souhaitez rendre disponibles en vertu de ce droit.

Article du RGPD	Conformité
Article 21 **Le droit d'opposition**	Un candidat peut avoir le droit de s'opposer au traitement de ses données personnelles si votre base juridique de traitement, en tant que responsable du traitement, repose sur des intérêts légitimes. Les candidats sont libres de choisir de passer ou non une évaluation. En cas d'opposition au traitement des données, un individu peut tout simplement se retirer de l'évaluation et aucun traitement ultérieur ne sera effectué par nous. Si le candidat s'oppose au traitement de ses propres données personnelles après avoir commencé une évaluation, cette opposition rentrera dans le droit de suppression conformément à l'Article 15.
Article 22 **Droits relatifs à la prise de décision automatisée et au profilage**	Le RGPD prévoit le droit des individus à ne pas être soumis à des décisions automatisées à moins que certaines exemptions ne s'appliquent. Nos clients font souvent appel à nos services pour les aider à prendre des décisions quant à l'opportunité d'offrir un emploi ou une promotion à un individu. Nos lignes directrices sur les meilleures pratiques recommandent que nos évaluations soient utilisées dans le cadre d'une évaluation globale, sans toutefois être considérées comme la seule base de décision quant à l'attribution d'un poste. Pour toute autre utilisation de nos évaluations, nous vous conseillons de demander un avis juridique indépendant sur vos obligations en matière de conformité à l'Article 22 du RGPD. En tant que responsable du traitement des données, si vous nous informez que vous avez l'intention d'utiliser notre évaluation dans le cadre d'une décision automatisée, nous pouvons suivre vos instructions concernant votre approche de toute exception autorisée, telle qu'une notification suffisante aux individus qu'ils peuvent faire l'objet d'une décision automatisée.

Nous nous conformons aux règles de transfert international: conformément à nos pratiques actuelles, nous continuerons à nous assurer de ne pas transférer de données en dehors de l'EEE en l'absence de structure de transfert de données appropriée. Nous disposons actuellement de clauses contractuelles types émises par l'UE (« Clauses types ») en matière de transferts en dehors de l'EEE. Suite à la FAQ du Comité européen de la protection des données (CEPD) adoptée le 23 juillet 2020 (disponible ici) concernant la décision Schrems II, nous sommes heureux d'aider nos clients à déterminer l'adéquation de ces transferts.

Nous mettons également à jour nos politiques et procédures à la lumière du retrait du Royaume-Uni de l'Union Européenne. Indépendamment du Brexit, SHL reste attachée au RGPD et nous évaluons actuellement les options possibles en ce qui concerne le transfert de données entre le Royaume-Uni et l'EEE.

Nous continuerons de surveiller toute proposition de modification des Clauses types conformément au RGPD et nous nous assurerons, le cas échéant, de mettre nos accords à niveau. Nous attendons également de plus amples informations de la part du Comité Européen de la Protection des Données (CEPD) dont les mesures supplémentaires pourraient consister en l'utilisation des Clauses contractuelles types de l'UE en matière de transfert des données vers des pays tiers.

Accords sur la protection des données: selon les besoins, nous concluons régulièrement des accords de protection des données avec nos clients. Merci de bien vouloir consulter votre représentant commercial et nous contacter afin de mettre à jour ou de mettre en oeuvre les Clauses contractuelles types de l'UE ou tout autre accord statutaire permettant de répondre à vos exigences.

Si vous avez d'autres questions, veuillez vous adresser à votre responsable de compte ou envoyer un e-mail à data.questions@shl.com.