Politique de gestion et de protection des renseignements personnels / Management and Protection of Personal Information Policy

Gouvernance, Risques et Conformité / Governance, Risk, and Compliance

Table of Contents

1 Objectif / Objective

Cette politique établit les responsabilités et les exigences minimales pour la mise en œuvre et le maintien d'un programme de gestion des renseignements personnels et de protection de la vie privée chez Consoltec (Ci-après « L'Entreprise »). Le programme de protection de la vie privée est conçu pour protéger tous les renseignements personnels identifiables des employés et des clients contre toute divulgation accidentelle.

This policy establishes the responsibilities and minimum requirements for the implementation and maintenance of a personal information management and privacy protection program at Consoltec (hereinafter "The Company"). The Privacy Protection Program is designed to protect all personally identifiable employee and customer information from accidental disclosure.

2 Portée / Scope

Cette politique s'applique à tous les employés, sous-traitants et tiers responsables de la mise en œuvre du programme de gouvernance en matière de protection de la vie privée.

This policy applies to all employees, subcontractors and third parties responsible for implementing the privacy governance program.

3 Politique / Policy

3.1 Base juridique du traitement des données personnelles / Legal Basis for Processing Personal Data

Tout le personnel de Consoltec doit adhérer aux principes relatifs au traitement des données personnelles énoncés dans le RGPD de l'UE (et de manière similaire dans la loi 25 du Québec), qui exigent que les données personnelles soient :

1. Traitées de manière licite, loyale et transparente par rapport à la personne concernée (Licéité, Loyauté et Transparence) ;
2. Collectées uniquement à des fins spécifiées, explicites et légitimes (limitation de la finalité) ;
3. Adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
4. Précises et, au besoin, tenues à jour (précision) ;
5. Ne soient pas conservées sous une forme permettant l'identification des personnes concernées plus longtemps que nécessaire aux fins pour lesquelles les données sont traitées (limitation de stockage) ;
6. Traitées de manière à garantir leur sécurité en utilisant des mesures techniques et organisationnelles appropriées pour se protéger contre tout traitement non autorisé ou illégal et contre toute perte, destruction ou dommage accidentels (Sécurité, Intégrité et Confidentialité) ;
7. Non transférées vers un autre pays sans que des garanties appropriées soient en place (limitation du transfert) ; et
8. Mises à la disposition des personnes concernées et permettre aux personnes concernées d'exercer certains droits relatifs à leurs données personnelles (Droits de la personne concernée).

All Consoltec personnel should adhere to the principles relating to the processing of personal data set out in the EU GDPR (and similarly in Quebec's Act 25), which require personal data to be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject (Lawfulness, Fairness and Transparency);
2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation);
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
4. Accurate and where necessary kept up to date (Accuracy);
5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
7. Not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
8. Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights).

3.2 Droits des personnes concernées / Data Subject Rights

La Société s'engage à faire respecter les droits des personnes concernées afin de maintenir la confiance, l'ouverture et la transparence. Vous devez connaître ces droits si vous voulez faire une demande ou si une demande vous est adressée afin de vous assurer qu'ils sont gérés efficacement et dans les délais légaux.

Les droits suivants existent :

1. retirer votre consentement au traitement en tout temps ;
2. recevoir certains renseignements sur les activités de traitement de la Société;
3. demander l'accès aux données personnelles que nous détenons ;
4. empêcher notre utilisation de données personnelles à des fins de marketing direct ;
5. nous demander d'effacer les données personnelles si elles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été recueillies ou traitées ou de rectifier des données inexactes ou de compléter des données incomplètes ;
6. restreindre le traitement dans des circonstances spécifiques ;
7. contester un traitement justifié sur la base de nos intérêts légitimes ou dans l'intérêt public ;
8. demander une copie d'un accord en vertu duquel les données personnelles sont transférées à l'extérieur de l'EEE ou du Canada ;
9. s'opposer aux décisions basées uniquement sur un traitement automatisé, y compris le profilage ;
10. empêcher un traitement susceptible de causer un dommage ou une détresse à la personne concernée ou à toute autre personne ;
11. être informé d'une violation de données personnelles susceptible d'entraîner un risque élevé pour leurs droits et libertés ;

The Company is committed to upholding the rights of data subjects in order to maintain trust, openness and transparency. You should be aware of these rights if you want to make a request or if a request is made to you in order to ensure they are managed efficiently and within statutory timeframes.

The following rights exist:

1. withdraw consent to processing at any time;
2. receive certain information about the Company's processing activities;
3. request access to the personal data that we hold;
4. prevent our use of personal data for direct marketing purposes;
5. ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
6. restrict processing in specific circumstances;
7. challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
8. request a copy of an agreement under which personal data is transferred outside of the EEA or Canada;
9. object to decisions based solely on Automated Processing, including profiling;
10. prevent processing that is likely to cause damage or distress to the data subject or anyone else;
11. be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
12. make a complaint to the supervisory authority / the Information Commissioner's Office or Privacy Commissioner of Canada;
13. in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

12. déposer une plainte auprès de l'autorité de surveillance / du Commissariat à l'information ou du Commissariat à la protection de la vie privée du Canada ;
13. dans des circonstances limitées, recevoir ou demander que leurs données personnelles soient transférées à un tiers dans un format structuré, couramment utilisé et lisible par machine.

La Société disposera généralement d'un mois pour répondre à ces demandes.

Si vous désirez faire une demande ou si vous recevez une demande de droits d'une personne concernée, vous devez la transmettre rapidement à : dpo@consoltec.ca[1].

The Company will typically have one month in order to respond to such requests.

If you want to make a request or if you receive a rights request from a data subject, you should forward this promptly to: dpo@consoltec.ca[2].

3.3 Informations personnelles recueillies / Personal Information Collected

3.3.1 Site web corporatif / Corporate Web Site

(http://www.consoltec.ca)

3.3.1.1 Données personnelles

Nous pouvons recueillir les renseignements que vous nous fournissez. Lorsque vous utilisez l'un des services de notre produit FlowFit, nous pouvons collecter et stocker :

- nom et prénom,
- adresse courriel corporative,
- numéro de téléphone,
- adresse postale,

3.3.1.2 Personal Data

We may collect the information you provide to us. When you use one of our FlowFit product's services we may collect and store:

- surname and name
- corporate email address,
- phone number,
- mailing address,
- country,

1 mailto:dpo@consoltec.ca
2 mailto:dpo@consoltec.ca

- pays,
- les langues que vous parlez,
- la nature et la taille de votre entreprise.

Nous pouvons également collecter des informations de base sur le profil d'utilisateur de tous nos visiteurs. Lorsque vous visitez notre site, nous pouvons collecter des informations sur l'appareil telles que le type de connexion, le système d'exploitation, le navigateur et les adresses IP.

- the languages you speak,
- the nature and size of your business.

We may also collect basic user profile information from all of our visitors. When you visit our site, we may collect device information such as connection type, operating system, browser and IP addresses.

3.3.1.3 Accès à vos données

À n'importe quel moment, vous avez le droit de demander que vos informations soient retirées, en tout ou en partie, de nos systèmes. Cependant, il serait possible que vous ne puissiez plus utiliser notre logiciel ou nos services si vous retiriez trop d'information.

En tout temps, vous avez le droit de nous demander par écrit l'ensemble des informations que nous détenons à votre sujet, complètement et précisément.

3.3.1.4 Access to your data

At any time, you have the right to request that your information be removed, in whole or in part, from our systems. However, you may not be able to use our software or services if you remove too much information.

At any time, you have the right to ask us in writing for all the information we retain about you, completely and accurately.

3.3.1.5 Données d'utilisation

Les données d'utilisation sont à notre disposition à tout moment. Nous pourrions utiliser ces données pour les statistiques d'utilisation, le profilage automatique et le ciblage. Avant de le faire, nous vous demanderons votre consentement exprès pour le faire. À cette fin, nous utilisons la technologies des cookies**.**

Un cookie est une petite quantité de données générées par un site Web et enregistrées par votre navigateur Web. Son but est de mémoriser des informations vous concernant, semblables à un fichier de préférences créé par une application logicielle.

3.3.1.6 Usage Data

Usage data is available to us at all times. We may use these data for usage statistics, automatic profiling and targeting. Before we do this, we will ask for your express consent to do so. We use Cookies to collect this data.

A cookie is a small amount of data generated by a website and saved by your web browser. Its purpose is to remember information about you, similar to a preference file created by a software application.

Cookies help to remember information like items in a shopping cart or to record the user's browsing activity including clicking particular buttons, logging in, or recording which pages were visited by the user. Most of the time,

Les cookies aident à mémoriser des informations telles que les articles dans un panier d'achat ou à enregistrer l'activité de navigation de l'utilisateur, y compris en cliquant sur des boutons particuliers, en se connectant ou en enregistrant les pages visitées par l'utilisateur. La plupart du temps, les cookies ne contiennent pas de données personnelles, mais un site Web peut les utiliser pour identifier un visiteur récurrent, souvent sans pouvoir identifier la *personne* derrière le navigateur Web.

Les navigateurs sont généralement configurés pour accepter les cookies. Cependant, vous pouvez désactiver les cookies en ajustant les paramètres de navigation de votre logiciel Internet. Vous pouvez également ajuster les paramètres de votre navigateur pour activer des cookies spécifiques ou pour vous avertir chaque fois qu'un nouveau cookie est sur le point d'être stocké sur votre ordinateur, ce qui vous permet de décider d'accepter ou de refuser le cookie.

cookies do not carry personal data, but a website can use them to identify a returning visitor, often without being able to identify the *person* behind the web browser.

Browsers are typically set to accept cookies. However, you can disable cookies through adjusting your internet software browsing settings. You can also adjust your browser settings to enable specific cookies or to notify you each time a new cookie is about to be stored on your computer enabling you to decide whether to accept or reject the cookie.

3.3.1.7 Durée de conservation

Nous conservons vos données personnelles pendant un (1) an, sauf si nous avons obtenu votre consentement clair pour utiliser vos données plus longtemps ou à d'autres fins similaires.

3.3.1.8 Data Retention Period

We retain your personal data for one (1) year unless we have obtained your clear consent to use your data longer or for another similar purpose.

3.3.1.9 Partage de l'information

Consoltec ne fournira jamais vos informations personnellement identifiables, ni ne partagera vos informations avec des tiers non affiliés à nous, sauf dans la mesure permise par la loi. Consoltec travaille avec des tiers pour fournir nos services. Des exemples de tels services comprennent l'hébergement de sites Web, l'infrastructure virtuelle, les plateformes de recrutement, le traitement des paiements et d'autres services. Si un fournisseur de services a besoin d'accéder à vos renseignements en notre nom, il le fait en vertu de ces règlements de politique.

3.3.1.10 Information Sharing

Consoltec will never provide your personally identifiable information, or share your information with any third party not affiliated with us, except as permitted by law. Consoltec works with third parties to provide our services. Examples of such services include website hosting, virtual infrastructure, recruitment platforms, payment processing and other services. If a service provider needs to access your information on our behalf, they do so under these policy regulations.

3.3.1.11 Traitement des données

À des fins d'envoi massif de courriels, d'enquêtes, d'analyses de marché et de recrutement, nous pouvons utiliser les agents de traitement de données externes tels que Google et d'autres services tiers pour diffuser nos annonces sur des sites Internet. Ces services utilisent des cookies pour diffuser des annonces basées sur les visites antérieures d'un utilisateur sur notre site Web. Vous pouvez refuser l'utilisation de cookies par Google en visitant la page de désactivation de la publicité de Google.

3.3.1.12 Data Processing

For the purposes of mass e-mailing, surveys, market analysis, and recruitment, we may use the following external data processing agents such as Google and other third-party services to show our ads on sites on the internet. These services use cookies to serve ads based on a user's prior visits to our website. You may opt-out of Google's use of cookies by visiting the Google advertising opt-out page.

3.3.2 Produit FlowFit / FlowFit Product

(xxx.flowfitservices.com[3])

3.3.2.1 Données personnelles

Vous pouvez charger une grande quantité de données sur votre serveur FlowFit hébergé, y compris les projets, les documents et les données personnelles des utilisateurs qui peuvent accéder à votre serveur FlowFit. Nous ne traitons ni n'utilisons ces données. À l'exception des données auxquelles nous devons accéder pour fournir nos services.

Vous êtes le responsable du traitement de toutes les données sur votre serveur FlowFit, avec tous les droits et responsabilités.

Référez-vous aux politiques relatives à la protection des informations personnelles de votre organisation pour connaître les détails.

3.3.2.2 Personal Data

You can load a large amount of data on your hosted FlowFit server, including projects, documents, and personal data of the users who may access your FlowFit server. We do not process or use these data. We act as a Data Processor only for the data we need to provide our services.

You are the data controller and data processor of all the data within the FlowFit services, with all rights and responsibilities.

Refer to your organization's Data Privacy policies for details.

3 http://xxx.flowfitservices.com

3.3.2.3 Données d'utilisation

Étant donné qu'un serveur FlowFit-TMS hébergé est techniquement géré par nous, les données d'utilisation sont à notre disposition à tout moment. Nous n'utilisons ces données que pour des fins de surveillance de sécurité. FlowFit-TMS utilise des cookies pour assurer la meilleure expérience pour tous les utilisateurs. En continuant à utiliser nos services, vous acceptez l'utilisation de cookies.

Lorsque vous utilisez un module tiers pour accéder à un service en ligne dans FlowFit, vous aurez un accord direct avec l'opérateur de ce service en ligne, sans l'intervention de Consoltec Inc. L'opérateur du service peut collecter des données directement auprès de vous, à notre insu. Nous ne serons pas responsables de la protection de ces données : veuillez consulter les politiques de confidentialité et les conditions de service de ces opérateurs.

3.3.2.4 Usage Data

Because a hosted FlowFit-TMS server is technically managed by us, usage data is available to us at all times. We do not use these data except for security surveillance. FlowFit-TMS uses cookies to ensure the best experience for everyone. By continuing to use our services, you are agreeing to the use of cookies.

When you use a third-party module to access an online service in FlowFit, you will have a direct agreement with the operator of that online service, without the intervention of Consoltec Inc. The operator of the service may collect data from you directly, without our knowledge. We will not be responsible for the protection of those data: please consult the privacy policies and service terms of those operators.

3.3.2.5 Durée de conservation

Référez-vous aux politiques relatives à la protection des informations personnelles de votre organisation pour connaître les détails.

3.3.2.6 Data Retention Period

Refer to your organization's Data Privacy policies for details.

3.3.2.7 Partage de l'information

Référez-vous aux politiques relatives à la protection des informations personnelles de votre organisation pour connaître les détails.

3.3.2.8 Information Sharing

Refer to your organization's Data Privacy policies for details.

3.3.3 Traitement des données / Data Processing

3.3.3.1 Microsoft Azure

Ces fournisseurs d'hébergement de serveurs agissent en tant que sous-traitants de données lorsque nous les utilisons pour héberger vos serveurs FlowFit. Sur ces serveurs, vos données personnelles ne sont jamais exploitées ni partagées à fins commerciales ou publicitaires.

Les serveurs hébergeant les serveurs FlowFit sont situés dans l'une de ces régions : Canada, États-Unis ou Europe. Lorsque vous vous inscrivez à l'hébergement du serveur FlowFit, vous pouvez choisir l'emplacement. Vous pouvez également choisir un emplacement différent de ceux énumérés ci-dessus.

3.3.3.2 Microsoft Azure

These server hosting providers act as data sub processors when we use them to host your FlowFit servers. On these servers, your personal data is never used nor shared for commercial or advertising purposes.

As a rule, the servers hosting the FlowFit servers are located in one of these regions: Canada, United States or Europe. When you sign up for FlowFit server hosting, you can choose the location. You can also choose a different location than the ones listed above.

3.3.3.3 Atlassian Jira

Nous utilisons leurs services pour gérer les tickets de support client. Nos clients (ou leurs représentants) peuvent envoyer une demande d'assistance via notre support client FlowFit. La politique de confidentialité d'Atlassian/Jira est disponible sur https://www.atlassian.com/legal/privacy-policy

Nous collectons les données personnelles suivantes auprès de vous :

- Nom complet
- Adresse courriel corporative
- Numéro de téléphone d'affaires
- La langue d'usage
- Informations techniques sur les systèmes que vous utilisez.

3.3.3.4 Atlassian Jira

We use their services to handle customer support tickets. Our customers (or their representatives) may send a support request through our FlowFit Customer Support. Atlassian/ Jira privacy policy is available at https://www.atlassian.com/legal/privacy-policy

We collect the following personal data from you:

- Full name
- Company E-mail address
- Business phone number
- The language you speak
- Technical information about the systems you use.

3.3.3.5 Modules tiers

Lorsque vous utilisez un module tiers pour accéder à un service en ligne dans FlowFit, vous aurez un accord direct avec l'opérateur de ce service en ligne, sans l'intervention de Consoltec Inc. L'opérateur du service peut collecter des données directement auprès de vous, à notre insu. Nous ne serons pas responsables de la protection de ces données : veuillez consulter les politiques de confidentialité et les conditions de service de ces opérateurs.

3.3.3.6 Third-party Modules

When you use a third-party module to access an online service in FlowFit, you will have a direct agreement with the operator of that online service, without the intervention of Consoltec Inc. The operator of the service may collect data from you directly, without our knowledge. We will not be responsible for the protection of those data: please consult the privacy policies and service terms of those operators.

3.3.4 Hébergement FlowFit / FlowFit Hosting

En règle générale, les serveurs hébergeant les serveurs FlowFit sont situés dans l'une de ces régions : Canada, États-Unis ou Europe. Lorsque vous vous inscrivez à l'hébergement du serveur FlowFit, vous pouvez choisir l'emplacement. Vous pouvez également choisir un emplacement différent de ceux énumérés ci-dessus.

Vous pouvez charger une grande quantité de données sur votre serveur FlowFit hébergé, y compris les projets, les documents et les données personnelles des utilisateurs qui peuvent accéder à votre serveur FlowFit. Nous ne traitons ni n'utilisons ces données. À l'exception des données auxquelles nous devons accéder pour fournir nos services.

Vous êtes le responsable du traitement de toutes les données sur votre serveur FlowFit, avec tous les droits et responsabilités.

As a rule, the servers hosting the FlowFit servers are located in one of these regions: Canada, United States or Europe. When you sign up for FlowFit server hosting, you can choose the location. You can also choose a different location than the ones listed above.

You can load a large amount of data on your hosted FlowFit server, including projects, documents, and personal data of the users who may access your FlowFit server. We do not process or use these data. Except for the data we need to access to provide our services.

You are the data controller of all the data on your FlowFit-TMS server, with all rights and responsibilities.

4 Programme de gouvernance en matière de protection de la vie privée / Privacy Governance Program

Programme officiel de gouvernance de la protection de la vie privée - L'Entreprise établira un programme officiel de gouvernance de la protection de la vie privée qui protégera les renseignements personnels identifiables (PII) des employés et des clients de l'Entreprise contre toute utilisation ou divulgation non autorisée. L'Entreprise attribuera des rôles et des responsabilités pour soutenir le programme et communiquera les objectifs et les activités du programme à l'ensemble du personnel.

Contenu du programme de protection de la vie privée - Au minimum, le programme de protection de la vie privée de l'Entreprise doit prendre en charge un ensemble complet de mesures qui permettent de se conformer aux lois en vigueurs en matière de protection des données.

Politique de sanctions en matière de protection de la vie privée - L'Entreprise appliquera des sanctions appropriées et cohérentes à tout employé ou partenaire d'affaires qui ne se conforme pas aux politiques de sécurité de l'information et de protection de la vie privée. Les sanctions de l'Entreprise peuvent comprendre des mesures disciplinaires pouvant aller jusqu'au congédiement ou à des poursuites judiciaires.

Formal Privacy Governance Program - Company will establish a formal privacy governance program that will protect the personally identifiable information (PII) of Company employees and customers from any use or unauthorized disclosure. The Company will assign roles and responsibilities to support the program and communicate program objectives and activities to all staff.

Content of the Privacy Program - At a minimum, the Company's privacy program must support a comprehensive set of measures that enable compliance with applicable data protection laws.

Privacy Sanctions Policy - The Company will apply appropriate and consistent sanctions to any employee or business partner who fails to comply with information security and privacy policies. The Company's sanctions may include disciplinary measures up to and including dismissal or legal action.

4.1 Licéité, équité et transparence / Lawfulness, Fairness & Transparency

Le personnel de Consoltec ne doit recueillir et utiliser des données personnelles que s'il est clair qu'il existe une **base juridique**, qu'il agit de manière équitable et que des **renseignements adéquats sur la politique de confidentialité** ont été fournis à la personne concernée . Ce qui veut dire :

Consoltec personnel should only collect and use personal data where they are clear that there is a **lawful basis**, they are acting fairly and where **adequate privacy notice information** has been provided to the data subject. This means:

- S'assurer qu'il existe une base juridique appropriée pour le traitement et, dans le cas de données personnelles de catégorie particulière, s'assurer qu'il existe une base supplémentaire pour le traitement.
- Lorsqu'il y a consentement, collecter et les conserver de manière conforme. Cela inclut d'informer les personnes concernées de la manière dont elles peuvent retirer leur consentement au traitement de leurs données personnelles.
- Fournir des avis de confidentialité aux personnes concernées au moment de la collecte et de la divulgation des données à des tiers. Ces avis garantissent qu'ils fournissent les renseignements nécessaires pour satisfaire aux exigences en matière d'avis de confidentialité et de transparence.
- Ne pas induire les personnes concernées en erreur sur la manière dont elles envisagent d'utiliser leurs données personnelles.

- Ensuring there is an appropriate lawful basis for processing and in the case of special category personal data ensuring there is a further basis for the processing.
- Where they rely upon consent they collect and retain this in a compliant manner. This includes informing data subjects how they may withdraw their consent for the processing of their personal data.
- Providing privacy notices to data subjects at the point of data collection and disclosure to third parties. These notices ensure that they supply the necessary information to satisfy privacy notice and transparency requirements.
- Not misleading data subjects about how they intend to use their personal data.

4.1.1 Limitation de la finalité / Purpose Limitation

Les données personnelles doivent être utilisées uniquement aux fins **spécifiées**, **explicites** et **légitimes**. Ce sont généralement les finalités mentionnées dans nos avis de confidentialité au moment de la collecte des données. Elles ne doivent pas être utilisées d'une manière incompatible avec ces finalités, sauf la personne concernée a été informée des nouvelles finalités et s'il existe une base légale appropriée ou si la personne concernée a donné son consentement, si nécessaire.

Il n'y aura strictement aucune utilisation personnelle des données personnelles auxquelles vous avez eu accès dans le cadre de l'exercice de votre rôle au sein de la Société.

La législation sur la protection des données contient des infractions pénales spécifiques liées à l'utilisation abusive des données personnelles. Celles-ci incluent :

Personal data must be used only for the **specified**, **explicit,** and **legitimate purposes**, these are typically the purposes cited within our privacy notices at the point of data collection. It should not be further used in any manner incompatible with those purposes unless we have informed the data subject of the new purposes and there is an appropriate lawful basis / the data subject has given their consent, where necessary.

There shall be strictly no personal use of the personal data to which you have been afforded access as part of fulfilling your role with the Company.

Data protection legislation contains specific recordable criminal offences relating to the misuse of personal data. These include:

- Knowingly or recklessly obtaining or disclosing personal data without the consent of the Company.
- Knowingly or recklessly procuring the disclosure of personal data without the consent of the Company.

- Obtenir ou divulguer sciemment ou imprudemment des données personnelles sans le consentement de la Société.
- Obtenir sciemment ou imprudemment la divulgation de données personnelles sans le consentement de la Société.
- Conserver sciemment ou imprudemment des données personnelles sans le consentement de la Société.

- Knowingly or recklessly retaining personal data without the consent of the Company.

4.1.2 Minimisation des jeux de données / Dataset Minimization

Les données personnelles recueillies et enregistrées doivent être **adéquates**, **pertinentes** et **limitées à ce qui est nécessaire** au regard des finalités pour lesquelles elles sont traitées. Tout ce qui est enregistré sur un individu doit être approprié et professionnel. Lorsque nécessaire, nous devons distinguer clairement les faits de l'opinion professionnelle.

Le personnel doit être convaincu que ce qui a été enregistré sur une personne est justifié et peut être expliqué en cas de contestation par la direction. Potentiellement, tout ce qui est enregistré sur un individu pourrait lui être divulgué dans le cadre d'une demande d'accès.

Personal data collected and recorded should be **adequate**, **relevant** and **limited to what is necessary** in relation to the purposes for which it is processed. Anything recorded about an individual should be appropriate and professional. Where necessary, we should clearly distinguish facts from professional opinion.

Staff should be satisfied that what has been recorded about an individual is justified and could be explained if ever challenged by line management. Potentially, anything recorded about an individual could be disclosed back to them as part of a Rights Request.

4.1.3 Précision / Accuracy

Les renseignements personnels doivent être exacts et, au besoin, tenus à jour. Il convient de les corriger ou de les supprimer sans délai lorsqu'ils s'avèrent inexacts.

Consoltec doit s'assurer que les données personnelles qu'elle utilise et détient sont exactes, complètes, tenues à jour et pertinentes aux fins pour lesquelles elles ont été collectées. Consoltec doit vérifier l'exactitude de toutes les données personnelles au moment de la collecte et à intervalles réguliers par la suite.

Personal data should be **accurate** and, where necessary, **kept up to date**. It should be corrected or deleted without delay when found to be inaccurate.

Consoltec should ensure that the personal data it uses and holds is accurate, complete, kept up to date and relevant to the purposes for which it was collected. Consoltec should check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

Tous les employés et sous-traitants sont tenus de vérifier que les renseignements qu'ils fournissent à la Société dans le cadre de leur emploi ou de leur contrat sont exacts et à jour.

All employees and subcontractors are responsible for checking that the information they provide to the Company in connection with their employment or contract is accurate and up to date.

4.2 Évaluation de la conformité / Conformity Assessment

Évaluation de la conformité - L'Entreprise doit déterminer si ses pratiques et sa situation actuelle exigent la conformité au GDPR et à la Loi 25 du Québec. L'entreprise doit déclarer explicitement cette décision dans un énoncé de gestion officiel.

Analyse de la collecte des données - La direction de l'Entreprise doit entreprendre une analyse des données afin de déterminer si la protection des données du GDPR et à la Loi 25 du Québec est nécessaire pour les types de données collectées.

Compliance Assessment - The Company must determine whether its practices and current situation require compliance with the GDPR and Quebec Law 25. The company must explicitly state this decision in a formal management statement.

Data Collection Analysis - Company management must undertake a data analysis to determine whether GDPR and Quebec Act 25 data protection is necessary for the types of data collected.

4.3 Rôles et responsabilités en matière de protection de la vie privée / Privacy Roles and Responsibilities

Attribuer des rôles et des responsabilités en matière de protection de la vie privée - L'Entreprise doit attribuer des responsabilités en matière de protection de la vie privée à son personnel et les intégrer à tous les postes qui traitent des PII.

Responsable de la protection des renseignements personnels (DPO) - L'Entreprise nommera un responsable de la protection des renseignements personnels qui supervisera et sera responsable de toutes les initiatives, activités et incidents liés à la protection des renseignements personnels de l'Entreprise. Parmi les fonctions spécifiques du responsable de la protection des renseignements personnels nous retrouvons notamment :

Assign Privacy Roles and Responsibilities - The Company must assign privacy responsibilities to its personnel and integrate them into all positions that deal with PII.

Data Protection Officer (DPO) - The Company will appoint a Data Protection Officer who will oversee and be accountable for all Company privacy initiatives, activities and incidents. Among the specific functions of the personal information protection manager we find in particular:

- Establish policy and governance practices regarding the protection of personal information;
- Ensure management of confidentiality incidents;

- Établir la politique et les pratiques de gouvernance en matière de protection des renseignement personnels;
- Assurer la gestion des incidents de confidentialité;
- Réaliser les Évaluations de Facteurs relatifs à la Vie Privée (ÉFVP);
- Sensibiliser et former le personnel de l'Entreprise.

- Conduct Privacy Impact Assessments (PIAs);
- Raise awareness and train Company staff.

4.4 Exigences en matière de politiques et de procédures / Policy and Procedure Requirements

Politiques de confidentialité des données - Des politiques doivent être rédigées, mises en œuvre et appliquées pour garantir la sécurité, la fiabilité, l'intégrité et la disponibilité des renseignements personnels identifiables (PII).

Procédures de confidentialité des données - Des procédures doivent être mises en œuvre et appliquées pour faire respecter les politiques de sécurité et garantir la sécurité, la fiabilité, l'intégrité et la disponibilité des renseignements personnels identifiables (PII).

Événements accidentels ou non autorisés - Des politiques doivent être mises en œuvre et appliquées pour répondre aux événements qui compromettent la sécurité ou l'intégrité des PII, y compris la réponse à une éventuelle atteinte à la confidentialité des PII.

Politiques de prévention des préjudices - L'Entreprise établira des procédures formellement documentées pour déterminer si les traitements de données personnelles sont légaux et ne causent pas de préjudices conformément à la norme sur la protection des données.

Data Privacy Policies – Policies should be written, implemented, and enforced to ensure the security, reliability, integrity, and availability of personally identifiable information (PII).

Data Privacy Procedures – Procedures must be implemented and enforced to enforce security policies and ensure the security, reliability, integrity, and availability of Personally Identifiable Information (PII).

Accidental or Unauthorized Events – Policies must be implemented and enforced to respond to events that compromise the security or integrity of PII, including responding to a possible breach of confidentiality of PII.

Harm Prevention Policies - The Company will establish formally documented procedures to determine whether the processing of personal data is lawful and does not cause harm in accordance with the data protection standard.

4.5 Inventaire des informations personnelles et flux de données / Personal Information Inventory and Data Flows

Inventaire complet des PII requis - L'Entreprise doit définir et documenter les PII qu'elle traite et communiquer ces informations aux employés responsable du traitement et de la manipulation de celles-ci afin de s'assurer qu'ils comprennent les PII qu'ils sont chargés de protéger.

Évaluation des flux de données PII - L'Entreprise doit cartographier les flux de données et identifier les points des flux où les PII sont les plus vulnérables, puis créer des contrôles et des protections appropriés.

Activités de traitement clés - Dans le cadre du programme de gouvernance en matière de protection de la vie privée, tous les processus commerciaux clés qui traitent les PII doivent être identifiés et documentés. Ils doivent être identifiés comme des contrôles clés dans le cadre de l'évaluation des risques de l'entreprise.

Complete Inventory of PII Required - The Company must define and document the PII it processes and communicate this information to employees responsible for processing and handling it to ensure that they understand the PII they are responsible for protecting.

Assessing PII Data Flows - The Company must map data flows and identify points in the flows where PII is most vulnerable, then create appropriate controls and protections.

Key Processing Activities – As part of the privacy governance program, all key business processes that handle PII must be identified and documented. They should be identified as key controls as part of the business risk assessment.

4.6 Évaluations de la protection de la vie privée / Privacy Assessments

Procédures relatives à l'impact sur la vie privée – L'évaluation des facteurs relatifs à la vie privée (ÉFVP) doit être réalisée conformément aux procédures spécifiques élaborées par le responsable de la protection des renseignements personnels. Le responsable doit analyser les menaces pesant sur les PII et déterminer l'impact potentiel sur l'entreprise en cas d'incident. Le responsable de la protection de la vie privée doit ensuite calculer les actions et les coûts associés pour aider à prévenir de tels incidents.

Évaluations ponctuelles des facteurs relatifs à la vie privée - L'Entreprise doit également procéder à une évaluation des facteurs relatifs à la vie privée

Privacy Impact Assessment – The Privacy Impact Assessment (PIA) must be conducted in accordance with specific procedures developed by the Data Privacy Officer. The manager must analyze threats to PII and determine the potential impact to the business in the event of an incident. The privacy officer must then calculate actions and associated costs to help prevent such incidents.

Ad hoc Privacy Impact Assessments - The Company must also conduct a Privacy Impact Assessment in specific situations when there is a significant change in the Company's data processing.

dans des situations particulières, lorsqu'il y a un changement important dans le traitement des données de l'entreprise.

4.7 Suivi du programme / Program Monitoring

Surveillance des lois sur la sécurité et la protection de la vie privée - L'Entreprise doit continuellement surveiller la conformité aux lois sur la sécurité de l'information et la protection de la vie privée de l'entreprise, les nouvelles lois et réglementations sur la sécurité et la protection de la vie privée, et mettre à jour les programmes au besoin pour assurer la conformité.

Dossiers des personnes concernées - L'Entreprise doit fournir aux personnes concernées des rapports sur l'historique de leurs données personnelles, y compris des copies complètes de leurs données personnelles dans un format acceptable, ainsi qu'un avis sur toute violation possible des données.

Rapports d'évaluation de la protection de la vie privée - Le responsable de la protection des renseignements personnels doit présenter régulièrement (par exemple, tous les trimestres ou tous les deux ans) un rapport sur l'état de l'environnement de protection de la vie privée aux dirigeants de l'Entreprise.

Monitoring Security and Privacy Laws - The Company shall continually monitor compliance with the Company's information security and privacy laws, new security and privacy laws and regulations. security and privacy protection, and update programs as necessary to ensure compliance.

Data Subject Records - The Company shall provide data subjects with historical reports of their personal data, including complete copies of their personal data in an acceptable format, as well as notice of any possible data breach.

Privacy Assessment Reports - The Data Privacy Officer must submit a regular (e.g., quarterly or bi-annual) report on the state of the privacy environment. private life of the Company's managers.

4.8 Exigences en matière de sélection des tiers et de protection de la vie privée / Third Party Selection and Privacy Requirements

Évaluation des incidences sur la vie privée des tiers - Des évaluation des facteurs relatifs à la vie privée satisfaisantes doivent être réalisées pour les tiers avant de permettre aux sous-traitants tiers d'accéder aux PII de l'Entreprise pour les gérer, les traiter, les transférer ou les manipuler d'une autre manière.

Third Party Privacy Impact Assessments - Satisfactory third party privacy impact assessments must be conducted for third parties before allowing third party processors to access and manage the Company's personal information, process, transfer or otherwise manipulate them.

Contrats officiels avec des tiers - L'Entreprise ne doit pas faire appel à des tiers pour le traitement des données, à moins que ces mêmes organisations aient donné l'assurance qu'elles respectent les bonnes pratiques en matière de protection de la vie privée.

Arrangements avec les sous-traitants - Les contrats de l'Entreprise avec des sous-traitants doivent exiger que ces mêmes sous-traitants précisent que les contrôles de protection de la vie privée doivent également s'appliquer à tous les sous-traitants.

Entrepreneurs individuels - L'Entreprise doit s'assurer que toute personne agissant au nom de l'organisation dans le traitement des personnes concernées respecte également toutes les politiques et procédures de l'Entreprise, y compris celles qui sont exigées par le contrat ou la législation en vigueur

Formal Contracts with Third Parties - The Company must not use third parties for data processing, unless these same organizations have ensured that they respect good practices in terms of privacy protection.

Arrangements with Subcontractors - The Company's contracts with subcontractors should require the same subcontractors to specify that privacy controls should also apply to all subcontractors.

Freelance Contractors - The Company must ensure that any person acting on behalf of the organization in processing data subjects also complies with all Company policies and procedures, including those required by contract or applicable law .

4.9 Gestion des brèches / Breach Management

Conformément à la politique et aux procédures de gestion des incidents de sécurité, un incident de gouvernance de l'information désigne une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux données personnelles transmises, stockées ou autrement traitées.

Des exemples d'incidents comprennent, sans toutefois s'y limiter :

- Mauvaise gestion des courriels : envoi d'un courriel contenant des données personnelles au mauvais destinataire, envoi de mauvaises informations ou téléchargement d'une pièce jointe incorrecte, ne pas couper le chemin du courriel afin de divulguer un excès de données personnelles et ne pas utiliser la fonctionnalité Cci le cas échéant.
- Perte ou vol de renseignements ou de matériel informatique contenant des données personnelles.

As per the Security Incident Management Policy & Procedures, an information governance incident means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Examples of incidents include, but are not limited to:

- E-mail mismanagement: sending an e-mail containing personal data to the incorrect recipient, sending the wrong information or uploading the incorrect attachment, not trimming the e-mail trail so excessive personal data is disclosed, and not using bcc functionality where appropriate / compromising the recipients of an e-mail to one another etc.
- Loss or theft of information or IT equipment containing personal data.
- Incorrectly deleting or destroying personal data prior to the expiration of its retention period.

- Supprimer ou détruire incorrectement des données personnelles avant l'expiration de leur période de conservation.
- Cas de supervision ou d'audition de consultations avec des clients ou de discussions sur des données personnelles par des personnes n'ayant pas besoin d'en être informées.
- Attaque par des moyens techniques. c'est-à-dire l'utilisation de piratage, de logiciels malveillants ou de ransomwares.
- Attaque par des moyens non techniques, c'est-à-dire l'ingénierie sociale et le phishing.

- Instances of overseeing or overhearing client consultations or the discussion of personal data by those without a business need to know.
- Attack via technical means. i.e. use of hacking, malware or ransomware.
- Attack via non-technical means, i.e. social engineering and phishing.

4.10 Exigences en matière de formation à la protection de la vie privée / Privacy Training Requirements

Formation annuelle sur la protection des renseignements personnels - Tout le personnel de l'Entreprise doit suivre une formation annuelle sur la protection des renseignements personnels et participer à des formations ciblées sur la protection des renseignements personnels, sur demande.

Annual Privacy Training - All Company personnel must complete annual privacy training and participate in targeted privacy training, upon request.

4.11 Conception et développement des systèmes internes / Internal Systems Design & Development

Exigences de confidentialité dans le développement des systèmes - L'Entreprise doit intégrer les exigences de confidentialité dans le cycle de vie du développement des systèmes et des applications de l'Entreprise et dans les procédures de mise à jour des systèmes et des applications.

Classification des informations PII - L'Entreprise doit classifier correctement les informations personnelles (PII) des personnes concernées afin que les contrôles de sécurité de l'information appropriés puissent être appliqués pour protéger les données.

Limites d'accès du personnel aux PII - L'Entreprise doit limiter le nombre de personnes ayant accès aux PII à celles qui en ont besoin pour mener à bien leurs activités professionnelles.

Privacy Requirements in Systems Development - The Company shall integrate privacy requirements into the Company's systems and application development lifecycle and into systems and application update procedures.

Classification of PII - The Company must properly classify the personal information (PII) of data subjects so that appropriate information security controls can be applied to protect the data.

Limits on Staff Access to PII - The Company must limit the number of people with access to PII to those who need it to carry out their professional activities.

Examen de la confidentialité des activités d'exploration de données - Toutes les activités d'exploration de données de l'Entreprise doivent être autorisées et approuvées par le responsable de la protection des renseignements personnels afin d'éviter toute violation potentielle des politiques de confidentialité de l'Entreprise.

Procédures de protection de la vie privée pour les activités de gestion des relations avec la clientèle - L'Entreprise mettra en œuvre des procédures visant à intégrer les pratiques de protection de la vie privée dans toutes les activités de gestion des relations avec la clientèle (CRM).

Privacy Review of Data Mining Activities - All data mining activities of the Company must be authorized and approved by the Privacy Officer to avoid any potential violation of the Company's privacy policies. the Company.

Privacy Procedures for Customer Relationship Management Activities - The Company will implement procedures to integrate privacy practices into all customer relationship management (CRM) activities.

4.12 Communication sur les programmes / Communication on Programs

Politique de confidentialité externe requise - L'Entreprise doit afficher sur les sites Web de l'entreprise une politique de confidentialité approuvée par le responsable de la protection des renseignements personnels. Chaque page de chaque site Web doit comporter un lien facile à trouver vers la politique de confidentialité.

Avis aux employés sur les politiques de confidentialité - Tous les employés de l'Entreprise qui traitent des renseignements personnels de quelque manière que ce soit doivent être informés des politiques de confidentialité qui s'appliquent à eux, ainsi que des sanctions prévues en cas de non-respect de ces politiques.

Avis clair des politiques de confidentialité des PII - Chaque fois que L'Entreprise recueille des PII, à quelque endroit que ce soit et de quelque manière que ce soit, un avis clair doit être donné aux personnes auprès desquelles les renseignements sont recueillis

1. que leurs renseignements sont recueillis et
2. que les détails des politiques de confidentialité de l'entreprise sont connus.

External Privacy Policy Required - The Company must post on Company websites a privacy policy approved by the Chief Privacy Officer. Every page of every website should have an easy-to-find link to the privacy policy.

Notice to Employees of Privacy Policies - All employees of the Company who handle personal information in any manner must be informed of the privacy policies that apply to them, as well as the sanctions provided for in the event of failure to do so. -compliance with these policies.

Clear Notice of PII Privacy Policies - Whenever The Company collects PII, in any location and in any manner, clear notice must be given to those from whom the information is collected

1. that their information is collected and
2. that the details of the company's privacy policies are known.

4.13 Transfert d'informations personnelles à des tiers / Transfer of Personal Information to Third Parties

Mesures de sécurité pour le transfert (contrôles) - L'Entreprise doit mettre en œuvre des contrôles techniques et de gestion spécifiques pour le transfert sécurisé de ces données à des tiers.

Security Measures for Transfer (Controls) - The Company must implement specific technical and managerial controls for the secure transfer of this data to third parties.

4.14 Politique de sanctions en matière de protection de la vie privée / Privacy Sanctions Policy

La politique de confidentialité de l'Entreprise protège la confidentialité, la disponibilité et l'intégrité des informations personnelles identifiables, conformément à la loi et aux règlements en vigueurs. Tous les employés doivent protéger l'intégrité, la disponibilité et la confidentialité des PII.

Tout employé qui croit qu'un autre employé a enfreint l'une des politiques de confidentialité de l'Entreprise doit immédiatement signaler cette infraction au responsable de la protection des renseignements personnels de l'Entreprise.

Un employé, un associé ou un agent fera l'objet de mesures disciplinaires pouvant aller jusqu'au congédiement ou à des poursuites criminelles s'il ne se conforme pas aux politiques de confidentialité, s'il viole délibérément ou par négligence grave la vie privée, s'il enfreint les lois relatives à la protection de la vie privée ou s'il commet tout autre acte contraire aux politiques, procédures et pratiques de l'Entreprise en matière de protection de la vie privée.

Toutes les sanctions seront documentées et conservées pendant six ans.

The Company's privacy policy protects the confidentiality, availability and integrity of personally identifiable information in accordance with applicable law and regulations. All employees must protect the integrity, availability and confidentiality of PII.

Any employee who believes that another employee has violated any of the Company's privacy policies must immediately report the violation to the Company's data protection officer.

An employee, associate or agent will be subject to disciplinary action, up to and including dismissal or criminal prosecution, if they fail to comply with the confidentiality policies, or if they deliberately or grossly negligently violate privacy, if they violate the laws relating to the protection of privacy or if they commit any other act contrary to the policies, procedures and practices of the Company with regard to the protection of privacy.

All sanctions will be documented and kept for six years.

5 Violations / Violations

Toute violation de cette politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement. L'Entreprise se réserve le droit d'aviser les autorités policières compétentes de toute activité illégale et de collaborer à toute enquête sur une telle activité. L'Entreprise ne considère pas qu'une conduite contraire à cette politique s'inscrive dans le cadre de l'emploi d'un employé ou d'un tiers, ou qu'elle soit la conséquence directe de l'exercice des fonctions de l'employé ou du tiers. Par conséquent, dans la mesure permise par la loi, L'Entreprise se réserve le droit de ne pas défendre ou de ne pas payer les dommages-intérêts accordés à des employés ou à des tiers à la suite d'une violation de cette politique.

Tout employé ou tiers à qui l'on demande d'entreprendre une activité qui, selon lui, enfreint la présente politique, doit déposer une plainte écrite ou verbale auprès de son responsable, de tout autre responsable ou du département des ressources humaines dans les plus brefs délais.

Any violation of this policy may result in disciplinary action, up to and including dismissal. The Company reserves the right to notify the appropriate law enforcement authorities of any illegal activity and to cooperate in any investigation into such activity. The Company does not consider that conduct contrary to this policy is part of the employment of an employee or a third party, or that it is the direct consequence of the exercise of the functions of the employee or third party. Therefore, to the extent permitted by law, The Company reserves the right not to defend or pay damages awarded to employees or third parties as a result of a violation of this policy.

Any employee or third party who is asked to undertake an activity that they believe violates this policy must file a written or verbal complaint with their manager, any other manager or the Human Resources Department as soon as possible. promptly.

6 Définitions / Definitions

Responsable du traitement - Le "responsable du traitement" est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel.

Processeur de données - Le terme "processeur" désigne une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Droits de la personne concernée - Il s'agit de l'ensemble des droits spécifiques dont dispose une personne en ce qui concerne le contrôle de ses informations personnelles.

Actif informationnel - Toutes les données de l'Entreprise, sous quelque forme que ce soit, et l'équipement utilisé pour gérer, traiter ou stocker les données de l'Entreprise, qui sont utilisées dans le cadre de l'exécution des activités. Cela comprend, sans s'y limiter, les données de l'entreprise, des clients et des partenaires.

Informations personnelles identifiables (PII) - Informations qui, seules ou combinées à d'autres informations personnelles ou d'identification, peuvent être utilisées pour identifier, contacter ou localiser une seule personne ou qui peuvent être utilisées avec d'autres sources pour identifier une seule personne.

Traitement - Le terme "traitement" désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Data Controller - "Controller" is the physical or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. staff.

Data Processor - The term "processor" means a physical or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Subject Rights - These are the set of specific rights an individual has in relation to control of their personal information.

Information Asset - All Company data, in any form, and equipment used to manage, process or store Company data, which is used in carrying out business. This includes, but is not limited to, company, customer and partner data.

Personally Identifiable Information (PII) - Information that, alone or in combination with other personal or identifying information, can be used to identify, contact, or locate a single person or that can be used in conjunction with other sources to identify a single person.

Processing - "Processing" means any operation or set of operations, whether or not carried out by automated means, and applied to personal data or sets of data, such as collection, recording, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, limitation, erasure or destruction.

Privacy Protection Program - Guidelines allowing The Company to retain information about individuals while protecting the rights of individuals against unjustified or illegal invasions of their privacy.

Third Party Controller - Any person who is not an employee of the Company and who is contractually required to provide a certain form of service to the Company.

Programme de protection de la vie privée - Directives permettant à L'Entreprise de conserver des informations sur les personnes tout en protégeant le droit des personnes contre les atteintes injustifiées ou illégales à leur vie privée.

Tiers responsable du traitement - Toute personne qui n'est pas un employé de l'Entreprise et qui est tenue par contrat de fournir une certaine forme de service à L'Entreprise.

Utilisateur - Tout employé de l'Entreprise ou tiers autorisé à accéder à une ressource d'information électronique de l'Entreprise.

User - Any employee of the Company or third party authorized to access an electronic information resource of the Company.

7 Références / References

- CPL: 16.2 Customer Privacy Management
- ISO 27002: 18.1.4 Privacy and protection of personally identifiable information
- HIPAA: Privacy Rules
- NIST: Appendix J: Privacy Controls (800-53 V5 P Controls)
- US-CSF: PR.DS-9: Privacy of individuals and (PII) is protected
- GDPR: General Data Protection Regulation
- Loi 25: Nouvelles dispositions protégeant la vie privée des Québécois

8 Historique des changements / Change History

Version	Date	Comment
Current Version[4] **(v. 4)**	**Dec 16, 2024 10:36**	Jean-Yves Allard[5]: Combined internal and external policies following internal audit
v. 3[6]	Oct 28, 2024 15:56	Jean-Yves Allard[7] Modified for GDRP certification
v. 2[8]	Jul 12, 2024 12:24	Jean-Yves Allard[9] Modified for ISO 27001 certification
v. 1[10]	Jan 11, 2024 11:55	Jean-Yves Allard[11]

4 https://consoltec.atlassian.net/wiki/display/ITOPS/viewpage.action?pageId=1982267438
5 https://consoltec.atlassian.net/wiki/people/6228ae32302c6b006af5caba
6 https://consoltec.atlassian.net/wiki/display/ITOPS/viewpage.action?pageId=2346778650
7 https://consoltec.atlassian.net/wiki/people/6228ae32302c6b006af5caba
8 https://consoltec.atlassian.net/wiki/display/ITOPS/viewpage.action?pageId=2287108167
9 https://consoltec.atlassian.net/wiki/people/6228ae32302c6b006af5caba
10 https://consoltec.atlassian.net/wiki/display/ITOPS/viewpage.action?pageId=2163834938
11 https://consoltec.atlassian.net/wiki/people/6228ae32302c6b006af5caba