

Le 11 juillet 2019

« PAR COURRIER ÉLECTRONIQUE »

À l'attention des présidents des assureurs de personnes et des assureurs de dommages faisant affaire au Québec

Objet : Rappel - Importance d'une gestion saine et prudente des risques liés à la sécurité de l'information

Considérant les événements récents liés à la fuite de renseignements personnels dont le Mouvement Desjardins a été victime, l'Autorité des marchés financiers (l'« Autorité ») juge qu'il est opportun de rappeler aux institutions financières l'importance d'une gestion saine et prudente des risques liés à la sécurité de l'information.

Dans un premier temps, l'Autorité désire réitérer que la protection des renseignements personnels obtenus des consommateurs est un enjeu prédominant pour une institution financière. Au-delà de l'obligation de se conformer aux dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c. P-39.1, cet exercice vise avant tout à conserver la confiance du public à l'égard de nos organisations. L'Autorité s'attend donc que les institutions financières identifient et évaluent adéquatement les risques associés à la sécurité de l'information et qu'elles mettent en place des mesures de contrôle robustes afin de mitiger les risques quant à la protection des renseignements personnels. À cet effet, la Ligne directrice sur les saines pratiques commerciales de l'Autorité énonce les attentes à l'égard de la protection des renseignements personnels.

De plus, considérant le rôle important des systèmes d'information dans la protection des données et l'impact de ceux-ci sur le risque opérationnel des organisations, et ce, dans un contexte où l'adoption des innovations technologiques a contribué à accentuer les risques de perte, de vol, de corruption et d'accès non autorisé aux données, l'Autorité désire réaffirmer l'importance de bien gérer les risques liés aux technologies de l'information et des communications. La Ligne directrice sur la gestion du risque opérationnel énonce les attentes générales de l'Autorité en cette matière et une Ligne directrice sur la gestion des risques liés aux technologies de l'information et des communications, pour laquelle une période de consultation a été tenue et qui sera publiée ultérieurement en 2019, viendra préciser ces attentes.

L'Autorité désire également rappeler qu'elle s'attend à ce que les institutions financières l'informent promptement des incidents opérationnels majeurs (cyberincident, dysfonctionnement des systèmes, vol, fraude, etc.) qui surviennent ainsi que de tout manquement à la protection des renseignements personnels.

Nous vous prions d'agréer l'expression de nos sentiments distingués.



Nathalie Sirois, CPA, CGA, MBA, CRMA
Directrice principale de la surveillance des assureurs et du contrôle du droit d'exercice

c.c. Fondés de pouvoir

Québec ☒	Montréal ☐
Place de la Cité, tour Cominar	800, square Victoria, 22 ^e étage
2640, boulevard Laurier, 3 ^e étage	C.P. 246, tour de la Bourse
Québec (Québec)	Montréal (Québec)
G1V 5C1	H4Z 1G3
tél. : 418.525.0337	tél. : 514.395.0337
ligne sans frais : 877.525.0337	ligne sans frais : 877.525.0337
téléc. : 418.525.9512	téléc. : 514.873.3090

July 11, 2019

BY E-MAIL

Attention: Presidents of life and health insurers and P&C insurers doing business in Québec

**Subject: Reminder - Importance of soundly and prudently managing information
 security risks**

In light of the recent personal information leak at Desjardins Group, the Autorité des marchés financiers (the "AMF") believes it is timely to remind financial institutions of the importance of soundly and prudently managing information security risks.

The AMF wishes to emphasize that the protection of consumers' personal information is a key issue for financial institutions. Beyond the obligation to comply with the provisions of the *Act respecting the protection of personal information in the private sector*, CQLR c. P-39.1, protecting personal information is about maintaining public confidence in our organizations. The AMF therefore expects financial institutions to adequately identify and assess information security risks and implement robust control measures to mitigate privacy risks. The AMF's Sound Commercial Practices Guideline sets out its expectations for the protection of personal information.

Furthermore, given the important role information systems play in data protection and their impact on organizations' operational risk in an environment where technological innovations have increased the risk of loss, theft, corruption and unauthorized data access, the AMF wishes to reaffirm the importance of effectively managing information and communications technology risks. The Operational Risk Management Guideline sets out the AMF's general expectations in this regard. A Guideline on Information and Communications Technology Risk Management, on which a consultation period has been held and which will be published later in 2019, will clarify those expectations.

The AMF also wishes to point out that financial institutions are expected to promptly advise it of any major operational incidents (e.g., cyber incident, system failure, theft or fraud) as well as any breach of privacy.

Yours truly,

Nathalie Sirois, CPA, CGA, MBA, CRMA
Senior Director, Supervision of Insurers and Control of Right to Practise

c.c.: Attorneys