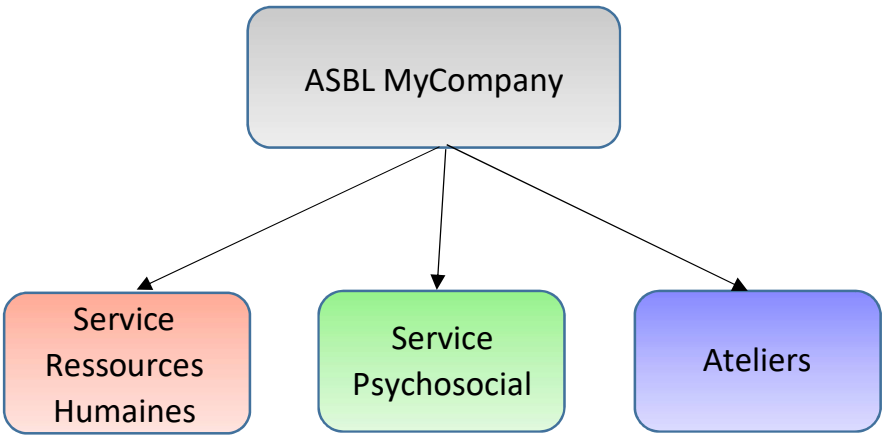

**Formation MONARC**

# MyCompany

## Contexte de l’entreprise

MyCompany est une ASBL (Association Sans But Lucratif) travaillant majoritairement à la réinsertion professionnelle pour les personnes fragilisées par des troubles psychologiques en proposant un accompagnement et un soutien tout particulier. Elle est composée d'environ 40 employés, et ce nombre reste stable depuis les dernières années malgré l'importante rotation du personnel ayant des contrats de 6 mois.
L'analyse de risque se passera sur l'ensemble de son système d'information. Néanmoins, avec les différentes données sensibles concernant les personnes qu'elle encadre, la société se doit de respecter scrupuleusement le GDPR à l'égard du traitement des données à caractère personnel. La perte des dossiers médicaux est de ce fait la plus grande menace à laquelle doit faire face l'entreprise.
MyCompany n'a pas de concurrents réels, mais elle a déjà connu un incident auparavant, à savoir le piratage et la perte de toutes les données antérieures à l'année 2005. Les locaux sont situés en centre-ville, dans un quartier extrêmement calme de Luxembourg. Aucune tentative d'effraction, ou aucun sinistre environnemental n'a eu lieu à l'emplacement.
Une des personnes clés de cette analyse des risques est Michael, Comptable et Administrateur Système pour l'association, bien qu'il n'utilise qu'un seul compte pour ses deux tâches. D'autres administrateurs sont externes à l'association.

Il est important de noter que l'entreprise ne dispose pas de charte utilisateur, de procédure d'installation ou de formation concernant la sécurité de l'information. Les droits administrateurs sont laissés aux employés utilisant les machines : ils laissent la session ouverte pour que l'IT puisse faire manuellement les mises à jour sur les machines, bien que les employés ont souvent un œil sur leur ordinateur. Les machines sont sur MAC sans antivirus, mais disposent d'une machine virtuelle Windows avec Bitdefender dessus.
Aucun NDA n'est signé avec les sous-traitants ayant accès aux données médicales. De plus, l'administrateur a aussi accès à ces données. Il est important de noter qu'il n'y a aucun contrôle sur les téléchargements. Tous les mots de passes des mails sont mis sur un fichier Excel sur le serveur.
Il est important de noter que le bâtiment dispose de portes automatiques ouvertes de 8h à 16h. En novembre, la température de la salle informatique s'élevait à 30°C, et la pièce n'a pas de climatisation. Elle est de plus utilisée pour stocker des affaires personnelles, et beaucoup de personnes disposent d'un double des clés.
Les backups sont réalisés trois fois par jour en local et une fois par semaine sur un autre site. Le temps de rétention n'est pas connu, même s'il est suffisant. Le sous-traitant teste les backups. Il n'y a personne qui est désigné responsable des backups. Il n'y a aucun contrat avec les sous-traitants en cas de litige. Le réseau est correctement géré, sans Wi-fi, avec un compte par utilisateur.



**Service Ressources Humaines** : 2 employés plein temps partageant le même mot de passe et les mêmes compétences sont dans le service. Ils connaissent suffisamment le logiciel utilisé pour pouvoir utiliser toutes les fonctions nécessaires. Les accès physiques aux bureaux sont correctement pensés, bien que l'entreprise de nettoyage agit hors des heures de bureau. L'intégrité des données semble assez importante pour l'équipe.

**Service Psychosocial** : 6 employés plein temps, qui partagent également le même mot de passe. Ils disposent des connaissances nécessaires pour l'utilisation de leur logiciel métier. Le télétravail y est pratiqué, et des mails, rares, avec des dossiers médicaux sont parfois envoyés non chiffrés. Les accès sont également bien gérés à l'exception de l'entreprise de nettoyage qui agit hors des heures de bureau. La confidentialité et l'intégrité des données semblent être cruciales d'après l'équipe.

**Ateliers** : Les ateliers dans lesquels travaillent les profils fragilisés sont au nombre de 3. Néanmoins, et ayant tous la même hiérarchie, ils ont étés considérés comme les mêmes. Le plus emblématique des ateliers est la menuiserie. Il y a en tout 25 à 35 employés, dont 3 chefs d'ateliers qui peuvent choisir de laisser l'accès à un PC de l'atelier aux employés y travaillant. La machine n'a accès ceci dit aucune information sensible. Les ateliers ont leur accès physique bien géré. Aucun tiers n'interviens dans le processus, et tout est géré en interne. D'après le management, aucune information réellement importante n'est dans les ateliers, en revanche ils se doivent de rester le plus possible disponibles.