

Annexe

Procédure Groupe P&V - Violation de données à caractère personnel (Data Breach)

1. Qu'est-ce qu'une violation de données à caractère personnel ?

- Une violation de données à caractère personnel (Data Breach) est un incident de sécurité susceptible d'entraîner une utilisation non autorisée de données à caractère personnel, y compris la perte, la destruction, l'altération, la divulgation, l'accès, le transfert, le stockage ou l'extraction non autorisés.
- Les données à caractère personnel sont toutes les informations se rapportant à une personne physique identifiée ou identifiable, y compris les informations de nature professionnelle et même les données qui sont (déjà) publiquement disponibles.
- Une violation de données à caractère personnel peut avoir différentes causes, telles que des actes ou des erreurs de travailleurs ou de collaborateurs (perte ou vol de matériel ou d'équipement, etc.), des attaques externes, des failles de sécurité dans le système informatique ou les logiciels, ou toute autre forme d'acte frauduleux ou malveillant, ainsi que des actes non intentionnels conduisant à une violation de données.
- Il n'y a pas de critère pour le nombre de données ou l'ampleur d'une violation de données. Même un incident mineur est préoccupant s'il peut mettre en danger des données à caractère personnel.

2. Que dois-je faire en cas de violation réelle ou potentielle de données à caractère personnel ?

Si vous avez connaissance d'un incident de sécurité susceptible de constituer une violation (réelle ou potentielle) de données à caractère personnel, vous devez en informer immédiatement le Helpdesk P&V en cliquant sur bouton « Signaler Data Breach » disponible sur la homepage Connect 360 ou en téléphonant au 0800 35 219.

- Prévenez également votre District Manager.
- Utilisez en priorité le bouton d'alerte sur Connect360.
- Si vous utilisez un autre moyen de communication, le Helpdesk vous contactera pour recueillir les informations nécessaires. N'oubliez donc pas d'indiquer le numéro de téléphone où l'on peut vous joindre.
- Ne menez pas d'enquête ou d'analyse vous-même, cela relève de la responsabilité de la Data Breach Team. Si nécessaire, celle-ci vous posera des questions supplémentaires.
- N'essayez pas de supprimer, de modifier ou d'enregistrer des données ou des informations relatives à l'incident. Votre notification au Helpdesk suffit.
- Ne communiquez pas vous-même sur l'incident et n'en parlez pas à d'autres, sauf à votre District Manager et le Helpdesk de P&V. La communication sur l'incident et la notification d'un Data Breach relèvent de la responsabilité de la Data Breach Team.

3. Collectez les informations nécessaires

Pour ce faire, utilisez le formulaire ci-joint et gardez-le à portée de main lorsque vous signalez l'incident par téléphone à l'opérateur du Helpdesk.

Si vous signalez l'incident à l'aide du bouton d'alerte via Connect 360, le questionnaire s'affichera automatiquement.