

Questions STRATEGIE DE SECURITE

1. Utilisez-vous des technologies qui pourrait être perçues comme intrusive pour la vie privée? Vidéosurveillance ? l'utilisation de la biométrie ou de la reconnaissance faciale ?
2. Avez-vous mis en place des mesures techniques et organisationnelles appropriées pour éviter un traitement non autorisé ou illégal de données personnelles et contre toute perte ou destruction accidentelle ou dommage à des données personnelles ?
3. Qui a accès aux données récoltées ? Est-ce que seul le personnel qui a besoin de l'information a accès aux données ?
4. Avez-vous mis en place une démarche de gestion de la sécurité de l'information (SGSI, Certification ISO 27001 ou SANS ou autre). Cette démarche est-elle auditée régulièrement en interne ? Des tests d'intrusion externes sont-ils pratiqués au moins annuellement ?
5. Est-ce que le personnel est informé ou sensibilisé à la protection des données ?
6. Existe-t-il une culture du contrôle de conformité (procédures internes qui garantissent à tout moment la prise en compte de la protection de données) ou de l'audit de la protection des données et de la sécurité de l'information ?
7. Avez-vous mis en place un système permettant de regrouper toute la documentation concernant la protection des données?
8. Avez-vous déjà subi des incidents de sécurité de l'information et de protection des données Si oui quand, combien et à quelle intervalle ?
9. Comment avez-vous réagi ? Existe-t-il un plan pour réagir aux incidents ?