



Politique de gouvernance sur la
protection des renseignements
personnels

INDEX

1. PRÉAMBULE.....	3
2. OBJECTIFS	4
3. RENSEIGNEMENTS PERSONNELS.....	4
4. COLLECTE.....	4
5. UTILISATION.....	5
6. COMMUNICATION	6
7. CONSERVATION	6
8. DESTRUCTION	8
9. ANONYMISATION	8
10. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE.....	9
11. DEMANDE D'ACCÈS OU DE RECTIFICATION	10
12. INCIDENTS DE CONFIDENTIALITÉ.....	10
13. INVENTAIRE DES RENSEIGNEMENTS PERSONNELS DE L'ENTREPRISE.....	12
14. FORMATION SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	12
15. DROIT À LA DÉINDEXATION	13
16. PORTABILITÉ DES DONNÉES	13
17. PROCESSUS DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.....	14
18. COORDONNÉES DE LA PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	14
19. ENTRÉE EN VIGUEUR DE LA POLITIQUE.....	14
20. LES ANNEXES.....	15
ANNEXE 1 - POLITIQUE DE CONFIDENTIALITÉ LORS D'UNE COLLECTE DE RENSEIGNEMENTS PERSONNELS PAR UN MOYEN TECHNOLOGIQUE.....	16
ANNEXE 2 – PROCÉDURE DE NUMÉRISATION.....	20
ANNEXE 3 – MODÈLE DE REGISTRE DE NUMÉRISATION.....	21
ANNEXE 4 - TECHNIQUES DE DESTRUCTION DÉFINITIVE DE DOCUMENTS.....	22
ANNEXE 5 – MODÈLE DE REGISTRE DE DESTRUCTION.....	23
ANNEXE 6 - MODÈLE REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ.....	24
ANNEXE 7 - PROCÉDURE DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS.....	25
ANNEXE 8 – MODÈLE D'INVENTAIRE DES RENSEIGNEMENTS PERSONNELS DE L'ENTREPRISE	26
ANNEXE 9 – SITE WEB ET DOCUMENTS DE RÉFÉRENCES.....	27

1. PRÉAMBULE

La Politique de gouvernance sur la protection des renseignements personnels (ci-après « la Politique ») est adoptée en application de la [Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels](#) (ci-après « Loi sur la protection des renseignements personnels »).

La Compagnie de danse Sursaut (ci-après « la Compagnie ») est une personne morale à but non lucratif qui traite des renseignements personnels dans le cadre de ses activités. Elle est donc assujettie à la *Loi sur la protection des renseignements personnels*.

Dans le cadre de ses activités, *la Compagnie* doit recueillir, détenir, utiliser ou communiquer des renseignements personnels.

Cette Politique s'applique à *la Compagnie*, ce qui inclut notamment les membres de son personnel, les membres du conseil d'administration, les stagiaires et bénévoles, le cas échéant, ainsi qu'à toutes personnes qui, autrement, fournissent des services pour le compte de *la Compagnie*.

Elle s'applique pour tous les renseignements personnels collectés, utilisés et conservés par *la Compagnie*, et ce, peu importe leur forme. La Politique vise les renseignements personnels contenus dans tous les types de documents physiques ou numériques, au sens large, que leur forme soit écrite, graphique, sonore, visuelle, informatisée ou autre. Un renseignement personnel est défini comme étant tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Elle s'applique également à l'égard du site internet et des médias sociaux gérés par *la Compagnie*, le cas échéant.

Les ANNEXES font partie intégrante de la Politique.

2. OBJECTIFS

La présente Politique décrit les normes de collecte, d'utilisation, de communication et de conservation des renseignements personnels afin d'assurer la protection de ces renseignements. Elle explique également les rôles et les responsabilités des membres du personnel de *la Compagnie* tout au long du cycle de vie de ces renseignements, ainsi que le processus de traitement des plaintes relatives à la protection de ceux-ci.

3. RENSEIGNEMENTS PERSONNELS

Dans le cadre de ses activités, *la Compagnie* peut recueillir et traiter différents types de renseignements personnels, y compris :

- des renseignements d'identité, comme un nom ou un prénom, âge, date de naissance;
- des coordonnées de contact, une adresse, une adresse électronique et un numéro de téléphone;
- des renseignements nécessaires lors de l'ouverture d'un dossier d'employé, le numéro de sécurité sociale, les coordonnées bancaires pour le dépôt de la paie, etc.;
- des renseignements nécessaires durant la période de travail de l'employé, notamment les rapports d'accidents CNESST, notes disciplinaires, etc.;
- des renseignements relatifs aux membres du personnel, stagiaires ou bénévoles de *la Compagnie*, notamment les dossiers du personnel, les certificats et diplômes de formation, etc.;
- des renseignements relatifs aux interprètes, diffuseurs, clients, pigistes, collaborateurs ou travailleurs externes de l'entreprise, notamment les numéros d'assurance sociale, les numéros de cartes d'assurance maladie, les coordonnées personnelles, etc.;
- tout autre renseignement personnel nécessaire dans le cadre de ses activités.

4. COLLECTE

La Compagnie collecte des renseignements personnels, notamment auprès de son personnel, ses clients, et des fournisseurs.

De façon générale, *la Compagnie* collecte les renseignements personnels directement auprès de la personne concernée et avec son consentement, sauf si une exception est prévue par la loi.

Le consentement peut être obtenu de façon implicite dans certaines situations, par exemple lorsque la personne consent à fournir volontairement ses renseignements personnels dans le cadre des activités de la Compagnie, comme lors d'une embauche.

Dans tous les cas, *la Compagnie* ne collecte des renseignements personnels que si elle a une raison valable de le faire. De plus, la collecte ne sera limitée qu'aux renseignements nécessaires dont elle a besoin pour remplir ses objectifs.

À moins d'une exception prévue par la loi, *la Compagnie* demandera le consentement de la personne concernée avant de recueillir des renseignements personnels la concernant auprès d'un tiers. Ce consentement sera obtenu directement auprès de la personne, soit par courriel, soit au moyen d'un formulaire dans lequel celle-ci devra cocher une case pour donner son accord.

Étant une compagnie de danse axée sur la jeunesse et intervenant auprès d'enfants, la Compagnie peut recueillir des renseignements personnels concernant des mineurs de moins de 14 ans. Dans ce cas, elle doit obtenir le consentement du titulaire de l'autorité parentale de l'enfant.

Considérant que *la Compagnie* collecte des renseignements personnels par un moyen technologique, elle s'est dotée d'une Politique de confidentialité disponible à l'ANNEXE 1, également disponible sur le site web de *la Compagnie* dans la section *Politique de confidentialité*.

5. UTILISATION

La Compagnie s'engage à utiliser les renseignements personnels en sa possession uniquement aux fins pour lesquelles ils ont été recueillis, et dans les limites prévues par la loi. Elle peut toutefois recueillir, utiliser ou divulguer ces renseignements sans le consentement de la personne concernée lorsque cela est permis ou exigé par la loi.

Dans certaines circonstances particulières, *la Compagnie* peut recueillir, utiliser ou divulguer des renseignements personnels sans que la personne concernée en soit informée ou qu'elle ait donné son consentement. De telles circonstances sont réunies, notamment lorsque, pour des raisons juridiques, médicales ou de sécurité, il est impossible ou peu probable d'obtenir son consentement, lorsque cette utilisation est manifestement au bénéfice de cette personne, lorsque cela est nécessaire pour prévenir ou détecter une fraude ou pour tous autres motifs sérieux.

La Compagnie limite l'accès des membres du personnel et du conseil d'administration aux seuls renseignements personnels et connaissances de nature personnelle qui sont nécessaires à l'exercice de leur fonction.

6. COMMUNICATION

En principe, *la Compagnie* ne peut communiquer les renseignements personnels qu'il détient sur une personne sans le consentement de celle-ci.

Toutefois, *la Compagnie* peut communiquer à un tiers des renseignements personnels sans le consentement de la personne concernée lorsque la communication est due à une exigence réglementaire ou légale ou lorsque la *Loi sur la protection des renseignements personnels* ou toute autre loi le permet.

7. CONSERVATION

Conservation

Dans le cadre de ses activités, *la Compagnie* doit conserver de nombreux documents comportant des renseignements personnels.

Certains documents doivent être conservés pendant une durée prescrite par la loi, notamment la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Cette durée peut varier selon le type de renseignement, les exigences légales ou contractuelles, et les objectifs pour lesquels les renseignements ont été collectés. Par exemple, certains renseignements doivent être conservés pendant une période minimale ou maximale définie par la loi, tandis que d'autres peuvent être conservés selon les besoins spécifiques de l'entreprise.

Afin de respecter les exigences légales et contractuelles, un calendrier de conservation des documents est établi et mis à jour régulièrement. Ce calendrier permet de garantir que les renseignements personnels sont conservés pendant la durée appropriée et sont détruits de manière sécurisée lorsque leur conservation n'est plus nécessaire.

Calendrier de conservation des renseignements personnels

La Compagnie applique un calendrier de conservation des renseignements personnels structuré afin d'assurer la conformité aux obligations légales et réglementaires. Ce calendrier établit des délais précis pour la conservation et la destruction des documents, en fonction des exigences légales applicables et des besoins organisationnels.

Les durées de conservation sont définies en fonction des types de documents et des obligations légales ou administratives associées. Elles sont établies selon les normes en vigueur et adaptées aux pratiques spécifiques de l'organisation. Chaque document est conservé pour la durée requise, puis détruit conformément aux procédures établies afin d'assurer la protection des renseignements personnels et de limiter les risques liés à une rétention excessive.

La Compagnie s'engage à réviser périodiquement son calendrier de conservation pour s'assurer de son alignement avec les exigences légales et réglementaires en constante évolution. Le respect de ces directives est essentiel pour garantir une gestion efficace et sécurisée des renseignements personnels.

Le détail des durées de conservation spécifiques aux différents types de documents est précisé dans le *Plan de classification et calendrier de conservation* qui constitue la référence officielle pour la gestion documentaire de l'organisation.

Qualité des renseignements personnels

La Compagnie s'assure de la qualité des renseignements personnels qu'il détient. En ce sens, les renseignements personnels conservés sont à jour, exacts et complets pour servir aux fins pour lesquelles ils ont été recueillis ou utilisés.

La mise à jour constante des renseignements personnels n'est pas nécessaire, sauf si cela est justifié par les fins pour lesquelles ce renseignement est recueilli. Cependant, si les renseignements doivent servir à une prise de décision, ils doivent être à jour au moment de celle-ci.

Documents physiques et numériques

Selon la nature des renseignements personnels, ceux-ci peuvent être conservés aux bureaux de *la Compagnie*, dans divers systèmes informatiques de *la Compagnie* ou de ses fournisseurs de services, ou dans les installations d'entreposage de *la Compagnie* situé au Centre des arts de la scène Jean-Besré ou de ses fournisseurs de services.

La Compagnie s'assure que les documents physiques et numériques sont protégés adéquatement pendant toute la période de conservation. Cela inclut l'accès restreint aux informations, l'utilisation de systèmes sécurisés pour le stockage numérique, ainsi que des mesures de sécurité appropriées pour les documents physiques.

Mesures de sécurité

La sécurité et la protection des renseignements personnels sont importantes pour *la Compagnie*. *La Compagnie* met en place des mesures de sécurité afin que les renseignements personnels demeurent strictement confidentiels et soient protégés contre la perte ou le vol et contre tout accès, communication, copie, utilisation ou modification non autorisée.

Ces mesures de sécurité peuvent inclure des aspects organisationnels, tels que la restriction des accès aux données nécessaires et la sauvegarde et l'archivage de ces données grâce à des systèmes internes et externes. Elles peuvent aussi comporter des aspects technologiques, comme l'utilisation de mots de passe et de cryptage (par exemple, le changement régulier des mots de passe et l'installation de pare-feu).

Par mesure de sécurité, l'accès aux documents est strictement contrôlé et attribué en fonction des tâches et des responsabilités de chaque employé. Les utilisateurs n'ont accès

qu'aux informations nécessaires à l'exercice de leurs fonctions. Les documents sensibles, notamment ceux concernant la direction générale, sont accessibles uniquement aux personnes autorisées, et des restrictions d'accès sont mises en place pour protéger ces renseignements.

La Compagnie utilise des systèmes et outils sécurisés pour la gestion et la sauvegarde des mots de passe et des identifiants en ligne, garantissant ainsi la protection et la confidentialité de ses informations sensibles.

Numérisation des documents

Dans l'éventualité où *la Compagnie* désire détruire les documents originaux à la suite de leur numérisation, il respecte les conditions suivantes :

1. L'information contenue dans les documents numérisés n'a pas été altérée et elle a été maintenue dans son intégralité ;
2. La numérisation ainsi que le support pour conserver les documents numérisés doit assurer la stabilité et la pérennité des documents.

La Compagnie choisit des supports et des technologies permettant la conservation sécurisée de ses documents, en conformité avec les exigences de protection des renseignements personnels. Ces outils garantissent l'accessibilité et la protection des documents, conformément aux mesures de sécurité décrites dans la section précédente.

Lorsque *La Compagnie* effectue une numérisation de document, il applique la procédure prévue à l'ANNEXE 2. *La Compagnie* consigne la numérisation dans le *Registre de numérisation*, dont un modèle est présenté à l'ANNEXE 3.

8. DESTRUCTION

La destruction des documents d'origine contenant des renseignements personnels ou confidentiels est faite de façon sécuritaire.

La Compagnie utilise des techniques de destruction définitive de documents adaptées au niveau de confidentialité du document à détruire.

Il se réfère à l'ANNEXE 4 pour les techniques de destruction définitive de documents.

La Compagnie remplit le *Registre de destruction*, dont un modèle est présenté à l'ANNEXE 5, lorsqu'il détruit des documents contenant des renseignements personnels.

9. ANONYMISATION

Dans le cadre de ses activités, *la Compagnie* applique un processus d'anonymisation afin de protéger les renseignements personnels qu'elle recueille. Concrètement, cela signifie que

lorsque *La Compagnie* utilise ou diffuse des données à des fins statistiques, de reddition de comptes ou de communication, elle s'assure qu'aucune information ne permet d'identifier directement ou indirectement une personne.

Par exemple, *la Compagnie* recueille les noms des participants à nos spectacles ou des enfants inscrits à notre camp de jour, mais ces renseignements personnels ne sont jamais partagés. Lorsque *la Compagnie* communique des données de participation ou des résultats d'activités, elle le fait de façon agrégée ou dépersonnalisée, garantissant ainsi la confidentialité des individus concernés.

La Compagnie conserve néanmoins certains renseignements personnels non anonymisés à l'interne, selon notre calendrier de conservation et dans un environnement sécurisé, afin de soutenir nos activités. Ces données peuvent notamment être utilisées à des fins de promotion ciblée ou de suivi personnalisé auprès de nos publics.

10. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

La Compagnie devra procéder à une évaluation des facteurs relatifs à la vie privée (ÉFVP) pour tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels. Cette évaluation doit permettre d'identifier et d'analyser les risques sur la vie privée associés au projet et de mettre en place des mesures d'atténuation adaptées.

L'ÉFVP réalisée devra être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. Elle devra inclure une analyse des obligations légales applicables, de l'utilisation prévue des renseignements personnels (collecte, conservation, communication, destruction) et des impacts potentiels sur la vie privée des personnes concernées. Lorsque possible, des mesures préventives et correctives devront être mises en place pour minimiser les risques identifiés.

La Compagnie s'engage à documenter chaque ÉFVP afin d'assurer la traçabilité des décisions et de démontrer sa conformité aux exigences légales. Un processus de suivi et de révision de l'ÉFVP devra être instauré afin d'adapter l'évaluation aux évolutions du projet et aux nouvelles exigences en matière de protection des renseignements personnels.

Pour guider la réalisation des ÉFVP, *la Compagnie* peut s'appuyer sur le *Guide d'accompagnement - Réaliser une évaluation des facteurs relatifs à la vie privée* et le *Modèle de Rapport d'évaluation des facteurs relatifs à la vie privée* de la *Commission d'accès à l'information*, ainsi que sur ses propres méthodologies internes (voir **ANNEXE 9** pour les références).

11. DEMANDE D'ACCÈS OU DE RECTIFICATION

Toute personne peut faire une demande d'accès ou de rectification concernant ses renseignements personnels détenus par *La Compagnie*.

La personne concernée doit soumettre une demande écrite à cet effet à la personne responsable de la protection des renseignements personnels *La Compagnie*.

Sous réserve de certaines restrictions légales, les personnes concernées peuvent demander l'accès à leurs renseignements personnels détenus par *La Compagnie* et en demander leur correction dans le cas où ils seraient inexacts, incomplets ou équivoques.

La personne responsable de la protection des renseignements personnels de *La Compagnie* doit répondre par écrit à ces demandes dans les 30 jours de la date de réception.

12. INCIDENTS DE CONFIDENTIALITÉ

Les incidents de confidentialité

Un incident de confidentialité correspond à un accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

Si l'entreprise a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel qu'elle détient s'est produit, elle doit agir rapidement en prenant toutes les mesures raisonnables pour réduire les risques de préjudice et prévenir la récurrence d'incidents similaires.

En cas d'incident de confidentialité, *La Compagnie* procède à l'évaluation du préjudice. Cette évaluation tient compte notamment des éléments suivants : la sensibilité des renseignements personnels concernés; les utilisations malveillantes possibles des renseignements et les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables.

Lorsqu'un incident présente un risque sérieux de préjudice pour les personnes concernées, l'entreprise a l'obligation d'en aviser rapidement la Commission d'accès à l'information. Elle doit également informer, dans les plus brefs délais, toutes les personnes dont les renseignements personnels sont touchés. Si elle ne le fait pas, la Commission peut l'y contraindre.

Cependant, l'entreprise peut s'abstenir d'aviser les personnes concernées si cet avis risque d'entraver une enquête en cours menée en vertu de la loi pour prévenir, détecter ou réprimer un crime ou une infraction.

Quand l'incident présente le risque qu'un préjudice sérieux soit causé aux personnes dont les renseignements sont concernés, *La Compagnie* avise par écrit :

- La Commission d'accès à l'information via le [formulaire d'avis](#) prescrit ;
- La ou les personnes concernées. L'avis doit permettre de la renseigner adéquatement sur la portée et les conséquences de l'incident.
 - Cet avis doit contenir :
 - Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'organisation doit communiquer la raison justifiant l'impossibilité de fournir cette description.
 - Une brève description des circonstances de l'incident;
 - La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue;
 - Une brève description des mesures prises ou envisagées pour diminuer les risques qu'un préjudice soit causé à la suite de l'incident;
 - Les mesures proposées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer celui-ci;
 - Les coordonnées d'une personne ou d'un service avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

Avis interne à l'entreprise

Dès qu'un incident de confidentialité est suspecté ou confirmé, tout employé ou collaborateur doit en aviser immédiatement la personne responsable de la protection des renseignements personnels de *la Compagnie*. Celle-ci est chargée de coordonner l'évaluation de l'incident, de déterminer les obligations légales qui s'appliquent, de veiller à la communication des avis requis, et d'assurer la tenue du registre des incidents.

Registre des incidents de confidentialité

La Compagnie tient un registre des incidents de confidentialité selon le modèle présenté à l'ANNEXE 6.

Le registre collige l'ensemble des incidents de confidentialité impliquant un renseignement personnel :

- ceux ne présentant pas de risque de préjudice sérieux et ;
- ceux présentant un risque de préjudice sérieux.

Les renseignements contenus au registre des incidents de confidentialité sont tenus à jour et conservés pendant une période minimale de cinq (5) ans après la date ou la période au cours de laquelle *La Compagnie* a pris connaissance de l'incident.

13. INVENTAIRE DES RENSEIGNEMENTS PERSONNELS DE L'ENTREPRISE

La Compagnie maintient un inventaire à jour des renseignements personnels qu'elle détient, tant à l'interne que dans les systèmes externes.

Cet inventaire, dont un modèle est présenté à l'**ANNEXE 8**, permet d'identifier avec précision où se trouvent les renseignements personnels, quels types d'informations sont collectés et stockés, ainsi que les sources dans lesquelles ils sont conservés. Il permet également de contrôler l'accès à ces données et de s'assurer que leur transfert respecte les politiques de protection de la vie privée établies par *la Compagnie*.

L'inventaire précise qui a accès aux renseignements personnels, dans quelles circonstances, et quelles données peuvent être transférées à des tiers. Par ailleurs, il permet de lier chaque renseignement personnel à la personne concernée, ce qui s'avère essentiel en cas d'incident, afin de déterminer rapidement les données touchées et les personnes à notifier conformément aux exigences légales.

14. FORMATION SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La Compagnie dispose d'un document intitulé « GUIDE DE BONNES PRATIQUES - CYBERSECURITE », remis aux nouveaux employés ou à ceux qui en ont besoin. Ce guide sert d'introduction aux bonnes pratiques en cybersécurité et inclut des informations sur la protection des renseignements personnels. La direction de *la Compagnie* s'assure également que tous les employés détiennent les formations nécessaires et que celles-ci sont à jour.

Dans le milieu artistique en Estrie, des organismes tels que *0/1 - Hub numérique* et le *Conseil de la culture de l'Estrie* offrent de l'aide, du soutien et des formations initiales et continues en cybersécurité ainsi qu'en protection des renseignements personnels. *La Compagnie* est également abonnée à TechSoup, une organisation canadienne qui offre du soutien technique et des outils technologiques aux organismes à but non lucratif. Ils proposent aussi des formations en cybersécurité ainsi que d'autres formations liées à la protection des données pour les OBNL. De plus, une multitude de formations sont disponibles un peu partout au Québec sur ces sujets. *La Compagnie* peut s'y référer au besoin; ces ressources sont accessibles aux employés, qu'ils soient nouveaux ou expérimentés, selon leur niveau de compétence informatique.

15. DROIT À LA DÉSINDEXATION

L'organisme reconnaît que toute personne concernée ou une tierce partie autorisée peut demander que ses renseignements personnels ne soient plus liés à son identité dans nos systèmes. Lorsqu'une demande de désindexation est reçue, elle est évaluée afin de déterminer si elle peut être acceptée, notamment en s'assurant qu'aucune obligation légale, réglementaire ou contractuelle ne s'y oppose.

Lorsque la demande est jugée recevable, la désindexation est réalisée par l'anonymisation ou la destruction des renseignements personnels, selon la nature des informations en cause et conformément à notre calendrier de conservation. Si la désindexation ne peut être effectuée, la personne sera informée des motifs empêchant la mise en œuvre de sa demande.

16. PORTABILITÉ DES DONNÉES

Le droit à la portabilité permet à toute personne concernée d'obtenir une copie des renseignements personnels à son sujet, ainsi que d'en demander le transfert vers une autre organisation, lorsque cela est possible. Ce droit s'applique uniquement aux renseignements fournis directement par la personne concernée, et non à ceux qui ont été créés ou dérivés à partir de ces données.

La personne concernée peut contacter directement *la Compagnie* pour obtenir ses renseignements personnels, lesquels seront transmis dans un format structuré et clair, y compris lorsque ces renseignements sont informatisés. *La Compagnie* veille également à ce que les personnes responsables de ces demandes soient formées pour assurer un traitement sécuritaire, confidentiel et dans un délai raisonnable.

Enfin, *la Compagnie* s'assure que tout transfert respecte les exigences légales applicables, notamment en ce qui concerne les destinataires autorisés à recevoir ces données. *La Compagnie* peut conserver et communiquer à un tiers des renseignements personnels sans le consentement de la personne concernée lorsque la communication est due à une exigence réglementaire ou légale ou lorsque la *Loi sur la protection des renseignements personnels* ou toute autre loi le permet.

17. PROCESSUS DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Toute personne concernée par l'application de la présente Politique peut porter plainte concernant l'application de la présente Politique ou, plus généralement, concernant la protection de ses renseignements personnels par *la Compagnie*.

La procédure de traitement de plainte relative à la protection des renseignements personnels est prévue à l'**ANNEXE 7**, également disponible sur le site web de *la Compagnie* dans la section *Politique de confidentialité*.

18. COORDONNÉES DE LA PERSONNE RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Nom de la personne : Nancy Rheault
Courriel : admin@sursaut.ca
Numéro de téléphone : 819 822-8912

Il est possible de communiquer avec la personne responsable de la protection des renseignements personnels pour toute question en lien avec l'application de la présente Politique en matière de protection des renseignements personnels.

19. ENTRÉE EN VIGUEUR DE LA POLITIQUE

La Politique entre en vigueur le 3 juin 2025.

La Politique a été approuvée par la personne responsable de la protection des renseignements personnels et le conseil d'administration de *la Compagnie*.

Si elle modifie la présente Politique, *la Compagnie* rend disponible la Politique telle que modifiée.

20. LES ANNEXES

Note : Les registres de numérisation, de destruction, des incidents de confidentialité, ainsi que l'inventaire des renseignements personnels sont des documents distincts utilisés à des fins de gestion interne. Les annexes 4, 6, 7 et 9 sont donc présentées à titre d'exemple seulement.

ANNEXE 1 – POLITIQUE DE CONFIDENTIALITÉ LORS D'UNE COLLECTE DE RENSEIGNEMENTS PERSONNELS PAR UN MOYEN TECHNOLOGIQUE

La compagnie de danse Sursaut (ci-après « *la Compagnie* ») s'engage à protéger la confidentialité des renseignements personnels que vous fournissez ou qu'elle recueille lors de votre visite sur son site Internet ou dans le cadre de toute interaction par moyen technologique. À cet égard, la présente politique de confidentialité (ci-après la « *Politique* ») vise à vous informer des renseignements personnels collectés, des fins pour lesquelles ceux-ci sont recueillis, des communications qui pourraient être effectuées et, de manière générale, des mesures de protection mises en place. Elle traite également du recours à des témoins de connexion, le cas échéant.

La Politique de confidentialité est adoptée en application de la [Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels](#) (ci-après « *Loi sur la protection des renseignements personnels* »).

Consentement

Si vous utilisez notre site internet ou nos services ou si vous soumettez vos renseignements personnels à *la Compagnie*, vous serez réputé avoir donné votre consentement aux fins énoncées ci-après, pour lesquelles *la Compagnie* recueille et utilise vos renseignements personnels.

Usage de cookies (ci-après « témoins de connexion »)

La Compagnie emploie la technologie des témoins de connexion pour aider les utilisateurs de son site Internet à naviguer plus rapidement et leur proposer le contenu qui les intéresse le plus.

Un témoin de connexion est une chaîne d'informations qui est envoyée par un site internet et stockée sur le disque dur ou temporairement dans la mémoire d'un ordinateur.

L'emploi des témoins de connexion se veut une pratique courante dans l'industrie et plusieurs fureteurs reconnus sont initialement configurés pour les accepter. Vous pouvez reconfigurer le vôtre afin qu'il refuse ou accepte les témoins de connexion ou encore qu'il vous alerte lorsqu'un témoin de connexion s'installe sur votre ordinateur. Notez qu'en refusant les témoins de connexion, vous pourriez ne pas être en mesure d'exploiter certaines fonctionnalités du site internet de *la Compagnie*.

Quel type d'information recueillons-nous?

La décision de fournir ou non vos renseignements personnels vous revient exclusivement. En règle générale, vous pouvez consulter notre site internet ou communiquer avec nous sans avoir à fournir vos renseignements personnels. Toutefois, dans certains cas, il sera nécessaire de recueillir vos renseignements personnels.

Lorsque vous visitez le site internet, *la Compagnie* peut notamment recueillir et utiliser les catégories de renseignements personnels suivants :

- Interactions : lorsque des communications sont établies par courriel, lors d'un abonnement à l'infolettre, de la soumission d'un formulaire ou de l'envoi d'un curriculum vitae dans le cadre d'une candidature, l'interaction est enregistrée, de même que, le cas échéant, les pièces jointes transmises.
- Utilisation du site : lors de la navigation sur le site Internet, certains renseignements personnels sont automatiquement recueillis par l'entremise des fichiers témoins du navigateur, notamment l'adresse IP, la langue de correspondance, la date et l'heure des visites, ainsi que les pages consultées.

Utilisation des renseignements personnels colligée par notre site

Les renseignements personnels que *la Compagnie* recueille ne sont utilisés qu'aux fins indiquées au moment de la collecte, soit lorsque vous naviguez ou divulguiez vos renseignements sur le site Internet. *La Compagnie* utilise vos renseignements personnels principalement pour :

- **Communiquer avec vous et vous tenir informés** : pour vous envoyer une confirmation de rendez-vous, pour répondre à une question posée, un commentaire ou une demande d'information, pour vous faire parvenir notre infolettre si vous avez accepté de recevoir de telles communications, etc.;
- **Personnaliser, améliorer ou faciliter votre expérience sur notre site Internet** : par exemple, afin d'emmagasiner de l'information de sorte que vous n'ayez pas à la réinscrire à chaque visite subséquente;
- **Traiter les demandes d'emploi et les curriculum vitæ**, le cas échéant;
- **Toute autre utilisation permise ou requise par les lois applicables.**

Partage et communication de l'information

La Compagnie ne peut transmettre vos renseignements personnels à d'autres organisations qu'avec votre consentement. Toutefois, des renseignements personnels peuvent être communiqués sans consentement si la loi l'exige ou le permet. Dans un tel cas, seuls les renseignements requis seront transmis.

Stockage et sécurité

Tous les renseignements personnels que vous fournissez à *la Compagnie* sont conservés sur des serveurs sécurisés, à accès restreint de *la Compagnie*. *La Compagnie* prend les moyens techniques raisonnables pour assurer un environnement sécuritaire et protéger vos renseignements personnels, tels que : barrières coupe-feu, usage d'antivirus, gestion des accès, détection des intrusions, copie de sauvegarde régulière. Cependant, étant donné la nature même du réseau public qu'est l'internet, vous reconnaissez et acceptez que la sécurité des transmissions via internet ne puisse être garantie. En conséquence, *la Compagnie* ne peut garantir ni n'assume aucune responsabilité pour toute violation de confidentialité, piratage, virus, perte ou altération des données transmises par Internet.

Conservation

La Compagnie utilise et conserve vos renseignements personnels aussi longtemps que nécessaire afin de satisfaire les finalités pour lesquelles ils ont été recueillis, ou comme la loi le permet ou l'exige.

La Compagnie se réserve le droit de détenir, pour une durée raisonnable, certains renseignements personnels pour se conformer à la loi, prévenir la fraude, résoudre une réclamation ou certains autres problèmes s'y rattachant, coopérer à une enquête et pour tout autre acte permis par la loi. À l'expiration de ce délai, vos renseignements personnels seront délestés des serveurs de *la Compagnie*.

Liens externes

Dans le cours de l'usage du site de *la Compagnie*, vous pourriez être amené à consulter d'autres sites web de tiers, via des hyperliens. Cependant, *la Compagnie* n'est pas responsable des pratiques, politiques ou actes de ces tiers en ce qui a trait à la protection de vos renseignements personnels. Il est donc recommandé de lire attentivement l'énoncé sur la protection des renseignements personnels apparaissant sur ces sites afin de pouvoir déterminer de manière éclairée dans quelle mesure vous souhaitez ou non utiliser ces sites.

De plus, un lien vers un tel site ne signifie pas que *la Compagnie* recommande ce site tiers ou qu'elle assume une quelconque responsabilité quant à son contenu ou à l'usage qui peut en être fait. Il vous incombe de prendre les précautions nécessaires pour vous assurer que le site que vous sélectionnez pour votre usage n'est pas infecté de virus ou d'autres parasites de nature destructrice.

Responsabilité

La Compagnie n'est pas responsable de l'exactitude des renseignements que vous fournissez sur notre site Internet ou par moyen technologique.

La Compagnie ne peut être tenue responsable de quelque dommage que ce soit causé de façon directe ou indirecte du fait de l'utilisation ou de la non-utilisation des informations diffusées sur le site.

La Compagnie ne garantit pas que le site ou son contenu ne seront pas l'objet d'interruptions ou d'erreurs, que les défauts éventuels seront corrigés, ni que le site ou le serveur qui l'héberge sont libres de virus ou d'autres éléments nuisibles.

Traitement des plaintes

Toute personne qui souhaite formuler une plainte relative à l'application de la présente politique ou, plus généralement, à la protection de ses renseignements personnels par *la Compagnie* doit le faire par écrit en s'adressant à la personne responsable de la protection des renseignements personnels de *La Compagnie*.

Responsable de la protection des renseignements personnels: Nancy Rheault

Courriel : admin@sursaut.ca

Numéro de téléphone : 819 822-8912

Pour consulter l'intégralité de la *Politique de traitement des plaintes*, veuillez vous référer au document PDF disponible dans la section « *Politique de confidentialité* » du site Web de *la Compagnie*, ou à l'annexe 7 de la *Politique de gouvernance en matière de protection des renseignements personnels*.

Informations additionnelles

Pour toute demande d'information ou mise à jour concernant vos renseignements personnels, veuillez communiquer avec la personne responsable de la protection des renseignements personnels, Nancy Rheault, directrice administrative, par téléphone au 819 822-8912 ou par courriel à l'adresse admin@sursaut.ca

Modification

La Compagnie se réserve le droit de modifier sa Politique de confidentialité à sa discrétion. *La Compagnie* rendra disponible, sur son site Internet, toute modification éventuelle de cette Politique de confidentialité.

ANNEXE 2 – PROCÉDURE DE NUMÉRISATION

La personne responsable de la numérisation :

1. Effectue la préparation physique des documents à numériser (enlève les trombones et les agrafes);
2. Numérise les documents et demeure présente tout au long du processus afin de protéger l'intégrité des données numérisées;
3. Effectue une vérification exhaustive des documents numérisés afin de s'assurer de la quantité, de la qualité et de l'intégrité des documents reproduits. Elle vérifie que :
 - les documents numérisés sont conformes aux documents sources;
 - les données sont lisibles et de bonne qualité (sans perte de détail ou d'information);
 - le recto verso a bien été fait, le cas échéant; si l'option recto verso a fait en sorte de laisser des pages blanches, elle élimine ces dernières;
 - les documents ou les pages ont été numérisés dans le bon sens.
4. Vérifie que le nombre de documents ou de pages est exact (si des pages manquent, elle reprend la numérisation au complet);
5. Renomme les fichiers PDF selon la convention de nommage établie dans *la Compagnie*
6. Enregistre-le ou les fichiers PDF selon le classement approprié de *la Compagnie* ;
7. Consigne la numérisation dans le registre.

ANNEXE 4 – TECHNIQUES DE DESTRUCTION DÉFINITIVE DE DOCUMENTS

Techniques de destruction définitive de documents¹

Support utilisé	Exemples de méthodes de destruction
Papier (originaux et toutes les copies)	<ul style="list-style-type: none"> • Déchiqueteuse, de préférence à découpe transversale
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 et 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, clés 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, etc.). <p>La plupart des déchiqueteuses pourront détruire les CD et les DVD.</p> <ul style="list-style-type: none"> • Démagnétiseur pour les disques durs. • Élimination écologique : Une fois les informations supprimées, <i>la Compagnie</i> peut également apporter le matériel physique à l'un des écocentres de Sherbrooke.
Machines contenant des disques durs Ex. photocopieur, télécopieur, numériseur, imprimante, 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. • Élimination écologique : Une fois les informations supprimées, <i>la Compagnie</i> peut également apporter les machines désuètes et non fonctionnelles à l'un des écocentres de Sherbrooke.

¹ Commission d'accès à l'information, Procédure de destruction, en ligne : <https://www.cai.gouv.qc.ca/entreprises/procedure-de-destruction/>

ANNEXE 6 – MODÈLE REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

Registre des incidents de confidentialité								
Date ou période de l'incident	Personnes concernées (informations compromises)	Description des circonstances de l'incident	Prise de connaissance de l'incident	Nombres de personnes concernées par l'incident	Description des éléments qui amènent à conclure qu'il existe ou non un risque qu'un préjudice sérieux ² soit causé aux personnes concernées	Date de transmission de l'avis à la Commission d'accès à l'information	Date de transmission des avis aux personnes concernées	Description des mesures prises afin de diminuer les risques qu'un préjudice soit causé

² L'évaluation du risque de préjudice sérieux tient compte notamment des éléments suivants : la sensibilité des renseignements personnels concernés; les utilisations malveillantes possibles des renseignements et les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables.

ANNEXE 7 – PROCÉDURE DE TRAITEMENT DES PLAINTES EN LIEN AVEC LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Réception de la plainte

Toute personne qui souhaite formuler une plainte relative à l'application de la présente politique ou, plus généralement, à la protection de ses renseignements personnels par *la Compagnie* doit le faire par écrit en s'adressant à la personne responsable de la protection des renseignements personnels de *La Compagnie*.

Responsable de la protection des renseignements personnels: Nancy Rheault

Courriel : admin@sursaut.ca

Numéro de téléphone : 819 822-8912

La personne devra indiquer son nom, ses coordonnées pour la joindre, incluant un numéro de téléphone, ainsi que l'objet et les motifs de sa plainte, en donnant suffisamment de détails pour que celle-ci puisse être évaluée par *la Compagnie*. Si la plainte formulée n'est pas suffisamment précise, la personne responsable de la protection des renseignements personnels peut requérir toute information additionnelle qu'elle juge nécessaire pour pouvoir évaluer la plainte.

Traitement de la plainte

La Compagnie s'engage à traiter toute plainte reçue de façon confidentielle.

La plainte est traitée dans un délai raisonnable. La personne responsable de la protection des renseignements personnels doit analyser la plainte et y répondre par écrit, en motivant sa décision.

Cette évaluation visera à déterminer si le traitement des renseignements personnels par *la Compagnie* est conforme à la présente politique et à la législation ou réglementation applicable.

Dossier de plainte

La Compagnie doit constituer un dossier distinct pour chacune des plaintes qui lui sont adressées en vertu de la présente procédure de traitement de plainte. Chaque dossier comprend la plainte, l'analyse et la documentation à l'appui de son évaluation, ainsi que la réponse écrite envoyée à la personne ayant déposé la plainte.

ANNEXE 8 – MODÈLE D'INVENTAIRE DES RENSEIGNEMENTS PERSONNELS DE L'ENTREPRISE

Inventaire des renseignements personnels de l'entreprise											
Nom du Fichier ou du Document	Type de support et type de fichier	Lieu(x) de conservation	Description du document	Catégorie de personnes ayant accès aux renseignements	Personnes qui ont accès au fichier dans l'exercice de leurs fonctions et leur titre	Catégories de renseignements	Présence de renseignements personnels sensibles	Provenance des renseignements	Fins de la conservation de ces renseignements	Durée générale de conservation	Mesures de sécurité pour assurer la protection des renseignements
	Ex.: Papier, informatique; Fichier DOC, Fichier PDF, Fichier Excel, etc			Ex.: Membres du conseil d'administration, Membres de la direction, Employé.es concerné.es, etc.		Ex. Renseignements concernant l'identité, Renseignements financiers	<input type="checkbox"/>	Ex. Personne visée par les renseignements, Information créée par la Compagnie, etc.	Ex. gestion interne (ex.rapports financiers), application de la loi (ex. sur les impôts) etc		Ex. Contrôle des droits d'accès, Mot de passe, etc.
							<input type="checkbox"/>				
							<input type="checkbox"/>				

ANNEXE 9 – SITE WEB ET DOCUMENTS DE RÉFÉRENCES

Sources d'information :

- Outils en matière de protection des renseignements personnels –
Gouvernement du Québec

[Outils en matière de protection des renseignements personnels | Gouvernement du Québec](#)

- Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la
vie privée

https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_EFVP.pdf

- Modèle de Rapport d'évaluation des facteurs relatifs à la vie privée

https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GAB_RAP_EFVP.docx?v=171565095

9