

Règlement interne sur la protection des données

de la

Fondation de prévoyance Musiques-Arts

1. Introduction

Le présent Règlement (le "**Règlement**") est établi par le Conseil de fondation de la Fondation de prévoyance Musiques-Arts (la "**Fondation**") sur la base de :

- la loi fédérale sur la protection des données (la "**LPD**");
- l'Ordonnance relative à la loi fédérale sur la protection des données (l'"**OPDo**");
- les articles 85a ss de la loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité (la "**LPP**");
- les articles 27i ss de l'ordonnance sur la prévoyance la prévoyance professionnelle vieillesse, survivants et invalidité (l'"**OPP 2**");
- les articles 28 ss du Code civil suisse;
- l'article 328 du Code des obligations; et
- l'article 26 de l'Ordonnance 3 relative à la loi sur le travail.

Le présent Règlement a pour but de fixer l'organisation interne de la Fondation et de définir les rôles et les responsabilités en vue du respect des exigences légales et réglementaires en matière de protection des données, en particulier de la LPD et de la LPP.

A cette fin, le Règlement décrit la structure mise en place par la Fondation en matière de protection des données, soit en particulier l'organisation interne, les procédures de traitement et de contrôle des données, ainsi que les mesures visant à garantir la sécurité des données.

2. Champ d'application

Ce Règlement s'applique à l'ensemble des traitements de données personnelles effectués par la Fondation.

3. Organisation

Le Conseil de fondation est responsable du respect de la réglementation relative à la protection des données au sein de la Fondation et fixe l'organisation établie dans le présent Règlement pour y parvenir.

Le Président du Conseil de fondation est chargé des questions relatives à la protection des données.

Afin d'assurer le respect de la législation suisse sur la protection des données, le Conseil de fondation nomme un conseiller externe à la protection des données au sens de l'article 10 de la nouvelle loi fédérale sur la protection des données et des articles 25 ss de son ordonnance (*Data Protection Officer* ; le "DPO"). Son rôle est le suivant:

- être l'interlocuteur principal des personnes concernées et des autorités chargées de la protection des données, en particulier le Préposé fédéral à la protection des données et à la transparence (le "PFPDT");
- concourir à la formalisation et à l'application des prescriptions relatives à la protection des données;
- apporter la formation nécessaire aux membres du Conseil de fondation;
- apporter tout conseil sollicité par le Conseil de fondation;
- conseiller la Fondation sur la gestion des demandes d'accès des personnes concernées relatives à la protection des données;
- proposer à la Fondation les mesures nécessaires à la bonne application de la législation en matière de protection des données;
- assister la Fondation dans la tenue du registre des activités de traitement.

Le DPO n'est pas responsable de la gestion opérationnelle, technique, informatique et/ou sécuritaire des données personnelles au sein de la Fondation et il ne dispose pas de pouvoir décisionnel.

La Fondation a délégué sa gestion administrative, technique, commerciale et comptable à un prestataire externe, Kessler Prévoyance SA ("Kessler"), qui effectue l'essentiel des activités de traitement de la Fondation. Kessler a désigné un de ses collaborateurs afin d'assurer la bonne marche du suivi de la mission, notamment s'agissant des aspects relatifs à la protection des données.

La Fondation a confié la sauvegarde de ses données informatiques au Conservatoire Populaire de Musique, Danse et Théâtre de Genève (le "CPMDT"). Le CPMDT a désigné un de ses collaborateurs afin d'assurer la bonne marche du suivi de la mission, notamment s'agissant des aspects relatifs à la protection des données.

4. Procédure de traitement

4.1 Traitements de données effectués par la Fondation

Dans le cadre de son activité, la Fondation traite des données en conformité des lois applicables et notamment sur la base de la législation sur la prévoyance professionnelle.

Une grande partie des activités de traitement de données est effectuée par Kessler et le CPMDT.

Par données personnelles, l'on entend toutes les informations concernant une personne physique identifiée ou identifiable. En droit suisse, le traitement de données personnelles par une personne privée est licite et ne requiert pas de motif justificatif.

Celui qui traite des données personnelles ne doit toutefois pas porter une atteinte à la personnalité des personnes concernées, notamment en:

- traitant des données personnelles en violation des principes légaux (notamment proportionnalité, bonne foi, finalité, exactitude, sécurité);
- traitant des données contre la manifestation expresse de la volonté de la personne concernée; et
- communiquant à des tiers des données sensibles.

Une atteinte à la personnalité est illicite à moins d'être justifiée par des motifs justificatifs, soit par la loi, par un intérêt privé ou public prépondérant ou par le consentement de la personne concernée.

Au surplus, les deux documents suivants décrivent de manière détaillée les traitements de données effectués par la Fondation:

- Registre des activités de traitement de la Fondation.
- Notice de confidentialité.

La Fondation révisé sur une base annuelle ces documents. A cette fin, elle peut solliciter l'appui du DPO.

4.2 Procédure en cas de requête d'accès

Kessler et/ou le CPMDT informent le Conseil de fondation et le DPO de toutes les requêtes qu'ils reçoivent.

Le Président du Conseil de fondation traite lui-même, sans retard, les requêtes qui concernent les données traitées par la Fondation ainsi que celles confiées au CPMDT. En cas de besoin, il peut solliciter l'aide du DPO.

Le Président du Conseil de fondation transmet, sans retard, à Kessler les requêtes en lien avec des données confiées à Kessler. Kessler, traite, sans retard, les requêtes qu'elle reçoit du Président du Conseil de fondation. En cas de besoin, Kessler peut solliciter l'aide du DPO.

Le Président du Conseil de fondation tient un journal des requêtes d'accès et s'assure qu'une suite est donnée à toutes les requêtes d'accès reçues. Le journal est communiqué au DPO lors de chaque mise à jour.

Le Président du Conseil de fondation et, le cas échéant, Kessler, pour les données qui lui ont été confiées, informent au moins une fois par année le Conseil de fondation des requêtes qu'ils ont traitées.

4.3 Procédure en cas d'incident de sécurité

En cas de violation de la sécurité entraînant la perte de données personnelles, leur modification, leur suppression ou leur destruction, ou leur divulgation ou un accès non autorisé, les démarches suivantes seront accomplies:

- Le CPMDT, Kessler, et/ou tout autre sous-traitant informe(nt) immédiatement la Fondation ainsi que le DPO de la survenance de l'incident de sécurité.
- Le Président du Conseil de fondation (le cas échéant avec l'aide du CPMDT, de Kessler ou du sous-traitant concerné) analyse l'incident et ses potentielles conséquences pour les personnes concernées et pour la Fondation, en faisant appel au besoin à un expert informatique.
- Le Président du Conseil de fondation procède dès que possible, avec le soutien du DPO, à une annonce au PFPDT ainsi que – lorsque les circonstances l'exigent ou que le PFPDT le demande – aux personnes concernées des atteintes à la sécurité des données susceptibles de mettre en péril la personnalité des personnes concernées.

L'annonce au PFPDT contient au moins une description de la nature de la violation (perte, modification, suppression ou destruction, ou divulgation à des tiers non autorisés), des conséquences de la violation pour les personnes concernées ainsi que des mesures prises ou envisagées pour remédier à la violation de la sécurité des données ou pour en atténuer les conséquences.

5. Conservation de données

Les données personnelles traitées par la Fondation sont conservées:

- s'agissant des données confiées à Kessler, sur ses propres serveurs physiques localisés en Suisse; et
- s'agissant des données confiées au CPMDT, sur ses propres serveurs localisés en Suisse.

La durée de conservation légale est en principe de 10 ans à compter de la fin du droit aux prestations, ou lorsqu'aucune prestation n'est versée parce que la personne assurée n'a pas fait usage de son droit, jusqu'au moment où l'assuré atteindrait l'âge de 100 ans, voire au-delà si l'intérêt de la Fondation le justifie.

6. Analyses d'impact relatives à la protection des données

Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, la Fondation procède au préalable à une analyse d'impact relative à la protection des données personnelles. Elle peut au besoin solliciter l'appui du DPO.

Il y a notamment un risque élevé pour la personnalité ou pour les droits fondamentaux de la personne lorsqu'un traitement de données implique :

- une évaluation/*scoring* (y compris profilage);

- une décision automatique avec effet légal ou similaire;
- une surveillance systématique;
- des données sensibles ou hautement personnelles;
- une collecte à large échelle (en fonction du nombre de personnes concernées, volume, durée, dimension géographique);
- un croisement de données;
- des personnes vulnérables (y compris patients, personnes âgées, enfants);
- l'usage de technologies innovantes; ou
- un processus qui peut empêcher une personne de conclure un contrat et/ou de bénéficier d'un service.

En général, deux critères suffisent pour remplir l'exigence du risque élevé.

7. Mesures de sécurité

La Fondation choisit, instruit et surveille adéquatement son personnel ainsi que ses prestataires tiers de sorte à garantir la confidentialité, la disponibilité et l'intégralité des données qu'elle traite. De plus, la Fondation :

- restreint l'accès des prestataires tiers ainsi que des membres du Conseil de fondation aux données personnelles dont ils ont besoin pour accomplir leurs tâches ;
- restreint l'accès aux locaux et aux installations aux membres du Conseil de fondation et aux personnes autorisées ;
- empêche que les personnes non autorisées ne puissent lire, copier, modifier, déplacer, effacer ou détruire des supports de données ;
- empêche que les personnes non autorisées ne puissent enregistrer, lire, modifier, effacer ou détruire des données personnelles dans la mémoire ;
- assure que la disponibilité des données personnelles et l'accès à celles-ci puisse être rapidement restaurés en cas d'incident physique ou technique ;
- assure qu'il soit possible de vérifier à qui sont communiquées les données personnelles ;
- assure que les violations de la sécurité des données puissent être rapidement détectées et que des mesures puissent être prises pour atténuer ou éliminer les conséquences.

* * *

Ce Règlement est revu sur une base annuelle par le Conseil de fondation.

Etat : février 2025

Pour le Conseil de fondation de la Fondation de prévoyance Musiques-Arts :



Nom: Cyril Ledermann

Position: président



Nom: Aude Joly

Position: vice- présidente