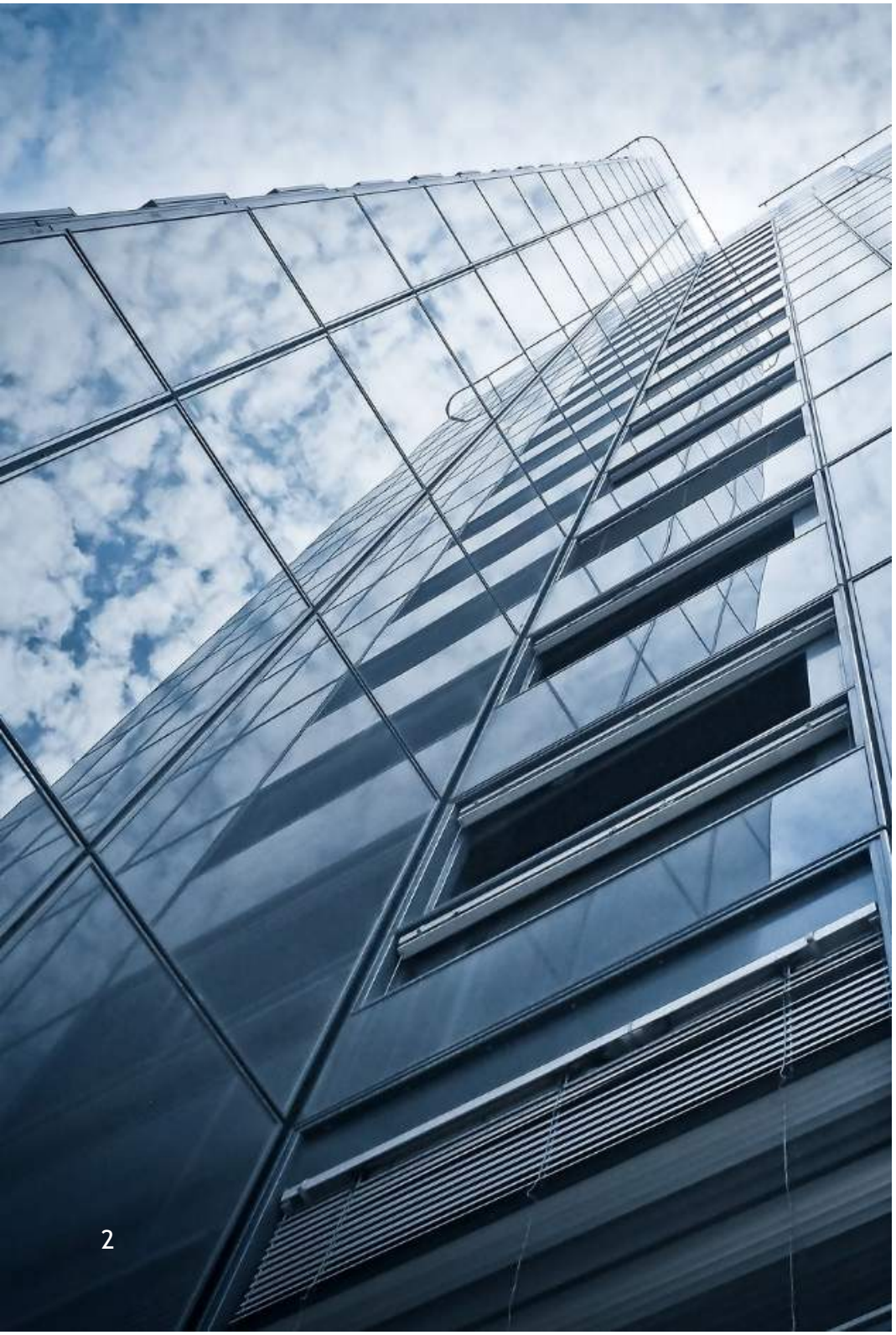
TRUCS ET ASTUCES POUR SURVIVRE À LA LOI 25

Présenté par
Me Nicolas Lassonde
Me Julien Ruchon
Le 25 octobre 2023



SOMMAIRE

- Introduction - survol du RGPD
- Aperçu de la nouvelle Loi QC
- Qu’est-ce qu’un renseignement personnel?
- Survol des principales obligations pour les entreprises
- Comment se préparer
- Questions

LJT AVOCATS

Le « *RGPD* »

- Le Règlement général sur la protection des données (RGPD) est un règlement qui **harmonise** les lois nationales de protection des données au sein de l'Union européenne (UE) et qui **renforce** la protection de tous les résidents de l'UE en ce qui a trait à la confidentialité de leurs données personnelles.
- Cette harmonisation crée de nouveaux droits pour les particuliers de même qu'un ensemble de règles plus strictes et plus claires pour les entreprises.
- Le RGPD s'**applique** à toutes les entreprises qui traitent les données personnelles de résidents de l'UE, y compris les entreprises établies à l'extérieur de l'UE si elles offrent des biens ou des services à des résidents de l'UE, ou suivent leur comportement.
- Le RGPD est entré en vigueur le **25 mai 2018**.

Nouveautés depuis le RGPD

- Mise à jour des définitions importantes (données personnelles, consentement)
- Imputabilité des entreprises (« *accountability* »)
- Renforcer et clarifier les droits des personnes concernées
- 2 principes clés:
  A) Minimisation des données
  B) « *Privacy by Design* »

APERÇU DE LA NOUVELLE LOI QUÉBÉCOISE

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (projet de loi n. 64, devenu la Loi 25) a été adoptée officiellement le 21 septembre 2021.

Elle vient modifier plusieurs lois, dont la *Loi sur la protection des renseignements personnels dans le secteur privé*.

LJT
AVOCATS

APERÇU DE LA NOUVELLE LOI QUÉBÉCOISE

Le Québec est la première province canadienne à avoir entrepris une réforme majeure de ses lois en matière de protection des renseignements personnels.

L'objectif était d'instaurer un régime plus strict afin de mieux protéger les renseignements personnels des québécois en responsabilisant les entreprises privées, les ministères et organismes face aux renseignements personnels qu'ils détiennent.

Influence claire du RGPD.

LJT
AVOCATS

APERÇU DE LA NOUVELLE LOI

La Loi 25 s’est d’ailleurs inspiré à plusieurs égards du RGPD et se rapproche donc de l’approche européenne.

L’entrée en vigueur se fera progressivement, en trois temps:

- septembre 2022;
- **septembre 2023;** et
- septembre 2024.

La grande majorité des modifications entreront en vigueur le **22 septembre 2023**, soit deux ans après la date de sanction de la Loi.

LJT
AVOCATS

SANCTIONS ET AMENDES

Trois mécanismes sont introduits:

- des sanctions administratives pécuniaires pouvant aller jusqu'à 10 000 000$ ou 2% du chiffre d'affaires mondial
- des sanctions pénales pouvant aller jusqu'à 25 000 000$ ou 4% du chiffre d'affaires mondial
- un droit privé d'action, fondé sur le régime général de la responsabilité civile

- Entrée en vigueur des sanctions administratives et pénales dès septembre 2023

LJT AVOCATS

DÉFINITION DE RENSEIGNEMENT PERSONNEL

« Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier. »

Les renseignements personnels sont les données qui concernent un individu identifiable.

Il s'agit de renseignements qui, seuls ou jumelés à d'autres données, permettent de vous identifier en tant qu'individu.

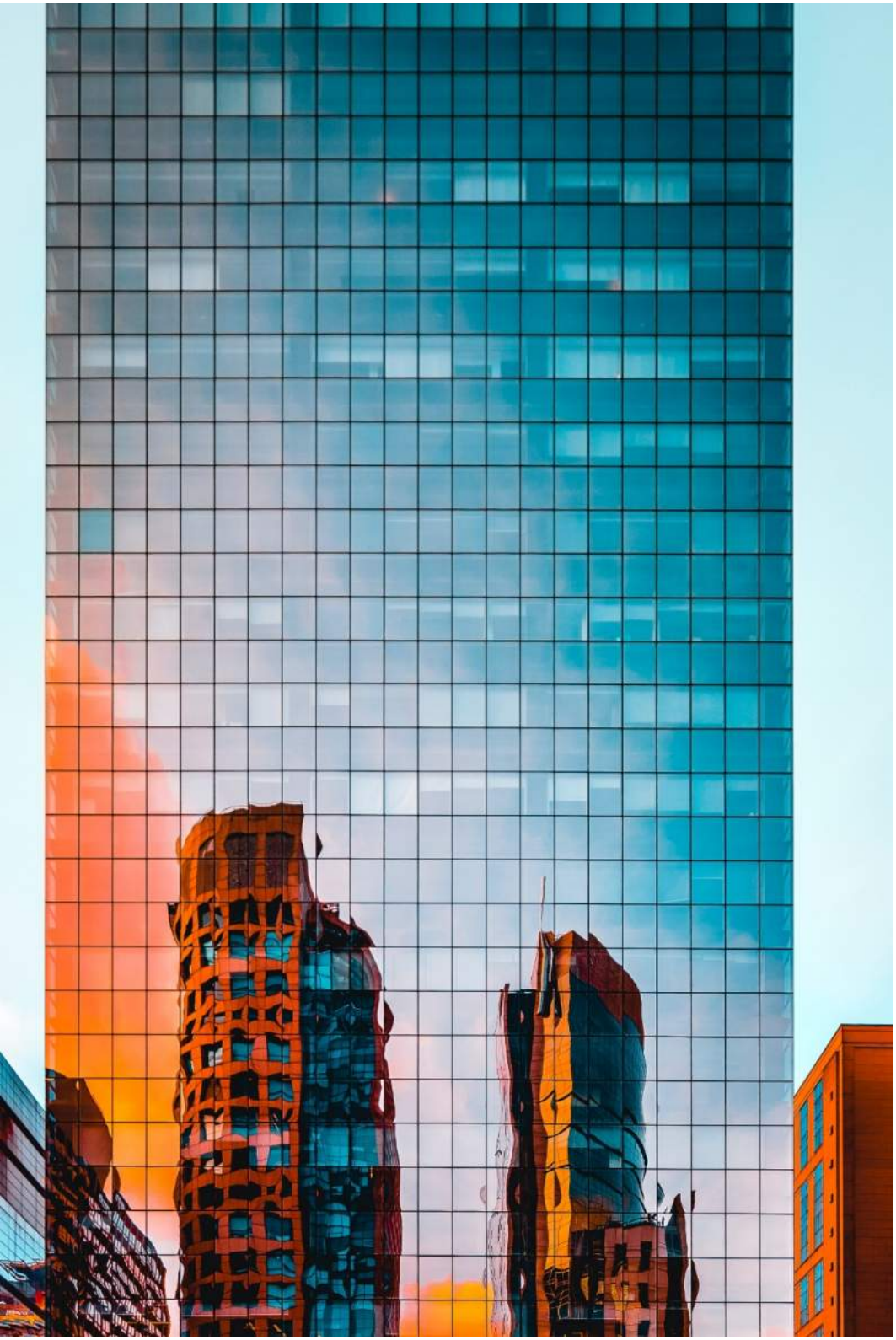
LJT AVOCATS

DÉFINITION DE RENSEIGNEMENT PERSONNEL

Il peut s'agir de renseignements qui portent sur :

- votre race, votre nationalité ou votre origine ethnique;
- votre religion;
- votre âge ou votre état civil;
- vos antécédents médicaux, scolaires ou professionnels;
- vos transactions financières;
- votre ADN;
- les numéros permettant de vous identifier (p. ex. numéro d'assurance sociale ou numéro de permis de conduire);
- Etc.

LJT
AVOCATS



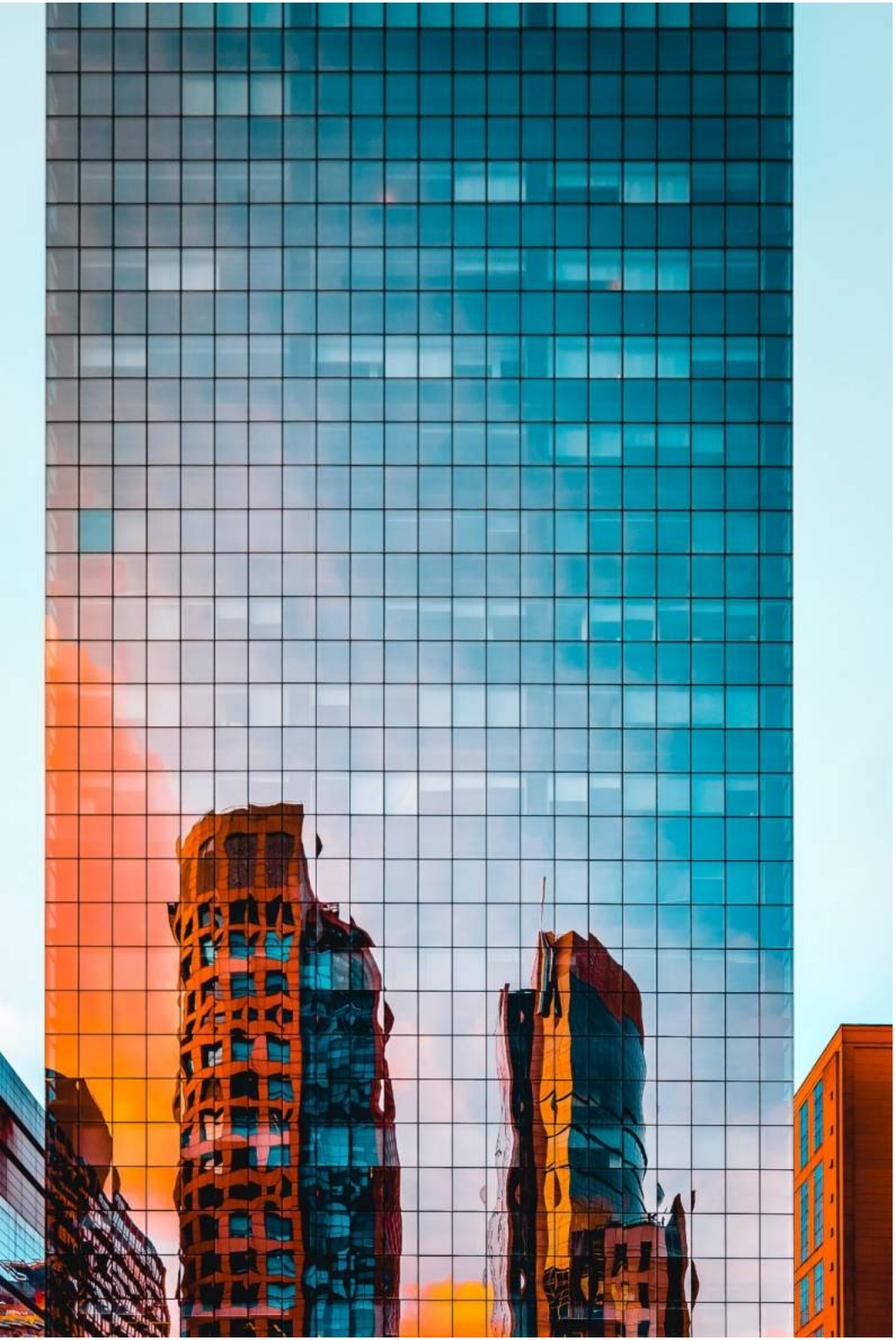
SURVOL DES OBLIGATIONS POUR LES ENTREPRISES

DISPOSITIONS ENTRANT EN VIGUEUR LE 22 SEPTEMBRE 2022

- Désignation d'un **responsable de la protection des renseignements personnels** au sein de l'entreprise et publier le titre et les coordonnées de cette personne sur le site internet de l'entreprise;

- **Signalement des incidents** de confidentialité avec risque de « préjudice sérieux » à la Commission d'accès à l'information (CAI) et tenir un registre des incidents.

LJT
AVOCATS



SURVOL DES OBLIGATIONS POUR LES ENTREPRISES

Qu’est-ce qu’un risque de préjudice sérieux?

Pas de définition dans la loi.

La loi énonce toutefois les facteurs à considérer pour évaluer le niveau de gravité:

1) La sensibilité des renseignements en cause. Les renseignements qui, en raison de leur nature (ex. médicale, financière, biométrique, etc.) ou du contexte de leur utilisation, feront croître le risque de préjudice;

2) Les conséquences appréhendées de leur utilisation. (renseignements susceptibles d’être utilisés pour commettre une fraude ou un vol d’identité)

3) La probabilité qu’ils soient utilisés à des fins préjudiciables (par exemple, en cas de demandes de rançons, si les données sont publiées sur le Dark Web).

LJT
AVOCATS

SURVOL DES OBLIGATIONS POUR LES ENTREPRISES

DISPOSITIONS ENTRANT EN VIGUEUR EN **SEPTEMBRE 2023**

- Mettre en œuvre des **politiques et des pratiques de gouvernance** propres à assurer la protection des renseignements personnels.

- Des informations au sujet de ces politiques et pratiques devront être publiées sur le site internet de l'entreprise en termes clairs et simples

- Lors de toute collecte de données, les personnes concernées devront être informés des fins de la collecte, des moyens de la collecte, des droits d'accès et de rectification et du droit de retirer son consentement.

SURVOL DES OBLIGATIONS POUR LES ENTREPRISES

DISPOSITIONS ENTRANT EN VIGUEUR EN **SEPTEMBRE 2023**

- **Consentement de la personne concernée**
  - Un renseignement personnel ne peut être utilisé qu'aux fins pour lesquelles il a été recueilli, à moins du consentement de la personne concernée.

  - Un consentement doit **être manifeste, libre, éclairé et être donné à des fins spécifiques** et ne vaut que pour la durée nécessaire à la réalisation des fin auxquelles il a été demandé.

  - Le consentement doit être **manifesté de façon expresse** dès qu'il s'agit d'un **renseignement personnel sensible** de par sa nature (médicale, biométrique ou autrement intime, haut degré d'attente raisonnable en matière de vie privée)

SURVOL DES OBLIGATIONS POUR LES ENTREPRISES

DISPOSITIONS ENTRANT EN VIGUEUR EN **SEPTEMBRE 2023**

- Informer la personne concernée lorsqu'elle fait l'objet d'une **décision fondée exclusivement sur un traitement automatisé** de ses renseignements personnels
  - Il doit être donné à la personne concernée l'occasion de présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision

- Avoir une **entente écrite** avec les fournisseurs de services ou mandataires
  - Une entreprise pourra communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise
    - Par écrit
    - Prévoir les mesures de protection des renseignements personnels communiqués

SURVOL DES OBLIGATIONS POUR LES ENTREPRISES

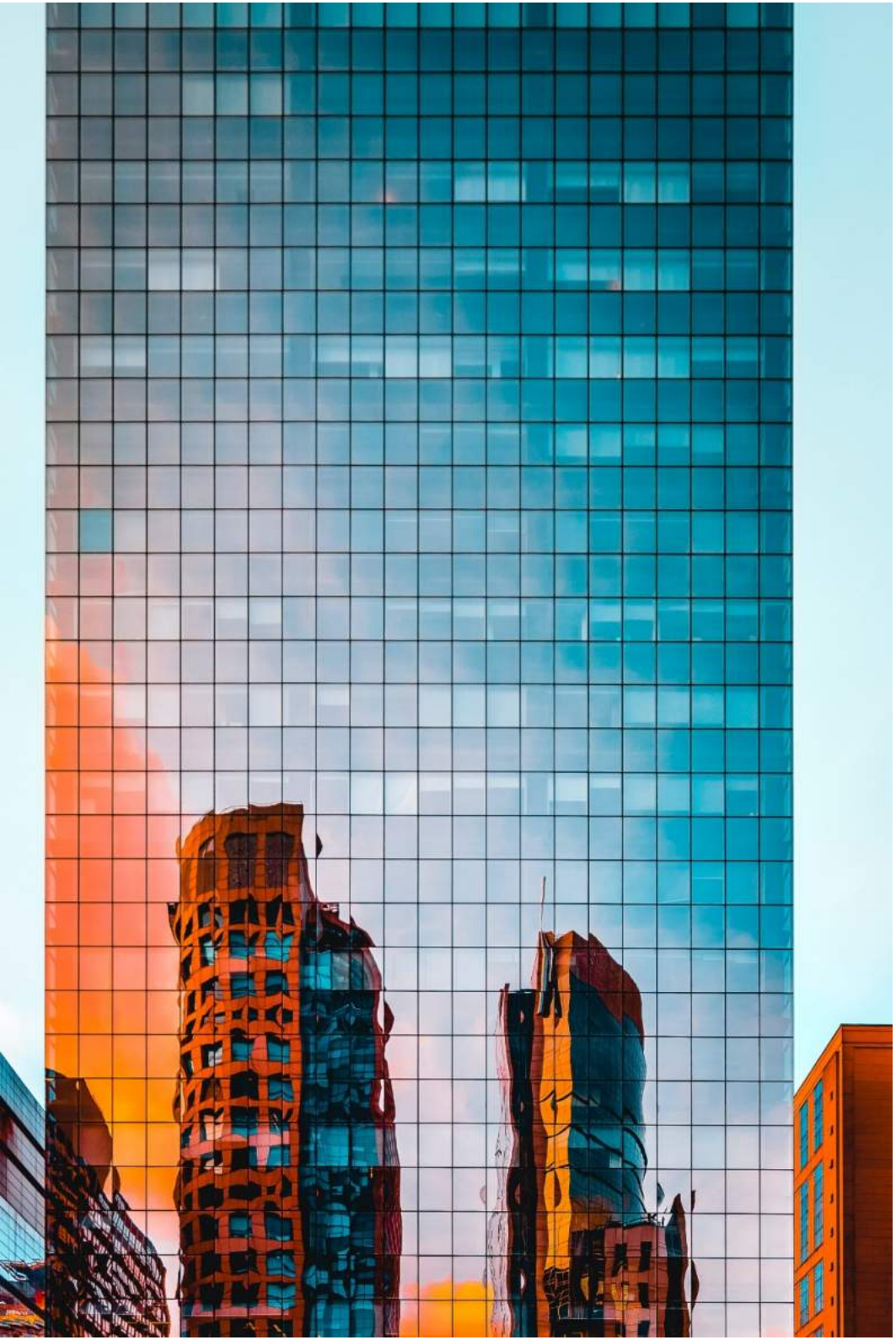
DISPOSITIONS ENTRANT EN VIGUEUR EN **SEPTEMBRE 2023**

- Procéder à des évaluations des facteurs relatifs à la vie privée (EFVP)
  - Des EFVP devront avoir lieu avant d'entreprendre tout projet ou prestation de services impliquant le traitement de de renseignements personnels;
  - Avant de transférer des renseignements à l'extérieur du Québec

- Droit à la désindexation (ou « droit à l'oubli »)
  - Il s'agit du droit pour un individu de limiter la diffusion publique de ses renseignements personnels, à certaines conditions

- Obligation de destruction ou anonymisation des données lors fins accomplies

- Offrir le plus haut niveau de confidentialité par défaut



SURVOL DES OBLIGATIONS POUR LES ENTREPRISES

DISPOSITION ENTRANT EN VIGUEUR EN **SEPTEMBRE 2024**

- Droit à la **portabilité des données**
  - Les entreprises devront, à la demande de la personne concernée, lui confirmer l'existence d'un renseignement personnel et lui donner communication de ce renseignement en lui permettant d'en obtenir une copie.
  - Communiqué sous la forme d'une **transcription écrite et intelligible**, dans un **format technologique structuré et couramment utilisé**.

COMMENT SE PRÉPARER

Les entreprises visées devraient dès maintenant entreprendre des démarches pour assurer leur conformité à la loi:

- Nommer un responsable de la protection de la vie privée et définir ses responsabilités;
- Faire un audit des politiques et des pratiques actuelles de l'entreprise;
- Évaluer les mesures de protection de la vie privée en place actuellement;
- Revoir les contrats conclus avec les fournisseurs de services;
- Implanter des processus afin de permettre aux individus d'exercer le droit à la portabilité des données, le droit à l'oubli et le droit d'être informé d'une prise de décision fondée exclusivement sur un traitement automatisé, lorsqu'applicable;
- Etc.

LJT AVOCATS

À retenir : 2 impacts clés

A) MINIMISATION DES DONNÉES

- Passer d'une logique quantitative à une logique qualitative: Plus les quantités de données collectées sont importantes, plus importants sont les risques. Une gestion optimale des risques implique de se recentrer sur les données les plus pertinentes et les plus récentes, sur les données nécessaires à l'atteinte des objectifs d'affaires. C'est ce que le règlement GDPR appelle la « minimisation des données ». La notion est mentionnée à plusieurs reprises dans le texte.

- Pour les entreprises, la minimisation des données impliquent de :

  a. Recenser toutes les données à disposition de manière systématique.

  b. Nettoyer la base de données : faire le tri dans les données et supprimer les données inutiles ou périmées.

  c. Revoir la stratégie de collecte de données en se recentrant sur les données créatrices de valeur.

➢ Le premier impact « global » réside bien là : forcer les entreprises à se doter d'une nouvelle philosophie de la data. Le GDPR oblige les entreprises à rationaliser leur collecte et leur traitement des données à caractère personnel.

À retenir : 2 impacts clés

B) « PRIVACY BY DESIGN »

- Pas nécessairement une approche ou méthode nouvelle, mais maintenant rendu obligatoire (*article 25 RGPD*)

- Approche qui consiste à se préoccuper des enjeux de **protection de la vie privée** – et donc des données personnelles numériques – **dès la phase de « design »**, c'est-à-dire dès la conception d'un produit (ou d'un service). Une application, par exemple, devra respecter les exigences du GDPR dès le jour de son lancement. La protection des données ne pourra plus être considérée comme un à-côté, comme un « add-on »

- Implique de faire de la protection des données une **priorité absolue**, prise en compte tout en amont des phases de développement des produits ou services. Dans la pratique, l'approche « *Privacy By Design* » consiste, pour le responsable des traitements, à mettre en œuvre des « mesures techniques et organisationnelles appropriées », comme par exemple la pseudonymisation, qui permet de dissocier les données des personnes physiques auxquelles elles sont rattachées.

- Il s'agit aussi de garantir que, par défaut (*Privacy By Default*), seules les données personnelles nécessaires aux objectifs du traitement seront traitées.

- Illustration: Barnett c. Apple Inc. (Illinois)
    - *Décision américaine concernant le* Biometric Information Privacy Act *rendue le 23 décembre 2022*
    - *Recours collectif pour la collecte des informations biometriques dans le cadre de* Face ID *et* Touch ID

COMMENT SE PRÉPARER

Objectifs globaux (RGDP + Loi québécoise):

1) Adopter une approche de la protection des données fondée sur le risque (minimisation, « *privacy by design* »)

2) S'assurer que des politiques et procédures appropriées sont en place pour assurer la transparence, la responsabilité et les droits des individus.

3) Créer une culture d'entreprise mettant de l'avant la confidentialité et la sécurité des données.

LJT AVOCATS

LJT
AVOCATS

MERCI

LJT Avocats
Me Nicolas Lassonde
nicolas.lassonde@ljt.ca

Me Julien Ruchon
julien.ruchon@ljt.ca

380, rue Saint-Antoine Ouest, Bureau 7100
Montréal (Québec) H2Y 3X7
Tél. : 514 842-8891 | Fax : 514 842-6202 | ljt.ca

LJT
AVOCATS