

CONFIDENTIAL



# **General Privacy and Data Protection Policy / Politique Générale de Confidentialité et de Protection des Données**

C3 Solutions

November 22, 2024

## Table of Contents

General Privacy and Data Protection Policy / Politique Générale de Confidentialité et de Protection des Données .....	4
Confidential.....	4
C3 Solutions General Privacy and Data Protection Policy .....	4
1.0 Purpose and Scope .....	4
2.0 General Privacy and Data Protection Obligations.....	5
3.0 Accountability.....	5
3.1 C3’s Confidentiality and Security Team (CST).....	5
3.2 C3 Employees and Departments Responsibilities .....	5
3.3 Data Protection Officer (DPO) .....	5
4.0 Data Protection by Design.....	7
5.0 Transparency and Fairness .....	7
6.0 Legal Basis for Processing.....	8
7.0 Purpose Limitation.....	8
8.0 Limiting Collection .....	8
9.0 Accuracy.....	8
10.0 Storage Limitation.....	8
11.0 Disclosure to Third-Party .....	9
12.0 Integrity, Confidentiality and Safeguards .....	9
13.0 Individual Privacy Rights.....	9
14.0 Data Transfers of Personal Information.....	10
15.0 General Inquiries & Concerns Related to this Policy .....	10
Confidentiel.....	13
Politique Générale de Confidentialité et de Protection des Données de C3 Solutions .....	13
1.0 Objectif et Portée.....	13
2.0 Obligations générales en matière de confidentialité et de protection des données....	14
3.0 Responsabilités .....	14
3.1 Équipe de confidentialité et de sécurité (CST) de C3 .....	14
3.2 Responsabilités des employés et des départements de C3.....	14
3.3 Responsable de la protection des données (DPO).....	14
4.0 Protection des données dès la conception.....	16

## CONFIDENTIAL

5.0	Transparence et équité.....	16
6.0	Base légale du traitement.....	17
7.0	Limitation des finalités.....	17
8.0	Limitation de la collecte.....	18
9.0	Exactitude.....	18
10.0	Limitation du stockage.....	18
11.0	Divulgence à des tiers.....	18
12.0	Intégrité, confidentialité et mesures de protection.....	18
13.0	Droits individuels en matière de confidentialité.....	19
14.0	Transferts de données personnelles.....	19
15.0	Questions générales et préoccupations liées à cette politique.....	20

## **General Privacy and Data Protection Policy / Politique Générale de Confidentialité et de Protection des Données**

This policy explains how C3 generally processes and safeguards the Personal Information it handles. It provides mandatory guidance for all C3 representatives.

Cette politique explique comment C3 traite et protège généralement les données personnelles qu'elle gère. Elle fournit des directives obligatoires pour tous les représentants de C3.

### **Confidential**

## **C3 Solutions General Privacy and Data Protection Policy**

### **1.0 Purpose and Scope**

In the course of its business, C3 may process (collect, use, store, disclose, etc.) Personal Information for its own legitimate purposes or on behalf of its customers, as part of Customer Data. **Personal Information** (also referred to as personal data) can generally be defined as any information about an identified or identifiable individual. This can include personal information about customers' and suppliers' representatives, business contacts, C3 employees and any other individual C3 has a relationship with or may need to contact. Examples of Personal Information include (but are not limited to):

- Name, date of birth and social security or other identity card number
- Contact information such as mailing address, email address and phone numbers, credit card and financial account numbers
- Health or medical information
- Information contained in employee files, including employment history and evaluations
- Information collected during the application and hiring process
- Information related to employee benefits, such as dependents, beneficiaries and insurance policy information

Properly anonymized and de-identified or aggregated data is not Personal Information.

Because C3 is committed to adequately protecting Personal Information and complying with applicable privacy and data protection laws in all countries where it does business, rather than having various sets of rules we've decided to apply the highest regulatory standards in dealing with Personal Information uniformly across all of our activities, regardless of regulatory requirements, while at the same time complying with any specific, local privacy requirements.

## CONFIDENTIAL

This policy explains how C3 generally processes and safeguards the Personal Information it handles. It provides mandatory guidance for all C3 representatives.

### **2.0 General Privacy and Data Protection Obligations**

All C3 representatives, employees and subcontractors, must respect this policy and act in compliance with applicable privacy and data protection laws including the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the Quebec Act respecting the protection of personal information in the private sector and the Quebec Act to modernize legislative provisions as regards the protection of personal information (Act 25), the General Data Protection Regulation (GDPR - Regulation (EU) 2016/679) and California Consumer Privacy Act (CCPA), as well as the ISO 27001:2013 standard Information technology - Security techniques - Information security management systems - Requirements published by the International Organization for Standardization (ISO) and by the (IEC). In doing so, they will respect the privacy of other C3 employees, subcontractors, prospects, customers and people working on their behalf, etc.

### **3.0 Accountability**

#### **3.1 C3's Confidentiality and Security Team (CST)**

C3's Chief Information Security Officer, together with C3's Confidentiality and Security Team ("CST"), develops, maintains, reviews and ensures application of various policies and related strict internal practices and procedures that comply with best industry standards and practices and applicable privacy laws to ensure that all C3 data, including Personal Information and/or Customer Data is adequately protected. However, every C3 representative has some responsibility for ensuring that Personal Information is collected, stored and handled appropriately.

#### **3.2 C3 Employees and Departments Responsibilities**

In addition, C3's CST together with C3's Human Resources Department also ensures that every C3 representative is appropriately informed and understands all C3 policies and appropriate internal practices and procedures in accordance with C3's training and awareness program.

Furthermore, the management of each C3 department must ensure that all employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, each C3 department must make sure all third parties engaged to process personal data on their behalf (i.e., their data processors), if any, are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained prior to granting them access to personal data controlled by C3.

#### **3.3 Data Protection Officer (DPO)**

To further demonstrate C3's commitment to data protection, and to enhance the effectiveness of compliance efforts, C3 has appointed a Data Protection Officer ("DPO"). The Data Protection Officer operates with rigor and is supported by C3's CST of which the

## CONFIDENTIAL

DPO is a member. The Data Protection Officer reports to the CEO. The Data Protection Officer's duties include:

- Informing and advising C3 and its employees who carry out personal data processing activities pursuant to privacy and data protection regulations, provincial laws, national laws or European Union-based data protection provisions such as: collection, storage, use, disclosure, destruction.
- Ensuring the alignment of this policy with privacy and data protection regulations, provincial laws, national laws or European Union based data protection provisions.
- If necessary, providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs).
- The establishment and operation of a system providing prompt and appropriate responses to data subject requests.
- Informing C3's senior managers, officers, and directors of any potential corporate, civil and criminal penalties that may be levied against C3 and/or its employees for violation of applicable privacy and data protection laws.
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any third party who:
  - Provides personal data to C3.
  - Receives personal data from C3.
  - Has access to personal data collected or processed by C3.
- Carrying out an annual personal data protection compliance audit (as described in the related section hereafter). and,
- Receiving and responding to any related complaints and inquiries related to privacy and data protection.

### *3.3.1 DPO's Compliance Monitoring*

To confirm that an adequate level of compliance is achieved by all C3 departments as well as all C3 Development (as defined in section 4 of this policy) in connection with privacy and data protection, the Data Protection Officer will carry out an annual personal data protection compliance audit. This audit will minimally assess:

- Compliance with C3 policies in relation to the protection of personal data, including:
  - - The assignment of responsibilities.
    - Raising awareness.
    - Training of employees.
- The effectiveness of personal data protection-related operational practices, including:
  - Data subject rights.
  - Personal data transfers.

## CONFIDENTIAL

- Personal data incident management.
- Personal data complaints handling.
- The level of understanding of data protection policies and privacy notices.
- The currency of data protection policies and privacy notices.
- The accuracy of personal data being stored.
- The conformity of data processor activities.
- The adequacy of procedures for redressing poor compliance and personal data breaches.

The Data Protection Officer, in cooperation with key C3 business stakeholders, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies and good practice identified will be reported to, monitored and shared by the CST.

### **4.0 Data Protection by Design**

To ensure that all data protection requirements are identified and addressed when designing significant new C3 features, solutions, systems or processes and/or when reviewing or expanding existing ones (“**C3 Development**”), each such C3 Development must go through an approval process that includes a risk assessment. If a C3 Development results in any way in the processing of Personal Information or may have an impact on its security, the Data Protection Officer must be involved in this risk assessment.

Furthermore, if such processing of Personal Information, in particular when using new technologies, considering the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a Data Protection Impact Assessment (DPIA) must be conducted. The subsequent findings of the DPIA must then be submitted to the CEO for review and approval.

### **5.0 Transparency and Fairness**

C3 processes Personal Information in a transparent and fair manner. Individuals should be well informed when making decisions related to their Personal Information and exercising their privacy rights should be as easy as possible.

Thus, C3 provides information about its policies and practices regarding the collection, use and/or disclosure of personal information namely through this policy and by being committed to respond to any related complaints or inquiries, as well as any access requests.

Furthermore, at the time or prior to processing of any Personal Information, C3 provides a concise, transparent and intelligible privacy notice to concerned individuals in order for them to be aware of the fact that Personal Information will be processed including how it will be collected, kept and used. Such privacy notice is tailored in accordance with the nature of the relationship C3 has with the individual and the purpose for which the processing is needed. Such C3 privacy notice must provide, inter alia, the following specific information in clear and plain language: C3 contact details, purpose and legal basis of

## CONFIDENTIAL

processing, possible recipients, possible data transfers, retention period, various rights of the individual with regards to such Personal Information, etc.

Furthermore, each external website provided by C3 will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling legal requirements.

### **6.0 Legal Basis for Processing**

C3 will only process Personal Information for its own purposes with an appropriate legal ground. Legal basis can include consent, contract performance, legal obligations, vital interests of individuals, public interest and legitimate interest.

If C3 processes Personal Information based on consent, the form of the consent sought before collecting, using or disclosing Personal Information may vary depending on the circumstances and the type of information. Consent includes express oral or written consent, implied consent or opt-out consent. The applicable laws, sensitivity of the information and the individual's reasonable expectations will be considered in determining how consent must be given.

C3 will obtain any required consent before using Personal Information for any purpose other than that for which it was originally collected.

### **7.0 Purpose Limitation**

C3 will process Personal Information on its own behalf responsibly and only for legitimate specifically identified purposes as communicated to individuals. C3 will not process Personal Information beyond such purposes unless additional processing can be considered compatible with the original purposes for which the Personal Information was initially collected.

### **8.0 Limiting Collection**

C3 limits the collection of Personal Information to what's necessary, reasonable and relevant in light of the purposes for which it is collected. The *as little as possible* approach must be used. In this regard, exclusion of certain data fields or the use of anonymous data must be considered. Thus, any information used by C3 for statistical analysis will be made anonymous before accumulating and using it.

### **9.0 Accuracy**

C3 ensures that the Personal Information it collects is accurate, complete, and up to date for the purposes for which it is being used. Appropriate means are available to individuals to update or correct any inaccuracies to such information, including following up on an individual's requests to rectify processed information.

### **10.0 Storage Limitation**

Considering the nature of the information collected as well as the purposes for which it was collected, C3 will retain Personal Information only as long as necessary. Applicable

## CONFIDENTIAL

retention periods may vary and will be determined to allow C3 sufficient time to use the information for its original purpose, satisfy any legal or contractual requirements, and allow time for an individual to exercise his or her rights to access Personal Information under applicable laws.

After a fixed retention period, C3 will safely and permanently destroy, erase, or otherwise make anonymous the Personal Information it has collected. This will be performed in accordance with any contractual or legal obligation and C3's strict internal practices and procedures on the subject. C3 will always dispose of such information in a secure manner.

### **11.0 Disclosure to Third-Party**

C3 will not use nor disclose Personal Information collected on its own behalf for other purposes than those for which they were originally collected.

Nevertheless, C3 may disclose Personal Information without additional consent or notice from related individuals when and as required to comply with applicable laws or in response to a court order, government request, or other legal proceedings.

### **12.0 Integrity, Confidentiality and Safeguards**

C3 diligently protects any Personal Information under its control with the appropriate technical and organisational means against loss or theft, unauthorized access, alteration, disclosure or destruction and as such, ensures its safety and confidentiality. The applied safeguards may vary depending on the nature and sensitivity of the information to protect but are, at the least, what is required by applicable laws. C3's safeguards cover a wide range of activities, including but not limited to taking reasonable steps to ensure the discretion and reliability of C3 representatives having access to Personal Information. They refer to C3 policies as well as strict internal practices and procedures namely related to access control, application security, asset management, hardening protection, monitoring and responsiveness, business continuity plan and compliance. C3's safeguards may take the simple form of physical access restriction tools such as locked doors, alarm systems, locked filing cabinets, or the more complex form of organizational and technological tools such as IT authentication, access controls, firewalls, encryption, data segregation, electronic audit trails, up to date anti-virus/malware software, vendor security patch management, etc.

### **13.0 Individual Privacy Rights**

Individuals have various privacy rights such as the right to be informed and access their Personal Information, to rectify or erase it, to transfer it, to restrict its processing, to withdraw consent, etc. Upon request, C3 will promptly investigate the matter, act and take appropriate measures when needed (i.e. provide an individual with **access** to its own Personal Information held by C3 for its own purpose, **rectify** any inaccuracy, etc.). C3 will address the matter within a reasonable time of request (usually within a month), but only after due verification of identity. Nevertheless, C3 may refuse access requests for a number of legitimate reasons. If access is refused, C3 will provide in writing the reasons for refusal and the details on complaint procedures.

## CONFIDENTIAL

However, if C3 is only processing the related Personal Information on behalf of one of its Customer, C3 will assist such Customer and facilitate the individual's exercise of its privacy rights by promptly forwarding any such request to the Customer's Data Protection Officer, if any, or appropriate representative.

### 14.0 Data Transfers of Personal Information

C3 is a Canadian company with headquarters in Montreal (Canada). C3 customers as well as C3 solutions users can access their accounts from anywhere in the world. From C3's perspective, data, if any, will be transferred and stored by C3 in Canada. Canada is considered by the European Commission as providing an adequate level of protection of personal data transferred from the European Community to recipients (such as C3) subject to the Canadian Personal Information Protection and Electronic Documentation Act (PIPEDA). Thus, Customer Data transfers originating from the European Union, if any, are done under such adequacy decision.

Furthermore, C3 could transfer Personal Information to internal or third-party recipients located in another country where that country is also recognized as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. third countries), other specifically approved transfer mechanisms will be used such as European Commission's current Standard Contractual Clauses (SCC) for data transfers from the European Union to third countries.

### 15.0 General Inquiries & Concerns Related to this Policy

Any concern (inquiries, complaints or simple comments) related to this policy, its related practices and procedures as well as its compliance to applicable laws should be addressed to C3's Confidentiality and Security Team (CST) who will promptly channel, respond, investigate the matter and/or take appropriate measures when needed. **C3's CST** can be reached by C3 Employees via C3's internal communication system or by email at: [informationsecurity@c3solutions.com](mailto:informationsecurity@c3solutions.com); or by mail at: 1751 Richardson, Suite 4408, Montreal (Quebec) H3K 1G6 Canada

Furthermore, **C3's Data Protection Officer**, also effectively receives and responds to any related complaints and inquiries related to privacy and data protection. C3's DPO can be reached by phone at: +1 (514) 315-3139; by email at: [privacy@c3solutions.com](mailto:privacy@c3solutions.com) or by mail at: 1751 Richardson, Suite 4408, Montreal, QC H3K 1G6, Canada

For more general concerns on the privacy legislation in the private sector, the appropriate privacy authority should be contacted.

Location and Entity	Contact Information
Québec – Montréal <b>Commission de l'accès à l'information du Québec</b>	2045, rue Stanley, bureau 900 Montréal (Québec) H3A 2V4

	<p>Phone: (514) 873-4196</p> <p>Toll-free: 1 (888) 528-7741</p> <p>Fax: (514) 844-6170</p> <p>Email: <a href="mailto:renseignements@cai.gouv.qc.ca">renseignements@cai.gouv.qc.ca</a></p> <p>Web Site: <a href="http://www.cai.gouv.qc.ca/a-propos/nous-joindre">www.cai.gouv.qc.ca/a-propos/nous-joindre</a></p>
<p>Canada</p> <p><b>Office of the Privacy Commissioner of Canada</b></p>	<p>30, Victoria Street</p> <p>Gatineau (Quebec) K1A 1H3</p> <p>Toll-free: 1 (800) 282-1376</p> <p>Phone: (819) 994-5444</p> <p>TTY: (819) 994-6591</p> <p>Web site: <a href="http://www.priv.gc.ca">www.priv.gc.ca</a></p>
<p>EU</p> <p><b>European Data Protection Supervisor</b></p>	<p>Postal address: Rue Wiertz 60, B-1047 Brussels</p> <p>Office address: Rue Montoyer 30, B-1000 Brussels</p> <p>Phone: +32 2 283 19 00</p> <p>Fax: +32 2 283 19 50</p> <p>E-mail: <a href="mailto:edps@edps.europa.eu">edps@edps.europa.eu</a></p> <p>Web Site: <a href="http://www.edps.europa.eu">www.edps.europa.eu</a></p>
<p>Switzerland</p> <p><b>Federal Data Protection and Information Commissioner</b></p>	<p>Postal address: Feldeggweg, 1 CH - 3003 Bern,</p> <p>Tel. 058 462 43 95.</p> <p>Web site: <a href="http://www.edoeb.admin.ch">www.edoeb.admin.ch</a></p>
<p>United Kingdom</p> <p><b>Information Commissioner' Office</b></p>	<p>Phone: 0303 123 1113</p> <p>Website: <a href="https://ico.org.uk/">https://ico.org.uk/</a></p>
<p>Australia</p> <p><b>Australian Information Commissioner</b></p>	<p>Postal address: GPO Box 5218, Sydney NSW 2001</p>

CONFIDENTIAL

<b>(OAIC)</b>	Fax: 02 9284 9666 Email: <a href="mailto:enquiries@oaic.gov.au">enquiries@oaic.gov.au</a>
USA <b>American Government</b>	Phone: 1 (844) 872-4681 Web Site: <a href="http://www.usa.gov/privacy">www.usa.gov/privacy</a>

## Politique Générale de Confidentialité et de Protection des Données de C3 Solutions

### 1.0 Objectif et Portée

Dans le cadre de ses activités, C3 peut traiter (collecter, utiliser, stocker, divulguer, etc.) des données personnelles pour ses propres besoins légitimes ou au nom de ses clients, dans le cadre des Données Client. Les données personnelles (également appelées données à caractère personnel) peuvent être définies généralement comme toute information concernant une personne identifiée ou identifiable. Cela peut inclure des données personnelles concernant les représentants des clients et des fournisseurs, les contacts professionnels, les employés de C3 et toute autre personne avec laquelle C3 a une relation ou pourrait avoir besoin de contacter. Des exemples de données personnelles incluent (mais ne se limitent pas à) :

- Nom, date de naissance et numéro de sécurité sociale ou autre numéro de carte d'identité
- Coordonnées telles qu'adresse postale, adresse courriel et numéros de téléphone, numéros de carte de crédit et de compte bancaire
- Informations de santé ou médicales
- Informations contenues dans les dossiers des employés, y compris l'historique d'emploi et les évaluations
- Informations collectées au cours du processus de candidature et d'embauche
- Informations relatives aux avantages des employés, telles que les personnes à charge, les bénéficiaires et les informations sur les polices d'assurance

Les données correctement anonymisées, dépersonnalisées ou agrégées ne sont pas considérées comme des données personnelles.

Parce que C3 s'engage à protéger adéquatement les données personnelles et à se conformer aux lois applicables sur la protection de la vie privée et des données dans tous les pays où elle exerce ses activités, au lieu d'avoir plusieurs ensembles de règles, nous avons décidé d'appliquer les normes réglementaires les plus élevées pour traiter les données personnelles uniformément dans toutes nos activités, quelles que soient les exigences réglementaires, tout en respectant les exigences locales spécifiques en matière de confidentialité.

Cette politique explique comment C3 traite et protège généralement les données personnelles qu'elle gère. Elle fournit des directives obligatoires pour tous les représentants de C3.

## **2.0 Obligations générales en matière de confidentialité et de protection des données**

Tous les représentants, employés et sous-traitants de C3 doivent respecter cette politique et agir en conformité avec les lois applicables en matière de confidentialité et de protection des données, y compris la Loi canadienne sur la protection des renseignements personnels et les documents électroniques (LPRPDE), la Loi sur la protection des renseignements personnels dans le secteur privé au Québec et la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25), le Règlement général sur la protection des données (RGPD - Règlement (UE) 2016/679) et la California Consumer Privacy Act (CCPA), ainsi que la norme ISO 27001:2013 relative aux technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Exigences publiées par l'Organisation internationale de normalisation (ISO) et la (IEC). En ce faisant, ils respecteront la vie privée des autres employés de C3, des sous-traitants, des prospects, des clients et des personnes travaillant en leur nom, etc.

## **3.0 Responsabilités**

### **3.1 Équipe de confidentialité et de sécurité (CST) de C3**

Le Responsable de la sécurité des systèmes d'information (RSSI) de C3, avec l'Équipe de confidentialité et de sécurité (CST) de C3, développe, maintient, examine et veille à l'application de diverses politiques ainsi que de pratiques et procédures internes strictes conformes aux meilleures normes et pratiques de l'industrie et aux lois applicables en matière de confidentialité, afin de garantir que toutes les données de C3, y compris les données personnelles et/ou les données client, soient adéquatement protégées. Cependant, chaque représentant de C3 a une part de responsabilité afin de s'assurer que les données personnelles soient collectées, stockées et traitées de manière appropriée.

### **3.2 Responsabilités des employés et des départements de C3**

De plus, le CST de C3, en collaboration avec le département des ressources humaines de C3, veille à ce que chaque représentant de C3 soit informé de manière adéquate et comprenne toutes les politiques de C3 ainsi que les pratiques et procédures internes appropriées, conformément au programme de formation et de sensibilisation de C3.

Par ailleurs, la direction de chaque département de C3 doit s'assurer que tous les employés responsables du traitement des données personnelles soient informés du contenu de cette politique et s'y conforment. En outre, chaque département doit s'assurer que tous les tiers engagés pour traiter des données personnelles en leur nom (leurs sous-traitants), le cas échéant, soient informés du contenu de cette politique et s'y conforment. Une garantie de conformité doit être obtenue avant de leur accorder l'accès aux données personnelles contrôlées par C3.

### **3.3 Responsable de la protection des données (DPO)**

Pour renforcer son engagement envers la protection des données et accroître l'efficacité des efforts de conformité, C3 a nommé un Responsable de la protection des données (DPO).

## CONFIDENTIAL

Le Responsable de la protection des données opère avec rigueur et est soutenu par le CST de C3, dont il est membre. Le DPO rend compte directement au Chef de la Direction. Les responsabilités du DPO incluent :

- Informer et conseiller C3 et ses employés qui effectuent des activités de traitement des données personnelles conformément aux réglementations, lois provinciales, nationales ou dispositions de l'Union européenne en matière de protection des données, telles que : la collecte, le stockage, l'utilisation, la divulgation, la destruction.
- Veiller à l'alignement de cette politique sur les réglementations en matière de confidentialité et de protection des données, les lois provinciales, nationales ou les dispositions de l'Union européenne en matière de protection des données.
- Fournir, si nécessaire, des conseils concernant la réalisation des analyses d'impact sur la protection des données (DPIA).
- Agir en tant que point de contact et coopérer avec les Autorités de protection des données (DPA).
- Établir et faire fonctionner un système garantissant des réponses rapides et appropriées aux demandes des personnes concernées.
- Informer les cadres supérieurs, dirigeants et administrateurs de C3 des sanctions potentielles civiles, pénales et commerciales pouvant être imposées à C3 et/ou à ses employés en cas de violation des lois applicables en matière de confidentialité et de protection des données.
- Veiller à l'établissement de procédures et de dispositions contractuelles standards pour garantir la conformité à cette politique par tout tiers qui :
  - Fournit des données personnelles à C3.
  - Reçoit des données personnelles de C3.
  - A accès à des données personnelles collectées ou traitées par C3.
- Réaliser un audit annuel de conformité en matière de protection des données personnelles (comme décrit dans la section correspondante ci-après).
- Recevoir et répondre à toute plainte ou demande liée à la confidentialité et à la protection des données.

### *3.3.1 Surveillance de la conformité par le DPO*

Pour s'assurer qu'un niveau adéquat de conformité est atteint par tous les départements de C3 ainsi que par tout le Développement C3 (tel que défini dans la section 4 de cette politique) en matière de confidentialité et de protection des données, le Responsable de la protection des données (DPO) effectuera un audit annuel de conformité en matière de protection des données personnelles. Cet audit évaluera au minimum:

- La conformité aux politiques de C3 en matière de protection des données personnelles, incluant :
  - L'attribution des responsabilités.
  - La sensibilisation.

- La formation des employés.
- L'efficacité des pratiques opérationnelles liées à la protection des données personnelles, incluant :
  - Les droits des personnes concernées.
  - Les transferts de données personnelles.
  - La gestion des incidents liés aux données personnelles.
  - Le traitement des plaintes relatives aux données personnelles.
  - Le niveau de compréhension des politiques de protection des données et des avis de confidentialité.
  - L'actualité des politiques de protection des données et des avis de confidentialité.
  - L'exactitude des données personnelles stockées.
  - La conformité des activités des sous-traitants de données.
  - L'adéquation des procédures visant à corriger les cas de non-conformité et les violations de données personnelles.

Le Responsable de la protection des données, en collaboration avec les principaux acteurs commerciaux de C3, élaborera un plan avec un calendrier pour corriger les insuffisances identifiées dans un délai défini et raisonnable. Toute déficience majeure et toute bonne pratique identifiée seront rapportées, surveillées et partagées par le CST.

#### **4.0 Protection des données dès la conception**

Pour garantir que toutes les exigences en matière de protection des données soient identifiées et prises en compte lors de la conception de nouvelles fonctionnalités, solutions, systèmes ou processus significatifs de C3 et/ou lors de la révision ou de l'expansion de ceux existants (« **Développement C3** »), chaque Développement C3 doit passer par un processus d'approbation incluant une évaluation des risques. Si un Développement C3 entraîne de quelque manière que ce soit le traitement de données personnelles ou peut avoir un impact sur leur sécurité, le Responsable de la protection des données (DPO) doit être impliqué dans cette évaluation des risques.

De plus, si ce traitement de données personnelles, en particulier lorsqu'il fait appel à de nouvelles technologies, compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques, une Analyse d'impact relative à la protection des données (DPIA) doit être réalisée. Les conclusions de cette DPIA doivent ensuite être soumises au Chef de la Direction pour examen et approbation.

#### **5.0 Transparence et équité**

C3 traite les données personnelles de manière transparente et équitable. Les individus doivent être bien informés lorsqu'ils prennent des décisions concernant leurs données personnelles, et l'exercice de leurs droits en matière de confidentialité doit être aussi simple que possible.

## CONFIDENTIAL

Ainsi, C3 fournit des informations sur ses politiques et pratiques concernant la collecte, l'utilisation et/ou la divulgation des données personnelles, notamment par le biais de cette politique, et s'engage à répondre à toute plainte ou demande liée, ainsi qu'aux demandes d'accès.

En outre, au moment ou avant le traitement de toute donnée personnelle, C3 fournit un avis de confidentialité concis, transparent et compréhensible aux personnes concernées afin qu'elles soient conscientes du fait que des données personnelles seront traitées, y compris la manière dont elles seront collectées, conservées et utilisées. Cet avis de confidentialité est adapté à la nature de la relation entre C3 et l'individu ainsi qu'à la finalité pour laquelle le traitement est nécessaire. Cet avis de confidentialité de C3 doit inclure, entre autres, les informations spécifiques suivantes dans un langage clair et simple : les coordonnées de C3, la finalité et la base légale du traitement, les destinataires possibles, les éventuels transferts de données, la durée de conservation, les divers droits de l'individu concernant ces données personnelles, etc.

De plus, chaque site web externe fourni par C3 inclura un « Avis de confidentialité » en ligne et un « Avis sur les cookies » en ligne répondant aux exigences légales.

### **6.0 Base légale du traitement**

C3 ne traitera les données personnelles pour ses propres besoins que si une base légale appropriée est établie. Les bases légales peuvent inclure le consentement, l'exécution d'un contrat, les obligations légales, les intérêts vitaux des individus, l'intérêt public et l'intérêt légitime.

Si C3 traite des données personnelles sur la base du consentement, la forme du consentement demandé avant de collecter, utiliser ou divulguer les données personnelles peut varier en fonction des circonstances et du type de données. Le consentement peut inclure un consentement explicite oral ou écrit, un consentement implicite ou un consentement par non-participation. Les lois applicables, la sensibilité des données et les attentes raisonnables des individus seront pris en compte pour déterminer comment le consentement doit être donné.

C3 obtiendra tout consentement requis avant d'utiliser des données personnelles à des fins autres que celles pour lesquelles elles ont été initialement collectées.

### **7.0 Limitation des finalités**

C3 traitera les données personnelles en son nom de manière responsable et uniquement à des fins légitimes spécifiquement identifiées, telles que communiquées aux individus. C3 ne traitera pas les données personnelles au-delà de ces finalités, sauf si un traitement supplémentaire peut être considéré comme compatible avec les finalités initiales pour lesquelles les données personnelles ont été collectées.

## **8.0 Limitation de la collecte**

C3 limite la collecte des données personnelles à ce qui est nécessaire, raisonnable et pertinent au regard des finalités pour lesquelles elles sont collectées. L'approche du « minimum nécessaire » doit être appliquée. À cet égard, l'exclusion de certains champs de données ou l'utilisation de données anonymes doit être envisagée. Ainsi, toute information utilisée par C3 à des fins d'analyse statistique sera rendue anonyme avant son accumulation et son utilisation.

## **9.0 Exactitude**

C3 veille à ce que les données personnelles qu'elle collecte soient exactes, complètes et à jour pour les finalités pour lesquelles elles sont utilisées. Des moyens appropriés sont mis à disposition des individus pour mettre à jour ou corriger toute inexactitude dans ces informations, y compris le suivi des demandes des individus pour rectifier les données traitées.

## **10.0 Limitation du stockage**

Compte tenu de la nature des informations collectées ainsi que des finalités pour lesquelles elles ont été collectées, C3 conservera les données personnelles uniquement aussi longtemps que nécessaire. Les périodes de conservation applicables peuvent varier et seront déterminées pour permettre à C3 d'utiliser les informations pour leur finalité initiale, de satisfaire à toute exigence légale ou contractuelle et de laisser suffisamment de temps à un individu pour exercer ses droits d'accès aux données personnelles en vertu des lois applicables.

Après une période de conservation déterminée, C3 détruira, effacera ou rendra anonymes de manière sécurisée et permanente les données personnelles collectées. Cela sera effectué conformément à toute obligation contractuelle ou légale et aux pratiques et procédures internes strictes de C3 sur le sujet. C3 s'assurera toujours d'éliminer ces informations de manière sécurisée.

## **11.0 Divulgence à des tiers**

C3 n'utilisera ni ne divulguera les données personnelles collectées pour son propre compte à d'autres fins que celles pour lesquelles elles ont été initialement collectées.

Néanmoins, C3 peut divulguer des données personnelles sans consentement supplémentaire ou avis des personnes concernées lorsque cela est requis pour se conformer aux lois applicables ou en réponse à une ordonnance judiciaire, une demande gouvernementale ou d'autres procédures légales.

## **12.0 Intégrité, confidentialité et mesures de protection**

C3 protège avec diligence toute donnée personnelle sous son contrôle en utilisant des moyens techniques et organisationnels appropriés contre la perte ou le vol, l'accès non autorisé, l'altération, la divulgation ou la destruction, garantissant ainsi leur sécurité et leur

## CONFIDENTIAL

confidentialité. Les mesures de protection appliquées peuvent varier en fonction de la nature et de la sensibilité des informations à protéger, mais elles respectent au minimum ce qui est requis par les lois applicables. Les mesures de protection de C3 couvrent un large éventail d'activités, notamment prendre des mesures raisonnables pour garantir la discrétion et la fiabilité des représentants de C3 ayant accès aux données personnelles. Faire référence aux politiques de C3 ainsi qu'à des pratiques et procédures internes strictes, telles que le contrôle d'accès, la sécurité des applications, la gestion des actifs, le renforcement de la protection, la surveillance et la réactivité, le plan de continuité des activités et la conformité. Les mesures de protection de C3 peuvent être simples, comme des outils de restriction d'accès physique (portes verrouillées, systèmes d'alarme, armoires verrouillées), ou plus complexes, comme des outils organisationnels et technologiques (authentification informatique, contrôles d'accès, pare-feu, chiffrement, séparation des données, pistes d'audit électroniques, logiciels anti-virus/malware à jour, gestion des correctifs de sécurité des fournisseurs, etc.).

### **13.0 Droits individuels en matière de confidentialité**

Les individus disposent de divers droits en matière de confidentialité, tels que le droit d'être informés et d'accéder à leurs données personnelles, de les rectifier ou de les effacer, de les transférer, de restreindre leur traitement, de retirer leur consentement, etc. Sur demande, C3 enquêtera rapidement sur la question, agira et prendra les mesures appropriées si nécessaire (par exemple, fournir à un individu l'accès à ses propres données personnelles détenues par C3 à ses propres fins, rectifier toute inexactitude, etc.). C3 traitera la demande dans un délai raisonnable (généralement dans un mois), mais uniquement après une vérification appropriée de l'identité. Cependant, C3 peut refuser des demandes d'accès pour certaines raisons légitimes. En cas de refus, C3 fournira par écrit les raisons du refus ainsi que les détails sur les procédures de plainte.

Néanmoins, si C3 ne traite les données personnelles concernées qu'au nom de l'un de ses Clients, C3 assistera ce Client et facilitera l'exercice des droits de confidentialité de l'individu en transmettant rapidement toute demande au Responsable de la protection des données du Client, s'il en existe un, ou au représentant approprié.

### **14.0 Transferts de données personnelles**

C3 est une entreprise canadienne dont le siège social est situé à Montréal (Canada). Les clients de C3 ainsi que les utilisateurs des solutions C3 peuvent accéder à leurs comptes depuis n'importe où dans le monde. Du point de vue de C3, les données, le cas échéant, seront transférées et stockées par C3 au Canada. Le Canada est considéré par la Commission européenne comme offrant un niveau adéquat de protection des données personnelles transférées depuis la Communauté européenne à des destinataires (tels que C3) soumis à la Loi canadienne sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Ainsi, les transferts de données clients provenant de l'Union européenne, le cas échéant, sont effectués sous cette décision d'adéquation.

De plus, C3 pourrait transférer des données personnelles à des destinataires internes ou tiers situés dans un autre pays lorsque ce pays est également reconnu comme offrant un

niveau adéquat de protection juridique des droits et libertés des personnes concernées. Lorsque des transferts doivent être effectués vers des pays ne disposant pas d'un niveau adéquat de protection juridique (c'est-à-dire des pays tiers), d'autres mécanismes de transfert spécifiquement approuvés seront utilisés, tels que les clauses contractuelles types actuelles (SCC) de la Commission européenne pour les transferts de données de l'Union européenne vers des pays tiers.

## 15.0 Questions générales et préoccupations liées à cette politique

Toute préoccupation (questions, plaintes ou simples commentaires) liée à cette politique, à ses pratiques et procédures connexes ainsi qu'à sa conformité aux lois applicables doit être adressée à l'Équipe de confidentialité et de sécurité (CST) de C3, qui acheminera rapidement, répondra, enquêtera sur la question et/ou prendra les mesures appropriées si nécessaire. L'équipe CST de C3 peut être contactée par les employés de C3 via le système de communication interne de C3 ou par courriel à : [informationsecurity@c3solutions.com](mailto:informationsecurity@c3solutions.com) ; ou par courrier à l'adresse suivante : 1751 Richardson, Suite 4408, Montréal (Québec) H3K 1G6 Canada.

De plus, le **Responsable de la protection des données (DPO)** de C3 reçoit et répond également efficacement à toute plainte ou question liée à la confidentialité et à la protection des données. Le DPO de C3 peut être contacté par téléphone au : +1 (514) 315-3139 ; par courriel à : [privacy@c3solutions.com](mailto:privacy@c3solutions.com) ou par courrier à l'adresse suivante : 1751 Richardson, Suite 4408, Montréal (Québec) H3K 1G6 Canada.

Pour toute préoccupation plus générale concernant la législation sur la confidentialité dans le secteur privé, l'autorité compétente en matière de confidentialité devrait être contactée.

Lieu et entité	Coordonnées
<p>Québec – Montréal</p> <p><b>Commission de l'accès à l'information du Québec</b></p>	<p>2045, rue Stanley, bureau 900</p> <p>Montréal (Québec) H3A 2V4</p> <p>Téléphone: (514) 873-4196</p> <p>Sans-frais: 1 (888) 528-7741</p> <p>Télécopieur: (514) 844-6170</p> <p>Courriel: <a href="mailto:renseignements@cai.gouv.qc.ca">renseignements@cai.gouv.qc.ca</a></p> <p>Site Web: <a href="http://www.cai.gouv.qc.ca/a-propos/nous-joindre">www.cai.gouv.qc.ca/a-propos/nous-joindre</a></p>
<p>Canada</p> <p><b>Commissariat à la protection de la vie privée du Canada</b></p>	<p>30, rue Victoria</p> <p>Gatineau (Québec) K1A 1H3</p> <p>Sans-frais: 1 (800) 282-1376</p>

	<p>Téléphone: (819) 994-5444</p> <p>ATS: (819) 994-6591</p> <p>Site Web: <a href="http://www.priv.gc.ca">www.priv.gc.ca</a></p>
<p>UE</p> <p><b>Contrôleur européen de la protection des données</b></p>	<p>Adresse postale: Rue Wiertz 60, B-1047 Bruxelles</p> <p>Adresse de bureau: Rue Montoyer 30, B-1000 Bruxelles</p> <p>Téléphone: +32 2 283 19 00</p> <p>Télécopieur: +32 2 283 19 50</p> <p>Courriel: <a href="mailto:edps@edps.europa.eu">edps@edps.europa.eu</a></p> <p>Site Web: <a href="http://www.edps.europa.eu">www.edps.europa.eu</a></p>
<p>Suisse</p> <p><b>Préposé fédéral à la protection des données et à la transparence</b></p>	<p>Adresse postale: Feldeggweg, 1 CH - 3003 Bern,</p> <p>Tel. 058 462 43 95.</p> <p>Site Web: <a href="http://www.edoeb.admin.ch">www.edoeb.admin.ch</a></p>
<p>Royaume-Uni</p> <p><b>Bureau du Commissaire à l'information (ICO)</b></p>	<p>Téléphone: 0303 123 1113</p> <p>Site Web: <a href="https://ico.org.uk/">https://ico.org.uk/</a></p>
<p>Australie</p> <p><b>Commissaire à l'information australien (OAIC)</b></p>	<p>Adresse postale: GPO Box 5218, Sydney NSW 2001</p> <p>Télécopieur: 02 9284 9666</p> <p>Courriel: <a href="mailto:enquiries@oaic.gov.au">enquiries@oaic.gov.au</a></p>
<p>USA</p> <p><b>Gouvernement américain</b></p>	<p>Téléphone: 1 (844) 872-4681</p> <p>Site Web: <a href="http://www.usa.gov/privacy">www.usa.gov/privacy</a></p>