ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données
Rue des Chanoines 2, 1700 Fribourg

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

La Préposée cantonale à la protection des données

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/atprd

—

Réf:
Courriel: secretariatatprd@fr.ch

Communication du mot de passe aux membres du Comité et surveillance des employés par l'employeur

(...),

(...)

Les questions que vous nous posez peuvent être exposées comme suit sous l'angle de la protection des données :

1. Est-il admissible sous l'angle de la protection des données de communiquer un mot de passe aux membres du Comité (notamment le Président) leur donnant accès aux données contenues dans le système informatique ?

2. L'employeur est-il légitimé, sans motif particulier, à s'introduire dans le système informatique de ses employés et de contrôler des données à leur insu, ainsi qu'à contrôler leurs connections Internet et leurs appels téléphoniques ?

Après avoir réuni les informations, nous sommes en mesure de vous répondre de la manière suivante (art. 31 al. 2 lit. b de la loi du 25 novembre 1994 sur la protection des données, LPrD), réservant un éventuel avis circonstancié sur la question.

Nous constatons que le problème soumis ne concerne pas vraiment le domaine de la protection des données mais résulte davantage d'un rapport employeur-employés et du droit du travail. Nous nous limitons donc à aborder la question sous l'angle de la protection des données en laissant la question ouverte sur la relation employeur-employés.

Nous relevons que vous ne nous avez pas autorisés à approcher le Comité sur ces questions. Le présent avis devrait, le cas échéant, être complété à la lumière des arguments complémentaires.

Nous traitons d'abord de la question relative à la communication de données (*in casu* mot de passe) aux membres du Comité (A), puis de la question de la surveillance des employés par l'employeur (B).

A. Communication du mot de passe aux membres du comité

1. **Généralités**

L'Association Z existe depuis (...). Elle est une association privée (au sens de l'art. 60 du Code des obligations) à but non lucratif dont les membres sont des services publics, des membres collectifs et des personnes physiques (statuts...)
Selon les informations, l'Association est une institution de santé reconnue au bénéfice d'une autorisation d'exploitation (art. 100 Loi du 16 novembre 1999 sur la santé ; décision de la Direction de la santé et des affaires sociales du canton de Fribourg du xxx). Dès lors, l'Association accomplit des tâches publiques et la LPrD lui est applicable (art. 2 al. 1 let. b LPrD).

Des données personnelles ne peuvent être communiquées que si une disposition légale le prévoit ou si, dans un cas d'espèce, l'organe public qui demande les données en a besoin pour l'accomplissement de sa tâche (art. 4 et 10 al. 1 litt. a LPrD). Il faut remarquer que les données doivent être traitées avec un devoir de diligence accru lorsqu'elles sont sensibles (art. 3 et 8 LPrD). Cela peut être le cas pour les adoptions, les reconnaissances de paternité, des données sur la santé des parents et enfants, etc.

Nous examinons donc si ces conditions sont remplies.

2. **Quant à la base légale et à l'accomplissement de la tâche de l'organe (art. 4 et 10 al. 1 litt. a LPrD)**

Aucune disposition légale ne prévoit cette communication. Toutefois, s'agissant d'une association privée, les statuts de l'association contiennent une disposition relative aux prérogatives du comité. Le comité a notamment pour attribution de *contrôler les activités* (art. xxx des statuts). L'art. xxx desdits statuts prescrit que l'activité du collaborateur est définie par un cahier des charges édicté par le comité. Le collaborateur est à disposition des consultants. Il prête bénévolement aide et assistance ; il se rend à domicile et donne des consultations.

Selon les statuts en notre possession, l'accès aux données contenues dans le système informatique du Service de Z n'y est pas réglementé, de sorte que cet aspect doit s'interpréter à la lumière des principes sur la protection des données. En matière de traitement de données personnelles, l'organe public qui traite des données personnelles doit prendre les mesures d'organisation et les mesures techniques appropriées contre tout traitement non autorisé des données et contre toute atteinte à leur confidentialité (art. 22 al. 1 LPrD et 3 al. 1 du Règlement du 29 juin 1999 sur la sécurité des données personnelles, RSD). Elle doit être assurée à l'égard de toute personne, à l'intérieur comme à l'extérieur de l'administration (art. 3 al. 2 RSD). En l'occurrence, l'accès aux informations personnelles contenues dans le système informatique de l'Association est garanti par un mot de passe qui ne doit en aucun cas être transmis à des tiers non autorisés.

Les membres du Comité ne sont pas habilités à traiter des données personnelles de personnes prises en charge. Dès lors, ils ne devraient pas avoir accès à ces données qui peuvent être sensibles de par leur nature. Ils devraient en revanche se limiter aux données nécessaires au contrôle de l'activité du collaborateur conformément aux statuts et à son cahier de charge, ce qui n'implique pas un accès sans limite aux données précitées.
Ainsi, dans la mesure où ces informations ne sont pas nécessaires à l'accomplissement des tâches statutaires ou légales, l'accès aux membres du Comité à ces données devrait être exclu.

3. **Quant au principe de proportionnalité**

Selon le principe de la proportionnalité, les données et les modes de traitement doivent être nécessaires et appropriés par rapport au but du traitement. Ainsi, les données sont limitées à ce qui est indispensable à accomplir la tâche de l'organe qui les demande.

En l'espèce et en application des statuts, le Comité exerce un contrôle sur l'activité de ses collaborateurs. Il apparait néanmoins que le procédé actuel tel que vous nous l'avez décrit (accès à l'ensemble des informations de l'Association par transmission du mot de passe) ne respecte pas le principe de proportionnalité énoncé ci-dessus. Les membres du Comité devraient se limiter à vous demander de leur fournir les informations utiles à leur pouvoir de contrôle sans pour autant se permettre un accès illimité à toutes les informations personnelles contenues dans les fichiers de l'Association. Dès lors, vous êtes soumis en qualité de collaborateur (infirmier(ère) diplômé(e)) au *secret professionnel*, votre travail est une profession de la santé, au sens de l'art. 89 al. 1 de la loi fribourgeoise du 16 novembre 1999 sur la santé. Il est donc probable que votre domaine d'activité soit soumis à des règles spécifiques en matière de secret professionnel. Toutefois, en l'état, nous nous référons aux règles sur le secret professionnel contenues dans la Loi cantonale du 16 novembre 1999 sur la santé, art. 89 ; RSF 821.0.1).

4. **Quant aux principes de finalité (art. 5 LPrD)**

Conformément au principe de finalité, les données personnelles ne peuvent être traitées dans le but pour lequel elles ont été collectées ou dans un but qui, selon les règles de la bonne foi, est compatible avec lui.

Il ne paraît pas conforme au principe de finalité d'octroyer un droit d'accès illimité aux membres du comité concernant des données personnelles sensibles, alors même que vous n'êtes pas informé de l'utilisation précise que le comité entend faire de cette collecte.

Dès lors, en l'état des informations, l'accès aux données personnelles contenues dans le système informatique de l'Association via un mot de passe commun aux collaborateurs et aux membres du Comité ne paraît pas admissible sous l'angle de la protection des données.

B. Surveillance des employés par l'employeur

Les limites juridiques mises à la surveillance des employés découlent principalement du droit du travail, de la législation relative à la protection des données et du droit pénal. Le domaine privé est également couvert par le secret des télécommunications.

Le Préposé fédéral à la protection des données s'est déjà exprimé sur le sujet de la surveillance de l'employé sur le lieu de travail (*cf. www.edoeb.admin.ch, Guide relatif à la surveillance de l'utilisation d'internet et du courrier électronique au lieu de travail, éd. par le préposé fédéral à la protection des données, Berne, état juillet 2002, pp. 22 et suivantes*). Il est d'avis que l'employeur a le droit de procéder à des *contrôles anonymes ou pseudonymes* s'il a annoncé ce type de contrôles, par exemple dans un règlement interne relatif à la surveillance (lequel doit pouvoir être consulté par tous les employés). La surveillance est dite « anonyme » si elle ne permet pas de déterminer la manière de naviguer sur Internet de chaque collaborateur pris individuellement. Si l'employeur constate l'existence d'un *abus*, il a le droit d'effectuer des *contrôles personnels*. Il faut souligner que les contrôles personnels ne sont autorisés que si, premièrement, il existe un règlement relatif à la surveillance qui précise de manière claire que l'employeur se réserve le droit de procéder à des contrôles personnels et si, deuxièmement, l'employeur a constaté un abus lors d'un contrôle anonyme ou pseudonyme ou qu'il soupçonne l'existence d'un abus. Il y a abus dès l'instant où un collaborateur ne respecte pas les dispositions prévues dans le règlement d'utilisation ou, s'il n'y a pas de règlement, lorsqu'il contrevient à son devoir de loyauté envers l'employeur ou qu'il ne respecte pas le principe de la proportionnalité. Il est toutefois conseillé de donner un premier avertissement au collaborateur concerné avant de procéder à des contrôles personnels. Même si ces conditions sont remplies, la surveillance devrait être effectuée au moyen de pseudonymes attribués aux employés (par ex. série de chiffres), afin que leurs activités puissent être analysées sous une forme anonyme par les services informatiques.

En revanche, **la surveillance permanente et personnalisée** des employés est interdite en Suisse (art. 26 OLT3). Cette interdiction a pour but de protéger l'employé contre une surveillance permanente et ciblée de son comportement (ATF 130 II 425).

A titre informatif et bien qu'il ne soit applicable qu'au personnel de l'Etat de Fribourg, nous attirons votre attention sur l'Ordonnance du 20 août 2002 relative à la surveillance de l'utilisation d'Internet par le personnel de l'Etat (RSF 122.70.17), prévoyant aux art. 7 et 8 des règles précises en matière de contrôles globaux anonymes, ainsi qu'en matière de contrôles personnalisés.
Dès lors, l'employeur a le droit de procéder à des *contrôles anonymes ou pseudonymes* s'il a annoncé ce type de contrôles, par exemple dans un règlement interne relatif à la surveillance (lequel doit pouvoir être consulté par tous les employés). Si l'employeur constate l'existence d'un *abus*, il a le droit d'effectuer des *contrôles personnels*. En revanche, **la surveillance permanente et personnalisée** des employés est interdite en Suisse.

Au vu de ce qui précède, nous parvenons aux **conclusions suivantes** :

1. En l'état des informations, l'accès aux données personnelles contenues dans le système informatique de l'Association via un mot de passe commun aux collaborateurs et aux membres du Comité ne paraît pas admissible sous l'angle de la protection des données.

2. L’employeur a le droit de procéder à des *contrôles anonymes ou pseudonymes* s'il a annoncé ce type de contrôles, par exemple dans un règlement interne relatif à la surveillance (lequel doit pouvoir être consulté par tous les employés). En cas de constatation d’abus, l’employeur peut effectuer des *contrôles personnels* mais doit en informer l’intéressé. En revanche, **la surveillance permanente et personnalisée** des employés est interdite en Suisse.

En vous souhaitant bonne réception de mes remarques et en restant à votre disposition pour des compléments d’informations ou échanges, nous vous prions de croire, (...), à l'assurance de notre considération distinguée.

Copie anonymisée à la personne de contact de la DSAS