CANTON DU VALAIS
KANTON WALLIS

Préposé cantonal à la protection des données et à la transparence
Kantonaler Datenschutz- und Öffentlichkeitsbeauftragter
Lauris Loat

Réalisation d'une Analyse d'impact en matière de protection des données

Pour élaborer une Analyse d'impact en matière de protection des données (ci-après : « AIPD »), on peut s'inspirer de la structure proposée ci-dessous, qui est fournie à titre purement indicatif par le Préposé cantonal à la protection des données et à la transparence.

I. Descriptif du projet

Informations générales

Nom du projet	**[Nom]**	
Évaluation réalisée par:	Personne responsable :	**[nom]**
	Conseiller externe :	**[nom]**
Version du document	Version XX, [date]	

Enjeu – qu'est-ce qui est prévu ?

[description du projet / de la modification]

Fonctionnement – quel est le fonctionnement du projet / de la modification ?

[description du fonctionnement du projet / de la modification]

But – pourquoi le projet / la modification est-il/elle entrepris(e) ?

[description des raisons qui motivent le projet / la modification]

Finalité – quelle est la finalité du traitement des données personnelles ?

[par exemple : l'analyse de la sécurité, l'audit, les rapports, l'administration du personnel, etc..]

Incidences sur la protection des données – quels sont les impacts potentiels de ce projet / cette modification sur les droits des personnes concernées ?

[Quel sera l'impact de ce projet / de cette modification sur les droits des personnes concernées ? Décrivez brièvement ces impacts.]

Parties prenantes – qui est impliqué dans le projet / la modification ?

[Veuillez énumérer les parties prenantes, y compris les participants internes et les organisations externes (publiques/privées/tiers) qui seront concernées par ce projet / cette modification (p. ex. en participant à leur développement/mise en œuvre ou en étant affectées par son fonctionnement).]

Nécessité d'une AIPD ?

[à compléter]

Précédentes AIPD effectuées ou autres formes d'évaluation effectuées en lien avec la protection des données personnelles dans le cadre de ce projet / cette modification ?

[Veuillez fournir des détails sur toute évaluation antérieure se rapportant directement ou indirectement à la protection des données (y compris la sécurité) effectuée dans le cadre de ce projet. S'il s'agit d'une modification d'un système existant, une évaluation peut avoir été réalisée lors du projet initial.]

II. Analyse des bases juridiques

Bases juridiques

Sur quelles bases juridiques se fonde le traitement des données ?

..

Cycle de vie des données

Décrivez le cycle de vie des données :

- Collecte de données : indiquez les sources et les formes de collecte

..

- Utilisation : indiquez le cercle des utilisateurs-trices et le type d'utilisation

..

- Stockage : indiquez le stockage et les lieux de stockage

..

- Conservation : indiquez les exigences légales pour la conservation des données

..

- Archivage : Indiquez la base juridique pour/contre l'archivage

..

- Suppression : Indiquez les exigences légales pour la suppression des données

..

Proportionnalité

Établissez la proportionnalité de l'utilisation prévue en tenant compte du principe de l'économicité et de la minimisation des données

..

III. Évaluation des risques du point de vue de la protection des données

Évaluation des risques principaux (sans les mesures)

Accès non autorisé à des données personnelles (confidentialité)	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
Manipulation non autorisée de données personnelles (intégrité)	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
Perte des données / aucun accès aux données (disponibilité)	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

	Probabilité d'occurrence	Impact :		
		faible	moyen	élevé
Communication/transmission non autorisée de données personnelles en Suisse et/ou à l'étranger	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

	Probabilité d'occurrence	Impact :		
		faible	moyen	élevé
Mise en péril des mesures de protection (ex : le cryptage, l'anonymisation / la pseudonymisation, la transmission du mot de passe, les logiciels malveillants, etc…)	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

	Probabilité d'occurrence	Impact :		
		faible	moyen	élevé
Autres risques	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

IV. Mesures visant à minimiser les risques

Parmi les mesures suivantes[1], lesquelles sont les plus propices à réduire les risques et seront mises en œuvre avant le début de l'exploitation.

	Non	Oui
Il existe un SMSI (Information Security Management System). Le traitement de données est lié à celui-ci.	☐	☐
Une organisation de la sécurité est établie : les responsabilités, les tâches et les compétences pour la protection des données sont définies et attribuées.	☐	☐
La sensibilisation des utilisateurs-trices au traitement des données personnelles est en place dans l'organisation (introduction, formation).	☐	☐
Les données sont classifiées et les propriétaires des données personnelles sont déterminés.	☐	☐
Le concept d'autorisation est établi et les principes de l'approche « need-to-know » sont pris en compte.	☐	☐
Tous les destinataires de données personnelles externes/internes sont désignés et il est assuré qu'ils sont autorisés à traiter des données.	☐	☐

[1] Inspiré de la norme ISO 27002

L'intégrité des données personnelles est assurée (aucune manipulation intentionnelle ou involontaire des données personnelles n'est possible).	☐	☐
Les mesures de cryptage/chiffrement nécessaires permettant la protection des données personnelles sont appliquées avec précision.	☐	☐
Les mesures pour une protection physique adéquate des données et des systèmes sont prises et leur efficacité est vérifiée.	☐	☐
Les processus d'exploitation pour la gestion du changement et de la mise en production sont établis.	☐	☐
Les données sont régulièrement sauvegardées (sauvegarde & restauration).	☐	☐
Il y a une protection appropriée contre les logiciels malveillants.	☐	☐
Les accès aux données sont répertoriés et vérifiés.	☐	☐
Les mises à jour de sécurité sont installées rapidement selon des procédures testées.	☐	☐
La sécurité du réseau est assurée.	☐	☐
Les canaux de communication sont définis et répondent aux exigences en matière de protection des données.	☐	☐
Les fournisseurs sont tenus de respecter les exigences en matière de protection des données (contrat, SLA).	☐	☐
Les mesures de sécurité sont contrôlées et adaptées périodiquement.	☐	☐
Autres mesures :	☐	☐

V. Évaluation des risques après la mise en œuvre des mesures

Évaluations des risques principaux (avec les mesures)

	Probabilité d'occurrence	**Impact :**		
		faible	moyen	élevé
Accès non autorisé à des données personnelles (confidentialité)	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

	Probabilité d'occurrence	**Impact :**		
		faible	moyen	élevé
Manipulation non autorisée de données personnelles (intégrité)	élevé	☐	☐	☐
	moyen	☐	☐	☐

	faible	☐	☐	☐
Perte des données / aucun accès aux données (disponibilité)	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
Communication/transmission non autorisée de données personnelles en Suisse et/ou à l'étranger	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
Mise en péril des mesures de protection (ex : le cryptage, l'anonymisation / la pseudonymisation, la transmission du mot de passe, les logiciels malveillant, etc…)	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐
Autres risques	**Probabilité d'occurrence**	**Impact :**		
		faible	moyen	élevé
	élevé	☐	☐	☐
	moyen	☐	☐	☐
	faible	☐	☐	☐

Risques résiduels

Indiquez les risques qui sont encore « jaunes » ou « rouges » dans l'évaluation après la mise en œuvre des mesures :

..
..

VI. Décision de consultation préalable

Si des risques résiduels sont mentionnés au chapitre précédent, une consultation préalable du Préposé valaisan à la protection des données et à la transparence est nécessaire.

Une consultation préalable est nécessaire	NON ☐	OUI ☐

Date: Nom du signataire : Signature :

Preuves et documentations

Il convient de mentionner ici les justifications et la documentation qui décrivent les mesures organisationnelles, juridiques et techniques assurant une exploitation conforme à la protection des données :

[Exemples

- Concept SIPD
- Concept de droit d'accès
- Plan architectural
- Cycle de vie des données, y compris le concept de suppression
- Règlement du personnel concernant le traitement des données personnelles
- Contrats des fournisseurs (contrats de services)
- Bases légales du traitement des données
- Autres documents]