Guide relatif à l'analyse d'impact relative à la protection des données personnelles

Table des matières

1. Destinataires du guide

Le guide relatif à l'analyse d'impact relative à la protection des données personnelles (AIPD) s'adresse avant tout aux institutions publiques genevoises qui sont tenues de réaliser une analyse d'impact relative à la protection des données personnelles (AIPD) au sens de l'art. 37B LIPAD.

2. Objectifs du guide

Le présent guide vise à expliciter le formulaire d'AIPD élaboré par le Préposé cantonal à la protection des données et à la transparence qui doit être utilisé par les institutions genevoises. Les explications générales sur l'AIPD se trouvent dans la fiche info du PPDT traitant de ce sujet: https://www.ge.ch/document/38352/telecharger

3. Structure du formulaire de l'AIPD

Le formulaire d'AIPD élaboré par le PPDT est structuré en deux parties.

La première partie constitue l'analyse préliminaire des risques qui permet de déterminer si le traitement envisagé présente ou non un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

La seconde partie constitue l'AIPD qui doit être complétée dans le cas où le traitement envisagé présente un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.

4. Première partie – Analyse préliminaire des risques

En préambule de l'analyse préliminaire, la première page du formulaire prévoit de collecter les informations sur l'institution concernée (le responsable du traitement envisagé) et de son/sa conseiller/conseillère LIPAD ainsi que d'identifier les bases légales existantes pour le traitement envisagé.

La seconde page du formulaire vise à décrire le traitement envisagé, sa ou ses finalité(s) et à préciser quelles sont les catégories de données, et notamment de données sensibles, qui seront traitées.

La troisième et la quatrième page du formulaire permettent d'évaluer le respect des principes fondamentaux en matière de protection des données du traitement envisagé, d'évaluer si le traitement envisagé tombe sous l'obligation de conduire une AIPD au sens de l'art. 37B al. 2 LIPAD et d'évaluer si le traitement envisagé présente des indices de traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

L'institution concernée doit procéder à une AIPD et compléter la Partie II lorsque le traitement envisagé tombe sous l'obligation de conduire une AIPD au sens de l'art. 37B al. 2 LIPAD. Le Préposé cantonal recommande également de procéder à une AIPD s'il y a au moins 1 indice de traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

5. Deuxième partie – Analyse d'impact relative à la protection des données personnelles

L'AIPD élaborée par le PPDT a été pensée en complément de l'analyse préliminaire des risques et est divisée en 6 parties.

5.1 Première partie - Analyse détaillée de la base légale

La première partie vise à procéder à une analyse plus détaillée de la base légale du traitement envisagé, notamment au sens de l'art. 36 LIPAD.

5.2 Deuxième partie - Description détaillée du traitement envisagé

La seconde partie a pour objectif de décrire plus en détail le traitement envisagé, notamment en précisant les entités participant au traitement (responsable de traitement conjoint et sous-traitant éventuels).

Cette partie vise également à identifier les catégories de personnes concernées par le traitement envisagé et à définir les étapes du traitement envisagé. Par catégories de personnes concernées, on entend des groupes présentant certaines caractéristiques communes, comme par exemple les personnes vulnérables, les personnes intéressées, les citoyens, le personnel ou les prestataires de services.

Cette partie va permettre également de préciser la nature du traitement envisagé et notamment de détailler les indices de traitement susceptible d'engendrer un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées qui auront déjà été identifiés au cours de l'analyse préliminaire des risques.

Elle vise également à identifier les technologies qui seront utilisées, en particulier l'utilisation de "Cloud" ou d'intelligence artificielle, et à préciser l'étendue du traitement envisagé.

5.3 Troisième partie - Évaluation du risque pour la personnalité ou les droits fondamentaux de la personne concernée

Cette partie permet dans un premier temps d'identifier les risques inhérents, c'est-à-dire en l'absence de toute mesure de réduction du risque, liés au traitement envisagé.

Il est nécessaire d'identifier tous les risques pour la personnalité ou les droits fondamentaux de la personne concernée. Il peut s'agir de risques systémiques, comme par exemple les risques liés au recours à des sous-traitants et aux transferts à l'étranger, de risques juridiques (ex. discrimination, inégalité de traitement) et de risques relevant de la sécurité (confidentialité, intégrité, disponibilité et traçabilité des données).

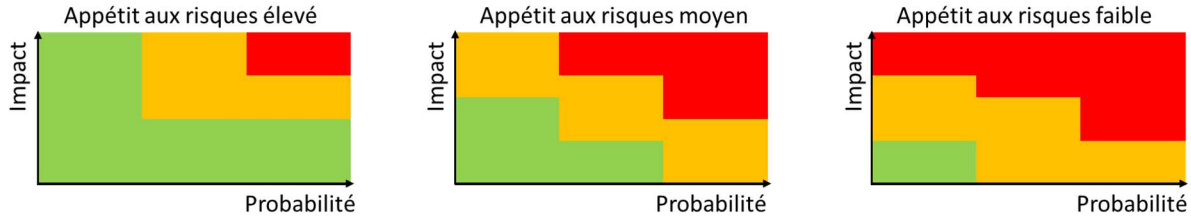
Cette partie devrait, en principe, être réalisée en étroite collaboration avec le RSI.

Les risques identifiés doivent ensuite être évalués en terme de probabilité et d'impact.

Le PPDT a fait le choix de ne pas donner d'échelle de probabilité ou d'impact. Ceux-ci étant en principe définis en fonction de l'appétit aux risques de chaque institution.

En effet, chaque institution peut avoir, en fonction de la criticité de ses activités, une appétence aux risques différente.

L'image ci-dessous illustre, à titre d'exemple, différents niveaux d'appétit aux risques:

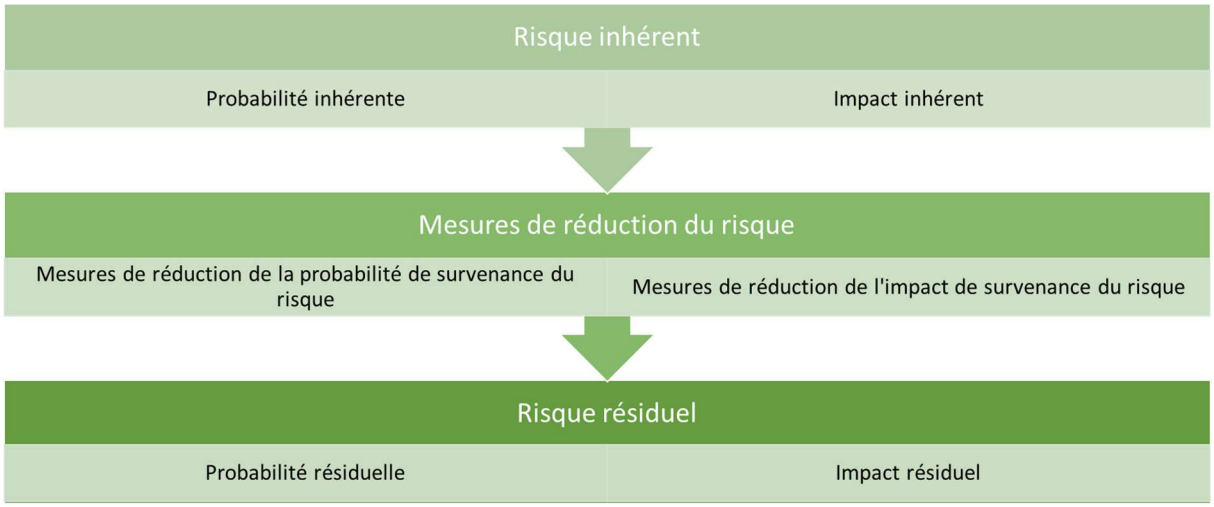


De plus, l'appétit aux risques peut être différent en fonction de la catégorie de risque (risque de sécurité de l'information, risque juridique, etc.)

Pour l'ensemble des risques inhérents jugés inacceptables, le responsable du traitement devra ensuite identifier les mesures de réduction des risques existantes (il peut s'agir de mesures techniques, organisationnelles ou contractuelles) et évaluer les effets de ces mesures sur la réduction de la probabilité ou de l'impact de la réalisation du risque. Cet exercice permet d'évaluer le niveau de risque résiduel pour la personnalité ou les droits fondamentaux de la personne concernée.

Enfin, le responsable du traitement doit évaluer si les risques résiduels sont acceptables ou non. Si ce n'est pas le cas, le responsable du traitement identifiera dans la partie suivante des mesures supplémentaires à mettre en œuvre.

Le schéma ci-dessous synthétise les liens entre risques inhérents et risques résiduels:



En théorie, il y a en principe 3 types de mesures de réduction des risques:

- L'évitement: il s'agit d'éviter le risque (en choisissant une autre solution par exemple) ou de renoncer à l'activité de traitement

- La mitigation: il s'agit de la mise en œuvre de différentes mesures afin de réduire la survenance ou les conséquences de la réalisation du risque

- Le transfert: il s'agit de transférer la responsabilité du risque technique à un tiers (il s'agit par exemple de la souscription d'une assurance ou du transfert de l'activité à un prestataire de services).

Si aucune mesure d'évitement, de mitigation ou de transfert du risque identifié n'est mise en œuvre, le risque peut être accepté en l'état ou non en fonction de l'appétit aux risques.

5.4 Quatrième partie – identification des mesures supplémentaires prévues pour protéger la personnalité et les droits fondamentaux de la personne concernée

Pour tous les risques résiduels inacceptables identifiés dans la troisième partie, le responsable du traitement doit identifier dans cette partie les mesures de réduction du risque supplémentaires qui pourront être mises en œuvre avant le début du traitement, afin de réduire les risques pour la personnalité ou les droits fondamentaux des personnes concernées à un niveau acceptable.

Le coût des mesures peut être évalué en fonction du coût en ressources humaines, matérielles ou financières. La prise en compte du coût des mesures supplémentaires permet d'évaluer s'il est raisonnable pour une institution de mettre en œuvre ces mesures.

5.5 Cinquième partie – évaluation des effets des mesures prévues pour protéger les droits fondamentaux de la personne concernée afin de déterminer s'il reste un risque résiduel élevé

Le responsable de traitement doit évaluer dans cette partie l'effet attendu des mesures de réduction du risque supplémentaires sur la réduction des risques résiduels afin de les amener à un niveau acceptable.

5.6 Sixième partie – synthèse et résultats de l'AIPD

Cette dernière partie permet de faire la synthèse des éléments les plus importants de l'AIPD et de décrire les résultats de l'AIPD. L'AIPD doit être signée par le responsable du traitement et le/la conseiller/conseillère LIPAD avant d'être soumise au PPDT.

6. Informations complémentaires

Afin de faciliter la compréhension du traitement envisagé et des risques associés, le responsable du traitement peut joindre tout document jugé utile, tel que la documentation des flux de données, le concept SIPD, le concept de gestion des droits d’accès, la documentation de l'architecture de l'application.

Annexe – Exemple fictif

Partie I - Analyse préliminaire des risques

Chapitre 1 - Description du traitement envisagé		
Indiquez brièvement quel est le traitement envisagé		
Pour améliorer le processus de recrutement, les ressources humaines veulent déployer un outil utilisant l'intelligence artificielle pour sélectionner directement les candidatures adéquates par rapport au poste proposé et refuser automatiquement les candidatures non retenues.		
Finalité(s) du traitement		
Indiquez la ou les finalité(s) du traitement envisagé:		
Finalité du traitement envisagé:	*Recruter les meilleurs candidats en fonction des cahiers des charges des postes proposés*	
Finalité du traitement envisagé:	*Automatiser les processus de sélection*	
Finalité du traitement envisagé:	*Refuser automatiquement les candidatures non retenues*	
Indiquez si la/les finalités du traitement présentent un risque élevé pour les droits fondamentaux de la personne concernée	*oui*	
Motivation	*Si le modèle d'intelligence artificielle est entraîné sur des données comportant des biais, le processus pourrait engendrer des discriminations à l'embauche*	
Catégories de données personnelles		
Indiquez les catégories de données personnelles concernées par le traitement envisagé:		
Données personnelles	*oui*	
Types de données personnelles	*Noms, prénoms, date de naissance, parcours professionnels, études et formations, centres d'intérêts*	
Données personnelles sensibles	*non*	
	données sur les opinions ou les activités religieuses, philosophiques, politiques ou syndicales	*non*
	données sur la santé, la sphère intime ou l'origine raciale ou ethnique	*non*
	données génétiques	*non*
	données biométriques identifiant une personne physique de manière univoque	*non*
	données sur des poursuites ou sanctions pénales et administratives	*non*
	données sur des mesures d'aide sociale	*non*

Chapitre 2 – Analyse préliminaire	
Principes fondamentaux	
Le traitement des données est-il proportionnel?	*oui*
La collecte des données ne porte que sur les données standard demandées lors d'un processus de recrutement. Il n'y a pas de collecte de données sensibles.	
Les données sont-elles minimisées?	*oui*
Seules les données utiles à l'appréciation de la formation, du parcours professionnels et des qualités des candidats sont demandées	
Qualité des données (comment est assurée l'exactitude des données et leur mises à jour)	*Seuls les candidats eux-mêmes peuvent saisir, modifier et mettre à jour leurs données*
Cycle de vie des données (quand les données sont-elles archivées / détruites / anonymisées?)	*Les données des candidats non retenus sont supprimées après un an*
Le traitement des données est-il reconnaissable pour les personnes concernées?	*oui*
Les données seront saisies par la personne concernée dans la plateforme de recrutement mise à disposition en ligne.	
A. Traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée selon art 37B LIPAD	
traitement de données personnelles sensibles à grande échelle	*non**
profilage	*non**
surveillance systématique de grandes parties du domaine public	*non**

* S'il est répondu oui à l'un de ces points, l'analyse d'impact est obligatoire

B. Indices de traitement susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée	
Envisagez-vous de collecter des données personnelles à l'insu de la personne concernée?	*non*
Envisagez-vous de recourir à de nouvelles technologies ou à des technologies comportant des risques pour les droits fondamentaux de la personne concernée ou dont on ne peut pas encore mesurer les effets? (par ex. intelligence artificielle)	*oui*
Est-ce que des données personnelles traitées dans des banques de données à des fins différentes ou par des responsables du traitement différents sont interconnectées ou comparées?	*oui*
Envisagez-vous d'utiliser les données personnelles dans le cadre d'une décision automatisée au sens de l'art. 38b LIPAD?	*oui*
Envisagez-vous d'utiliser les données personnelles à des fins de surveillance? (p*ar ex.: suivi de l'activité d'un employé sur son poste de travail à des fins de contrôle horaire; surveillance par lecture automatique des plaques des comportements routiers…)*	*non*
Envisagez-vous de communiquer de manière systématique les données personnelles ou d'y donner accès à des tiers de droit privé (y.c. sous-traitants, mandataires, …), à des institutions, corporations ou établissements de droit public?	*oui*
Envisagez-vous de rendre des données personnelles accessibles en ligne (selon le principe de self-service (ex. : e-démarches)	*oui*
Existe-t-il d'autres facteurs de risques pertinents dans le présent contexte?	*oui*

Si oui, lesquels?	*autre facteur*	*La solution technique envisagée repose sur une plateforme cloud avec partage des données anonymisées pour améliorer l'IA (apprentissage) au prestataire tiers situé à l'étranger (USA)*

Les facteurs de risque sont un indice de l'existence possible d'un risque élevé pour les droits fondamentaux des personnes concernées. Pour déterminer si tel est le cas, ils doivent être considérés dans leur contexte.

Plus il y a de facteurs de risque cochés, plus grandes sont la probabilité de l'existence d'un risque élevé pour les droits fondamentaux des personnes concernées et la nécessité de réaliser une AIPD. Selon le contexte dans lequel les données personnelles sont traitées, il est aussi possible qu'un seul facteur de risque entraîne un risque élevé pour les droits fondamentaux des personnes concernées et la nécessité de procéder à une AIPD.

En cas de doute quant à la nécessité d'effectuer une AIPD, il est recommandé d'en effectuer une.

Est-ce que le traitement de données personnelles envisagé est susceptible d'entraîner un risque élevé pour les droits fondamentaux des personnes concernées au vu de l'évaluation globale des facteurs de risques?	*oui*
Motivation:	*Le traitement envisagé repose sur une technologie relativement nouvelle et encore mal maîtrisée (intelligence artificielle), qui sera déployée dans le but de prendre des décisions individuelles automatisées (sélection ou non d'un candidat) qui peut, en cas de données d'entraînement non représentatives ou de modèle mal conçu, favoriser les discriminations à l'embauche.*

Conclusion:	*Le traitement de données personnelles envisagé est susceptible d'entraîner un risque élevé pour les droits fondamentaux des personnes concernées : une AIPD doit être réalisée (Partie II).*
Signature du responsable du traitement	*Veuillez remplir le champ*
Signature du conseiller ou de la conseillère LIPAD	*Veuillez remplir le champ*
Signature du RSI	*Veuillez remplir le champ*
Consultation du PPDT si le conseiller ou la conseillère l'estime nécessaire	*oui/non*

Partie II - Analyse d'impact

Première Partie – Analyse détaillée de la base légale	
Bases légales ou règlementaires existantes ou prévues pour le traitement envisagé (art. 36 al. 1 1ère hypothèse LIPAD)	*oui*
Loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux (LPAC) et son règlement d'application (RPAC)	
Si non, le traitement est-il nécessaire à l'accomplissement d'une tâche légale? (art. 36 al. 1 2ème hypo LIPAD)	*oui*
Si oui, précisez	*Recrutement du personnel*
Le traitement nécessaire à l'accomplissement d'une tâche inclut-il des données sensibles ou du profilage? (art. 36 al. 2 LIPAD)	*non*
Si oui, précisez	*n.a.*
- une loi au sens formel prévoit-elle expressément ce traitement? (art. 36 al. 2 let. a LIPAD)	*n.a.*
Si oui, laquelle?	*n.a.*
- Si non, le traitement est-il indispensable à l'accomplissement d'une tâche définie elle-même dans une loi au sens formel (art. 36 al. 2 let. b LIPAD)	*n.a.*
Si oui, laquelle ?	*n.a.*
Si vous avez répondu négativement aux questions précédentes, est-ce que l'une des situations suivantes est remplie ? :	*n.a.*
- la personne concernée a consenti au traitement en l'espèce; le responsable du traitement doit être en mesure de démontrer l'existence d'un tel consentement (art. 36 al. 3 let. a LIPAD); *pour rappel: le consentement peut être retiré en tout temps par la personne concernée*	*n.a*
- la personne concernée a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement (art. 36 al. 3 let. b LIPAD)	*n.a.*
- la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement et le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique (art. 36 al. 3 let. c LIPAD)	*n.a.*

Deuxième Partie - Description détaillée du traitement envisagé	
Indiquez quel est le traitement envisagé (quelles catégories de données personnelles sont traitées par qui, comment et à quelle fin).	
Il s'agit de collecter les données de recrutement des candidats aux postes ouverts au sein de l'administration via une plateforme en ligne qui ensuite analyse les données des candidats avec les critères des postes et l'expérience de l'IA pour sélectionner les 5 meilleurs profils pour la suite du processus de recrutement. Les données collectées sont les données classiques lors d'un recrutement à savoir: le nom, prénom, la date de naissance, l'adresse postale et de courrier électronique, la nationalité, le parcours académique et le parcours professionnel, une lettre de motivation et un CV.	
Entités participantes au traitement	
Responsable du traitement	*Ressources humaines*
Responsable du traitement conjoint	*n.a.*
Sous-traitant(s)	*BestEmployee4YOU*
Sous-traitant(s) à l'étranger	*oui*
Si oui, dans quel pays?	*USA*
Le pays est-il dans la liste des pays autorisés par le Conseil fédéral?	*Oui, et l'entreprise figure sur la liste des entreprises certifiées qui offrent un niveau de protection des données adéquat*
Destinataire(s)	*BestEmployee4YOU*
Catégories de personnes concernées	
Personnes en recherche d'emploi	

Description du traitement envisagé	
Les données seront collectées via la plateforme en ligne et enregistrée dans les bases de données de l'application (cloud aux USA). Les données sont conservées dans ses bases de données pour la durée du traitement et jusqu'à un an pour les candidats non retenus. Les données sont utilisées par le système d'IA pour déterminer les meilleurs profils et par les ressources humaines. Les données ne peuvent pas être modifiées par le responsable du traitement, seule la personne concernée pouvant modifier ses données en ligne. Les données sont archivées et sauvegardées régulièrement. Un effacement automatique des données des candidats non retenus est mis en œuvre.	
Collecte	*oui*
Enregistrement	*oui*
Conservation	*oui*
Utilisation	*oui*
Modification	*non*
Communication	*oui*
Archivage	*oui*
Effacement	*oui*
Nature du traitement envisagé	
Collecte de données personnelles à l'insu de la personne concernée	*non*
Si oui, selon quelle(s) base(s) légale(s)?	*n.a.*
Interconnexion ou appariement avec d'autres bases de données	*oui*
Si oui, lesquelles?	*Base de données du prestataire de la solution qui, selon son modèle d'IA, permet de sélectionner les meilleurs profils pour les postes proposés*
Données personnelles accessibles en ligne selon le principe de self-service (ex. e-démarches)	*oui*
Si oui, précisez	*Les candidats accèdent à leurs données via la plateforme BestEmployeed4YOU en ligne*
Profilage	*non*
Si oui, précisez	*n.a.*
Évaluation ou notation des personnes concernées	*oui*
Si oui, précisez	*Les candidats et leurs données seront évalués directement par le système d'IA selon son modèle de sélection.*

Décision individuelle automatisée	*oui*	
Si oui, précisez	*L'outil sélectionne automatiquement les 5 meilleurs candidats et envoie automatiquement une réponse négative aux autres personnes concernées.*	
Surveillance	*non*	
Si oui, précisez	*n.a.*	
Technologies utilisées		
Logiciels	*oui*	*BestEmployee4YOU*
Informatique en nuage (Cloud)	*oui*	*Software as a Service (SaaS)*
- Le Cloud est-il situé à l'étranger?	*oui*	*États-Unis*
- Le pays est-il dans la liste des pays autorisés par le Conseil fédéral?	*Oui et l'entreprise est dans la liste des entreprises certifiées*	
Intelligence artificielle	*oui*	*IA propre au fournisseur de la solution qui, pour des questions de secret des affaires, ne communique pas d'information sur les données d'entrainement ou son modèle. C'est toutefois l'outil le plus recommandé aux États-Unis et les commentaires sur internet sont très positifs.*
Autres nouvelles solutions technologiques	*non*	*n.a.*
Étendue du traitement		
Grande quantité de données personnelles		*non*
Grande quantité de personnes concernées		*non*
Traitement de longue durée		*non*
Traitement sur une grande étendue géographique		*non*
Durée de conservation des données personnelles courantes		*1 an pour les candidats non retenus. Jusqu'à un an après la fin du contrat pour les autres.*
Durée de conservation des données personnelles archivées de manière intermédiaire		*10 ans*
Durée de conservation des journaux techniques		*10 ans*

Justification des durées de conservation (bases légales)	*Loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux (LPAC)*
Mécanisme de suppression et/ou règles d'archivage à la fin du traitement	*1 an pour les candidats non retenus. Jusqu'à un an après la fin du contrat pour les autres.*
Conclusion: indiquez si le traitement dépasse dans son étendue le cadre ordinaire d'un traitement de données (traitement à grande échelle)	*non*
Motivation	*non*

Troisième partie – Évaluation du risque pour les droits fondamentaux de la personne concernée						
Évaluation du risque inhérent[1]						
Réf.	Risque	Description	Probabilité inhérente	Impact inhérent	Évaluation du risque inhérent	Risque acceptable ?
1	*Non-respect de l'art. 38B al. 2 LIPAD*	*L'absence de documentation et de transparence sur le modèle d'IA de la part du sous-traitant ne permettra pas à l'institution publique de respecter son devoir d'information prévu à l'art. 38B al. 2 LIPAD.*	Forte	Fort	*L'institution publique doit être en mesure d'expliquer les mécanismes de prise de décisions individuelles automatisées et cela ne peut pas être le cas en l'absence d'information sur le modèle d'IA développé par BestEmployee4YOU-*	*non*
2	*Discrimination à l'embauche*	*La sélection automatique de candidats par l'IA pourrait engendrer une discrimination à l'embauche si les données d'entraînement favorisent la sélection de candidats en se fondant exclusivement sur des critères comme l'origine ethnique ou nationale, la couleur de peau ou l'appartenance religieuse (art. 8 al. 2 Cst.)-*	Faible	Faible	*Les données relatives à l'origine ethnique ou nationale, la couleur de peau ou l'appartenance religieuse ne sont pas collectées par l'application d'IA.*	*oui*
3	*Biais à l'embauche*	*Les filtres alimentés par l'IA pourraient favoriser par erreur des candidats spécifiques en fonction de leur sexe, de leur race, de leur âge ou d'une autre caractéristique. (Les biais du recrutement augmenté à l'IA : ce qu'il faut savoir | LeMagIT - Insight - Amazon scraps secret AI recruiting tool that showed bias against women | Reuters)-*	Forte	Moyen	*En l'absence de documentation du modèle d'IA et d'informations précises sur les données d'entraînement du modèle, la probabilité de biais ne peut être exclue. L'impact serait en particulier en terme d'image pour l'institution-*	*non*

[1] Le risque inhérent se définit comme le risque théorique lié à l'activité de traitement des données. On peut aussi le définir comme le risque initial, avant toute mesure de maîtrise/réduction du risque. Dans cet exemple fictif, seuls quelques risques sont développés à titre d'exemple de la méthode et l'analyse des risques n'est pas exhaustive.

4	*Transfert de données à l'étranger*	*Les données personnelles des candidats pourraient être obtenues par des personnes non autorisées dans le Cloud ou par des autorités étrangères (Cloud Act).*	Forte	Moyen	*Dès lors que les données sont transmises sur la plateforme cloud, il n'est pas possible d'exclure le risque d'un accès non autorisé.*	*Non*
5	*Sécurité des données*	*La confidentialité, l'intégrité et la disponibilité des données pourraient être impactées en cas de cyber attaque visant l'application.*	Forte	Fort	*Il s'agit du risque lié à tous les systèmes connectés.*	*Non*

Évaluation du risque résiduel[2]						
Réf.	Risque	Mesures de réduction des risques existantes	Probabilité résiduelle	Impact résiduel	Évaluation du risque résiduel	Risque acceptable ?
1	*Non-respect de l'art. 38B al. 2 LIPAD*	*Le fournisseur de la solution refuse contractuellement de diffuser les informations sur son modèle d'IA et les tentatives de négociations sont restées vaines.*	Forte	Fort	*Aucune mesure ne permet de réduire le risque à ce stade.*	*non*
3	*Biais à l'embauche*	*S'agissant d'un système nouveau, il n'existe pas de mesure à ce jour.*	Forte	Moyen	*En l'absence de documentation du modèle d'IA et d'informations précises sur les données d'entraînement du modèle, la probabilité de biais ne peut être exclue.* *L'impact serait important en terme d'image pour l'institution.*	*non*
4	*Transfert de données à l'étranger*	*L'application permet un chiffrement des données de bout en bout avec gestion des clés de chiffrement au sein de l'institution.*	Faible	Faible	*Le risque est parfaitement maîtrisé par le niveau de chiffrement et la gestion des clés.*	*oui*

[2] Le risque résiduel est le risque subsistant après la mise en œuvre de dispositifs de maîtrise/réduction du risque.

5	*Sécurité des données*	*L'application permet un chiffrement des données de bout en bout avec gestion des clés de chiffrement au sein de l'institution.* *Les données de l'application seront sauvegardées régulièrement au sein du SI de l'institution en sus des systèmes de sauvegarde du fournisseur cloud de la solution.* *Le fournisseur garantit par SLA la haute disponibilité avec des systèmes de redondances.*	Moyen	Faible	*Les mesures techniques identifiées permettent de réduire principalement l'impact de la survenance de ce risque et nous jugeons le risque résiduel acceptable.*	*oui*

Quatrième partie – identification des mesures prévues pour protéger les droits fondamentaux de la personne concernée					
Réf.	Risque	Mesures prévues	Responsable de la mise en œuvre	Délai de mise en œuvre	Coût de la mise en œuvre de la mesure pour rendre le risque acceptable ?
1	*Non-respect de l'art. 38B al. 2 LIPAD*	*En l'absence d'accès à la documentation du modèle d'IA, la seule solution est de trouver un autre fournisseur ayant une solution similaire mais acceptant la transparence sur le modèle d'IA et éventuellement sur les données d'entraînement dudit modèle. Ces points d'évaluation doivent être ajoutés dans le nouveau formulaire d'appel d'offre qui sera émis.*	*Département IT*	*Avant le début du projet*	*Un nouvel appel d'offre doit être effectué et le coût de la mise en œuvre est surtout en termes de ressources humaines.*
3	*Biais à l'embauche*	*L'outil d'IA sera rigoureusement testé avec des CVs fictifs pour évaluer s'il présente des biais. Notamment des CVs en tous points équivalents, mais avec des différences uniquement sur le sexe, l'âge ou l'origine seront créés afin de s'assurer que l'outil ne présente pas de biais. Ces tests seront effectués à chaque changement/modification/mise à jour de l'application.*	*Département RH*	*Avant le début du projet*	*Le coût de la mise en œuvre est surtout en termes de ressources humaines.* *La mise œuvre des tests, non seulement avant le début du projet, mais également à chaque modification / mise à jour du logiciel devrait permettre de réduire le risque à un niveau acceptable.*

Cinquième partie – évaluation des effets des mesures prévues pour protéger les droits fondamentaux de la personne concernée afin de déterminer s'il reste un risque résiduel élevé				
Réf.	Risque	Mesures prévues	Évaluation et description des effets desdites mesures	Risque résiduel élevé?
1	*Non-respect de l'art. 38B al. 2 LIPAD*	*Sélection d'un nouveau fournisseur de solution*	*Le fait de disposer de la documentation du modèle d'un nouveau fournisseur permettra de justifier des mécanismes de décision individuelle au sens de l'art. 38B al.2 et d'assurer un traitement licite.*	*non*
3	*Biais à l'embauche*	*Test du système avec des CVs fictifs avant le déploiement et les changements*	*Le fait de tester le système de manière robuste ne permet pas d'exclure totalement le fait que celui-ci puisse produire ou non des biais en l'absence de maitrise du modèle et d'information sur les données d'entraînement. Par contre, le fait de le tester au maximum réduit l'impact, notamment en terme d'image, puisque nous pourrions démontrer avoir pris les mesures de tests nécessaires et adéquates.*	*non*

Sixième partie – synthèse et résultats de l'AIPD	
Le risque résiduel identifié comme étant élevé est celui de mettre en œuvre une solution favorisant des biais au moment de l'embauche. On peut penser par exemple au fait que la solution favoriserait des profils masculins pour des professions pour lesquelles la représentation masculine est plus importante aujourd'hui (ex. dans les métiers informatiques). *En l'absence de documentation disponible sur les données d'apprentissage du modèle et sur le modèle d'IA, nous proposons de définir notamment des CVs en tous points équivalents, mais avec des différences uniquement sur le sexe, l'âge ou l'origine afin de s'assurer que l'outil ne présente pas de biais. Ces tests seront effectués à chaque changement/modification/mise à jour de l'application.* *Nous pensons que la mise en œuvre systématique et documentée de ces tests permettra de réduire ce risque résiduel à un niveau acceptable.* *Le second risque résiduel identifié comme étant élevé par le département juridique au cours de l'AIPD est celui du non-respect de l'art. 38B al. 2 LIPAD s'il n'est pas possible de justifier les mécanismes de prise de décisions individuelles automatisées en l'absence de documentation du modèle d'IA. Toutes les négociations avec le fournisseur de BestEmployee4YOU n'ayant pas abouti, une autre solution doit donc être trouvée. L'obligation de transparence du modèle d'IA et des données d'entraînement du modèle sera ajoutée au formulaire d'appel d'offre. Si une nouvelle solution est sélectionnée, la présente AIPD sera mise à jour.*	
Date	
Signature du responsable du traitement	
Date	
Signature de la/le conseillère/conseiller LIPAD	
Date	
Signature du RSI	