Le candidat doit-il être informé des mesures de sécurité appliquées à ses données lors du recrutement ?

Réponse courte

Oui, le candidat doit être informé des mesures de sécurité appliquées à ses données lors du recrutement. Cette information doit être fournie de manière claire, accessible et compréhensible, dès la collecte des données, et doit détailler les dispositifs techniques et organisationnels mis en place pour protéger ses données personnelles.

L'employeur doit remettre cette information par écrit, généralement via une notice d'information spécifique au recrutement, qui mentionne explicitement les mesures de sécurité, la durée de conservation, les accès autorisés, et les procédures en cas de violation de données. Il doit également pouvoir prouver que cette information a bien été communiquée au candidat.

Définition

L'information du candidat sur les mesures de sécurité des données à caractère personnel consiste à communiquer, lors du processus de recrutement, les modalités de protection appliquées aux données collectées et traitées par l'employeur. Cette obligation vise à garantir la transparence sur les dispositifs techniques et organisationnels mis en place pour assurer la confidentialité, l'intégrité et la disponibilité des données personnelles du candidat.

Cette information s'inscrit dans le cadre du respect du droit à la protection des données à caractère personnel, qui impose à tout responsable de traitement d'informer la personne concernée sur la manière dont ses données sont protégées contre tout accès non autorisé, perte, altération ou divulgation.

Conditions d'exercice

L'obligation d'information s'applique dès la collecte de données à caractère personnel auprès du candidat, quel que soit le support utilisé (électronique, papier, oral). L'employeur doit fournir cette information de manière claire, accessible et compréhensible, avant ou au moment de la collecte des données, conformément au principe de transparence.

Cette obligation concerne tous les traitements de données réalisés dans le cadre du recrutement, y compris les mesures de sécurité techniques (chiffrement, contrôle d'accès) et organisationnelles (limitation des accès, procédures internes). L'information doit également porter sur les droits du candidat, l'existence d'une prise de décision automatisée, et l'encadrement humain des traitements automatisés, le cas échéant.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Modalités pratiques

L’information doit être délivrée par écrit, généralement via une notice d’information jointe à l’offre d’emploi, au formulaire de candidature ou accessible sur le site internet de l’employeur. Cette notice doit mentionner explicitement les mesures de sécurité mises en œuvre, telles que le chiffrement, la limitation des accès, la conservation sécurisée des dossiers, ou encore les procédures en cas de violation de données.

Il est recommandé de détailler les catégories de personnes ayant accès aux données, la durée de conservation, les modalités de destruction ou d’anonymisation des informations à l’issue du processus de recrutement, ainsi que les coordonnées du délégué à la protection des données (DPO) si applicable. L’employeur doit être en mesure de prouver que cette information a bien été communiquée au candidat, par exemple via un accusé de réception électronique ou une signature manuscrite.

Pratiques et recommandations

Il est conseillé d’élaborer une notice d’information spécifique au recrutement, distincte de celle destinée aux salariés, afin de couvrir les particularités du traitement des données des candidats. Cette notice doit être régulièrement mise à jour pour refléter l’évolution des mesures de sécurité, des pratiques internes et des technologies utilisées.

L’employeur doit veiller à utiliser un langage compréhensible, éviter les formulations techniques obscures et privilégier la transparence sur les dispositifs concrets de sécurité. Il est également recommandé de conserver une preuve de la remise de l’information, et de sensibiliser les personnes impliquées dans le recrutement à la confidentialité et à la protection des données.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Cadre juridique

- **Code du travail luxembourgeois** :
  - Article L.261-1 (principe de protection des données à caractère personnel dans le cadre de la relation de travail)
  - Article L.261-2 (obligation d'information du salarié et du candidat sur les traitements de données)
  - Article L.261-3 (droit d'accès, de rectification et d'opposition)
- **Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données** :
  - Article 41 (obligation d'information de la personne concernée sur les finalités, destinataires, durée de conservation et mesures de sécurité)
- **Règlement (UE) 2016/679 (RGPD)** :
  - Article 13 (informations à fournir lors de la collecte de données)
  - Article 32 (sécurité du traitement)
- **Principes généraux** :
  - Égalité de traitement (Code du travail, article L.241-1)
  - Traçabilité et preuve de l'information (obligation implicite de documentation)
  - Encadrement humain des traitements automatisés (Code du travail, article L.261-2, RGPD art. 22)

Adaptez systématiquement la notice d'information à chaque campagne de recrutement, en tenant compte des spécificités des traitements, des évolutions technologiques et des recommandations de la CNPD. Assurez-vous de pouvoir prouver la remise de l'information à chaque candidat, afin de garantir la conformité et d'éviter tout risque de contentieux.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.