Code de conduite interne de protection des données de l'établissement Institut Saint-Laurent de Promotion Sociale

1. **Pourquoi une politique de protection des données ?** Notre institution collecte et traite de nombreuses informations à caractère personnel relatives aux personnes physiques : élèves/étudiants, parents, membres du personnel, fournisseurs, partenaires et toute personne avec qui notre établissement entretient des relations.

   La présente politique interne de protection des données décrit comment ces données à caractère personnel doivent être collectées, traitées et stockées pour rencontrer les standards de protection et maintenir celles-ci en conformité avec la loi et le règlement général de protection des données (RGPD).

   Notre institution est responsable de sa conformité aux lois relatives à la protection des données personnelles et doit être capable de démontrer celle-ci à tout moment, notamment auprès de l'autorité de contrôle. Pour la Belgique, la loi du 3 décembre 2017 a transformé la Commission vie privée en une Autorité de protection des données (« APD ») et lui a conféré les pouvoirs nécessaires pour (entre autres) appliquer les nouvelles sanctions en cas de violation des dispositions du RGPD.

2. **A qui et à quoi s'applique cette politique de protection des données ?** Cette politique s'applique à toutes les opérations que notre institution réalise sur des données à caractère personnel. Ce code de conduite doit donc être respecté par tous les membres du personnel, quels que soit leur fonction et leur statut, en ce compris les volontaires et les stagiaires.

   Les traitements de données à caractère personnel sont toute action (collecte, encodage, reproduction, transformation, partage, effacement,…) exercée sur des données relatives à des personnes physiques identifiées ou identifiables (entre autres et par exemple du personnel de l'institution scolaire ou du CPMS, d'employés de fournisseurs, de personnes de contact auprès d'autres institutions, d'étudiants, des membres du Pouvoir organisateur, etc.).

   La Politique de protection des données à caractère personnel est adoptée et peut être mise à jour par la direction de l'institution.

   Le P.O. a désigné un délégué à la protection des données (DPO) qui conseille le P.O. et la direction.

3. **Quel est le droit applicable ?** Diverses lois et régulations nationales et internationales protègent les droits des individus en ce qui concerne leur vie privée et le traitement de leurs données, en ce compris le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogeant la directive 95/46/CE (règlement général sur la protection des données : ci-après "RGPD"). Certains termes utilisés dans cette Politique ont des significations particulières qui sont établies à l'article 4 du RGPD.

4. **Principes généraux.** Le traitement des données à caractère personnel par ou au nom du P.O. et de notre institution doit se conformer aux principes généraux ci-dessous.

Toutes les données personnelles doivent être traitées de manière **équitable**, **légale** et **transparente**. Ainsi les données ne peuvent être traitées que si l'une des conditions suivantes est satisfaite :

- La personne concernée a donné son consentement ;
- Le traitement est nécessaire pour l'exécution du contrat auquel la personne concernée est partie ou, à la demande de la personne concernée, dans les étapes précédant la conclusion d'un contrat dans l'optique de conclure ce contrat ;
- Le traitement est nécessaire pour que le P.O. et notre institution scolaire soient en conformité avec ses obligations légales ;
- Le traitement est nécessaire en vue de protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont serait investi le P.O. ;
- Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le P.O ;

Les données à caractère personnel ne peuvent être traitées qu'à des fins clairement limitées et définies qui sont licites et qui ont été communiquées à la personne concernée avant que le traitement n'ait eu lieu.

Le P.O. et notre institution ont une obligation de minimisation des données, à savoir que le nombre et la nature des données traitées doivent être adéquats, pertinents et non excessifs au regard du but pour lequel les données sont traitées.

Toutes les données à caractère personnel doivent être précises, complètes et tenues à jour.

Dans la mesure du possible, toute donnée inexacte, incomplète ou périmée doit être corrigée ou effacée.

Les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire. Les délais de conservation des données à respecter sont ceux prévus dans notre déclaration de protection des données.

Il est interdit de transférer ou divulguer des données à caractère personnel sans que la personne concernée ait consenti au transfert ou que ce transfert ne soit nécessaire pour l'exécution d'un contrat, auquel la personne concernée est partie, ou, à la demande de la personne concernée dans les étapes précédant la conclusion d'un contrat, dans l'optique de conclure ce contrat, ou à moins que ce transfert ne soit imposé par la loi ou un cadre règlementaire.

Toutes les données à caractère personnel traitées par ou au nom du P.O. et notre institution doivent faire l'objet de mesures organisationnelles et de sécurité appropriées pour s'assurer qu'elles sont sécurisées et que les niveaux appropriés de confidentialités sont maintenus. Les personnes non autorisées ne doivent pas avoir accès aux données à caractère personnel.

Les copies papier des données à caractère personnel doivent être traitées comme des déchets confidentiels et déchiquetés.

5. **Droit des personnes concernées.** Comme le précise notre déclaration de protection des données, chaque personne dispose de droits quant aux données que le P.O. et l'institution détiennent à son sujet, à savoir :
   - Droit d'accès aux données ;
   - Droit de rectification des données ;
   - Dans certains cas, droit à la suppression des données non indispensables au suivi et à l'exécution du contrat de travail ;
   - Droit d'opposition à un traitement de données et ce en motivant spécifiquement votre demande, tenant compte que le responsable de traitement peut démontrer qu'il existe des motifs légitimes et impérieux qui justifient le traitement contesté et ce bien évidemment en conformité avec le RGPD.

6. **Traitement des demandes adressées par les personnes concernées.** Les personnes qui souhaitent exercer leurs droits doivent en faire la demande par écrit auprès du délégué à la protection des données vie.privee@isllg.be

   Aucune demande orale ne sera prise en compte.

   La demande écrite sera accompagnée d'une copie recto/verso de la carte d'identité de la personne concernée.

   Les personnes concernées peuvent faire des demandes répétées à des intervalles raisonnables. Elles ont également le droit d'adresser des contestations au P.O. concernant leur conformité avec les dispositions de la présente Politique et les lois applicables en matière de protection des données. De telles contestations doivent également être adressées par écrit au délégué à la protection des données/à la personne de contact.

7. **Délégué à la protection des données.** Le P.O. a désigné un Délégué à la Protection des Données (ci-après également désigné "DPO") sur la base de ses qualités professionnelles et, en particulier, sa connaissance du droit et des pratiques de la protection des données et sa capacité à remplir ses missions.

   Les personnes concernées peuvent contacter le DPO pour toutes les questions liées au traitement de leurs données à caractère personnel et à l'exercice de leurs droits.

   Le DPO/la personne de contact peut être contacté à l'adresse : vie.privee@isllg.be

8. **Gestion et révision des traitements de données.** Les activités de traitement des données à caractère personnel dont le P.O. est responsable ou que le P.O. effectue à titre de sous-traitant sont reprises dans un registre de traitement.

   Lors de tout traitement, la direction, mandatée par le P.O. et conseillée par le DPO intégrera les mesures appropriées dans le traitement, en ce compris les mesures techniques et organisationnelles, afin de protéger les droits des personnes concernées.

   Avant d'introduire de nouvelles technologies ou de lancer un nouveau traitement de données à caractère personnel susceptible d'entraîner un risque élevé pour les droits et libertés de la personne concernée, la direction mandatée par le P.O., en collaboration avec le DPO, évaluera la

nécessité de réaliser une analyse d'impact sur la protection des données pour évaluer l'impact des traitements envisagés sur la protection des données à caractère personnel et adopter les meilleures mesures de protection.

La direction mandatée par le P.O., en collaboration avec le DPO, met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que, par défaut, seules les données personnelles nécessaires à chaque finalité spécifique du traitement sont traitées. Cette obligation s'applique à la quantité de données personnelles collectées, à l'étendue de leur traitement, à la durée de leur stockage et à leur accessibilité. En particulier, de telles mesures doivent garantir que, par défaut, les données personnelles ne sont pas accessibles à un nombre indéfini de personnes physiques sans l'intervention de l'individu (choix des individus en matière de paramètres, utilisation de fonctionnalités optionnelles, …). Lorsque des traitements peuvent faire l'objet de paramétrages par les personnes concernées, les paramétrages initialement fixés par défaut sont ceux qui assurent des risques minimaux quant à la protection des données et la vie privée des personnes concernées.

9. Lignes directrices pour le personnel de notre institution

Toute personne travaillant au sein de notre institution et ayant accès aux données personnelles qui sont traitées en son sein doit lire et comprendre la présente politique et se conformer aux bonnes pratiques mises en place, parmi lesquelles figurent les principes comportementaux suivants :

- Lorsque vous traitez des données personnelles, faites-le avec les outils prévus à cet effet et respectez la procédure (utilisez les logiciels et bases de données pourvus par le SEGEC/ évitez d'utiliser des logiciels, bases de données, services, sites web, … qui ne sont pas préalablement validés par la direction).
- Ne dupliquez pas les données personnelles à moins que cela ne soit absolument nécessaire.
- Lorsque vous enregistrez des données personnelles, enregistrez uniquement ce qui est nécessaire et évitez les erreurs.
- Lorsque vous collectez les données auprès d'une personne, expliquez à celle-ci pourquoi vous en avez besoin et dans quel but. Vous pouvez vous référer à notre politique interne.
- Mettez les données à jour quand l'opportunité se présente (demandez la confirmation des données à la personne concernée, corrigez les erreurs, effacez les données dépassées et obsolètes).
- Ne les transférez pas / ne les communiquez que s'il s'agit de la procédure normale (Ex.: ne communiquez pas de données personnelles à un collègue ou à un tiers si ce n'est pas justifié).
- Si vous transférez ou recevez des données, supprimez les copies non-nécessaires / résiduelles. (Ex.: les fichiers téléchargés sont sauvegardés dans le bon dossier et effacés du dossier de téléchargement).
- Respectez une éthique de confidentialité générale (ne consultez pas un fichier si vous n'y êtes pas habilité, ne discutez pas extensivement des informations personnelles si ce n'est pas nécessaire …)
- Respectez les règles de sécurité des systèmes informatiques (secret du mot de passe, rapport des dysfonctionnements, utilisation de programmes officiels…).

- Si vous accédez à des données auxquelles vous ne devriez pas avoir accès, contactez le DPO/personne de contact.

- Si vous pensez que des données pourraient avoir été perdues, endommagées ou accédées par des personnes non-autorisées (à cause d'un virus, d'une attaque informatique, d'un vol, d'une perte de matériels, etc…), informez-en immédiatement le DPO/personne de contact.

- Si vous avez des doutes ou des questions, contactez le DPO/personne de contact.

La direction organisera des séances d'information afin d'aider son personnel à comprendre ses responsabilités et à traiter au mieux les données à caractère personnel auxquelles il a accès.

10. **Sécurité des données.** Il est de la responsabilité du P.O. et de notre institution de sécuriser les données à caractère personnel et leur traitement. Pour ce faire, le P.O. et la direction mettent en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié aux risques. Une grande majorité des incidents de sécurité impliquent des erreurs humaines. La vigilance est donc de mise.

11. **Contrats avec des tiers et des sous-traitants.** Lorsqu'on exécute des contrats avec des tiers en vertu desquels des données à caractère personnel doivent être transférées ou divulguées à ce tiers, ledit contrat doit inclure des dispositions exigeant que le tiers se conforme aux dispositions légales relatives à la vie privée.

    Les contrats avec des tiers qui traitent des données à caractère personnel au nom du P.O. (sous-traitants) doivent respecter de nombreuses exigences légales. Une copie de tout contrat impliquant le transfert de données à caractère personnel à des tiers doit être fournie au DPO qui l'examinera.

12. **Transfert de données hors de l'Union européenne**. On permet le transfert de données personnelles en dehors de l'UE uniquement après s'être assuré que ces données bénéficieront du même niveau de protection que celui garanti par le droit européen (RGPD), et plus particulièrement si le pays de destination bénéficie d'une décision d'adéquation de la Commission de l'UE ou si des garanties appropriées sont en place.

13. **En cas de fuite de données.** Il incombe à la direction mandatée par le P.O. de réagir promptement et de manière adéquate aux incidents de sécurité (violation de données personnelles) ; ces obligations pouvant être résumées comme suit:
    - ✓ Evaluer la gravité de l'incident et ses conséquences éventuelles (risques éventuels en ce qui concerne les données à caractère personnel et les personnes concernées);
    - ✓ Dans certains cas, aviser l'autorité de protection des données (dans les 72 heures après avoir pris connaissance de l'incident) et / ou les personnes concernées (sans retard injustifié).

    Des exemples de tels incidents sont : le vol ou la perte d'ordinateurs, d'ordinateurs portables, de dispositifs électroniques portables (gsm, smartphones,…), de supports électroniques (tels que des clés USB) ou de dossiers sous format papier; mot de passe piraté ou révélé; stockage ou transmission non sécurisée; la détection des vulnérabilités dans les systèmes informatiques et les infrastructures; détection de virus ou de malwares; installation de logiciels à risque; accès non autorisé aux systèmes informatiques; détection d'activités anormales sur, ou utilisation, des systèmes informatiques, etc.

Tout événement ou incident suspect pouvant entraîner une violation des règles de sécurité ou d'accès aux données doit être signalé sans délai à la direction et au DPO.

14. **Collaboration avec l'autorité de protection des données**. Le P.O. et la direction collaborent avec les autorités officielles de protection des données et répondent à leurs questions sans retard injustifié et au moins dans les délais légaux le cas échéant. Le DPO assura la liaison avec les autorités de protection des données.

15. **Application de la politique et sanctions**. Ce code de conduite est adopté pour assurer que le P.O. et l'institution scolaire se conforment aux dispositions légales. En cas de violation, le P.O. s'expose à des sanctions importantes. Le non-respect par un membre du personnel du présent Code et sans excuse raisonnable constitue une faute qui peut entraîner une sanction disciplinaire conformément aux dispositions propres au statut du membre du personnel concerné et en application du règlement de travail.

Mis à jour le 01/07/2019