Résumé de l'évaluation des facteurs relatifs à la vie privée : Gambit ID

INTRODUCTION

Cette évaluation des facteurs relatifs à la vie privée (EFVP) visait à examiner les exigences en matière de protection des renseignements personnels applicables à l'utilisation de Gambit ID. Les Services de sécurité de l'entreprise recourront à Gambit ID pour recueillir des renseignements de sécurité sur les personnes au service de la Commission de la capitale nationale (CCN) ou collaborant avec celle-ci (c.-à-d. membres du personnel, personnel étudiant, bénévoles, tiers fournisseurs, etc.). Ce système servira également à traiter électroniquement les évaluations de sécurité auprès d'organisations externes, notamment la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS), aux fins de vérifications d'antécédents et d'approbations finales. Les renseignements prélevés sur Gambit ID seront stockés électroniquement dans des centres de données Amazon dotés d'une certification de sécurité valide et situés à Montréal, au Canada. Toutes les bases de données sont physiquement ou logiquement indépendantes des autres bases de données. Par conséquent, la solution comporte des dispositions garantissant que les données de la CCN ne seront pas divulguées à quiconque en dehors de la société d'État. Les renseignements personnels sont protégés en vertu de la *Loi sur la protection des renseignements personnel*s, L.R.C. 1985, c. P -21.

Dans le contexte de cette EFVP, le projet n'affecte pas d'autres programmes ou activités en cours, et tous les renseignements personnels recueillis et gérés demeurent inchangés. La CCN exploite plutôt une nouvelle technologie pour soutenir ces programmes. Un audit d'évaluation et d'autorisation de sécurité ainsi qu'un examen de nos politiques et marches à suivre opérationnelles nous permettront d'évaluer les risques liés aux mesures de protection techniques, physiques, opérationnelles et juridiques de Gambit ID.

Une évaluation des facteurs relatifs à la vie privée a été effectuée pour identifier les enjeux de confidentialité et élaborer des mesures pour minimiser les risques associés à la collecte, à l'utilisation, au stockage et à la divulgation de données personnelles au sein de la CCN par l'intermédiaire de Gambit ID.

CONTEXTE

Cette initiative vise à améliorer le processus d'administration et de contrôle de la sécurité et à l'harmoniser avec les dernières directives du gouvernement du Canada, tout en offrant une plus grande flexibilité au moyen d'une nouvelle solution infonuagique. Le gouvernement canadien ayant adopté une stratégie basée sur le nuage, la CCN s'est engagée dans une transition vers les services infonuagiques. Ces derniers procurent des avantages que ne peuvent offrir les capacités actuelles de la CCN. Pour répondre aux attentes de la population canadienne, tout en fournissant des services de renseignements fiables à son personnel, la CCN doit s'orienter vers des solutions technologiques plus rentables, plus innovantes et plus sûres.

DESCRIPTION ET CHAMP D'APPLICATION

Cette EFVP visait à examiner les exigences en matière de protection des renseignements personnels applicables à l'utilisation de Gambit ID aux fins des vérifications de sécurité de la CCN. Cela comprend les vérifications de casier judiciaire, de crédit, des antécédents

professionnels et scolaires et la gestion des dossiers de candidature, dans un module distinct de gestion postérieure des renseignements. Le champ d'application ne comprend pas les processus et la technologie qu'utilisent les collaborateurs (GRC et SCRS). Gambit ID est une application infonuagique de type logiciel-service (SaaS), hébergée dans une installation sécurisée et maintenue par Gambit ID. La CCN fait office d'« organisatrice » et Gambit ID de « fournisseur de services ».

Bien que Gambit ID offre plusieurs options, la CCN utilise les modules similaires aux processus actuels d'évaluation de sécurité et de prise d'empreintes digitales (Gambit ID et Gambit ID Scan).

• Gambit ID offre des flux de travail pour traiter les renseignements de sécurité des candidatures remplies en ligne. Le système automatise la création de fichiers SCRS, mais le processus d'envoi des fichiers au SCRS demeure le même : les fichiers sont joints à un courriel chiffré et envoyés à une boîte aux lettres sécurisée. Après réception de la réponse du SCRS, les résultats sont téléchargés dans Gambit ID, et le processus se poursuit.

• Le processus Gambit ID Scan recueille les empreintes digitales de la personne, les envoie par un processus sécurisé à la GRC, qui transmet les résultats ultérieurement. Le personnel de sécurité télécharge les résultats dans le système Gambit ID. Le système ne prend aucune décision. Tous les résultats doivent être examinés et approuvés par le personnel de sécurité.

Pourquoi l'évaluation des facteurs relatifs à la vie privée était-elle nécessaire ?

L'évaluation des facteurs relatifs à la vie privée s'imposait afin d'identifier les enjeux de confidentialité et élaborer des mesures pour minimiser les risques associés à la collecte, à l'utilisation, au stockage et à la divulgation de données personnelles au sein de la CCN.

Identification et catégorisation des risques

La solution recueille des renseignements au moyen des formulaires du SCT et du SCRS, y compris les nouveaux formulaires 330-61 du SCT et 4195 et 4160 du SCRS. L'échelle de risque numérotée se décline dans un ordre croissant : le premier niveau (1) représente le niveau le plus faible pour le domaine de risque donné ; le quatrième niveau (4) représente le niveau le plus élevé pour le domaine de risque donné.

La première étape de l'analyse consiste à évaluer chaque domaine de risque indépendamment. La deuxième étape consiste à regrouper les résultats individuels afin de déterminer si une analyse plus approfondie est nécessaire. Plus le nombre de domaines de risque correspondant aux niveaux 3 ou 4 est élevé, plus il est probable qu'il faille les traiter plus en profondeur.

Types de renseignements personnels concernés et contexte

La solution recueille des renseignements au moyen des formulaires du SCT et du SCRS, y compris les nouveaux formulaires 330-61 du SCT et 4195 et 4160 du SCRS. Il s'agit notamment des renseignements figurant aux dossiers de candidature (nom, adresse, identification des membres de la famille, lieu de naissance, genre, date de naissance et antécédents professionnels). En outre, le personnel de sécurité de la CCN peut effectuer des vérifications sur les formations et les antécédents professionnels des personnes ayant soumis leur candidature,

selon la situation ou le niveau de contrôle de sécurité, au fil de leur progression dans le processus de contrôle de sécurité, tout en prenant des notes sur les entretiens pertinents.

Divulgation des renseignements personnels

Les personnes se voient communiquer les informations suivantes par le biais d'un avis de confidentialité : les renseignements figurant sur le formulaire de vérification du SCT sont nécessaires à une évaluation de sécurité. Ils sont recueillis en vertu du paragraphe 7(1) de la *Loi sur la gestion des finances publiques* et de la Politique sur la sécurité du gouvernement (PSG) du gouvernement du Canada et sont protégés par les dispositions de la *Loi sur la protection des renseignements personnels* dans les institutions qui y sont assujetties. Il est obligatoire de les recueillir pour vérifier des antécédents auprès du SCRS. Les renseignements recueillis dans le formulaire de vérification du SCT peuvent être divulgués à la GRC, aux fins des vérifications ou des enquêtes requises conformément à la Politique sur la sécurité du gouvernement, ainsi qu'à des entités extérieures au gouvernement fédéral (p. ex., agences d'évaluation du crédit).

Résidence des données

Gambit ID est une société de technologie d'identité basée à Ottawa, dont l'infrastructure de production de services infonuagiques est hébergée à Montréal, au Canada. Toutes les bases de données sont physiquement ou logiquement indépendantes des autres bases de données. Sa solution infonuagique est desservie par le protocole TLS (sécurité de la couche transport). TLS est le successeur du protocole SSL (couche de sockets sécurisés) et constitue la norme industrielle pour le chiffrement du contenu web et la protection de l'intégrité et de la confidentialité des données transférées des serveurs vers d'autres ordinateurs.

Accès et partage des données

Gambit ID dispose de contrôles et de pratiques de sécurité conçus pour protéger la confidentialité, l'intégrité et la disponibilité du contenu client (données de la CCN) hébergé sur Amazon Web Services (AWS) et pour le protéger contre toute activité de traitement non autorisée, notamment la perte ou la destruction illégale de données.

▪ Gambit ID emploie des mesures conçues pour empêcher les personnes non autorisées d'accéder aux installations informatiques dans lesquelles le contenu client (CCN) est hébergé.

▪ L'accès de Gambit ID au contenu client se limite au personnel d'assistance autorisé, selon le principe d'accès sélectif et dans le cadre d'un accord de confidentialité. Aucun partage de données n'a lieu en dehors des limites du système, à moins que la CCN n'en fasse explicitement la demande.

▪ Gambit ID requiert l'utilisation de mots de passe forts aux fins d'authentification. Les mots de passe y sont stockés en toute sécurité sous une forme chiffrée (chiffrement des données AES256).

▪ Amazon Web Services (AWS), qui se veut l'infrastructure-service (IaaS) qu'utilise Gambit ID, n'a pas d'accès logique aux données de la CCN. Le contenu client sur l'environnement Gambit ID de

la CCN est logiquement ou physiquement séparé du contenu du reste de la clientèle de Gambit ID.

▪ Gambit ID respecte la confidentialité de sa clientèle et s'engage à la protéger conformément à sa politique en la matière. Cette politique se retrouve à l'adresse suivante : https://www.gambitid.com/privacy.html.

Le système Gambit ID est un système déployé à l'échelle de l'entreprise. Il est possible de partager des renseignements avec d'autres ministères, lorsque cela s'avère nécessaire aux fins d'identification, d'enquête et de traitement des candidatures. Le système dispose d'une connectivité sécurisée avec la GRC et le SCRS pour la vérification de divers antécédents, notamment criminels. Par conséquent, les résultats des évaluations de sécurité effectuées au moyen de Gambit ID sont communiqués à ces services sous forme de fichiers de données cryptés transmis par voie électronique.

Conservation des fichiers

Les formulaires de candidature sont conservés pendant deux ans après la date de cessation d'emploi, après quoi les Services de sécurité de l'entreprise de la CCN détruisent les dossiers concernés. Si l'évaluation de sécurité fait l'objet d'un refus ou d'une révocation, le dossier d'évaluation de sécurité est conservé pendant au moins 10 ans après le départ de la personne concernée de l'administration publique fédérale. La solution Gambit ID permet de configurer la période de conservation en fonction de différents statuts. Le personnel de sécurité peut également rechercher et exporter des fichiers sur le point d'être éliminés à des fins informatives.

Mesures de protection

Les renseignements sont protégés contre les abus et les accès non autorisés au moyen de diverses mesures de sécurité administratives, techniques et physiques. Le fournisseur de services, Gambit ID, gère ces contrôles. Seuls les Services de sécurité de l'entreprise de la CCN disposent d'un accès en écriture pour gérer le processus d'évaluation. Quelques membres du personnel des RH disposent d'un accès en lecture seule au module de gestion postérieure selon le principe d'accès sélectif afin d'exercer leurs fonctions.

Contrôles techniques : les mesures de sécurité technique de la solution Gambit ID comportent des restrictions visant à limiter l'accès aux ordinateurs aux personnes autorisées, l'utilisation obligatoire de mots de passe forts aux fins d'authentification, et des mots de passe stockés en toute sécurité dans un format chiffré (chiffrement des données AES256) au repos et en transit.

Contrôles des procédures : afin d'assurer une sécurité accrue de son système, un auditeur tiers procède à un examen régulier des pratiques et procédures opérationnelles et de sécurité de Gambit ID.

Atteintes à la vie privée

Veiller à ce que des mesures de protection appropriées soient mises en place pour protéger les renseignements personnels relève d'un processus continu, dans la mesure où les enjeux de sécurité (administratifs, physiques et techniques) évoluent et changent. La CCN se conforme à la Directive sur les pratiques relatives à la protection de la vie privée du SCT et a notamment élaboré des procédures documentées pour la gestion des atteintes à la protection des renseignements personnels.

Atténuation des risques : résumé des recommandations

1. L'autorité opérationnelle doit revoir et mettre à jour l'EFVP si des changements significatifs interviennent avec Gambit ID (processus, renseignements recueillis, nouveau module, etc.).

2. Une surveillance continue (sécurité dans la passation des marchés) doit être mise en place pour s'assurer que le service infonuagique de Gambit ID et la CCN respectent les dispositions contractuelles et les recommandations formulées.

3. Gambit ID doit fournir à la CCN des attestations ou démontrer l'application de principes de sécurité communs par la mise en œuvre de contrôles de sécurité répondant aux critères de la CCN en matière de sécurité, de disponibilité, d'intégrité du traitement et de confidentialité et de protection de ses données. Ces certifications ou attestations doivent être reconfirmées une fois tous les deux ans.

4. Il convient de procéder à un audit d'évaluation et d'autorisation de sécurité afin de valider les mesures de protection existantes.

5. Gambit ID doit démontrer qu'elle dispose de politiques et de protocoles actualisés de gestion et de réponse aux incidents, ainsi que d'un mécanisme de signalement des atteintes à la sécurité et à la vie privée. Des procédures doivent être mises en place pour signaler de telles atteintes dès que possible à la CCN, au plus tard cinq jours après leur constatation.

6. Les documents de formation ou d'orientation du personnel des Services de sécurité de l'entreprise devraient inclure des notions de base sur la protection des renseignements personnels.

7. La dirigeante ou le dirigeant principal de la sécurité doit veiller à ce que l'ensemble des membres du personnel accédant aux systèmes ait suivi une formation sur l'accès à l'information et la protection des renseignements personnels (I015), indépendamment du statut (personnel étudiant, contractuel, etc.). Il convient de tenir un registre des formations et de mettre en place un processus de mise à jour des connaissances du personnel tous les trois à cinq ans.

8. Le processus de déprovisionnement doit être documenté et intégré au processus de déprovisionnement de la CCN.

9. Les Services de sécurité de l'entreprise doivent mettre en œuvre des processus et définir des critères appropriés pour procéder aux dispositions régulières.