



**Concept de
protection
des données**



**TRAVAIL ET
INTÉGRATION**



TABLE DES MATIÈRES

1.	But et portée	3
2.	Bases juridiques.....	3
3.	Définitions	3
4.	Champ d'application	3
5.	But et Finalité.....	3
6.	Les principes régissant la protection des données.....	4
6.1	Licéité	4
6.2	Proportionnalité	4
6.3	Finalité	4
6.4	Transparence	4
6.5	Qualité des données	4
6.6	Bonne foi.....	4
7.	Type de données personnelles traitées et finalité du traitement	4
7.1	Données personnelles traitées	4
7.2	Finalités du traitement.....	5
8.	Sécurité des données : mesures préconisées	5
8.1	Mesures organisationnelles	5
8.2	Mesures techniques	5
8.3	Archivage & Suppression	6
9.	Droits des personnes concernées.....	6
9.1	Information/Sensibilisation	6
9.2	Droit d'accès/de consultation	6
9.3	Droit de rectification.....	6
9.4	Blocage/Refus de communication des données.....	6
10.	Recommandations pratiques	7
10.1	Comment gérer les demandes par téléphone ou par écrit.....	7
10.2	Principes applicables à l'utilisation des courriers électroniques	7
10.3	Utilisation d'images/d'enregistrements	7
11.	Responsabilités.....	7
11.1	Comité	7
11.2	Direction	7
11.3	Référente à la protection des données.....	8
11.4	Service RH.....	8
11.5	Encadrement	8
11.6	Collaboratrices et collaborateurs.....	8
12.	Annexe : Définitions.....	10

1. But et portée

Le présent concept sur la protection des données de l'OSEO Vaud 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 nos participant-e-s, de nos collaborateurs-trices et également, si applicable, de nos partenaires commerciaux. Il constitue la base incontournable applicable à l'ensemble des mesures et activités de l'OSEO Vaud, en particulier en ce qui concerne le traitement

- Des données personnelles des participant-e-s;
- 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 mesure 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 relative à la loi fédérale sur la protection des données ainsi que les dispositions cantonales vaudoises du 11.09.2007 en matière de protection des données.

L'OSEO Vaud est une association de moins de 250 collaborateurs. Les données collectées sont pour l'essentiel des données personnelles. La collecte de données personnelles sensibles représente une part minoritaire de son activité. De par son activité, l'OSEO Vaud n'est pas soumise à la tenue d'un Registre des activités de traitement au sens de l'article 12 alinéa 5 LPD.

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 l'OSEO Vaud ayant à traiter des données personnelles dans le cadre de l'accomplissement de leurs tâches et fonctions.

5. But et 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 l'OSEO Vaud d'être en parfaite conformité avec les exigences relatives à la protection des données, en toute connaissance de cause.

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. Les 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.

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

L'OSEO Vaud traite les données personnelles en respectant le principe de la bonne foi.

7. Type de données personnelles traitées et finalité du traitement

7.1 Données personnelles traitées

L'OSEO Vaud collecte directement les données de ses collaborateurs-trices, participant-e-s et membres par l'intermédiaire de formulaire numérique, papier ou renseignements oraux fournis :

- Les données d'identification ;
- Les coordonnées de contact ;
- Les données relatives à la nationalité et au titre de séjour ;
- Pour les participant-e-s mineur-e-s ou sous curatelle : les données relatives aux personnes responsables ;
- Les données relatives à la formation, à la carrière préprofessionnelle et professionnelle ;
- Les données relatives à la participation à des mesures d'insertion ;
- Les données relatives aux assurances sociales, notamment l'AI et l'AC.

Les données ci-dessus peuvent aussi être collectées auprès de tiers, notamment les assurances sociales, les institutions publiques en charge de la formation ou de l'insertion ou encore d'autres prestataires de mesures d'insertion.

Les collaborateurs-trices fournissent spontanément ou sur demande toutes les données qui portent sur leurs aptitudes à remplir leur emploi ou qui sont nécessaires à l'exécution du contrat de travail (art.328b CO).

7.2 Finalités du traitement

Les données personnelles des participant-e-s aux mesures de l'OSEO sont traitées dans le but de les identifier, d'assurer un suivi adéquat des mesures, d'attester de leur bon déroulement auprès des commanditaires et de conseiller les participant-e-s quant à la suite de leur carrière. Elles peuvent aussi être collectées à des fins de statistiques ou d'évaluation des politiques publiques après avoir été anonymisées.

Les données personnelles des collaborateurs-trices sont traitées dans la mesure où elles portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail (art.328b CO).

8. 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.

8.1 Mesures organisationnelles

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

Les cadres compétent-e-s, fixent les règles applicables à chaque fichier de données, détermine qui a accès aux données personnelles, et sous quelles conditions, et précise la manière dont ces processus sont supervisés.

Conformément aux exigences légales, la qualité tient un registre cartographique, et s'assure qu'il soit toujours à jour.

8.2 Mesures techniques

La protection des données informatisées est garantie en particulier par l'utilisation appropriée qui en est faite aux moyens de l'utilisation de pare-feu, de programmes anti-virus, etc...

De plus une connexion sécurisée sur une plateforme informatique (bureau virtuel), une gestion des accès et supports de données personnelles permettent d'empêcher que des personnes non autorisées aient accès à des bases de données ou puissent les modifier, les effacer, s'en emparer, etc...

La protection des données informatisées est garantie :

- Par une utilisation appropriée des personnes.
- Par des moyens appropriés tels que l'utilisation d'une identité personnelle électronique sécurisée (si le destinataire fait partie de la communauté), de pare-feux, de programmes anti-virus, etc...
- Par une connexion sécurisée à une plateforme informatique (bureau virtuel) dont les accès empêchent les personnes non autorisées de pouvoir consulter, modifier, supprimer ou de s'emparer de données personnelles.

8.3 Archivage & Suppression

Les données personnelles dont le traitement n'est plus utile et qu'il n'est pas nécessaire de conserver pour respecter une obligation légale ou pour la bonne tenue des archives sont supprimées. La procédure d'archivage est régie dans une directive.

9. 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.

9.1 Information/Sensibilisation

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

9.2 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. Elle a également le droit de connaître les personnes responsables du traitement et, en cas de transmission les destinataires ou catégories de 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 (art.25 alinéa 7 LPD).

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 (art. 26 LPD).

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.

9.3 Droit de rectification

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

9.4 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.

10. 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.

10.1 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* (mineur).

Dans le cas de demandes par téléphone, il convient de s'assurer de manière claire et sans équivoque de l'identité de la personne qui appelle. Lorsque les appels sont enregistrés, il est obligatoire de le signaler et d'obtenir le consentement de l'interlocuteur-trice.

10.2 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 échanges 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 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 l'OSEO Vaud informent les collaborateurs-trices et les participants-es sur l'utilisation de l'informatique qui s'appliquent également en l'espèce.

10.3 Utilisation d'images/d'enregistrements

Seules les personnes ayant donné leur consentement exprès 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.

11. Responsabilités

11.1 Comité

Le Comité est responsable, au niveau stratégique, de la garantie de la protection des données pour l'OSEO Vaud.

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.

11.2 Direction

La direction est responsable, en collaboration avec le/la responsable de la protection des données, 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-trices soient régulièrement sensibilisé-e-s aux enjeux liés à la protection des données et informé-e-s des directives du présent concept et de leur application dans leur quotidien professionnel.

Il désigne le/la référent-e 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 référent-e lui soumet régulièrement.

11.3 Référente à la protection des données

Le/La référent-e de la protection des données 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.

Il/Elle participe lors d'un échange annuel à la licéité du traitement des données effectué au sein de l'OSEO Vaud.

Il/Elle est autorisé-e à établir et à sensibiliser 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 sur une base d'un rapport d'audit (non-conformité), approuvé par le Comité et la Direction, un signalement aux préposés fédéraux et/ou cantonaux à la protection des données.

Il/Elle rend compte à la direction pour tout ce qui relève de la protection des données au sein de l'OSEO Vaud signale les risques identifiés, et recommande les dispositions à prendre pour d'éventuelles améliorations. Il/Elle rapporte immédiatement tout incident sur la base d'audit annuel ou de rapport de non-conformité sortant de l'ordinaire ou de portée particulière.

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

Il/Elle se tient à la disposition de la direction, des responsables de secteurs, des services centraux, des collaborateurs-trices ainsi que des participant-es pour les conseiller sur tout ce qui concerne la protection des données. Mail to : Qualité@oseo-vd.ch

11.4 Service RH

Le services 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.

11.5 Encadrement

Les supérieurs-es 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.

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.

11.6 Collaboratrices et collaborateurs

L'ensemble des collaborateurs-trices de l'OSEO Vaud 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 qui s'y rattachent.

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

Le présent concept entre en vigueur 1^{er} février 2024

Vevey, le 30 janvier 2024

OSEO Vaud

La Présidente

Myriam Romano-Malagrifa

Le Directeur

Yves Ecoeur

Annexe : Définitions

11.6.1 Données personnelles	11.6.2 Informations relatives à une personne physique identifiée ou identifiable.
11.6.3 Données personnelles sensibles	<ul style="list-style-type: none"> 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.
11.6.4 Traitement de données personnelles	11.6.5 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.
11.6.6 Communication de données personnelles	11.6.7 Toute transmission ou mise à disposition de données personnelles.
11.6.8 Collecte de données	11.6.9 Ensemble de données personnelles dont la structure permet de rechercher les données en fonction de personnes déterminées.
11.6.10 Personnes référente	11.6.11 Personne chargée à l'interne de la conformité et du respect des dispositions relatives à la protection des données.
11.6.12 Personne responsable du fichier	11.6.13 Personne responsable du traitement de données. Il ou elle décide seul-e ou avec d'autres de la finalité et des moyens du traitement.
11.6.14 Profil de personnalité	11.6.15 Ensemble de données permettant d'évaluer des aspects essentiels de la personnalité d'une personne physique.
11.6.16 Profilage	11.6.17 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).