Directive sur la protection et la sécurité des données

Table des matières

1. Généralités

1.1. Buts

La présente directive a pour objet de sensibiliser et informer les collaborateurs des mesures prises afin de traiter, dans le respect du cadre légal relatif au domaine de la protection des données, les données personnelles des participants aux mesures délivrées par l'Association InVia - ci-nommés participant.es - ainsi que celles de ses collaboratrices et collaborateurs.

1.2. Principes

1 L'Association InVia garantit aux participant.es et aux collaborateurs une protection efficace contre l'emploi abusif des données personnelles.
2 Le traitement des données collectées par InVia doit être conforme au principe de proportionnalité et de bonne foi.
3 Seules les données absolument nécessaires InVia dans le cadre de son mandat ou de la gestion administrative RH peuvent être collectées.
4 La personne concernée doit être informée du but et du type de traitement des données. Le traitement de données à l'insu de la personne concernée est interdit.

1.3. Bases légales applicables

Les bases légales suivantes sont notamment applicables à la protection des données :
a. La Constitution fédérale, notamment l'art. 13 al. 2 selon lequel « toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent » ;

b. Loi fédérale sur la protection des données (LPD) ;

c. Loi fédérale sur la partie générale du droit des assurances sociales (LPGA) ;

d. Loi fédérale sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité (LACI) ;

e. Loi vaudoise sur la protection des données personnelles (LPrD).

1.4. Définitions

1 Les notions telles que définies à l'art. 3 LPD sont applicables à la présente directive.
2 Pour rappel, on entend par :
a. données personnelles : toutes les informations qui se rapportent à une personne identifiée ou identifiable ;

b. données personnelles sensibles : les données sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, l'appartenance fondée sur une origine raciale ou ethnique, la sphère intime, en particulier la santé psychique, mentale ou physique, les mesures d'aide sociale, les donnée génétiques, les données biométriques, les poursuites ou les sanctions pénales et administratives.

c. personne concernée : la personne physique au sujet de laquelle des données sont traitées ;

d. traitement des données : toute opération destinée notamment à collecter, conserver, modifier, combiner, communiquer ou détruire des données personnelles ;

e. communication des données : le fait de rendre des données personnelles accessibles (octroi de droit d'accès à des tiers), notamment par voie de consultation, de publication ou d'information par oral ;

f. fichier : le recueil de l'ensemble des données personnelles dont la structure permet de rechercher les données de façon nominative ;

g. Responsable du traitement des données : la personne physique ou morale ou autorité publique qui détermine le contenu ainsi que les finalités du fichier.

h. finalité : le but pour lequel des données sont traitées.

1.5. Principe de proportionnalité

1 Il ne peut y avoir collecte de données que si elles sont appropriées et nécessaires au but visé.
2 La forme de traitement la moins intrusive et permettant d'atteindre le but visé doit être choisie.
3 Toute collecte anticipée de données sans but défini préalablement est prohibée.

1.6. Principe de bonne foi

1 Le traitement ainsi que la finalité du traitement des données doivent être reconnaissables par la personne concernée.
2 La personne concernée doit impérativement être informée de la finalité du traitement des données lors de la collecte.
3 Tout traitement de données à l'insu de la personne concernée est interdit.

1.7. Exigences d'exactitudes

1 Celui qui traite les données doit s'assurer qu'elles sont complètes, exactes et à jour.
2 Les données collectées doivent être rectifiées lorsqu'elles s'avèrent inexactes ou plus actuelles, soit à l'initiative du responsable du traitement des données soit sur demande de la personne concernée (voir art. 14 ss Droit d'accès).

1.8. Sécurité des données

1 Celui qui traite des données personnelles doit prendre les mesures organisationnelles et techniques appropriées afin d'empêcher tout accès, traitement ou manipulation illicites (protection physique et électronique).
2 Plus les données sont sensibles, plus l'exigence de sécurité doit être stricte.

2. Protection des données des participant.es des prestations

2.1. Principes relatifs à la collecte de données

1 Sauf consentement écrit du mandant, le traitement de données personnelles n'est possible que lorsqu'il est indispensable à l'exécution du contrat conclu avec le mandant.
2 Les données pertinentes pouvant faire l'objet d'un traitement de données peuvent être des données personnelles, y compris les données sensibles qui sont nécessaires pour accomplir les tâches requises par le mandat, notamment pour :
a. enregistrer, conseiller et placer les participant.es des prestations ;

c. gérer l'exécution des prestations ;

d. établir des statistiques.

3 Par contrat conclu avec le mandant, il faut entendre :
a. le cahier des charges, le mandat ainsi que la convention de prestations des autorités cantonales de subvention ;

b. les accords d'objectifs conclus avec les participants ;

c. les contrats conclus avec les clients privés (entreprises ou particuliers).

2.2. Traitement de données personnelles sensibles

1 Le traitement de données personnelles sensibles est possible uniquement avec le consentement de la personne concernée.
2 Le traitement de données personnelles sensibles doit être nécessaire à l'exécution du mandat.
3 Seules des données personnelles sensibles ayant été rendues crédibles par un document écrit ou ayant été communiquées directement par la personne concernée peuvent être traitées.

2.3. Enregistrements d'entretiens

1 L'enregistrement d'un entretien à l'aide d'un appareil, notamment un enregistreur audio, vidéo, un Smartphone ou tout autre appareil électronique, est illicite s'il n'a pas reçu l'assentiment de la personne enregistrée et qu'il n'entre pas dans une démarche directement indispensable à l'exécution du mandat.
2 Il est rappelé aux collaborateurs la teneur de l'art. 179 CP :

- Celui qui, sans le consentement de tous les participants, aura écouté à l'aide d'un appareil d'écoute ou enregistré sur un porteur de son une conversation non publique entre d'autres personnes,
- celui qui aura tiré profit ou donné connaissance à un tiers d'un fait qu'il savait ou devait présumer être parvenu à sa propre connaissance au moyen d'une infraction visée à l'al. 1,
- celui qui aura conservé ou rendu accessible à un tiers un enregistrement qu'il savait ou devait présumer avoir été réalisé au moyen d'une infraction visée à l'al. 1,

sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

2.4. Obligation de conserver le secret

1 Les collaborateurs sont tenus, conformément à l'art. 321a al. 4 CO, à garder secrets les faits destinés à rester confidentiels.
2 Une violation de l'obligation de garder le secret pourrait être sanctionnée par l'art. 162 CP ainsi que l'art. 35 LPD. L'art. 320 CP relatif à la violation du secret de fonction pourrait également être applicable.
3 Sauf exceptions prévues par accord de la personne concernée, la loi ou la présente directive, la communication des données personnelles à des tiers est interdite.
4 Le secret de fonction est applicable aussi bien à l'interne de la Fondation qu'à l'externe. Les collaboratrices et collaborateurs sont toutefois autorisés à échanger, dans l'intérêt du participant.e, des informations utiles et nécessaires à l'accomplissement du mandat.
5 L'obligation de garder le secret reste également applicable après la fin des rapports de travail.
6 Lorsqu'un collaborateur est amené à témoigner au tribunal à propos d'un participant.e, son secret de fonction doit être levé par écrit par la direction. S'il a l'obligation de témoigner, il doit communiquer de manière factuelle et précise sans porter de jugement et sans prendre parti.

2.5. Communication de données personnelles à des tiers

1 Sauf dispositions contraires de la présente directive, la communication de données personnelles à des tiers est interdite.
2 Des données personnelles peuvent être communiquées à des tiers si celles-ci sont nécessaires au but visé, à savoir conclure ou exécuter un contrat avec la personne concernée, par exemple dans le cadre d'un placement en entreprise. Les données sensibles ou permettant d'établir un profil de personnalité ne peuvent en aucun cas être divulguées à des tiers.
3 La communication des données pertinentes n'est autorisée que si elle est destinée à une partie liée à l'exécution du mandat.
4 Dans la mesure où aucun intérêt privé prépondérant ne s'y oppose, et sous réserve de l'aval du prescripteur, il est possible de communiquer des données dans le cadre de la réalisation du mandat, notamment à d'autres organes d'exécution, aux autres assureurs sociaux (AVS, AI, LAA, LACI,…) pour les données nécessaires à la fixation, la modification ou la restitution des prestations.

5 Sur demande écrite, il est possible de communiquer des données aux autorités judiciaires (par exemple aux tribunaux). Dans tous ces cas la demande doit être transmise à la direction pour traitement.
6 Il est possible de communiquer des données à d'autres personnes ou autorités moyennant le consentement écrit et éclairé de la personne concernée.
7 La communication illicite de données personnelles sensibles peut être considérée comme une faute professionnelle grave pouvant justifier un licenciement avec effet immédiat. Un tel acte peut également être constitutif d'une infraction pénale.
8 Au vu de la difficulté d'application de ces règles, il est vivement recommandé de demander au participant.e s'il autorise à fournir à des tiers des renseignements le concernant. Et en cas de doute, il est indispensable de s'adresser à la direction.

2.6. Droit de consulter

1 Les participant.es peuvent, sur demande, avoir accès aux données qui les concernent.
2 Toutes les données ainsi que le but et les catégories de données personnelles traitées doivent être communiquées au participant.e qui en a fait la demande. Si le traitement des données est justifié par une base légale, celle-ci doit être indiquée au participant.e.

2.7. Droit de rectification ou de destruction

1 Les participant.es peuvent demander l'actualisation des données les concernant et leur rectification si celles-ci s'avèrent erronées.
2 Les participant.es peuvent demander la destruction de données indûment conservées.

2.8. Sécurité des données

1 Le dossier physique du participant.e est conservé dans les seuls endroits définis et reconnus comme étant le lieu de stockage avec protection des accès aux locaux. La porte du local doit être fermée à clé et les dossiers rangés sous clé.
2 Le dossier électronique ne doit être accessible que via un mot de passe d'accès au réseau informatique.

2.9. Archivage

1 L'archivage doit être limité aux pièces utiles et aux durées légales prescrites.
2 Les dossiers des participant.es doivent être détruits au bout de 3 ans (maximum) après la fin de la mesure, 10 ans pour des mesures AI.
3 Les éventuels documents appartenant aux participant.es (support de cours, portfolio, CV, dossier de candidature, tests psychométriques, etc.) doivent leur être remis dès la fin de la prestation. S'ils ne sont pas récupérés, ils sont détruits.
4 Seules les données personnelles pertinentes pour l'exécution du mandat peuvent être saisies et stockées ; ce sont, en principe, celles nécessaires à l'appréciation de l'employabilité du participant.e ainsi que les différents rapports fournis aux prescripteurs.
5 Toutes les correspondances électroniques concernant un participant.e doivent être effacées dans un délai de deux mois (intervenant.es dans les mesures) ou maximum au bout de 3 ans (InVia).

2.10. Sécurité informatique

La Directive & Déclaration relative à l'informatique doit être respectée afin de garantir la sécurité des données informatiques.

3. Données des collaboratrices et collaborateurs de l'Association

3.1. Bases légales applicables

Les règles du Code des obligations, notamment l'art. 328b CO, ainsi que les dispositions de la loi fédérale du 25 septembre 2020 sur la protection des données sont applicables au traitement des données des employé.es de l'Association.

3.2. Traitement des données

Les données concernant les collaboratrices et collaborateurs ne peuvent être collectées que de manière licite. Les principes de proportionnalité et de bonne foi doivent être respectés.

3.3. Dossier du collaborateur

1 L'employeur tient un dossier comprenant l'ensemble des observations écrites le concernant et étant indispensables à l'exécution du travail, en particulier les indications ayant trait à l'établissement, au déroulement, aux modalités et à la résiliation du contrat de travail.
2 Le dossier du collaborateur peut comprendre, notamment :
a. les coordonnées et l'adresse ;
b. le dossier de candidature et les références demandées lors de l'engagement ;
c. le contrat de travail ;
d. les renseignements relatifs aux arrêts de travail et aux vacances ;
e. les certificats médicaux ;
f. les données relatives aux salaires et aux assurances ;
g. les formations continues effectuées ;
h. les entretiens de collaboration ;
i. les avertissements et leurs suivis ;
j. la correspondance entre employé.e et employeur ;
k. les notes rédigées à la suite d'entretiens particuliers ;
l. les extraits de registre.

3.4. Conservation des données

1 Tous les deux ans, un tri est effectué afin de retirer des dossiers du personnel les documents devenus inutiles.
2 Lorsque les rapports de travail ont pris fin, seules sont conservées les données indispensables ; peuvent être également conservées les données dont l'association a besoin pour un litige. La conservation de ces données est limitée à 10 ans suivant la fin des relations de travail.

3.5. Droit de consultation du dossier

1 Le collaborateur peut, sur demande adressée à la direction, consulter son dossier personnel.
2 Sauf circonstances exceptionnelles, la collaboratrice ou le collaborateur n'a aucun droit d'accès aux notes que l'employeur a établies à des fins personnelles et qui ne sont pas communiquées à des tiers ; il ne peut pas non plus consulter les dossiers relatifs à la planification des besoins en personnel ou aux plans de carrière.
3 Il peut exiger la rectification des informations erronées ou la destruction des données indûment conservées (voir art. 13 s.).
4 Conformément à l'art. 25 LPD, l'employé.e conserve un droit d'accès même lorsque les rapports de travail ont pris fin.

Art. 24 – Accès au dossier

1 Les données contenues dans le dossier sont traitées uniquement par le département RH et ne sont accessibles qu'aux services et cadres de direction fondés à les utiliser de par les fonctions qu'ils exercent.

5 Le dossier physique est conservé en un seul endroit avec protection des accès aux locaux, fermeture de la porte de bureau à clé, rangement des dossiers sous clé. Le dossier électronique sur le réseau informatique est protégé par un accès réservé aux collaborateurs RH et à la direction.

4. Données des intervenantes et intervenants au sein de l'Association

4.1. But du recueil des données

Les données des intervenant.es sont recueillies dans le cadre notamment des exigences de la certification Eduqua. En effet, il est de la responsabilité de l'Association de s'assurer que les personnes intervenant auprès de nos participant.es sont au bénéfice de l'expérience et des titres requis.

4.2. Traitement des données

Les données concernant les intervenant.es ne peuvent être collectées que de manière licite. Les principes de proportionnalité et de bonne foi doivent être respectés.

4.3. Dossier de l'intervenant.e

Le dossier peut comprendre notamment :

a. Les coordonnées et l'adresse de l'intervenant.e, privées et/ou professionnelles
b. Le CV contenant les données usuelles
c. Les diplômes, titres, certificats, attestations de cours suivis
d. Les évaluations, notamment les rapports de satisfaction des participant.es
e. Les directives signées
f. Toute correspondance utile

4.4. Conservation des données

Les données sont conservées pendant la durée des rapports de collaboration, sous format électronique.
Dans le cas d'un litige, les données sont conservées 10 ans.

5. Droits d'utilisation des supports pédagogiques

Les accords sur les droits d'utilisation des supports pédagogiques sont réglés dans les conventions de mandat avec les prestataires. Voici les principes de base. Les conventions de mandat font foi en cas de différence avec la présente directive.

5.1. Propriété et utilisation des supports de cours et d'animation

Les supports de cours et d'animation sont mis à disposition libre de l'Association InVia, qui les met à disposition de l'ensemble des intervenant.es d'une même mesure. La propriété reste réservée aux auteurs/autrices des documents.

5.2. Propriété et utilisation des plans de cours

Les plans de cours, plans pédagogiques et tout document d'ingénierie sont mis à disposition de l'Association InVia. Ils sont partagés uniquement avec le prestataire concerné et avec l'institut d'audit Eduqua.

5.3. Conservation des données

Les différents supports et plans sont conservés jusqu'à 3 ans après leur dernière utilisation au sein d'une prestation Invia.