Comment les RH doivent-ils interagir avec la House of Cybersecurity pour protéger les données RH ?

Réponse courte

Les RH doivent désigner un **interlocuteur dédié** à la cybersécurité pour assurer la liaison avec la **House of Cybersecurity** (HoC), formaliser cette désignation et l'intégrer dans les **procédures internes**. En cas d'**incident** ou de suspicion de **violation de données** RH, ils doivent **notifier immédiatement** la HoC via les **canaux sécurisés**, fournir toutes les **informations nécessaires** à l'analyse et collaborer à la mise en œuvre des **mesures correctives** et des **notifications obligatoires**.

Il est recommandé d'intégrer la HoC dans la **politique interne** de gestion des risques, d'organiser des **sessions de sensibilisation** à la cybersécurité en collaboration avec elle, et d'aligner les **procédures internes** sur ses recommandations. Toute interaction avec la HoC doit être **documentée** et **horodatée** pour garantir la **traçabilité** et la **conformité** en cas de contrôle ou de contentieux.

Définition

La **House of Cybersecurity** (HoC) est l'**entité nationale luxembourgeoise** chargée de la coordination, du conseil et de l'assistance en matière de **cybersécurité**. Elle agit comme **point de contact** pour les organisations publiques et privées, y compris les départements RH, afin de **prévenir**, **détecter** et **gérer** les incidents de sécurité affectant les systèmes d'information et les **données à caractère personnel**, notamment les données RH.

Les interactions entre les RH et la HoC visent à garantir la **confidentialité**, l'**intégrité** et la **disponibilité** des données RH, conformément aux **exigences légales luxembourgeoises**. Cette collaboration s'inscrit dans le cadre de la **protection des droits** des salariés et du respect des **obligations de sécurité** imposées aux employeurs.

Conditions d’exercice

Les responsables RH sont **légalement tenus** d'assurer la sécurité des **données à caractère personnel** traitées dans le cadre de la gestion du personnel, conformément à la **loi du 1er août 2018** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette obligation implique la mise en œuvre de **mesures techniques et organisationnelles** appropriées pour garantir un niveau de sécurité adapté aux risques.

En cas d'**incident de sécurité** ou de suspicion de **violation de données**, les RH doivent solliciter l'expertise de la HoC, notamment pour l'**analyse**, la **gestion de crise** et la **remédiation**. La collaboration avec la HoC devient **indispensable** lorsque les capacités internes de l'entreprise sont insuffisantes pour traiter un incident ou pour se

conformer aux **obligations de notification** auprès de la **Commission nationale pour la protection des données** (CNPD).

Les RH doivent également veiller à l'**égalité de traitement** des salariés, à la **traçabilité** des actions entreprises et à l'**encadrement humain** des processus automatisés, conformément aux principes généraux du **Code du travail luxembourgeois**.

Modalités pratiques

Organisation interne :

- **Désignation d'un interlocuteur** dédié à la cybersécurité, chargé de la liaison avec la HoC
- **Formalisation** de cette désignation et communication à la direction et aux équipes informatiques
- **Intégration** dans les procédures internes de gestion des incidents

Gestion des incidents :

- **Notification immédiate** à la HoC via les **canaux sécurisés** mis à disposition (portail sécurisé, ligne téléphonique dédiée)
- **Fourniture** de toutes les informations nécessaires à l'analyse : **nature des données** concernées, **circonstances** de la compromission, **mesures déjà prises**
- **Collaboration** étroite avec la HoC pour la qualification de l'incident et la mise en œuvre de **mesures correctives**
- **Préparation** des notifications obligatoires à la **CNPD** et aux **personnes concernées** le cas échéant

Documentation et traçabilité :

- **Documentation** et **archivage** de tous les échanges avec la HoC
- **Horodatage** de toutes les actions entreprises
- **Conservation** des preuves conformément aux exigences de traçabilité

Pratiques et recommandations

Il est recommandé aux RH de :

- **Intégrer la HoC** dans leur **politique interne** de gestion des risques liés aux données personnelles
- **Organiser des sessions** de sensibilisation à la cybersécurité en collaboration avec la HoC, notamment sur les **risques spécifiques** aux données RH (phishing, accès non autorisé, fuite de données)
- **Aligner les procédures internes** sur les **guides et recommandations** publiés par la HoC, en particulier en matière de gestion des mots de passe, de contrôle d'accès et de chiffrement des données RH
- **Réaliser des audits réguliers** de sécurité en impliquant la HoC pour évaluer la **robustesse** des dispositifs existants
- **Consulter préalablement** la HoC en cas de projet impliquant de nouveaux traitements de données RH pour anticiper les risques
- **Sensibiliser régulièrement** les salariés à la **protection des données** et à la **cybersécurité**
- **Maintenir une veille** sur les **menaces émergentes** et les **bonnes pratiques** recommandées par la HoC

Cadre juridique

- **Loi du 1er août 2018** relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, notamment :
  - Article 32 : obligation de mettre en œuvre des **mesures techniques et organisationnelles** appropriées pour garantir la **sécurité des données**
  - Articles 33 et 34 : **notification des violations** de données à la CNPD et aux personnes concernées
- **Loi du 28 mai 2019** relative à la sécurité des réseaux et des systèmes d'information (transposant la **directive NIS**), qui confère à la HoC un **rôle central** dans l'assistance aux entités en matière de cybersécurité
- **Code du travail luxembourgeois** :
  - Articles L.261-1 et suivants : **respect de la vie privée** et **protection des données** des salariés
  - Article L.414-3 : **égalité de traitement** et **non-discrimination** dans la gestion des données RH
- **Règlement (UE) 2016/679 (RGPD)** : obligations en matière de **sécurité** et de **notification** des violations de données

La **documentation précise** et **horodatée** de chaque interaction avec la House of Cybersecurity est essentielle pour démontrer la **conformité** en cas de contrôle de la CNPD ou de contentieux relatif à la **protection des données RH**. Il est impératif de garantir la **traçabilité** et l'**encadrement humain** de toutes les démarches entreprises. La **collaboration proactive** avec la HoC renforce significativement la **posture de sécurité** de l'entreprise et facilite le respect des **obligations légales** en matière de protection des données.