

ANNEXE 1

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS ET LA SÉCURITÉ DE L'INFORMATION

PRÉAMBULE

En plus des conditions générales applicables à l'offre de services transmise au Parc olympique. Le Fournisseur doit se conformer aux modalités de la présente annexe. Dans la mesure où l'une ou l'autre des dispositions de la présente annexe pourrait entrer en conflit avec celles des conditions générales ou de l'offre de services, les dispositions de la présente annexe prévalent.

Afin de fournir les services requis par le Parc olympique et décrits dans le bon de commandes et/ou l'offre de services du Fournisseur (les « Services »), il est entendu que le Fournisseur aura accès à certains renseignements personnels et confidentiels.

Par la présente Annexe, le Parc olympique souhaite s'assurer que les Renseignements personnels communiqués au cours de la prestation des services bénéficient d'une sécurité adéquate permettant ainsi de préserver leur confidentialité ainsi que les droits des personnes physiques concernées.

La présente Annexe a pour objet de définir les conditions dans lesquelles le Fournisseur s'engage à effectuer, pour le compte du Parc olympique, des services impliquant le traitement de renseignements personnels et confidentiels, en conformité avec les lois applicables.

1. Définitions

« **Renseignement Personnel** » : tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier.

« **Renseignement Confidentiel** » : tout renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1), notamment un renseignement ayant des incidences sur les relations intergouvernementales, sur les négociations entre organismes publics, sur l'économie, sur l'administration de la justice et la sécurité publique, sur les décisions administratives ou politiques ou sur la vérification.

2. Engagements du Fournisseur

Le Fournisseur s'engage à ne pas révéler ou divulguer, sans y être dûment autorisé par le Parc olympique, quoi que ce soit en regard des Renseignements Personnels et Renseignements Confidentiels dont il aurait eu connaissance dans l'exécution du Contrat. Il s'engage en particulier à respecter chacune des dispositions applicables aux Renseignements Personnels et Renseignements Confidentiels ci-dessous énumérés que ces renseignements lui soient communiqués dans le cadre de la réalisation du Contrat ou soient générés à l'occasion de sa réalisation.

- a) Respecter toutes les lois applicables en matière de protection des Renseignements Personnels et Renseignements Confidentiels, incluant mais non limitativement la *Loi sur*

l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1).

- b) Informer les personnes affectées à l'exécution du Contrat des règles prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1) et notamment, mais non limitativement, de celles prévues aux articles 53 à 60.1, 62, 63.8 à 63.11, 64 à 67.2, 83, 89 et 158 à 164 ainsi que des obligations stipulées aux présentes dispositions et diffuser à cet égard toute l'information pertinente.
- c) Utiliser les Renseignements Personnels et Renseignements Confidentiels divulgués uniquement aux fins pour lesquelles ils ont été divulgués.
- d) Prendre tous les moyens raisonnables appropriés pour limiter l'accès aux Renseignements Personnels et Renseignements Confidentiels.
- e) Rendre accessibles les Renseignements Personnels et Renseignements Confidentiels, au sein des membres de son personnel, uniquement à ceux qui ont qualité pour les recevoir, lorsqu'ils sont nécessaires à l'exercice de leurs fonctions et sont utilisés aux fins pour lesquelles ils ont été recueillis ou que la loi autorise leur utilisation.
- f) Faire signer à toute personne affectée à l'exécution du présent Contrat, préalablement à l'accès à des Renseignements Personnels et Renseignements Confidentiels, des engagements au respect de la confidentialité de ces renseignements selon l'**Annexe 2** et les transmettre aussitôt au Parc olympique, sous peine de se voir refuser l'accès aux locaux, à l'équipement du Parc olympique ou aux données à être transmises par celui-ci, le cas échéant.
- g) Ne pas permettre à un tiers d'avoir accès à ces Renseignements Personnels et Renseignements Confidentiels sauf si une divulgation de ceux-ci s'avère nécessaire à la réalisation de l'objet de sa divulgation.
- h) Prendre toutes les mesures appropriées, lorsque la divulgation de Renseignements Personnels et Renseignements Confidentiels à un tiers devient nécessaire, afin de protéger la confidentialité de ceux-ci en requérant notamment de la part du tiers un engagement de confidentialité visant à assurer le même régime de protection de cette information que celui prévu aux présentes et se conformer à toute demande du Parc olympique relativement à l'établissement de mesure de sécurité additionnelle.
- i) Obtenir l'autorisation écrite du Parc olympique avant de communiquer ou de transférer quelque donnée que ce soit, même à des fins techniques, hors du Québec :
 - i. Les infrastructures informatiques utilisées aux fins d'héberger quelque donnée que ce soit, doivent être situées au Québec. En aucun temps ces données ne peuvent être transférées à l'extérieur du Québec sans l'autorisation écrite du Parc olympique.
 - ii. Le Parc olympique doit s'assurer que ces données bénéficient d'une protection adéquate, notamment au regard des principes de protection des Renseignements Personnels généralement reconnus. Cette exigence est fondée sur les obligations du Parc olympique aux termes de la *Loi sur l'accès aux documents des*

organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1) et concerne tout site et toute infrastructure informatique utilisée aux fins d'hébergement, incluant, le cas échéant, les environnements de redondance/sites de relève et de sauvegarde.

- j) Prendre toutes les mesures de sécurité propres à assurer la confidentialité des Renseignements Personnels et Renseignements Confidentiels à toutes les étapes de la réalisation du contrat.
- k) Conserver les Renseignements Personnels et Renseignements Confidentiels uniquement pour la durée nécessaire aux fins pour lesquelles ils ont été recueillis, après quoi ils doivent être détruits/supprimés ou anonymiser en toute sécurité conformément aux meilleures pratiques, en outre :
 - i. Ne conserver, à l'expiration du contrat, aucun document contenant un Renseignement Personnel ou Renseignements Confidentiel, quel que soit le support, en les retournant au Parc olympique dans les soixante (60) jours suivant la fin du contrat et en remettant au Parc olympique une confirmation écrite que lui et toute personne affectée à l'exécution du Contrat ont retourné tous ces documents; ou
 - ii. Procéder, à ses frais, à la destruction des Renseignements Personnels et Renseignements Confidentiels ou confier leur destruction à une entreprise de récupération. Dans les deux cas, le Fournisseur ou l'entreprise de récupération doivent se conformer à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec joint à l'**Annexe 3**, ainsi qu'aux directives que lui remettra le Parc olympique, le cas échéant. Ils doivent ensuite transmettre au Parc olympique, dans les soixante (60) jours suivant la fin du contrat, l'attestation de destruction des Renseignements Personnels, jointe à l'**Annexe 4**, signée par une personne autorisée qu'il aura désignée à cette fin.
- l) Aviser par écrit le Parc olympique, dans les plus brefs délais et au maximum 24 heures après en avoir pris connaissance, de tout accès non autorisé ou tout usage non autorisé des Renseignements Personnels et Renseignements Confidentiels, connus ou raisonnablement soupçonnés, y compris les tentatives de violations relatives aux obligations de confidentialité (un « **Incident** »). L'avis écrit peut être transmis par courriel à l'adresse suivante : Incident.Confidentialite@parcolympique.ca.
- m) Fournir, à la demande du Parc olympique, toute l'information pertinente au sujet de la protection des Renseignements Personnels et Renseignements Confidentiels et donner accès, à toute personne désignée par le Parc olympique, à la documentation, aux systèmes, aux données et aux lieux physiques relatifs au contrat afin de s'assurer du respect des présentes dispositions.
- n) Sur demande du Parc olympique, lui communiquer les Renseignements Personnels informatisés concernant toute personne que lui indique le Parc olympique, et ce, dans un format technologique structuré et couramment utilisé, étant entendu que le Fournisseur peut s'assurer préalablement de la légitimité de la demande.

- o) Assister le Parc olympique dans le cadre de poursuites ou procédures légales visant à protéger les Renseignements Personnels et Renseignements Confidentiels.

EN FOI DE QUOI, le Fournisseur a signé la présente Annexe à la date indiquée ci-dessous :

À Montréal , ce _____ jour de _____ 2024

Par: _____

(Nom du représentant autorisé)

(Nom du Fournisseur)

ANNEXE 2
ENGAGEMENT DE CONFIDENTIALITÉ

Je, soussigné(e), _____, exerçant mes fonctions au sein de _____
_____, déclare formellement ce qui suit :

1. Je suis un(e) employé(e) de cette entreprise, et, à ce titre, j'ai été affecté(e) à l'exécution du mandat faisant l'objet du contrat de services concernant _____ entre le Parc olympique et mon employeur en date du _____;
2. Je m'engage, sans limite de temps, à garder le secret le plus entier, à ne pas communiquer ou permettre que soit communiqué à quiconque quelque renseignement ou document, quel qu'en soit le support, qui me sera communiqué ou dont je prendrai connaissance dans l'exercice ou à l'occasion de l'exécution de mes fonctions, à moins d'avoir été dûment autorisé à ce faire par le Parc olympique ou par l'un de ses représentants autorisés;
3. Je m'engage également, sans limite de temps, à ne pas faire usage d'un tel renseignement ou document à une fin autre que celle s'inscrivant dans le cadre des rapports contractuels entretenus entre mon employeur et le Parc olympique;
4. J'ai été informé que le défaut par le (la) soussigné(e) de respecter tout ou partie du présent engagement de confidentialité m'expose ou expose mon employeur à des recours légaux, des réclamations, des poursuites et toutes autres procédures en raison du préjudice causé pour quiconque est concerné par le contrat précité;
5. Je confirme avoir lu les termes du présent engagement et en avoir saisi toute la portée.

ET J'AI SIGNÉ À _____

CE _____ JOUR DU MOIS DE _____ DE L'AN _____

(Signature du déclarant ou de la déclarante)

ANNEXE 3

LA DESTRUCTION DES DOCUMENTS CONTENANT DES RENSEIGNEMENTS PERSONNELS

#FicheInfo



Les documents contenant des renseignements personnels ont un cycle de vie qui leur est propre : de leur naissance (ou création) à leur mort (destruction), ils passent par des phases d'utilisation et de conservation, parfois par une étape de communication à des tiers. À titre d'organisme public ou d'entreprise, vous êtes responsable d'assurer la gestion confidentielle des renseignements personnels tout au long de ce cycle de vie.



BIEN IDENTIFIER ET GÉRER POUR BIEN DÉTRUIRE !

Tout d'abord, la Commission d'accès à l'information vous recommande de mettre en place une **procédure de gestion documentaire et d'identifier** des responsables chargés de veiller à sa bonne application. Il est important de faire connaître cette procédure à tout le personnel.

Cette procédure vise notamment à :

- **inventorier les types de documents contenant des renseignements personnels** (ex : fichier des ressources humaines, fichier clientèle, ...);
- **définir les niveaux de confidentialité des documents** (ex : protégé, confidentiel et secret) en fonction des critères de sensibilité, de finalité, de quantité, de répartition et de support;
- **distinguer les types de supports pour y associer une méthode de conservation et de destruction appropriées** (ex : support papier, informatisé, ou électronique);
- **déterminer un calendrier de conservation respectant les exigences légales.**

UNE OBLIGATION LÉGALE

Les lois applicables¹ prévoient des règles en matière de sécurité et de destruction.

Ainsi, vous devez « prendre des mesures de sécurités propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés, ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition, et de leur support ».

QUAND FAUT-IL DÉTRUIRE LES DOCUMENTS ?

Les documents contenant des renseignements personnels doivent être détruits dès que la finalité pour laquelle ils ont été collectés est accomplie, sous réserve du délai prévu par la loi ou par un calendrier de conservation.



Commission
d'accès à l'information
du Québec

¹ Pour les organismes publics : Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q. c. A-2.1 : articles 63.1, 67.2, et 73. Pour les entreprises : Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q. c. P-39.1 : articles 10 et 12

CHOISISSEZ UNE MÉTHODE DE DESTRUCTION ADAPTÉE !

La méthode de destruction doit être adaptée au support et au niveau de confidentialité des documents et assurer la destruction définitive de son contenu.

Plusieurs techniques permettent une destruction définitive :

Support utilisé	Exemples de méthodes de destruction
Papier Original et toutes les copies	<ul style="list-style-type: none">Déchetuse, de préférence à découpe transversale. <i>Si les documents sont très confidentiels : déchiqueteuse + incinération</i>
Médias numériques que l'on souhaite réutiliser ou recycler Ex : cartes de mémoire flash (cartes SD, XD, etc.) clés USB, disque dur d'ordinateur	<ul style="list-style-type: none">Formatage, réécriture, déchiquetage numérique (logiciel effectuant une suppression sécuritaire qui écrira de l'information aléatoire à l'endroit où se trouvait le fichier supprimé).
Médias numériques non réutilisables Ex : certains CD, DVD, cartes de mémoire flash, USB et disques durs qui ne seront plus utilisés	<ul style="list-style-type: none">Destruction physique (déchiquetage, broyage, meulage de surface, désintégration, trouage, incinération, ...) <i>La plupart des déchiqueteuses pourront détruire CDs et DVDs.</i>Démagnétiseur (ou dégausseur¹) pour les disques durs.
Machines contenant des disques durs Ex : photocopieur, fax, numériseur, imprimantes, etc.	<ul style="list-style-type: none">Écrasement des informations sur le disque dur ou disque dur enlevé et détruit lorsque les machines sont remplacées.

¹ Dispositif pour supprimer l'aimantation d'un matériau magnétique.

DESTRUCTION EN INTERNE VS DESTRUCTION PAR UN TIERS ?

Vous pouvez détruire vous-même les documents contenant des renseignements personnels ou conclure un contrat avec un prestataire externe si votre équipement ne vous permet pas de détruire les documents de manière sécuritaire. Une déchiqueteuse de petite taille pourrait être suffisante pour garantir une destruction sécuritaire aux petites entreprises ou organismes publics ne traitant pas de renseignements personnels sensibles. Par contre, la destruction définitive des données contenues dans un disque dur peut nécessiter de recourir à une firme externe.

Lorsqu'un tiers (prestataire) est impliqué, il faut prévoir un contrat écrit précisant :

- le procédé utilisé pour la destruction ;
- le prestataire reconnaît que les renseignements traités sont confidentiels ;
- le prestataire informera son client s'il fait appel à un sous-traitant pour la destruction ;
- qu'un engagement à la confidentialité sera signé par les employés ;
- l'entreposage sécuritaire des documents à détruire (dans des locaux sécuritaires avec accès limités) ;
- la possibilité pour le client d'accéder aux locaux du prestataire pendant la durée du contrat ;
- l'obligation pour le prestataire de faire régulièrement rapport de la destruction au client.

Pensez à sécuriser les documents à détruire en attendant le passage du fournisseur chargé de la destruction des documents !

Enfin, si le prestataire ne respecte pas ses engagements, vous devrez mettre fin au contrat et demander la restitution des renseignements personnels.



Commission
d'accès à l'information
du Québec

Mars 2014

ANNEXE 4

ATTESTATION DE DESTRUCTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

Je, soussigné(e), _____
(Prénom et nom de l'employé(e))

exerçant mes fonctions au sein de _____, déclare solennellement que je suis dûment autorisé(e) pour certifier que les renseignements personnels et confidentiels communiqués par le **Parc olympique** ou toute autre personne dans le cadre du projet octroyé à _____
(Nom du Fournisseur de services)

et qui prend fin le _____, ont été détruits selon les méthodes suivantes :
(Date)

(Cochez les cases appropriées)

<input type="checkbox"/>	par déchiquetage : renseignements sur support papier
<input type="checkbox"/>	par destruction logique et effacement physique en utilisant un logiciel de réécriture : renseignements sur support informatique
<input type="checkbox"/>	par un autre mode de destruction : préciser le support et le mode de destruction _____ _____ _____

EN FOI DE QUOI, J'AI SIGNÉ À _____,
CE _____ JOUR DU MOIS DE _____ DE L'AN _____.

(Signature de l'employé(e))