

Omar Hafez

De: Jacques, Nathalie
Envoyé: 28 août 2019 15:35
À: Gauthier, Gisèle
Objet: TR: NOTE_Daniel À Francine 2019.docx
Pièces jointes: NOTE_Daniel À Francine 2019.docx

Suivi:	Destinataire	Lire
	Gauthier, Gisèle	Lu: 2019-08-28 16:06

Suggestion de réponse comme mon 1^{er} réflexe. On en parle demain. Je répondrais aux 2.

Bonjour Francine et Daniel,

Gisèle et moi avons relu la note et souhaitons vous faire les mises au point et les commentaires suivants :

La DAJ offre du conseil quant à la protection des renseignements personnels (règles, gestion des risques, mesure de sécurité...);

La DAJ offre du conseil lorsque survient un incident de sécurité impliquant des renseignements personnels;

La DAJ n'effectue aucun contrôle ni aucun suivi quant à la détection d'incident de sécurité impliquant des renseignements personnels;

La DAJ n'est plus détentrice du Registre des bris de confidentialité impliquant des renseignements personnels;

Ainsi, dans ce contexte, nous serions plus à l'aise si le DVIEP indiquait simplement dans la note que la DAJ a été consulté par la DGFCO et par la DVIEP.

Néanmoins, nous trouvons important de rectifier les faits, tel qu'ils nous apparaissent avoir été vécu de notre côté :

Texte de la note de Daniel **en jaune** et réponse de la DAJ entre () :

Au cours des dernières semaines, le directeur de la vérification interne et de l'évaluation des programmes a été informé par la directrice générale des finances et du contrôle organisationnel (DGFCO) qu'un bris de confidentialité aurait été commis par la DVIEP sur la prétention que cette dernière aurait eu en sa possession des données sur des ressources internes de la SAAQ contenues dans les fichiers analysés. (la DAJ ne peut commenter cette phrase, elle n'était pas présente) La DGFCO avait au préalable consulté la DAJ dans le but d'étayer sa décision sans obtenir toutes les informations de la DVIEP. (La DGFCO avait plutôt validé auprès de la DAJ la portée d'un bris de confidentialité ainsi que s'il était vrai que la DAJ avait conseillé au DVIEP de conserver les fichiers des employés internes, ce à quoi la DAJ a répondu par la négative à la DGFCO, le tout basé sur les faits connus à cette date) Le DVIEP a donc par la suite rencontré la DAJ afin de comprendre la nature du prétendu bris (Le DVIEP a plutôt rencontré la DAJ pour connaître la définition d'un bris de confidentialité, basé sur les faits connus à cette date) et les représentantes de la DAJ ont accueilli les informations complètes de la DVIEP expliquant la nécessité de posséder l'ensemble des données contenues dans les fichiers (ce n'est que lors d'une seconde rencontre plusieurs semaines plus tard que la DVIEP a rencontré à nouveau la DAJ pour expliquer l'utilisation qu'avait fait son équipe des fichiers obtenus par la Gestion immobilière et présenter ses explications avec des précisions quant aux faits. La DAJ a rappelé les règles en matière d'utilisation et de communication de renseignements personnels ainsi que les règles entourant le critère de nécessité.)

Nous demeurons disponibles

Nathalie Jacques, directrice, direction de l'accès à l'information et du support juridique

Gauthier, Jacques & Dussault, Direction générale des affaires juridiques, Société de l'assurance automobile du Québec

333, boulevard Jean-Lesage, N-6-1 | Québec (Québec) G1K 8J6 | [REDACTED]

Ce message peut contenir des renseignements **confidentiels**. Il est à l'usage exclusif de son destinataire. Toute copie ou divulgation de son contenu est interdite. S'il vous a été transmis par erreur, veuillez le détruire et m'en aviser aussitôt. Merci

De : Lépinay, Francine

Envoyé : 28 août 2019 13:28

À : Gauthier, Gisèle ; Jacques, Nathalie

Cc : Bellenfant, Sandrine

Objet : NOTE_Daniel À Francine 2019.docx

Bonjour mesdames

Daniel Pelletier a produit cette note pour expliquer pourquoi il doit conserver certaines informations obtenues lors du mandat sur le contrôle organisationnel sur la surfacturation des ressources externes. Vous êtes mentionnés dans la note puisqu'il dit vous avoir consultés. J'ai convenu avec Daniel que je vous soumettrais la note pour obtenir vos commentaires. Merci de porter une attention particulière au paragraphe surligné en jaune.

En fait je pense qu'on pourrait nuancer...il y a eu un incident pouvant amener à un bris de confidentialité....et finalement en conclusion qu'il n'y a pas eu de bris mais selon nous l'incident demeure.

Merci de nous éclairer, bonne fin de journée.

Francine Lépinay CPA, CA

Directrice générale des finances et du contrôle organisationnel

Société de l'assurance automobile du Québec |  333, boul. Jean-Lesage, E-5-36 | Québec (Québec) G1K 8J6 |  [REDACTED]

NOTE À LA DIRECTRICE GÉNÉRALE DES FINANCES ET DU CONTRÔLE ORGANISATIONNEL

DE : Daniel Pelletier, CPA, CA
Directeur de la vérification interne et de l'évaluation de programme

DATE : Le 20 août 2019

OBJET : Justification pour l'extraction de données effectuées aux portillons dans le cadre du mandat d'audit de SGPE	OBJECTIF DE LA NOTE : ➤ Pour information
--	--

CONTEXTE

Afin d'émettre une opinion sur l'efficacité des contrôles entourant la Solution de gestion de projet d'entreprise (SGPE) dans le cadre de leur mandat d'audit interne, les auditeurs de la DVIEP ont procédé à une comparaison des heures facturées par les ressources externes avec leur présence physique inscrite dans le système de gestion des portillons de sécurité au siège social de la Société. Dans un premier temps, la DVIEP a demandé l'extraction des informations d'environ 60 ressources externes sur une période d'environ six mois afin de procéder à des analyses qui ont permis de dégager les premiers constats et où des écarts importants ont été soulevés. Par la suite, il a été demandé à la DVIEP d'étendre ses travaux à l'ensemble des ressources externes en TI et ce pour une période d'environ trois années se terminant au printemps 2018.

ÉTAT DE SITUATION

Dès les premières extractions effectuées pour environ 60 ressources externes, les auditeurs ont constaté des écarts importants entre le temps facturé et la présence physique des ressources externes au siège social de la Société. À la suite d'une discussion à ce sujet avec la haute direction, il a été demandé à la DVIEP d'étendre l'analyse à l'ensemble des ressources externes de la VPTI, et ce, pour toute la période disponible dans le système (environ 625 ressources externes). Conséquemment, de nouvelles requêtes d'extractions ont dû être adressées au service de la gestion immobilière ainsi qu'aux pilotes de SGPE. Étant donné la lourdeur, la complexité et la difficulté d'obtenir des informations fiables et vérifiables dans un temps raisonnable, et vu le risque important d'erreurs, il a été proposé par le service de la gestion immobilière de fournir à la DVIEP l'ensemble des données disponibles pour permettre une analyse complète et précise des données. Il a donc été convenu, entre les auditeurs et la personne déléguée par le détenteur des données pour répondre à notre requête, de procéder à

une extraction complète des informations disponibles pour la période couverte par l'analyse afin de s'assurer de l'intégrité des données.

À la suite de cette demande élargie et étant donné les éléments de risque d'erreurs mentionnés précédemment, il s'est avéré nécessaire pour la réalisation de notre mandat d'avoir et d'analyser les informations reçues intégralement, considérant notamment :

- 1) qu'il n'existe aucun d'identifiant unique, dans les journaux produits par le système de gestion des portillons, permettant d'extraire seulement les ressources visées par la demande d'extraction;
- 2) que la clé utilisée dans les journaux extraits du système soit composée du nom de la ressource auquel est ajouté le numéro de puce;
- 3) que le numéro de puce d'un individu peut changer à la suite d'un vol, d'un bris, de la perte ou de l'oubli de la puce. Donc une même ressource peut posséder plusieurs numéros de puce pour la période visée par l'extraction;
- 4) que pour la période visée par l'extraction, un même numéro de puce peut être partagé par plusieurs individus autant internes qu'externes;
- 5) que dans les extractions effectuées, il soit impossible de distinguer les ressources internes des ressources externes;
- 6) que la population analysée par les auditeurs est composée de plus de 600 ressources externes dont plusieurs possèdent des homonymes avec des ressources internes;
- 7) que lors d'une extraction précédente, le Service de la gestion immobilière avait transmis par erreur l'information d'une ressource interne, plutôt que de son homonyme externe tel que demandée;
- 8) qu'il existe plusieurs fichiers qui nécessitent chacun leur propre requête d'extraction;
- 9) qu'il existe des coupures dans la séquence des journaux qui nécessite chacune des analyses spécifiques pour identifier certaines ressources visées par l'analyse;
- 10) que l'ampleur de la nouvelle analyse représente un volume colossal de données et augmente considérablement le risque d'erreurs lors d'extractions multiples;
- 11) qu'il soit impossible avec des efforts raisonnables d'extraire seulement les ressources externes visées par la requête d'extraction sans une analyse complète de la banque de données.

Au cours des dernières semaines, le directeur de la vérification interne et de l'évaluation des programmes a été informé par la directrice générale des finances et du contrôle organisationnel (DGFCO) qu'un bris de confidentialité aurait été commis par la DVIEP sur la prétention que cette dernière aurait eu en sa possession des données sur des ressources internes de la SAAQ contenues dans les fichiers analysés. La DGFCO avait au préalable consulté la DAJ dans le but d'étayer sa décision sans obtenir toutes les informations de la DVIEP. Le DVIEP a donc par la suite rencontré la DAJ afin de comprendre la nature du prétendu bris et les représentantes de la DAJ ont accueilli les informations complètes de la DVIEP expliquant la nécessité de posséder l'ensemble des données contenues dans les fichiers

CONCLUSION

Tel que prévu dans la politique de vérification interne à la Société, qui mentionne notamment que les auditeurs internes doivent avoir accès à toute l'information nécessaire et utile à la réalisation de leurs travaux, les auditeurs ont effectivement eu besoin de toutes les informations leur ayant été fournies afin de procéder à des analyses précises et ainsi dégager des constats et des conclusions fiables et sans erreur sur les ressources concernées. Toujours selon cette politique, la DVIEP doit se conformer aux normes internationales pour la pratique professionnelle de la vérification interne et assurer la confidentialité des informations et des documents auxquels elle a accès dans le cadre de la réalisation de ses mandats. Les auditeurs internes doivent documenter et conserver les informations pertinentes selon des règles en matière de conservation qui sont cohérentes avec les orientations définies par l'organisation et avec toute exigence réglementaire.

Finalement, étant donné l'absence d'identifiant unique dans l'information disponible, il n'aurait pas été possible pour les auditeurs d'émettre une opinion fiable sur le temps effectué par les ressources externes visées sans l'analyse complète des informations disponibles (incluant les ressources internes) dans la banque de données des portillons. Considérant les éléments mentionnés ci-haut, la DVIEP est d'avis qu'il n'y a pas eu de bris de confidentialité dans ce dossier.

Préparée par : Martin Lapierre CPA, CMA, CISA
Révisée et approuvée par : Daniel Pelletier, CPA, CA