swissstaffing

Mémento: Loi fédérale révisée sur la protection des données (nLPD)

Conséquences pour les prestataires des services de l'emploi en Suisse

1. Situation initiale

La loi fédérale sur la protection des données totalement révisée (loi sur la protection des données; nLPD) et les nouvelles ordonnances sur la protection des données (OPDo) et sur les certifications en matière de protection des données (OCPD) entreront en vigueur le 1er septembre 2023. Il n'y aura pas de période transitoire.

Avec l'entrée en vigueur de la nLPD, les prestataires des services de l'emploi devront se conformer à de nouvelles obligations et avoir pris des mesures en conséquence. Celles-ci sont décrites plus précisément ci-dessous. Les renvois aux dispositions légales respectives se réfèrent à celles de la loi révisée sur la protection des données (nLPD).

La nLPD vise à protéger la personnalité et les droits fondamentaux des personnes dont les données personnelles (ci-après dénommées «données») font l'objet d'un traitement (art.1 nLPD). Elle s'applique au traitement de données personnelles de personnes physiques par des sociétés privées et des organes fédéraux (art. 2 al. 1 nLPD).

Les objectifs de la nLPD sont les suivants:

- en raison d'une évolution rapide de la technologie, la LPD actuelle, qui date de 1992, montre des déficiences qu'il convient de pallier;
- Il s'agit de tenir compte des réformes de l'Union européenne en la matière et d'aligner la protection des données en Suisse avec le Règlement européen sur la protection des données (RGPD européen). Celui-ci est entré en vigueur le 25 mai 2018 (voir mémento swissstaffing de mai 2018). [Concernant les adaptations pour les entreprises qui ont déjà mis en œuvre les exigences du RGPD européen, se reporter à l'annexe CHECK-LIST 1: DU RGPD EUROPÉEN À LA NLPD];
- La mise en œuvre de bonnes pratiques doit être encouragée: des devoirs plus stricts sont imposés aux personnes en charge des traitements de données, les droits des personnes concernées par le traitement de données et les compétences de surveillance du Préposé fédéral à la protection des données et à la transparence (PFPDT) sont renforcés.

2. Qu'est-ce qui reste inchangé avec l'entrée en vigueur de la nLPD révisée?

Les principes généraux du traitement des données restent inchangés dans la nLPD. Par conséquent, si les principes de traitement suivants sont respectés, le traitement de données personnelles ne requiert en principe ni consentement ni motif justificatif (art. 6, 7 et 8 en combinaison avec art. 30 nLPD):

- Les données personnelles ne peuvent être collectées que de manière licite. Cela signifie qu'elles ne doivent pas être obtenues par la menace ou la tromperie, ou à l'insu des personnes concernées (art. 6 al. 1 nLPD).
- Le traitement des données doit être effectué conformément au principe de la bonne foi. Celui-ci implique l'obligation d'être honnête, digne de confiance et prévenant (art. 6 al. 2 nLPD).

- Le principe de la proportionnalité doit être respecté. Celui-ci implique qu'il faut traiter autant de données nécessaires que l'exige le cas d'espèce, tout en veillant à ce qu'il y en ait le moins possible (art. 6 al. 2 et 4 nLPD).
- La collecte de données personnelles et en particulier le but de leur traitement doivent être reconnaissables pour la personne concernée; lors de la collecte, le but du traitement des données doit être indiqué ou ressortir des circonstances (art. 6 al. 3 nLPD).
- Celui qui traite des données personnelles doit s'assurer qu'elles sont exactes (art. 6 al. 5 nLPD).
- La sécurité des données doit être garantie; cela signifie que les données personnelles doivent être protégées par des mesures techniques et organisationnelles appropriées contre tout traitement non autorisé (art. 8 nLPD).

Il y a atteinte illicite à la personnalité, comme dans l'ancienne LPD, lorsque des données personnelles sont traitées en violation des principes généraux énoncés ci-dessus ou contre la volonté expresse de la personne concernée (art. 30 al. 1 et 2 nLPD). Dans ces cas, le traitement de données personnelles peut néanmoins être autorisé s'il existe un motif justificatif. Des motifs justificatifs sont, par exemple, le consentement de la personne concernée, un intérêt prépondérant privé ou public, ou une loi (art. 31 al. 1 nLPD). L'art. 31 al. 2 nLPD énumère plusieurs autres cas dans lesquels les intérêts prépondérants de la personne qui traite des données personnelles (responsable au sens de la nLPD) peuvent entrer en considération.

Outre les dispositions générales de la nLPD, le traitement des données personnelles est également régi en Suisse par l'art. 328b du Code des obligations (CO) et, pour les bailleurs de services, par la Loi sur le service de l'emploi et la location de services (LSE) et l'Ordonnance sur le service de l'emploi (OSE). Ces dispositions concrétisent avant tout le principe de proportionnalité en matière de protection des données (art. 6 al. 2 nLPD). On peut donc se référer, pour le traitement des données personnelles dans le contexte du recrutement de personnel, aux clauses déjà élaborées dans le cadre du RGPD de l'UE [voir aussi EXEMPLE 1: MODÈLE D'UNE CLAUSE DE CONSENTEMENT et EXEMPLE 2: MODÈLE DE CLAUSE DE PROTECTION DES DONNÉES ET DE CONSENTEMENT DANS LES CG en annexe à ce mémento avec un modèle mis à jour en tenant compte de la nLPD]. Il convient notamment de tenir compte des points suivants:

- Le bailleur de services n'est habilité à traiter des données personnelles que dans la mesure où et aussi longtemps que ces données sont nécessaires au placement (art. 7 al. 3 et art. 18 al. 3 LSE). S'il demande des références sur des candidats, ceci nécessite l'assentiment de la personne concernée (art. 47 al. 1 let. b et art. 19 al. 1 let. b, OSE).
- Le traitement d'une candidature pour un emploi représente un intérêt privé prépondérant du placeur ou du bailleur de services et justifie le traitement des données personnelles pour l'examen de la candidature ainsi que pour leur transmission à l'employeur ou à l'entreprise locataire de services. La collecte d'autres données ou l'enregistrement et l'utilisation ultérieure des données de candidature, après la fin de la procédure de recrutement, nécessitent le consentement du candidat en raison de la finalité du traitement des données.
- Au terme de la procédure de candidature, les données y afférentes doivent en principe être effacées. Seules les bases du contrat peuvent encore être conservées pour la facturation, la loi prévoyant à cet effet un délai de conservation de 10 ans. La conservation de plus longue durée et, par conséquent, une renonciation à l'effacement du dossier personnel ou à la transmission de celui-ci à d'autres employeurs potentiels exigent le consentement du candidat.

Dans certains cas, il peut s'avérer nécessaire à l'exécution de l'activité de location de services resp. de placement de traiter des données personnelles sensibles (par exemple des données relatives à la santé) (voir aussi le chiffre 3.3 de ce mémento). Si des données sensibles sont communiquées par le candidat avec les documents de sa postulation, celles-ci ne peuvent être traitées que dans le cadre de la candidature. Si ces données sont utilisées ultérieurement et qu'un consentement du candidat est nécessaire, ceci exige un consentement explicite de sa part.

3. Quelles nouveautés apporte la nLPD?

3.1 Suppression de la protection des personnes morales

Selon la nLPD, seules les données des personnes physiques sont dorénavant couvertes, et non plus celles des personnes morales comme les sociétés anonymes ou les associations (cf. art. 2 nLPD). Les personnes morales pourront toujours se référer au droit des sociétés et à la protection de la personnalité prévue par le Code civil.

3.2 Nouveaux concepts: responsable et sous-traitant

Au lieu de parler de maître de fichier comme jusqu'à présent, la notion de responsable et de sous-traitant est désormais introduite. Les responsables sont des entreprises privées (personnes morales) qui, seules ou conjointement avec d'autres, décident des finalités et des moyens du traitement des données personnelles (art. 5 let. j nLPD). Dans le cas de la location de services, le bailleur de services est responsable, le cas échéant avec la future entreprise locataire de services. En tant qu'employeur légal, le bailleur de services est le premier point de contact du travailleur et traite les données personnelles pour le processus de candidature. Si une entreprise locataire de services adéquate est trouvée, les données personnelles sont transmises, de sorte que l'entreprise locataire de services et le bailleur de services traitent parfois les données personnelles en même temps et sont donc, selon la nLPD, tous deux responsables à ce moment-là.

En revanche, à l'issue d'un placement réussi, c'est l'employeur qui traitera à l'avenir les données personnelles à ses propres fins et sera donc à partir de ce moment-là le seul responsable.

Les sous-traitants sont des privés, en général également des personnes morales, qui traitent des données personnelles pour le compte du responsable (art. 5 let. j nLPD). Il peut s'agir du prestataire de services informatiques à qui le prestataire des services de l'emploi confie le traitement des données en recourant à la technologie « cloud », ou des prestataires qui établissent les fiches de paie pour le compte d'un prestataire des services de l'emploi.

3.3 Élargissement du catalogue des données sensibles

Le catalogue des données personnelles sensibles (comme les données relatives à la santé, les données sur opinions politiques) a été étendu aux données génétiques et biométriques (art. 5 let. c nLPD). Le traitement de données personnelles sensibles est soumis à des exigences plus strictes que le traitement de données personnelles «normales». Si le traitement nécessite le consentement de la personne concernée, celui-ci doit être donné de manière explicite (art. 6 al. 7 let. a nLPD).

3.4 Profilage et profilage à risque élevé

L'évolution technologique permet aujourd'hui, et toujours plus intensivement, de saisir, de traiter, de combiner et d'analyser de manière automatisée d'énormes quantités de données, afin de pouvoir par exemple déterminer des tendances, des corrélations ou d'autres caractéristiques qui peuvent à leur tour être attribuées à certains groupes. À l'aide de tels groupes de comparaison, il est possible de déterminer ou de prédire les

caractéristiques ou le comportement de personnes physiques. C'est la raison pour laquelle la notion de profilage fait son entrée dans la nLPD. Une différence est faite entre le profilage «normal» et le profilage à risque élevé. Le profilage (normal) est toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique (art. 5 let. f nLPD). Un tel profilage normal se produit par exemple lorsqu'un vendeur écrit à tous les acheteurs de certains vins parce qu'il pense qu'ils sont les plus susceptibles d'être intéressés par une nouvelle livraison de ces mêmes vins. La nLPD ne restreint un tel comportement ni plus ni moins que n'importe quel autre traitement de données.

Si le profilage conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique, il s'agit alors de profilage à risque élevé. Un tel traitement comporte un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Le contrôle de solvabilité et les analyses de fraude sont ici des exemples. À l'avenir, de tels traitements devraient jouer un rôle plus important dans les processus de candidature. Pour le profilage à risque élevé, des conditions plus strictes s'appliquent en ce qui concerne le traitement des données personnelles. Si le traitement nécessite le consentement de la personne concernée, celui-ci doit être donné de manière explicite (art. 6 al. 7 let. b nLPD). En général, une analyse d'impact relative à la protection des données (AIPD) doit être effectuée (voir chiffre 3.11).

3.5 Protection des données dès la conception et protection des données par défaut

Avec le principe de protection des données dès la conception (data protection by design) nouvellement introduit dans la nLPD, le responsable du traitement est tenu de mettre en place des mesures techniques et organisationnelles afin que le traitement respecte les prescriptions de protection des données (art. 7 al. 1 et 2 nLPD). En d'autres termes, le software et le hardware doivent être conçus et développés de manière à respecter les principes du traitement (cf. chiffre 2 ci-dessus). De plus, selon le principe de protection des données par défaut (data protection by default), le responsable du traitement est tenu de garantir, par le biais de préréglages appropriés, que le traitement des données personnelles est limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement (art. 7 al. 3 nLPD).

3.6 Devoir d'informer étendu

Selon la nLPD, les informations relatives au traitement des données personnelles doivent être mises à la disposition des personnes concernées de manière adéquate (art. 19 ss nLPD). Les déclarations de protection des données sur les sites web, les applications et les formulaires sont des exemples indiquant comment les données personnelles sont concrètement traitées et comment les informations peuvent être mises à la disposition des personnes concernées. Au minimum, les informations suivantes doivent être mises à la disposition des personnes concernées:

- l'identité et les coordonnées du responsable du traitement;
- la finalité du traitement;
- si les données personnelles ne sont pas collectées auprès de la personne concernée, les catégories de données traitées;
- le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles

sont communiquées;

- et les pays auxquels les données personnelles sont transmises et sur quelle base juridique cela se fait (le cas échéant, les garanties contractuelles ou les exceptions appliquées) [voir chiffre 3.9 et annexe CHECK-LIST 2: MISE EN ŒUVRE DES EXIGENCES DE LA NLPD].

3.7 Extension des droits des personnes concernées

Selon la nLPD, les droits actuels des personnes concernées à l'information, à l'effacement ou au blocage (restriction) de leurs données personnelles sont maintenus et partiellement adaptés. La personne concernée reçoit les informations nécessaires pour qu'elle puisse faire valoir ses droits selon la présente loi et pour que la transparence du traitement soit garantie (art. 25 al. 2 nLPD). En principe, les renseignements sont fournis gratuitement et doivent être transmis en général dans un délai de 30 jours (art. 25 al. 6 et 7 nLPD). Un droit à la portabilité des données est également introduit (art. 28 ss. nLPD). En conséquence, toute personne peut exiger du responsable du traitement qu'il lui remette sous un format électronique couramment utilisé les données personnelles la concernant et qui lui ont été préalablement communiquées ainsi que celles qui ont été traitées de manière automatisée sur la base d'un consentement ou d'un contrat ou qu'il transmette ces données personnelles la concernant à un autre responsable du traitement (art. 28 nLPD).

3.8 Droit de veto sur le traitement de données personnelles par des sous-traitants

Selon la nLPD, le traitement de données personnelles peut être confié à un tiers pour autant qu'un contrat ou la loi le prévoie, si seuls sont effectués les traitements que le prestataire des services de l'emploi serait en droit d'effectuer lui-même et si aucune obligation légale ou contractuelle de garder le secret ne l'interdit (art. 9 al. 1 nLPD). Les traitements de données pour les décomptes salaires, la comptabilité financière par des centres de traitement, l'externalisation du traitement des données à un prestataire de services informatiques via la technologie « cloud » ou le recours à des prestataires pour l'envoi de newsletters sont des exemples de transfert du traitement des données personnelles à des tiers (sous-traitants). Dans ce cas, le responsable demeure toujours responsable du traitement des données. Il doit ainsi s'assurer que le tiers mandaté garantit la sécurité des données (art. 8 al. 2 nLPD). Désormais, le sous-traitant ne peut lui-même sous-traiter un traitement à un tiers qu'avec l'autorisation préalable du responsable du traitement (droit de veto) (art. 9 al. 3 nLPD). Le sous-traitant annonce dans les meilleurs délais au responsable du traitement tout cas de violation de la sécurité des données (art. 24 al. 3 nLPD). Il est par conséquent recommandé de formuler, dans une annexe au contrat ou dans les CG, un engagement afin que les obligations en matière de protection des données soit respectées. Le modèle d'une formulation type dans les conditions générales est présenté en annexe [EXEMPLE 3: MODÈLE CLAUSE DE SOUS-TRAITANCE DANS LES CG].

3.9 Liste des pays ayant une protection des données équivalente publiée par le Conseil fédéral

Selon la nLPD, en cas de communication de données à l'étranger, comme c'est par exemple le cas lorsqu'on fait appel à un prestataire se trouvant à l'étranger (p. ex. un fournisseur de services IT ayant son siège aux USA), il convient de s'assurer que la personnalité des personnes concernées n'est pas mise en danger. Les données personnelles peuvent être transférées vers des pays disposant d'une protection des données équivalente, l'externalisation vers des sous-traitants étrangers est donc tout à fait autorisée (art. 16 al. 1 nLPD). Les pays disposant d'une protection des données équivalente sont publiés dans une liste. Y figurent la Suisse et tous les autres pays de l'UE. La liste des pays disposant d'une protection des données

équivalente sera désormais publiée par le Conseil fédéral et non plus par le Préposé fédéral à la protection des données et à la transparence (PFPDT).

En l'absence de législation garantissant une protection appropriée, des données personnelles peuvent être communiquées à l'étranger si des garanties sont amenées pour assurer un niveau de protection adéquat (art. 16 al. 2 nLPD). De telles garanties sont notamment les clauses contractuelles types européennes (CCT). Les dérogations sont possibles lorsque notamment la personne concernée a expressément donné son consentement à la communication (art. 17 al. 1 let. a nLPD).

3.10 Devoir d'annoncer les violations de la sécurité des données

En cas de violation de la protection des données, l'entreprise responsable du traitement annonce dans les meilleurs délais au PFPDT (et le cas échéant aux personnes concernées) les cas de violation de la sécurité des données entraînant vraisemblablement un risque élevé pour les personnes concernées (art. 24 al. 1 nLPD). Il s'agit par exemple de la soustraction ou du vol de données personnelles par des personnes internes ou externes (par exemple pirates informatiques) ou de la destruction d'informations, par exemple en raison d'erreurs d'utilisation, d'erreurs techniques, de virus ou d'attaques de pirates informatiques. En règle générale, il revient à la direction de procéder à l'annonce. Cette tâche incombe toutefois en dernier ressort aux membres du conseil d'administration qui sont ici responsables dans le cadre de la gestion des risques (cf. art. 754 al. 1 CO). L'entreprise responsable doit documenter les violations. La documentation doit contenir les faits liés aux incidents, leurs conséquences et les mesures prises. Elle doit être conservée pendant au moins deux ans à compter de la date de l'annonce (art. 15 al. 4 OPDo).

3.11 Nouvelles obligations formelles selon la nLPD

Les bailleurs de services doivent respecter à l'avenir des obligations formelles relatives au traitement des données personnelles:

- Désignation d'une autorité centrale chargée de la protection des données (p. ex. service juridique ou informatique).
- Une entreprise de plus de 250 salariés doit tenir un registre de ses activités de traitement des données personnelles (art. 12 nLPD). Les travailleurs temporaires sont à prendre en compte dans les 250 salariés. Dans quelques cas rares, des entreprises de moins de 250 salariés doivent également tenir un registre, à savoir lorsqu'elles traitent des données personnelles sensibles à grande échelle ou pratiquent le profilage à risque élevé.

  Le registre du responsable du traitement contient au moins les indications suivantes:
  - l'identité du responsable du traitement,
  - la finalité du traitement,
  - une description des catégories de personnes concernées et des catégories de données personnelles traitées,
  - les catégories de destinataires,
  - la duréede conservation des données personnelles ou les critères pour déterminer la durée de conservation,
  - une description générale des mesures visant à garantir la sécurité des données,
  - en cas de communication de données personnelles à l'étranger, le nom de l'État concerné et les garanties prévues pour assurer une protection appropriée des données.
- Le prestataire des services de l'emploi en tant que responsable au sens de la nLPD, doit assurer, par

des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles (art. 8 nLPD) (cf. annexe LIENS UTILES, lien vers le guide relatif aux mesures techniques et organisationnelles du PFPDT en référence à la LPD actuelle).

- Lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, l'entreprise responsable du traitement procède au préalable à une analyse d'impact relative à la protection des données personnelles (AIPD). Pour les projets plus sensibles, comme la mise en place d'applications particulières, il existe donc une obligation d'effectuer une analyse des risques formalisée et de la documenter. L'existence d'un risque élevé, en particulier lors du recours à de nouvelles technologies, dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement des données personnelles. L'AIPD contient une description du traitement envisagé, une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée, ainsi que les mesures prévues pour protéger sa personnalité et ses droits fondamentaux. Il s'agit donc essentiellement d'une analyse de risques (art. 22 ss. nLPD). Quelques cantons, comme le canton de Zurich ont publié des formulaires permettant de procéder à une AIPD [voir en annexe: LIENS UTILES].
- Enfin, il convient également de sensibiliser et de former l'ensemble des collaborateurs à la protection des données.

4. Sanctions

Avec la nLPD, les amendes seront également considérablement augmentées. Celui qui contrevient aux obligations de la nLPD énumérées ci-dessous (y compris en acceptant par dol éventuel le comportement sanctionné) sera puni d'une amende de 250 000 francs au plus (art. 60 ss. nLPD) s'il:

- fournit intentionnellement des renseignements inexacts ou incomplets;
- omet intentionnellement d'informer la personne concernée;
- ne respecte pas les exigences minimales en matière de sécurité des données;
- communique des données personnelles à l'étranger sans que les conditions requises soient remplies;
- fait un sous-traitement des données personnelles qui ne répond pas aux exigences légales;
- viole le devoir de confidentialité.

Il en résulte que, selon la nLPD, les responsables au sein des entreprises comme les CEO, CFO ou CIO peuvent être directement sanctionnés. La plupart des dispositions pénales sont des délits poursuivis sur plainte. Une infraction n'est donc poursuivie que si une personne concernée dépose une plainte pénale.

5. Besoin d'agir pour les bailleurs de services suisses

N°1 **Vérification du site web** (déclaration de protection des données, CG, applications, envoi de newsletters, déclarations de consentement)	**N°2** **Examen/conclusion de contrats en cas de traitement des données par des tiers (y compris transfert de données à l'étranger)** (contrat, droit de donner des instructions, pas de violation des clauses de confidentialité, sécurité des données, droit de veto, obligation de notification en cas de transfert de données, le cas échéant, garanties appropriées)
N°3 **Vérifier que les principes de protection des données sont respectés** (légalité, bonne foi, proportionnalité, finalité, exactitude des données, sécurité des données)	**N°4** **Élaboration d'un processus de notification en cas de violation de la sécurité des données** (en cas de risque élevé au PFPDT/à la personne concernée)
N°5 **Élaboration de processus concernant les droits des personnes concernées** (processus de renseignement, processus de rectification, processus de suppression, processus d'opposition, processus de portabilité des données)	**N°6** **Respect des obligations formelles** (service central de protection des données, formation des collaborateurs, registre des activités de traitement à partir de 250 collaborateurs AIPD)

Pour connaître les actions concrètes à mener pour les bailleurs de services suisses, se reporter aussi à l'annexe CHECK-LIST 2: MISE EN ŒUVRE DES EXIGENCES DE LA NLPD.

Le service juridique de swissstaffing se tient volontiers à votre disposition pour toute question, par téléphone au 044 / 388 95 75 ou par e-mail à l'adresse legal@swissstaffing.ch.

Zurich, mars 2023

swissstaffing

CHECK-LIST 1: ADAPTATIONS DU RGPD EUROPÉEN À LA NLPD

Si vous avez déjà mis en œuvre les exigences du RGPD de l'UE, cette check-list vous permet d'identifier les adaptations à mettre en place en vertu de la nLPD.

Important: il est tout à fait possible que le RGPD de l'UE s'applique en plus de la nLPD, dans ce cas les exigences s'appliquent en parallèle.

<table>
<tr><td>N°1</td><td>Applicabilité de la nLPD

Souvent, les documents élaborés renvoient uniquement au RGPD de l'UE. Il convient de procéder à une adaptation des renvois et d'inclure également la nLPD.</td><td>En plus de l'application du RGPD de l'UE, il est nécessaire de renvoyer également à l'application de la nLPD.</td><td>☐</td></tr>
<tr><td>N°2</td><td>Définitions

La terminologie de la nLPD est légèrement différente de celle du RGPD de l'UE:

<table><tr><th>nLPD</th><th>RGPD de l'UE</th></tr><tr><td>Traitement (modification en allemand: Bearbeitung)</td><td>Traitement (modification en allemand: Verarbeitung)</td></tr><tr><td>Données personnelles</td><td>Données à caractère personnel</td></tr><tr><td>Données personnelles sensibles (données sensibles)</td><td>Catégories particulières de données à caractère personnel</td></tr><tr><td>Violation de la sécurité des données</td><td>Violation de la protection des données</td></tr></table></td><td>Les termes suivants ont été adaptés dans les documents: en allemand Verarbeitung/Bearbeitung (traitement), données à caractère personnel/données personnelles, catégories particulières de données/données sensibles, violation de la protection des données/violation de la sécurité des données</td><td>☐</td></tr>
<tr><td>N°3</td><td>Définition plus large pour les données sensibles

Les données sur des poursuites ou sanctions pénales et administratives et les données sur des mesures d'aide sociale sont, selon la nLPD, des données dites sensibles. Par conséquent, le consentement doit être expressément donné si nécessaire.</td><td>Si le traitement des données sur des poursuites ou sanctions pénales et administratives et des données sur des mesures d'aide sociale est nécessaire, le consentement doit être donné de manière explicite.</td><td>☐</td></tr>
</table>

N°4	**Respect des devoirs d'information** Les devoirs d'information applicables à la Suisse prévoient certaines différenciations par rapport au RGPD de l'UE. La déclaration de protection des données doit mentionner le pays de destination en cas de transfert de données à l'étranger.	La déclaration de protection des données a été complétée avec le pays de destination dans le cas d'un transfert des données à l'étranger.	☐
N°5	**Registre des activités de traitement** Selon la nLPD, il convient d'indiquer le pays de destination dans le registre des activités de traitement en cas de transfert des données à l'étranger.	Le registre des activités de traitement a été complété avec le pays de destination choisi pour le traitement des données.	☐
N°6	**Processus de violation de la sécurité des données** En vertu du RGPD de l'UE, les violations de protection des données susceptibles d'engendrer un risque pour les personnes concernées sont à notifier 72 heures au plus tard après en avoir pris connaissance (vol et utilisation abusive de données). En vertu de la nLPD, une violation de la sécurité des données susceptibles d'engendrer un risque élevé pour les personnes concernées doit être annoncée dans les meilleurs délais au Préposé fédéral à la protection des données et à la transparence (PFPDT). Le niveau de risque déclenchant une annonce à l'autorité de protection des données et/ou aux personnes concernées est ainsi défini différemment dans la nLPD et dans le RGPD de l'UE.	Le délai de l'annonce est passé de 72 heures à «dans les meilleurs délais» et le niveau de risque a été modifié.	☐
N°7	**Processus en cas de requête de personnes concernées** Contrairement à la RGPD de l'UE, la nLPD comprend, en plus des informations minimales qui doivent dans tous les cas être mises à la disposition d'une personne concernée faisant valoir son droit d'accès, une règle générale selon laquelle une personne concernée doit recevoir les informations nécessaires pour qu'elle puisse faire valoir ses droits et pour que la transparence du traitement soit garantie.	Le processus pour les requêtes de personnes concernées a donc été complété par la possibilité pour une personne concernée de recevoir les informations nécessaires pour faire valoir ses droits et garantir un traitement transparent des données.	☐

N°8	**Obligation de journalisation** Contrairement au RGPD de l'UE, la nLPD ne connaît pas «d'obligation générale de rendre des comptes». En ce qui concerne la sécurité des données, le traitement de données sensibles à grande échelle et la réalisation d'un profilage à risque élevé sont toutefois soumis à des obligations plus étendues que celles prévues par le RGPD de l'UE, si les mesures préventives ne garantissent pas la protection des données. En conséquence, l'enregistrement, la rectification, la lecture, la communication, l'effacement et la destruction de données sont soumis à une obligation de journalisation et un règlement de traitement doit être établi avec des indications sur l'organisation interne, la procédure de traitement et de contrôle des données ainsi que sur les mesures visant à garantir la sécurité des données (art. 4 OPDo). Une journalisation est notamment nécessaire lorsqu'il n'est pas possible de déterminer a posteriori si les données ont été traitées de manière compatible avec la finalité déterminée lors de leur collecte ou de leur communication.	Dans la mesure où des données sensibles font l'objet d'un traitement automatisé à grande échelle ou d'un profilage à risque élevé et que les mesures préventives ne garantissent pas la protection des données, les exigences en matière de journalisation sont respectées.	☐

swissstaffing

CHECK-LIST 2: MISE EN ŒUVRE DES EXIGENCES DE LA NLPD

Cette check-list doit vous permettre de mettre en œuvre les exigences de la nLPD et de vérifier votre statut actuel.

N°1	**Vérification de votre site web** Votre site web est votre enseigne. Il est gratuit et accessible au public. La déclaration de protection des données permet de fournir des informations sur le traitement des données personnelles et répond donc aux exigences du devoir d'information selon la nLPD.	La déclaration de protection des données est correcte, complète et actualisée.	☐
		La déclaration de protection des données est placée à un endroit bien visible sur le site web.	☐
		Si le site web est disponible en plusieurs langues, la déclaration de protection des données a été traduite dans les langues concernées.	☐
		Lorsqu'il existe des conditions générales (CG), leur conformité avec la protection des données a été vérifiée.	☐
		Si une newsletter est envoyée, sa conformité avec la protection des données a été vérifiée.	☐
N°2	**Examen/conclusion de contrats en cas de traitement de données par des tiers (y compris le thème de la transmission de données à l'étranger)** Exemples: contrats avec des prestataires de services informatiques prévoyant l'externalisation du traitement des données via la technologie «cloud» ou contrats avec des prestataires pour les décomptes salaires des salariés du bailleur de services. Selon la nLPD, le traitement des données personnelles peut être confié à un tiers pour autant qu'un contrat ou la loi le prévoie, si seuls sont effectués les traitements que le prestataire des services de l'emploi serait en droit d'effectuer lui-même et si aucune	La conformité avec la protection des données des contrats avec les prestataires a été vérifiée.	☐
		Des clauses contractuelles types de l'UE ont été convenues avec le prestataire issu d'un pays ne disposant pas d'un niveau adéquat de protection des données ou d'autres garanties appropriées et, le cas échéant, des mesures supplémentaires ont été prises.	☐

	obligation légale ou contractuelle de garder le secret ne l'interdit. En outre, l'entreprise donneuse d'ordre doit s'assurer que le tiers mandaté garantit la sécurité des données (art. 9 al. 1 et 2 nLPD). Désormais, le sous-traitant ne peut lui-même sous-traiter un traitement à un tiers qu'avec l'autorisation préalable du responsable du traitement (droit de veto) (art. 9 al. 3 nLPD). Le sous-traitant annonce dans les meilleurs délais au responsable du traitement tout cas de violation de la sécurité des données (art. 24 al. 3 nLPD). Le prestataire des services de l'emploi (qui externalise le traitement) reste responsable du traitement des données. En cas de communication de données à l'étranger, il convient de s'assurer que la personnalité des personnes concernées n'est pas mise en danger.		
N°3	**Vérifier que les principes de protection des données sont respectés** Il s'agit des principes de légalité, finalité, bonne foi, proportionnalité et exactitude des données, le cas échéantdu consentement, la sécurité des données, Privacy by Design et Privacy by Default.	Le respect des principes lors du traitement des données a été vérifié.	☐
		Les exigences en matière de sécurité des données sont respectées.	☐
		Les cas où le consentement est requis ont été examinés et, le cas échéant, il a été vérifié que celui-ci avait bien été donné.	☐
		Les principes de Privacy by Design et Privacy by Default ont bien été pris en compte.	☐
N°4	**Élaboration d'un processus de notification en cas de violation de la sécurité des données**	Un processus a été élaboré pour réagir dans les meilleurs délais en cas d'incident de sécurité des données et pour annoncer l'incident au Préposé fédéral à la protection des données et à la transparence (PFPDT) et, le cas échéant, informer les personnes	☐

		concernées.	
N°5	**Élaboration de processus appropriés en cas de requêtes de personnes concernées**	Il existe un processus pour les requêtes de personnes concernées permettant à la personne concernée de recevoir les informations nécessaires pour faire valoir ses droits et pour garantir un traitement transparent des données. L'information est en général à fournir dans un délai de 30 jours.	☐
N°6	**Respect des obligations formelles**	Un service central en charge de toutes les questions relatives à la protection des données a été mis en place (p.ex. service juridique, service informatique). Le cas échéant, un conseiller à la protection des données a été désigné conformément à l'art. 10 de la nLPD, ce dernier devant disposer des connaissances techniques nécessaires. Il doit exercer sa fonction de manière indépendante par rapport au responsable du traitement et ne doit pas recevoir d'instruction de celui-ci. Il ne doit pas exercer d'activités incompatibles avec ses fonctions.	☐
		Le cas échéant, un registre des activités de traitement a été élaboré.	☐
		Le cas échéant, une analyse d'impact sur la protection des données (AIPD) a été réalisée.	☐
		Les collaborateurs ont été formés aux exigences de la nLPD ainsi qu'aux mesures prises au sein de l'entreprise.	☐
		Dans la mesure où des données sensibles font l'objet d'un traitement automatisé à grande échelle ou d'un profilage à risque élevé et que les mesures préventives ne garantissent pas la protection des données, les exigences en matière de journalisation sont respectées.	☐

swissstaffing

EXEMPLE 1: MODÈLE D'UNE CLAUSE DE CONSENTEMENT

[*Ce modèle est non exhaustif, donné à titre d'exemple et doit être adapté à chaque cas particulier*]

Nous traitons les documents de candidature dans la plus stricte confidentialité et ne les utilisons qu'aux fins convenues.

- Placement de personnel: les données ne sont traitées que dans la mesure et aussi longtemps que cela s'avère nécessaire au placement. Les données peuvent être transmises à de potentiels employeurs.
- Location de services: les données sont traitées jusqu'au terme du contrat de location et les profils peuvent être transmis à de (potentielles) entreprises locataires.

Sans votre consentement, le dossier (électronique) de candidature sera effacé/détruit au terme de la procédure de candidature pour autant qu'il ne soit pas soumis à une obligation légale de conservation.

Je consens explicitement par la présente au traitement, enregistrement ou transmission de mes données personnelles:

☐ Je consens à ce que le [le prestataire des services de l'emploi] enregistre, traite ou transmette mes données personnelles que je lui ai communiquées en lien avec ma candidature, au sein des sociétés du [prestataire des services de l'emploi], dans le pays et à l'étranger [si la protection des données n'est pas appropriée: indication du pays] aux fins de la location de services et/ou du placement de personnel.

☐ Je consens à ce que mes données personnelles que j'ai communiquées dans le cadre de ma candidature soient enregistrées, traitées et communiquées - pendant la procédure de location de services resp. de placement et après la fin de cette procédure - à des tiers, dans le pays et à l'étranger, aux fins de la location de services et/ou du placement de personnel. Par ces tiers, il faut notamment entendre des sociétés, prestataires liés au [prestataire des services de l'emploi], qui mettent à disposition et exploitent des applications IT utilisées, ainsi que d'autres entreprises participant aux processus nécessaires à la fourniture des prestations contractuelles du [prestataire des services de l'emploi] (par ex. prestataire de paiement). Dans cette mesure, je consens à ce que mes données soient transmises dans des pays [indication du pays] où il n'existe pas de niveau approprié de protection des données. Pour autant que, en lien avec ma candidature, j'aie transmis des «données personnelles sensibles» selon art. 5 let. c de la nLPD (par ex. une photographie laissant apparaître l'origine ethnique, etc.), mon consentement porte aussi sur ces données.

☐ Je consens à ce que le [prestataire des services de l'emploi] fasse parvenir une newsletter à l'adresse e-mail que je lui ai donnée. Cette newsletter contient en particulier des informations sur des offres d'emploi susceptibles de m'intéresser.

Les consentements sont indépendants les uns des autres et sont donnés volontairement. Je peux révoquer en tout temps mes consentements sans indication de motifs et j'ai le droit d'exiger à tout moment l'effacement de mes données. Je peux me désabonner de toute newsletter en cliquant sur le lien figurant à la fin de celle-ci. Je prends acte du fait qu'en cas de révocation de mes consentements au traitement de mes données personnelles (à l'exception du consentement à recevoir des newsletters par e-mail), les prestations proposées par le [prestataire des services de l'emploi] ne pourront plus être fournies et que cette révocation met fin aux relations contractuelles sous-jacentes.

swissstaffing

EXEMPLE 2: MODÈLE DE CLAUSE DE PROTECTION DES DONNÉES ET DE CONSENTEMENT DANS LES CG

[*Ce modèle est non exhaustif, donné à titre d'exemple et doit être adapté à chaque cas particulier*]

Protection des données

Les parties s'engagent à respecter en tout temps les prescriptions en vigueur en matière de protection des données. Dans le cadre du contrat en question, le [prestataire des services de l'emploi] est autorisé à collecter, traiter les données des collaborateurs, directeurs et autres employés du client (ci-après «données personnelles» du client), de les utiliser et les divulguer à toutes les fins en rapport avec l'exécution du contrat. À cet effet, le [prestataire des services de l'emploi] est également autorisé en particulier à transmettre - pour autant qu'éventuellement nécessaire à l'exécution du contrat - les données personnelles du client à l'étranger pour des fins susmentionnées [si la protection des données n'est pas appropriée: indication du pays]. De plus, le [prestataire des services de l'emploi] est explicitement habilité à traiter les données personnelles du client sous toute forme et à les divulguer à d'éventuelles sociétés du groupe ou à des tiers à l'étranger.

Le consentement englobe également l'utilisation des données à des fins de marketing. Le client déclare expressément que le consentement de la personne concernée existe. Le [prestataire des services de l'emploi] peut l'exiger en tout temps du client.

swissstaffing

EXEMPLE 3: MODÈLE DE CLAUSE DE SOUS-TRAITANCE DANS LES CG

[*Ce modèle est non exhaustif, donné à titre d'exemple et doit être adapté à chaque cas particulier*]

Traitement de données personnelles par des tiers (sous-traitance)

Le mandataire s'engage à ne traiter les données personnelles qui lui ont été transmises ou auxquelles il a eu accès via le [prestataire des services de l'emploi] que dans la mesure où cela est nécessaire à l'exécution du contrat et exclusivement aux fins prévues.

Le mandataire s'engage à prendre les mesures organisationnelles et techniques appropriées afin d'assurer la protection des données et la sécurité de l'information.

Le mandataire traite les données personnelles (y compris accès et localisation serveur web) uniquement en Suisse, au sein de l'UE ou dans l'Espace économique européen.

Le mandataire divulgue, avant la conclusion du contrat, au moins les sous-traitants qui traitent les données personnelles en son nom. Il impose à tous les sous-traitants, auxiliaires d'exécution et tiers impliqués, les obligations découlant du présent contrat de sous-traitance. Le mandataire ne recrute pas un sous-traitant sans l'autorisation écrite préalable du [prestataire des services de l'emploi]. Tant que l'autorisation écrite n'a pas été obtenue, le mandataire ne peut faire appel à aucun autre sous-traitant. L'acceptation ou le refus d'un tiers en tant que futur sous-traitant relève de la discrétion exclusive du mandant.

Le mandataire garantit la confidentialité des données personnelles obtenues dans le cadre du contrat. Il garantit en particulier au [prestataire des services de l'emploi] qu'il ne transmettra pas, ni ne rendra accessibles sous une autre forme les données personnelles à des tiers non autorisés. Le mandataire impose l'obligation de respecter la confidentialité à tous les sous-traitants, auxiliaires d'exécution et tiers impliqués.

Le mandataire aide le [prestataire des services de l'emploi] à se conformer aux exigences de la législation applicable en matière de protection des données. Il répond notamment sans délai et en bonne et due forme à toutes les demandes du donneur d'ordre en rapport avec le traitement de données personnelles. Il transmet immédiatement les demandes des personnes concernées ou des autorités au [prestataire des services de l'emploi], sans y répondre lui-même. Le mandataire est tenu de coopérer dans le cadre d'éventuelles procédures de surveillance concernant les prestations qu'il doit fournir et de mettre à disposition les renseignements et documents qui lui sont demandés.

Le mandataire informe immédiatement le [prestataire des services de l'emploi] lorsqu'il a connaissance ou soupçonne que des données personnelles qu'il a traitées pour le compte du [prestataire des services de l'emploi] ont fait l'objet d'un accès non autorisé, ont été transmises à des tiers non autorisés, ont été perdues ou endommagées ou ont été ou pourraient être traitées de manière illicite ou non conforme à la loi ou au contrat. Le mandataire doit en outre prendre immédiatement les mesures d'urgence nécessaires pour sécuriser les données personnelles et prévenir ou minimiser d'éventuelles conséquences négatives.

Le [prestataire des services de l'emploi] a le droit de contrôler à tout moment le respect par le mandataire des dispositions applicables en matière de protection des données.

Au terme du contrat, sur instruction expresse du [prestataire des services de l'emploi], le mandataire s'engage à renvoyer ou à détruire toutes les données personnelles (y compris toutes les copies existantes) traitées pour le compte du [prestataire des services de l'emploi], sous réserve d'une autre règle prévue au contrat. Le mandataire doit documenter la destruction des données et envoyer spontanément au [prestataire des services de l'emploi] une copie de cette documentation.

ANNEXE: LIENS UTILES

Vous trouverez ici le message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et surla modification d'autres lois fédérales du 15 septembre 2017.

Vous trouverez ici et ici les communiqués de presse de l'Office fédéral de la justice.

Vous trouverez le site web du Préposé fédéral à la protection des données et à la transparence (PFPDT) ici.

Le guide relatif aux mesures techniques et organisationnelles de la protection des données (2015) du PFPDT peut être consulté ici.

Le formulaire pour l'élaboration d'une analyse d'impact sur la protection des données du canton de Zurich (en allemand) se trouve ici.