Projet de règlement sur le télétravail dans l'administration cantonale

Avis du 7 juin 2022

Mots clés : veille réglementaire, télétravail, données personnelles, données personnelles sensibles, sécurité numérique, confidentialité.

Contexte : Le 31 mai 2022, le Département des finances et des ressources humaines (DF) a requis l'avis du Préposé cantonal à la protection des données et à la transparence (ci-après le Préposé cantonal) au sujet d'un projet de règlement sur le télétravail dans l'administration cantonale. Les art. 14 al. 1, 17 et 18 du projet ont trait à la protection des données personnelles, particulièrement aux services et outils numériques, à la confidentialité et à la sécurité de l'information.

Bases juridiques : art. 56 al. 3 litt. e LIPAD; art. 23 al. 8 RIPAD

1. Caractéristiques de la demande

Par courriel du 31 mai 2022, le Département des finances et des ressources humaines (DF) a requis l'avis du Préposé cantonal à la protection des données et à la transparence (ci-après le Préposé cantonal) au sujet d'un projet de règlement sur le télétravail dans l'administration cantonale. L'avis du Préposé cantonal est souhaité pour le 7 juin 2022. Sont joints au courriel le projet de règlement susmentionné, ainsi qu'un tableau comparatif contenant des commentaires par disposition.

Les dispositions ayant trait à la protection des données personnelles sont les suivantes :

Art. 14 Services et outils numériques

[1] Le membre du personnel doit, cas échéant, télétravailler en n'utilisant que les services numériques que l'employeur lui a fournis ou dont ce dernier a validé l'usage.

Art. 17 Secret de fonction, sécurité de l'information et protection des données

[1] Dans son espace de télétravail, le membre du personnel doit garantir le secret de fonction, la sécurité de l'information, ainsi que la protection des données vis-à-vis de tout tiers non autorisé qui peut accéder à son espace de travail, y compris des membres de sa famille.

[2] Le membre du personnel doit, notamment :

a) protéger les données et les documents contre tout accès non autorisé et tout vol;

b) empêcher qu'ils soient lus, copiés ou modifiés par des tiers non autorisés;

c) prendre toute mesure utile afin que les services et outils numériques que l'office cantonal des systèmes d'information et du numérique a mis à sa disposition ne soient pas utilisés par un tiers non autorisé, y compris les membres de sa famille, ni qu'ils soient endommagés ou volés.

[3] Le membre du personnel doit effacer de ses moyens numériques privés toute donnée professionnelle dès qu'il n'en a plus besoin mais, au plus tard, à la fin de l'accord de télétravail ou des rapports de service.

Le commentaire relatif à cette disposition précise que toutes les directives relatives à la sécurité de l'information ainsi qu'à la protection des données au sein de l'administration cantonale s'appliquent.

Art. 18 Restrictions au télétravail

[1] Le membre du personnel n'a pas le droit de télétravailler à l'étranger, sauf si c'est pour accéder occasionnellement aux services et outils numériques, et pour autant que le pays de séjour ait un niveau de protection des données adéquat. L'alinéa 3 est réservé.

[2] Le membre du personnel de nationalité suisse peut télétravailler en France métropolitaine, sous réserve de l'alinéa 3.

[3] Le membre du personnel de l'administration fiscale cantonale n'a pas le droit de traiter des données fiscales à l'étranger.

Les précisions suivantes sont apportées par le tableau comparatif : « *Ad al. 1 : l'interdiction de télétravailler à l'étranger est dictée pour des raisons fiscales. La liste des pays "sûrs" peut être consultée sur le site Internet du Préposé fédéral à la protection des données.*

Ad. al. 2 : L'interdiction de télétravailler à l'étranger, et particulièrement en France, sera reconsidérée en cas de modification des dispositions fiscales applicables afin de permettre de conserver l'imposition en Suisse de la rémunération correspondant aux jours de télétravail en dessous d'un certain seuil.

Ad. al. 3 : l'interdiction de télétravailler à l'étranger s'appliquant uniquement si les membres du personnel de l'administration fiscale ont à traiter des données fiscales ».

2. Les dispositions légales pertinentes

La loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 (LIPAD ; RSGe A 2 08) a fait l'objet d'une révision importante en 2008, par laquelle la protection des données personnelles a été ajoutée au champ d'application matériel de la loi en sus de son volet relatif à la transparence.

Depuis le 1er janvier 2010, date de l'entrée en vigueur de cette modification législative, un autre objectif figure désormais dans le texte légal à son art. 1 al. 2 litt. b : *« protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant »*.

Par données personnelles, il faut comprendre *« toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable »* (art. 4 litt. a LIPAD).

Par donnée personnelle sensible, la loi vise les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles ; la santé, la sphère intime ou l'appartenance ethnique ; des mesures d'aide sociale ; des poursuites ou sanctions pénales ou administratives (art. 4 litt. b LIPAD).

La LIPAD énonce un certain nombre de principes généraux régissant la collecte et le traitement des données personnelles (art. 35 à 40 LIPAD).

- Base légale (art. 35 LIPAD)

  Le traitement de données personnelles ne peut se faire que si l'accomplissement des tâches légales de l'institution publique le rend nécessaire. En outre, la loi stipule que lorsqu'il s'agit de traiter de données personnelles sensibles ou de profils de la personnalité, la tâche considérée doit soit être définie clairement par la loi, soit être absolument indispensable à l'accomplissement de la tâche en cause soit encore être nécessaire et, si c'est le cas, intervenir avec le consentement – libre et éclairé – de la personne concernée.

- Bonne foi (art. 38 LIPAD)

  Il n'est pas permis de collecter des données personnelles sans que la personne concernée en ait connaissance, ni contre son gré. Quiconque trompe la personne concernée

lors de la collecte des données – par exemple en collectant les données sous une fausse identité ou en donnant de fausses indications sur le but du traitement – viole le principe de la bonne foi. Il agit également contrairement à ce principe s'il collecte des données personnelles de manière cachée.

- Proportionnalité (art. 36 LIPAD)

  En vertu du principe de la proportionnalité, seules les données qui sont nécessaires et qui sont aptes à atteindre l'objectif fixé peuvent être traitées. Il convient donc toujours de peser les intérêts en jeu entre le but du traitement et l'atteinte à la vie privée de la personne concernée en se demandant s'il n'existe pas un moyen moins invasif permettant d'atteindre l'objectif poursuivi.

- Finalité (art. 35 al. 1 LIPAD)

  Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre un but légitime qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi. Les données collectées n'ont ensuite pas à être utilisées à d'autres fins, par exemple commerciales.

- Reconnaissabilité de la collecte (art. 38 LIPAD)

  La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Cette exigence de reconnaissabilité constitue une concrétisation du principe de la bonne foi et augmente la transparence d'un traitement de données. Cette disposition implique que, selon le cours ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont éventuellement être collectées (principe de prévisibilité). Elle doit pouvoir connaître ou identifier la ou les finalités du traitement, soit que celles-ci lui sont indiquées à la collecte ou qu'elles découlent des circonstances.

- Exactitude (art. 36 LIPAD)

  Quiconque traite des données personnelles doit s'assurer de l'exactitude de ces dernières. Ce terme signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.

- Sécurité des données (art. 37 LIPAD)

  Le principe de sécurité exige non seulement que les données personnelles soient protégées contre tout traitement illicite et tenues confidentielles, mais également que l'institution en charge de leur traitement s'assure que les données personnelles ne soient pas perdues ou détruites par erreur.

- Destruction des données (art. 40 LIPAD)

  Les institutions publiques détruisent ou rendent anonymes les données personnelles dont elles n'ont plus besoin pour accomplir leurs tâches légales, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi.

Plus précisément, les dispositions légales en matière de sécurité des données se lisent comme suit :

Art. 37 LIPAD Sécurité des données personnelles

[1] Les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées.

[2] Les institutions publiques prennent, par le biais de directives ainsi que de clauses statutaires ou contractuelles appropriées, les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données personnelles qu'elles traitent ou font traiter.

[3] Les institutions publiques sont tenues de contrôler le respect des directives et clauses visées à l'alinéa 2. S'il implique l'exploitation de ressources informatiques et le traitement de données personnelles, ce contrôle doit s'exercer conformément à des procédures spécifiques que les instances mentionnées à l'article 50, alinéa 2, doivent adopter à cette fin, après consultation du préposé cantonal.

Art. 13 RIPAD Sécurité des données personnelles

En général

[1] Les institutions publiques prennent les mesures organisationnelles et techniques propres à assurer la sécurité des données personnelles.

[2] Pour l'administration cantonale, les mesures techniques et organisationnelles nécessaires à la sécurité des données personnelles sont définies notamment par le respect :

a) du règlement sur l'organisation et la gouvernance des systèmes d'information et de communication, du 26 juin 2013;

b) de l'article 23A, alinéa 5, du règlement d'application de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux, du 24 février 1999;

c) des directives approuvées par la commission de gouvernance des systèmes d'information et de communication;

d) des règles et mesures de sécurité édictées par les maîtres de fichiers, les responsables départementaux de la sécurité de l'information et l'office cantonal des systèmes d'information et du numérique, sur la base des compétences définies par les règlements visés aux lettres a et b;

e) des prescriptions réglementaires et des directives en matière d'archivage.

3. Appréciation

Les Préposés relèvent que le télétravail implique un risque accru dans le traitement des données personnelles, particulièrement au regard de la sécurité des données. En effet, le télétravail nécessite le plus souvent un accès à distance aux systèmes d'informations, et /ou que le membre du personnel emporte des documents physiques (dossiers) chez lui. De plus, l'utilisation de matériel privé (ordinateur, téléphone) à des fins professionnelles peut également comporter des risques pour la sécurité des données (par exemple selon les éventuelles configurations d'enregistrement automatique de documents dans un cloud du membre du personnel). Le risque de perte de données, de vulnérabilité à des cyberattaques ou d'utilisation d'outils informatiques non conformes aux règles de protection des données personnelles est donc accru.

Les art. 14 et 17 du projet de règlement prévoient des règles qui pallient ces risques : d'une part, le membre du personnel doit télétravailler en n'utilisant que les services numériques que l'employeur lui a fournis ou dont ce dernier a validé l'usage. D'autre part, il incombe au membre du personnel de prendre les mesures nécessaires pour garantir le secret de fonction, la sécurité de l'information, ainsi que la protection des données « *vis-à-vis de tout tiers non autorisé qui peut accéder à son espace de travail, y compris des membres de sa famille* ».

Ces dispositions sont saluées et doivent être, selon les Préposés, accompagnées d'une sensibilisation des membres du personnel sur les questions de sécurité des données en lien avec le télétravail. En effet, les enjeux ne sont pas toujours aisés à saisir et des directives claires et détaillées sont à recommander.

Les Préposés constatent que l'art. 17 al. 3 prévoit que « *Le membre du personnel doit effacer de ses moyens numériques privés toute donnée professionnelle dès qu'il n'en a plus besoin mais, au plus tard, à la fin de l'accord de télétravail ou des rapports de service* ». A con-

trario, ceci signifie que le membre du personnel peut être amené à sauvegarder des données sur son infrastructure privée. Ces enregistrements ne sont pas sans risques au regard de la sécurité des données, de sorte que les Préposés insistent sur l'importance de la sensibilisation en la matière afin d'éviter que, notamment, des communications de données à l'étranger (transfert automatique dans un cloud par exemple) n'interviennent par négligence ou méconnaissance des membres du personnel.

S'agissant de l'art. 18 du projet, il a trait aux restrictions au télétravail. Selon le commentaire de cette disposition, les limitations au télétravail à l'étranger sont surtout dictées pour des raisons fiscales. Toutefois, les Préposés saluent l'interdiction de télétravailler depuis des pays qui n'auraient pas un niveau de protection des données adéquat, conformément à la liste établie par le Préposé fédéral.

* * * * * *

Les Préposés remercient le DF de les avoir consultés et se tiennent à disposition pour tout renseignement complémentaire.

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal