

Règlement Principales mesures à appliquer par le courtier en assurances

Baloise Insurance met tout en œuvre pour protéger le mieux possible ses services ainsi que les informations traitées. La protection de l'environnement de travail du courtier en assurances sous-traitant constitue également un facteur d'importance. C'est pourquoi le courtier en assurances sous-traitant qui utilise les services et les informations de Baloise Insurance est également lié aux règles qui définissent l'utilisation autorisée. Ces mesures minimales sont nécessaires pour la sécurité de l'information.

1. Réseau sécurisé

Le courtier en assurances sous-traitant communique avec Baloise Insurance via un réseau reconnu par Baloise Insurance:

- soit via le réseau Portima: AS/Web (VPN Belgacom);
- soit via l'internet standard.

2. Mesures en matière de sécurité informatique

Le courtier en assurances sous-traitant prend en compte les mesures suivantes en matière de sécurité informatique:

- Le courtier en assurances veille à la protection adéquate de sa propre infrastructure informatique et applique les mesures relatives à la politique en matière de sécurité informatique en vigueur de Baloise Insurance, comme indiqué dans l'accord d'utilisation relative à MyBaloise.
- Les moyens informatiques (ordinateurs et appareils mobiles) qui permettent un accès aux services et à l'information de Baloise Insurance, doivent être protégés de manière performante contre les différents risques liés à l'internet (e.a. les virus, le spam, le piratage).
- Le courtier en assurances veille également à prendre les mesures nécessaires afin de protéger l'accès des autres appareils liés à son réseau et connectés à l'internet.

3. Confidentialité du mot de passe

- Le mot de passe qui permet d'accéder au système informatique du courtier en assurances sous-traitant et aux services de Baloise Insurance est strictement personnel et confidentiel.
- Il ne peut en aucun cas être divulgué à des tiers ou partagé avec d'autres utilisateurs du système informatique.
- Le mot de passe doit être difficile à deviner et il est préférable d'en changer régulièrement.
- Si la confidentialité de ce mot de passe n'est plus garantie, il doit être modifié.

4. Classification de l'information

Le courtier en assurances sous-traitant veille également à ce que les informations de Baloise Insurance soient traitées avec précaution et reçoivent un niveau de protection adapté. C'est surtout valable pour les données personnelles des clients (e.a. médicales et judiciaires), dans le cadre de la gestion de la police et des sinistres. Ces données sont considérées par défaut par Baloise Insurance comme confidentielles. Le niveau de classification attribué doit être respecté et ne peut dès lors pas être abaissé.

5. Protection des données

- Le courtier en assurances sous-traitant veille à ce que les personnes non expressément autorisées ne puissent pas obtenir d'accès aux données. Il est notamment interdit de laisser un ordinateur en mode de fonctionnement sans surveillance.
- Lorsqu'un collaborateur quitte sa fonction, toutes les actions nécessaires dans ce contexte sont menées dans les délais impartis, comme la fermeture du (des) compte(s) d'accès et la restitution des moyens informatiques éventuellement mis à disposition.
- Les données ne peuvent pas être copiées sur un support amovible (sauf pour la sauvegarde), puisque ces supports sont exposés à un risque accru de perte ou de vol. Les informations qui ont subi une fuite peuvent être utilisées contre le courtier en assurances et Baloise Insurance et nuire ainsi à leur réputation et avoir des conséquences juridiques.
- Le courtier en assurances sous-traitant fait preuve de prudence lorsque des informations sont échangées avec d'autres parties via des moyens de communication. Il est d'ailleurs vivement déconseillé d'envoyer des informations sur les clients de manière non sécurisée via des espaces de stockage publics sur internet car il est aisé d'en perdre le contrôle.

- Au cours d'entretiens téléphoniques, le collaborateur doit s'assurer de l'identité du demandeur et vérifier s'il est habilité à communiquer ces données. Il convient également de tenir compte du fait que si des informations sont transmises à une partie non concernée, cela pourrait avoir de lourdes conséquences.
- Le courtier en assurances sous-traitant doit vérifier l'adresse web (URL) et le certificat de protection (le petit cadenas dans la barre d'adresse de votre navigateur) des services internet interactifs proposés par Baloise Insurance afin de s'assurer qu'il ne visite pas un site falsifié ou non sécurisé (via des courriels de "phishing"). Il ne peut compléter aucune information sensible si l'adresse n'est pas correctement écrite ou s'il n'y a pas de petit cadenas dans son barre de navigation.

6. Collaboration avec des tiers

Lorsque l'on collabore avec des tiers et que certaines activités sont sous-traitées, il y a lieu de respecter de saines pratiques en matière de gestion dès que des informations de Baloise Insurance sont traitées. Il convient de toujours s'assurer de prendre les mesures nécessaires pour protéger la confidentialité et l'intégrité des données relatives à l'assurance.

7. Protection physique

Le courtier en assurances sous-traitant doit prendre toutes les mesures raisonnables pour protéger les bâtiments, les locaux et les équipements contre le feu, les dégâts des eaux, le vol, l'effraction etc.

Il convient également d'éviter que les visiteurs aient accès à des informations ou des moyens auxquels ils n'ont pas besoin d'avoir accès et qu'ils pourraient endommager.

Le courtier en assurances sous-traitant veille aussi à prêter suffisamment d'attention à la protection physique des documents comportant des informations personnelles.

Tout support de stockage qui, pour une quelconque raison, doit être enlevé afin d'être détruit ou réparé et réutilisé, et qui contient des informations confidentielles doit être détruit physiquement ou réécrit à plusieurs reprises.

8. Instructions matérielles

Le courtier en assurances sous-traitant suit les instructions de Baloise Insurance relatives à l'utilisation des applications MyBaloise et les dispositions administratives associées.

9. Signalement des incidents concernant la sécurité

Le courtier en assurances sous-traitant a l'obligation de signaler les cas suivants:

- perte ou divulgation à des tiers non habilités d'informations confidentielles, ou suspicion d'un tel événement;
- fuites ou problèmes de sécurité, vulnérabilités et/ou menaces constatées ou remarquées, ou suspicion d'un tel événement;
- utilisation illicite de systèmes informatiques, ou suspicion d'un tel événement;
- perte, vol ou divulgation de mots de passe ou d'autres formes de mécanismes d'accès logiques et/ou physiques, ou suspicion d'un tel événement;
- vol de biens ou d'informations appartenant à l'entreprise, ou suspicion d'un tel événement.

Il y a lieu de signaler immédiatement de tels incidents de sécurité au helpdesk de Baloise Insurance. Dès qu'une infraction de ce type est remarquée, les utilisateurs doivent au moins effectuer une réinitialisation de leur mot de passe et le certificat attribué doit être retiré et renouvelé.

Votre sécurité nous tient à cœur.

www.baloise.be