
DONNEES
PERSONNELLES

Concept de protection des données

1. But et portée

Le présent concept sur la protection des données de **RJCFormationSarl** met en exergue l'importance et la valeur de la notion de confidentialité des données, comprise dans le sens du respect de la sphère privée et des droits de la personnalité de vos clients, de vos collaborateurs/-trices et également, si applicable, de vos partenaires commerciaux. Il constitue la base incontournable applicable à l'ensemble des mesures et activités de **RJCFormationSarl** , en particulier en ce qui concerne le traitement

- des données personnelles des clients et de leur employés;
- des données personnelles des collaborateurs/-trices, y compris les données se rapportant à des personnes ayant déposé leur candidature pour un poste ou celles d'ancien·ne·s collaborateurs /-trices.
- des informations relatives aux partenaires commerciaux et à d'autres tiers, dans la mesures où elles incluent des données personnelles.

2. Bases juridiques

Le présent concept de protection des données repose sur la loi fédérale sur la protection des données (LPD ; RS 235.1) et sur l'ordonnance sur la protection des données du 31 août 2022 (OPDo ; RS 235.11) ainsi que, si applicable, les dispositions cantonales de Genève (LIPAD A2 08) en matière de protection des données.

3. Définitions

Les principales notions sont définies dans l'annexe 1.

4. Champ d'application

Le présent concept de protection des données s'applique à tous les organes et collaborateurs/-trices de **RJCFormationSarl** ayant à traiter des données personnelles dans le cadre de l'accomplissement de leurs tâches et fonctions.

Il s'applique également aux personnes et aux entreprises externes mandatées pour une action spécifique, dans la mesure où elles s'engagent à le respecter expressément et par écrit.

5. Finalité

L'objectif premier du présent concept est de garantir la protection de la personnalité des personnes physiques contre l'utilisation illégale ou disproportionnée des données personnelles détaillées au point 1.

Ce concept constitue une directive à valeur obligatoire, destinée à permettre à l'ensemble des personnes travaillant au sein de **RJCFormationSarl** d'être en parfaite conformité avec les exigences relatives à la protection des données, en toute connaissance de cause.

La réalisation de cet objectif doit également permettre à **RJCFormationSarl** d'éviter les préjudices matériels et les atteintes à l'image pouvant résulter pour elle d'agissements contrevenant aux règles de protection des données.

6. Les principes régissant la protection des données

6.1 Licéité

Le traitement des données est réputé licite lorsqu'il est justifié par le consentement de la personne concernée, une autorisation légale, ou un intérêt public ou privé prépondérant.

6.2 Proportionnalité

La collecte de données doit répondre à une nécessité. Elle doit de surcroît se justifier par un intérêt prépondérant. Les collectes de données à titre préventif sont illégales, et les données devenues inutiles doivent être effacées.

6.3 Finalité

Les données ne peuvent être utilisées que dans le but annoncé au préalable pour justifier leur collecte. Vos données ne peuvent en aucun cas être utilisées à des fins non identifiables par la personne concernée.

6.4 Transparence

La collecte et le traitement de données doivent être clairement identifiables. Les informations nécessaires doivent avoir été obtenues directement auprès de la personne concernée.

6.5 Qualité des données

Il convient de s'assurer que les données traitées sont exactes, complètes et à jour. Les données inexactes et incomplètes doivent être corrigées ou supprimées.

6.6 Bonne foi

Les comportements abusifs et allant à l'encontre de ces règles sont contraires à la loi.

7. Sécurité des données : mesures préconisées

La protection des données et des données personnelles doit être assurée par le biais de mesures organisationnelles et techniques, tout particulièrement en ce qui concerne l'accès par des personnes non autorisées, l'utilisation abusive, la destruction, la perte, les erreurs techniques, la falsification, le vol, etc.

7.1 Mesures organisationnelles

Au sein de **RJCFormationSarl** , l'accès aux données personnelles se fait selon le principe « autant que nécessaire, aussi peu que possible ».

L'accès aux données personnelles sont accessible uniquement par le directeur et la secrétaire dans le cadre du traitement des formations et la facturation. Les formateurs peuvent être sollicité dans la collecte de données personnelles dans le cadre des formations OACP et certaines formations certifiantes. Il collecte les données, les stockes dans le dossiers de formation et le remette directement aux secrétariats.

7.2 Mesures techniques

La protection des données informatisées stockées dans le NAS de l'entreprise est garantie en particulier par l'utilisation appropriée qui en est faite et l'utilisation de pare-feu, de programmes anti-virus géré par notre informaticien XEFI. L'ensemble des locaux sont protéger par une alarme dynamique.

Les accès aux dossiers concernant des données personnelles sont gérés par les accès aux dossiers interne du NAS et le directeur est le seul habilité à délivrer ceux-ci.

7.3 Archivage

Les données personnelles sous forme numérique sont stockées sur le NAS de l'entreprise, seul les personnes habilités ont accès et il est protégé sous la responsabilité de notre informaticien. Les données personnelles sous forme papier sont stockées sous clés sous la responsabilité du secrétariat.

7.4 Suppression

Les données considérées comme secondaires sont supprimées (physiquement détruites pour celles sur support matériel ou effacées de manière définitive pour celles sur support informatique) dès que l'objectif de leur traitement a été réalisé et immédiatement après.

Les dossiers spontanés ou de candidatures seront détruits après une période de 90 jours après leur réception si les personnes n'ont pas été retenue

8. Droits des personnes concernées

Le but des consignes listées ci-après est de permettre de gérer au mieux – du point de vue de la protection des données – des situations courantes du quotidien.

8.1 Information/Sensibilisation

Les clients et les collaborateurs/-trices sont informé·e·s de leurs droits et obligations en matière de protection des données à leur entrée en fonction.

Le directeur les sensibilise ensuite de manière appropriée sur la collecte de données personnelles les concernant.

8.2 Droit d'accès/de consultation

Toute personne concernée a le droit d'exiger d'être renseignée sur la collecte, l'origine, le contenu, la finalité, la catégorie et la base juridique de l'utilisation de ses données personnelles et de consulter le fichier de données. Elle a également le droit de connaître les participants au fichier et les destinataires de ces données.

Toute personne demandant l'accès à ou la consultation de ses données doit justifier de son identité.

Les renseignements demandés doivent être communiqués dans les 30 jours, de manière aisément compréhensible, sous forme écrite et sans frais.

La communication de renseignements et le droit de consultation peuvent, à titre exceptionnel, être restreints ou refusés si des intérêts publics importants et prépondérants, ou des intérêts de tiers particulièrement sensibles, s'y opposent.

Si le fait de fournir des renseignements ou un droit de consultation risque de soumettre la personne concernée (en particulier les personnes mineures) à un stress trop important, cette dernière a la possibilité de

désigner une personne tierce, à qui seront communiqués, à sa place, les renseignements ou le droit de consultation demandés.

8.3 Droit de rectification

Les données traitées de manière illicite ou incorrecte ainsi que les données inexactes doivent être rectifiées ou supprimées.

8.4 Blocage/Refus de communication des données

Toute personne concernée peut faire bloquer la communication de ses données si elle prouve un intérêt légitime à le faire. Cela ne s'applique pas si la communication des données constitue une obligation légale, si elle est nécessaire en raison d'intérêts prépondérants de tiers, ou si elle est nécessaire pour élucider des actes présumés abusifs de la personne concernée.

9. Recommandations pratiques

Le but des consignes listées ci-après est de permettre de gérer au mieux – du point de vue de la protection des données – des situations courantes du quotidien.

9.1 Comment gérer les demandes par téléphone ou par écrit

Les données personnelles ne peuvent être transmises à des tiers sans le consentement exprès de la personne concernée ou sans autorisation légale *ad hoc*.

Les demandes sont formalisées par écrit précisant l'identité du demandeur et la justification de celle-ci. Aucune demande téléphonique est acceptée.

9.2 Principes applicables à l'utilisation des courriers électroniques

Les courriers électroniques (e-mails) peuvent être lus ou modifiés par des tiers. Raison pour laquelle il est recommandé de transmettre le moins de données personnelles possible par courrier électronique, et de s'assurer que ces courriels ne contiennent pas d'informations sensibles, d'indications de mots de passe ou autres données d'accès.

En règle générale, les données sensibles ne sont transmises par courrier électronique que lorsqu'elles sont cryptées, à moins que la personne concernée ne l'ait dûment autorisé autrement, par écrit.

Les données personnelles utilisées à des fins professionnelles ne doivent pas être conservées sur des dispositifs électroniques à usage privé.

Par ailleurs, les dispositions du règlement en vigueur pour RJCFormationSarl sur l'utilisation de l'informatique s'appliquent également en l'espèce.

9.3 Utilisation d'images/d'enregistrements

Seules les personnes ayant donné leur consentement express peuvent être photographiées, filmées et/ou enregistrées.

Le consentement de la personne concernée doit être libre, explicite et préalablement éclairé quant au but et à l'utilisation des prises de vue ou de son. Le consentement peut être donné par écrit ou – en présence de

plusieurs personnes – oralement ou de manière non verbale, et doit être documenté.

10. Responsabilités

10.1 Direction

La direction est responsable, au niveau stratégique, de la garantie de la protection des données pour RJCFormationSarl .

Il intègre la protection des données en tant que thématique essentielle dans son système de gestion des risques et procède à l'évaluation des risques liés de manière stratégique et différenciée selon les niveaux concernés.

Il valide le présent concept de protection des données et le passe régulièrement en revue.

Il désigne le/la responsable de la protection des données, définit ses attributions, ses responsabilités et ses compétences dans un cahier des charges, en tenant compte des dispositions légales en vigueur, et prend connaissance des rapports que le/la responsable lui soumet régulièrement.

10.2 Direction

La direction est responsable, en collaboration avec le secrétariat, de la mise en œuvre du présent concept et du respect des prescriptions légales en matière de protection des données dans le cadre de l'ensemble des traitements de données réalisés au niveau opérationnel.

Elle prend les mesures nécessaires pour que tous les collaborateurs soient régulièrement sensibilisées aux enjeux liés à la protection des données et informés des directives du présent concept et de leur application dans leur quotidien professionnel.

10.3 Responsable de la protection des données

Le secrétaire de direction veille à l'interne à la sécurité des données selon la législation en vigueur et son cahier des charges.

Il/Elle est la personne de référence pour tout ce qui concerne la protection des données, à l'interne et à l'externe.

Il/Elle supervise la licéité du traitement des données effectué au sein de RJCFormationSarl.

Il/Elle est autorisée à établir et faire respecter les directives nécessaires à assurer le respect de la législation en vigueur et la mise en application du présent concept.

Le cas échéant, il/elle peut adresser un signalement aux préposés fédéraux et/ou cantonaux à la protection des données.

Il/Elle rend régulièrement compte à la direction pour tout ce qui relève de la protection des données au sein de RJCFormationSarl , signale les risques identifiés, et recommande les dispositions à prendre pour d'éventuelles améliorations.

Il/Elle rapporte immédiatement tout incident sortant de l'ordinaire ou de portée particulière.

Il/Elle procède régulièrement à des audits relatifs à la protection des données, en faisant appel, si nécessaire, à des ressources externes.

Il/Elle se tient à la disposition de la direction, de la direction des RH, des collaborateurs/-trices ainsi que des clients pour les conseiller sur tout ce qui concerne la protection des données.

10.4 Direction des RH

La direction des RH est responsable, dans le cadre de sa gestion du personnel de l'entreprise, du traitement diligent et conforme à la protection des données des collaborateurs/-trices.

10.5 Encadrement

Les supérieurs hiérarchiques, à tous les niveaux, ont une fonction d'exemplarité et encouragent leurs collaborateurs/-trices à intégrer la protection des données dans leurs tâches et fonctions professionnelles.

Dans le cadre de leurs attributions, ils et elles sont responsables de la mise en application et du respect des dispositions relatives à la protection des données, en particulier en lien avec le présent concept et les divers processus opérationnels.

En collaboration avec le/la responsable de la protection des données, ils et elles s'assurent que leurs collaborateurs/-trices soient sensibilisé·e·s à la protection des données et veillent à les épauler dans la pratique.

10.6 Collaboratrices et collaborateurs

L'ensemble des collaborateurs/-trices de RJCFormationSarl ayant à traiter des données personnelles sont responsables à titre personnel de la protection de ces données et le font en conformité avec les dispositions du présent concept et les directives établies par le responsable de la protection des données.

Pour toute question ou besoin d'éclaircissement, ils et elles se réfèrent à leur hiérarchie ou à la personne responsable de la protection des données.

Le présent concept entre en vigueur au 01 octobre 2024.

Genève le 1er octobre 2024

RJCFormationSarl

Jean-Charles ROUILLER

11. Annexe : Définitions

Données personnelles	Informations relatives à une personne physique identifiée ou identifiable.
Données personnelles sensibles	a) Les données relatives aux opinions ou activités religieuses, philosophiques, politiques ou syndicales ; b) Les données relatives à la santé, à l'intimité ou à l'appartenance à un groupe ethnique ou à une origine ; c) Les données génétiques ; d) Les données biométriques identifiant sans équivoque une personne physique ; e) Les données relatives aux poursuites ou sanctions administratives et pénales; f) Les données relatives aux mesures d'aide sociale.
Traitement de données personnelles	Tout traitement de données personnelles, quels que soient les moyens et procédés utilisés, tels que la collecte, l'enregistrement, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données.
Communication de données personnelles	Toute transmission ou mise à disposition de données personnelles.
Collecte de données	Ensemble de données personnelles dont la structure permet de rechercher les données en fonction de personnes déterminées.
Responsable de la protection des données	Personne chargée à l'interne de la conformité et du respect des dispositions relatives à la protection des données. Il ou elle tient notamment un registre des fichiers.
Maître du fichier	Personne responsable du traitement de données. Il ou elle décide seul·e ou avec d'autres de la finalité et des moyens du traitement.
Profil de personnalité	Ensemble de données permettant d'évaluer des aspects essentiels de la personnalité d'une personne physique.
Profilage	Évaluation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée (afin d'analyser ou de prédire, par exemple, le rendement au travail, la situation économique, la santé, le comportement, certaines préférences, le lieu de séjour ou la mobilité).