# PROCÉDURE EN CAS D'ATTEINTE AUX DONNÉES À CARACTÉRE PERSONNEL ET FUITES DE DONNÉES

## 1. INTRODUCTION

BPC SA (ci-après la « Société ») accorde une grande importance à la protection des données à caractère personnel et à la protection des informations confidentielles. La Société prend très au sérieux ses obligations résultant du Règlement Général sur la Protection des Données.

La Société tient à ce que tous ses collaborateurs entrant en contact avec des données à caractère personnel et des informations confidentielles traitent celles-ci avec la plus grande prudence.

Cette politique s'applique à toute personne qui, de quelque manière que ce soit, entre dans l'exercice de ses fonctions en contact avec des informations confidentielles (secrets d'affaires, informations professionnelles ou avec des données pouvant être considérées comme données à caractère personnel au sens du Règlement Général sur la Protection des Données (p. ex. données à caractère personnel de clients, fournisseurs et tiers). Cette Politique s'applique à tous les collaborateurs de la Société, y compris aux administrateurs, aux membres de la direction, aux collaborateurs indépendants, aux travailleurs intérimaires, étudiants jobistes et stagiaires (ci-après « le Collaborateur »).

Par cette Politique, la Société entend informer les Collaborateurs de la façon dont il convient de gérer les données à caractère personnel et les informations confidentielles, afin de réduire autant que possible le risque d'atteintes éventuelles. Le Collaborateur est tenu de respecter scrupuleusement les consignes ci-dessous.

## 2. ACCES

Dans le cadre de l'exercice de sa fonction, le Collaborateur a accès à des informations confidentielles et des données à caractère personnel. Ces informations confidentielles et données à caractère personnel ne peuvent être utilisées que dans la mesure rendue indispensable par l'exercice de la fonction. Le Collaborateur veillera à ce que les informations confidentielles et données à caractère personnel ne soient pas partagées avec des personnes non habilitées (en ce compris les collègues non habilités).

Le Collaborateur s'engage en outre à ne pas prendre connaissance d'informations confidentielles et données à caractère personnel dont il sait ou devrait savoir qu'il n'a pas le droit d'y accéder.

Le Collaborateur n'utilisera jamais les informations confidentielles et données à caractère personnel au détriment de la Société.

## 3. OBLIGATIONS ET RESPONSABILITES

Le Collaborateur traitera toujours les informations confidentielles et données à caractère personnel avec prudence et diligence. En particulier, il observera les règles et mesures suivantes :

- Les documents ou fichiers professionnels ne peuvent être conservés que sur des systèmes prévus à cet effet.
- Les documents ou fichiers professionnels ne seront jamais transmis à une mailbox privée ou un tiers, à moins que cela soit indispensable à l'exécution des activités de l'entreprise ;
- Tous les collaborateurs sont responsables de la gestion correcte et prudente des mots de passe : les mots de passe doivent être suffisamment compliqués, ne pas être évidents et doivent être changés régulièrement (au moins tous les six mois) ;
- Les ordinateurs seront automatiquement verrouillés après 15 minutes d'inactivité et nécessiteront ensuite l'introduction d'un mot de passe pour la réactivation. Les ordinateurs portables, tablettes, smartphones, clés USB ou autres équipements, doivent être éteints et mis sous clef en cas de non-utilisation prolongée et en fin de journée.
- La Société s'efforce d'appliquer une « clean desk policy ». Les dossiers papier contenant des informations confidentielles ou des données à caractère personnel doivent être retirés du bureau en cas d'absence de plus de 15 minutes et sont mises sous clef à la fin de la journée de travail.
- L'impression de documents est traitée de manière confidentielle, ce qui signifie entre autres que le Collaborateur ne pourra en lancer l'impression que depuis le périphérique de sortie et moyennant l'usage de son badge d'accès, empêchant ainsi que les documents imprimés demeurent sur l'imprimante.
- Les informations confidentielles et données à caractère personnel ne seront jamais jetées avec les déchets papier ordinaires, mais toujours détruits dans la déchiqueteuse papier.
- Les informations confidentielles et données à caractère personnel seront le moins possible transportées à l'extérieur de la Société. Le transport de documents doit être strictement limité aux nécessités de la fonction, comme les réunions.
- Les Collaborateurs prendront toutes les dispositions nécessaires pour que les informations confidentielles et données à caractère personnel ne soient pas volées ou égarées. Aucun des supports possibles, comme les dossiers sur papier, un ordinateur portable, tablette, smartphone, clé USB, etc. ne sera ainsi laissé sans surveillance ou de façon non sécurisée en dehors du lieu de travail (p. ex. dans la voiture). Si un Collaborateur devait néanmoins être confronté à la perte ou au vol d'un de ces supports, il en informera son responsable ou le responsable de la protection des données dans les six heures qui en suivent la découverte.

- Lors de l'utilisation d'une connexion Wi-Fi, le Collaborateur s'assurera au préalable que celle-ci est sécurisée. Il ne peut jamais être fait usage de réseaux non sécurisés.
- Tout problème de sécurisation ou toute fuite de données, de même que la perte ou le vol d'un ordinateur portable, d'une tablette, d'une clé USB, d'un smartphone, etc., doivent être signalés immédiatement et au plus tard dans les six heures qui suivent leur découverte, conformément à la procédure en cas de fuite de données décrite dans la présente Politique.

## 4. PROCEDURE EN CAS D'ATTEINTE AUX DONNEES A CARACTERE PERSONNEL / FUITE DE DONNEES

Cette procédure s'applique à tout Collaborateur qui constate ou suspecte une atteinte à une donnée à caractère personnel.

Au sens du Règlement Général sur la Protection des Données (RGPD), une atteinte à une donnée à caractère personnel ou une fuite de données est « une violation » de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une façon quelconque ».

Le concept est à prendre au sens large et comprend notamment les fuites de données suivantes :
- hacking / phishing / ransomware ;
- fuite de données hors ligne (bac à papier, imprimante, ...) ;
- e-mail envoyé à une adresse e-mail erronée ;
- vol ou perte d'une clé USB ;
- vol ou perte d'un dossier papier ;
- vol ou perte d'un GSM, ordinateur portable, tablette ;
- diminution ou disparition de l'accessibilité (p. ex. panne de serveur).

La notion de donnée à caractère personnel est à comprendre conformément au Règlement Général sur la Protection des Données (p.ex. données à caractère personnel de clients, fournisseurs, travailleurs, tiers). En cas de doute quant à savoir si un élément constitue ou non une donnée à caractère personnel, le Collaborateur s'adressera immédiatement au responsable de la protection des données au sein de la Société.

En cas de fuite de données, il convient de respecter la procédure suivante :

### Phase 1 – Notification en interne

Le Collaborateur constatant une (possible) fuite de données, en informe immédiatement et au plus tard dans les six heures qui en suivent la découverte,

la personne ou les personnes au sein de la Société concernée qui est (sont) responsable(s) de la protection des données (ci-après le « Responsable du traitement des données »). Pour la Société cette personne est Monsieur Bernard Palange, agissant pour la srl. BPA Consult (info@bpc.be).

Cette notification s'effectuera si possible par e-mail. Dans son e-mail, le Collaborateur mentionnera au moins : 1) la nature de la fuite de données (p.ex. perte, plus d'accès, atteinte à la confidentialité), 2) de quelles données à caractère personnel il s'agit, 3) la cause possible (p.ex. piratage, perte, vol).

**Phase 2 – Evaluation, concertation et enregistrement dans un registre interne**

Le Responsable du traitement des données examine la notification dès réception, et en effectue une évaluation en fonction de la nature de la fuite et des données à caractère personnel concernées, ainsi que de la cause et des conséquences de la fuite de données. Cette procédure est également d'application si une personne chargée du traitement informe la Société d'une fuite de données.

- **Première hypothèse** : pas de fuite de données / pas de données à caractère personnel / pas de risques

  Si la notification ne porte pas sur une fuite de données, si aucune donnée à caractère personnel n'a fuité ou si la fuite de données ne pose aucun risque pour les droits et libertés des personnes concernées, le Responsable du traitement des données rapportera la notification interne à un membre du management de la Société concernée, enregistrera la fuite de données dans le registre interne de la Société concernée et en informera le collaborateur interne. Dans ce cas, la procédure prend fin ici.

- **Deuxième hypothèse : risques pour les personnes concernées ou pour la Société**

  Si la fuite de données comprend des données à caractère personnel et comporte un risque pour les droits et libertés des personnes concernées, ou si la fuite de données engendre des risques ou conséquences considérables pour la Société (p.ex. impact sur l'infrastructure IT, actes de malveillance, fuite de données sensibles ou très nombreuses), le Responsable de la protection des données contactera immédiatement un membre du management de la Société concernée afin d'aborder et évaluer la fuite de données (p.ex. conséquences pour les personnes concernées et la Société concernée, mesures afin de limiter les conséquences et de les éviter à l'avenir). Si nécessaire, le Responsable de la protection des données réunira une équipe de crise, composée : d'un membre du management de la Société concernée et, le cas échéant, d'autres personnes pouvant être utiles à la concertation (p.ex. le responsable IT, le responsable de la sécurité des systèmes d'information, etc.). Un rapport de cette concertation sera établi, et la fuite de données sera également enregistrée dans le registre interne de la

Société concernée. Si aucun risque n'est constaté pour les droits et libertés des personnes concernées, la procédure prend fin ici. Dans le cas contraire, l'on passe à la phase 3.

**Phase 3 – Notification à l'Autorité de Protection des Données (APD)**

Si un risque est constaté pour les droits et libertés des personnes concernées, le Responsable de la protection des données communiquera, après concertation avec un membre du management, la fuite de données à l'Autorité de Protection des Données. Cette communication s'effectue à l'aide du formulaire, comme prévu sur le site Internet de l'Autorité de Protection des Données.

La notification s'effectuera sans délai et au plus tard 72 heures après en avoir pris connaissance. Si la notification se fait plus tard ou seulement partiellement, il convient de le motiver.

La notification comprendra les données obligatoires prévues à l'article 33 du Règlement Général sur la Protection des Données : la nature de la fuite de données, les catégories et le nombre de personnes concernées, les catégories et le nombre de données à caractère personnel (si possible), les conséquences éventuelles de la fuite de données, les mesures destinées à remédier à la fuite de données et à éviter ou réduire les conséquences de la fuite de données.

Si la fuite de données n'engendre pas de grands risques pour les droits et libertés des personnes concernées, la procédure prend fin ici. Dans le cas contraire, l'on passe à la phase 4.

**Phase 4 – Notification aux personnes concernées**

En cas de risque élevé pour les droits et libertés des personnes concernées, la fuite de données est en principe communiquée sans délai aux personnes concernées. Conformément à l'article 34 du Règlement Général sur la Protection des Données, cette communication décrit, en des termes clairs et simples, la nature de la fuite de données, les conséquences probables de celle-ci, et les mesures destinées à remédier à la fuite de données et à en éviter ou en réduire les conséquences.

Cette notification n'est toutefois pas nécessaire si des mesures techniques et organisationnelles ont été prises afin de rendre les données illisibles (p.ex. cryptage, cryptographie) ou si des mesures ont été prises afin de s'assurer que le risque élevé pour les droits et libertés des personnes concernées ne se produira plus.

A chaque fuite de données, tout est mis en œuvre pour exécuter les mesures nécessaires ainsi que les éventuelles mesures techniques et organisationnelles nécessaires (p.ex. points de vigilance pour l'avenir, réduire les causes, réparer les pannes et les systèmes, éliminer les infections). Le Responsable de la

protection des données veille à leur exécution correcte et à leur suivi ultérieur. Tout ceci est évalué et documenté.

Si une fuite de données doit être communiquée à l'Autorité de Protection des Données, le Responsable du traitement des données établit un rapport qui reflète la nature de la fuite de données, la façon dont il a été procédé, les mesures prises, les personnes concernées et les points de vigilance pour l'avenir. Après approbation par un membre du management, le Responsable du traitement des données transmet ce rapport à la personne ou à l’organe en charge de la direction de la Société.