Guide de gestion des données

Version 1

Licence

Le *Guide de gestion des données* de l'Université de Montréal :

Clause de non-responsabilité : Ceci est une adaptation d'une œuvre originale de Nord Ouvert. Les points de vue et les opinions exprimés dans l'adaptation relèvent de la seule responsabilité de l'auteur et l'adaptation n'est pas approuvée par Nord Ouvert.

Historique du document

VERSION	ACTION	PERSONNE	DATE
0.1	Rédaction initiale	Dominic Boisvert, Karolanne Laurendeau-Goupil, Cristel Silva Silva	2023-06-02
0.**2**	Intégration de commentaires et séparation des informations complémentaires des fiches des tactiques	Dominic Boisvert, Karolanne Laurendeau-Goupil, Cristel Silva Silva, Carolle Djima, Merci à Annick Lachapelle pour la relecture externe.	2023-10-10
1.0	Version 1.0	Dominic Boisvert, Karolanne Laurendeau-Goupil, Cristel Silva Silva, Carolle Djima	2023-10-11

Table des matières

Contexte

Dans son *Cadre de gouvernance des données* opérationnelles, et son plan d'architecture d'entreprise, l'Université de Montréal affirme, sous la forme de principes, l'importance de la valorisation des données comme un actif et du partage de celles-ci.

Objectif

Pour réaliser ces principes, le *Guide de gestion des données* fournit aux unités un coffre à outils s'appuyant sur un processus solide et des tactiques[1] fondamentales et opérationnelles reproductibles.

Il permet, par l'application des tactiques, de valoriser les données et de mettre en place les conditions nécessaires pour le partage des données, et ce, dans le respect du cadre normatif de l'Université de Montréal.

Avant d'appliquer les tactiques

Nous vous recommandons de débuter par la lecture du *Cadre de gouvernance des données opérationnelles*, qui détermine la vision de la gouvernance des données et les rôles et responsabilités qui en découlent.

Après une première lecture du *Guide de gestion des données*, nous vous proposons de vous approprier le contenu des documents suivants avant de mettre en œuvre les tactiques :

- Le *Diagramme décisionnel d'un cas d'utilisation des données* pour connaître et suivre le processus ;
- La liste de contrôle d'un cas d'utilisation des données pour documenter le cas d'utilisation ;
- L'échelle de maturité, utile pour identifier le point de départ et mesurer la progression ;
- Le glossaire de la gouvernance des données, utile pour assurer une compréhension commune des termes.

Méthodologie

Le G*uide de gestion des données* présente un ensemble de tactiques nécessaires à la bonne gestion des données en tant qu'actif de l'Université. Ces tactiques sont regroupées par thème, eux-mêmes associés au cycle de vie des données.

Diagramme décisionnel et liste de contrôle d'un cas d'utilisation

En suivant les étapes du *Diagramme décisionnel d'un cas d'utilisation des données*, compléter la documentation nécessaire pour chaque tactique. Pour ce faire, vous disposez d'un gabarit de *Liste de contrôle d'un cas d'utilisation des données*. La liste reprend la même séquence que vous retrouverez plus loin dans la section intitulée « Fiches de cas d'utilisation des données ».

Dans certains cas, il ne sera pas possible de documenter pleinement une tactique dans la liste de contrôle. Lorsque cela se produit, nous vous recommandons de documenter la tactique dans un document et d'enregistrer celui-ci dans le même dossier que la liste de contrôle d'un cas

[1] Pour une définition des termes spécifiques, veuillez consulter le glossaire.

d'utilisation des données. Il est aussi souhaitable de copier toute documentation pertinente à une tactique dans le dossier du cas d'utilisation.

Le gabarit *Liste de contrôle d'un cas d'utilisation des données* contient des instructions supplémentaires pour vous guider.

Tactiques

Les tactiques sont les actions concrètes qui doivent être posées pour se conformer aux principes du C*adre de gouvernance des données opérationnelles* de l'Université de Montréal. Cette section présente une série de tactiques (sous forme de fiche), organisées par thème, qui traduisent les principes du cadre de gouvernance des données opérationnelles en directives. Les unités doivent s'assurer de bien faire la distinction entre les tactiques fondamentales et les tactiques opérationnelles.

Attention	
	Cette icône signifie que la tactique s'applique à l'ensemble de l'Université et ne peut être modifiée par le domaine, l'unité ou la partie prenante.

Tactiques fondamentales

Les tactiques fondamentales sont des actions de haut niveau qui sont mises en œuvre soit une fois, globalement pour l'Université, soit au niveau d'un domaine de données ou d'une unité ou d'un partenariat de données[2]. Elles peuvent inclure la rédaction de politiques, de lignes directrices ou de stratégies, ainsi que le choix de normes et de standards.

Lorsqu'elles sont combinées, les tactiques forment la stratégie de données de l'institution. Les tactiques fondamentales doivent être mises en œuvre de manière proportionnelle à la nature, à l'importance et à l'ampleur des activités liées aux données.

> *Les tactiques fondamentales mises en œuvre au niveau de l'institution et celles au niveau des unités sont révisées séparément aux trois ans par le Forum des intendants[e]s, avec le support du responsable de la gouvernance des données.*

Tactiques opérationnelles

Les tactiques opérationnelles sont des actions de terrain qui sont mises en œuvre grâce à la collaboration de toute partie prenante impliquée dans un cas d'utilisation de données, qui appuie l'unité dans une prise de décision, et ce tout au long du cycle de vie des données (figure 1).

Les tactiques opérationnelles sont le prolongement des tactiques fondamentales appliquées à un cas d'utilisation. Elles sont des occasions d'approfondir les tactiques fondamentales à la lumière de la mise en pratique des cas d'utilisation concrets.

> *Les tactiques opérationnelles sont révisées aux trois ans par l'unité, sous la supervision de l'intendant[e] des données de l'unité et avec la collaboration du responsable de la gouvernance des données.*

Tactiques fondamentales ou opérationnelles qui sont conditionnelles

Afin de tenir compte des besoins et des réalités particulières de certains partenaires, de certains domaines ou de certaines unités, des tactiques fondamentales et opérationnelles conditionnelles sont proposées. Comme leur nom l'indique, les tactiques conditionnelles s'appliquent que si le cas d'utilisation remplit une condition particulière, comme la collecte ou le partage de renseignements personnels ou sensibles. Une tactique fondamentale ou opérationnelle conditionnelle est reconnaissable, dans les pages suivantes, par l'icône (voir encadré ci-dessous) qui l'accompagne.

Conditions particulières qui justifient le recours aux tactiques conditionnelles	
	Collecte, utilisation ou partage de données confidentielles ou hautement confidentielles
	Utilisation d'une solution technologique interne pour collecter des données confidentielles ou hautement confidentielles
	Utilisation d'une solution technologique interne pour partager des données confidentielles ou hautement confidentielles
	Externalisation d'une ou plusieurs étapes du cycle de vie des données associées au thème en question (par exemple : externalisation de l'analyse de vos données)

En plus des tactiques consignées par le guide, il faudra vous assurer dans la planification de vos cas d'utilisation, d'avoir les ressources nécessaires pour les mener à bien, de clarifier et d'attribuer les rôles et les responsabilités concernant la gestion des données dans l'unité ; et d'identifier des occasions de formation, le cas échéant, pour s'assurer que les personnes assignées ont les moyens de remplir leurs responsabilités.

Le contenu des fiches se veut succinct pour faciliter la lecture du guide. Vous pourrez trouver davantage d'informations en dernière partie du document dans laquelle chaque thème se voit bonifier par des précisions, de l'information complémentaire susceptible de vous intéresser en plus de ressources pouvant vous être utiles.

Le cycle de vie

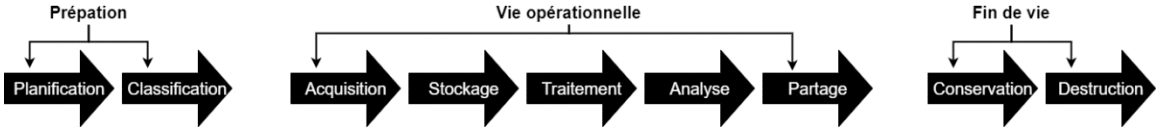
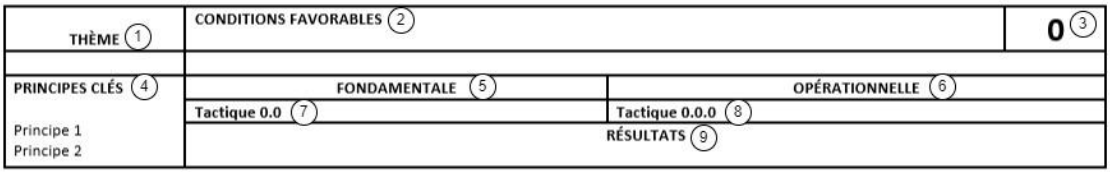


Figure 1 Cycle de vie des données.

Les tactiques opérationnelles peuvent s'appliquer à une ou plusieurs étapes du cycle de vie des données présenté à la figure 1. Il faut noter que chaque jeu de données peut avoir un cycle de vie dont la durée des phases peut différer.

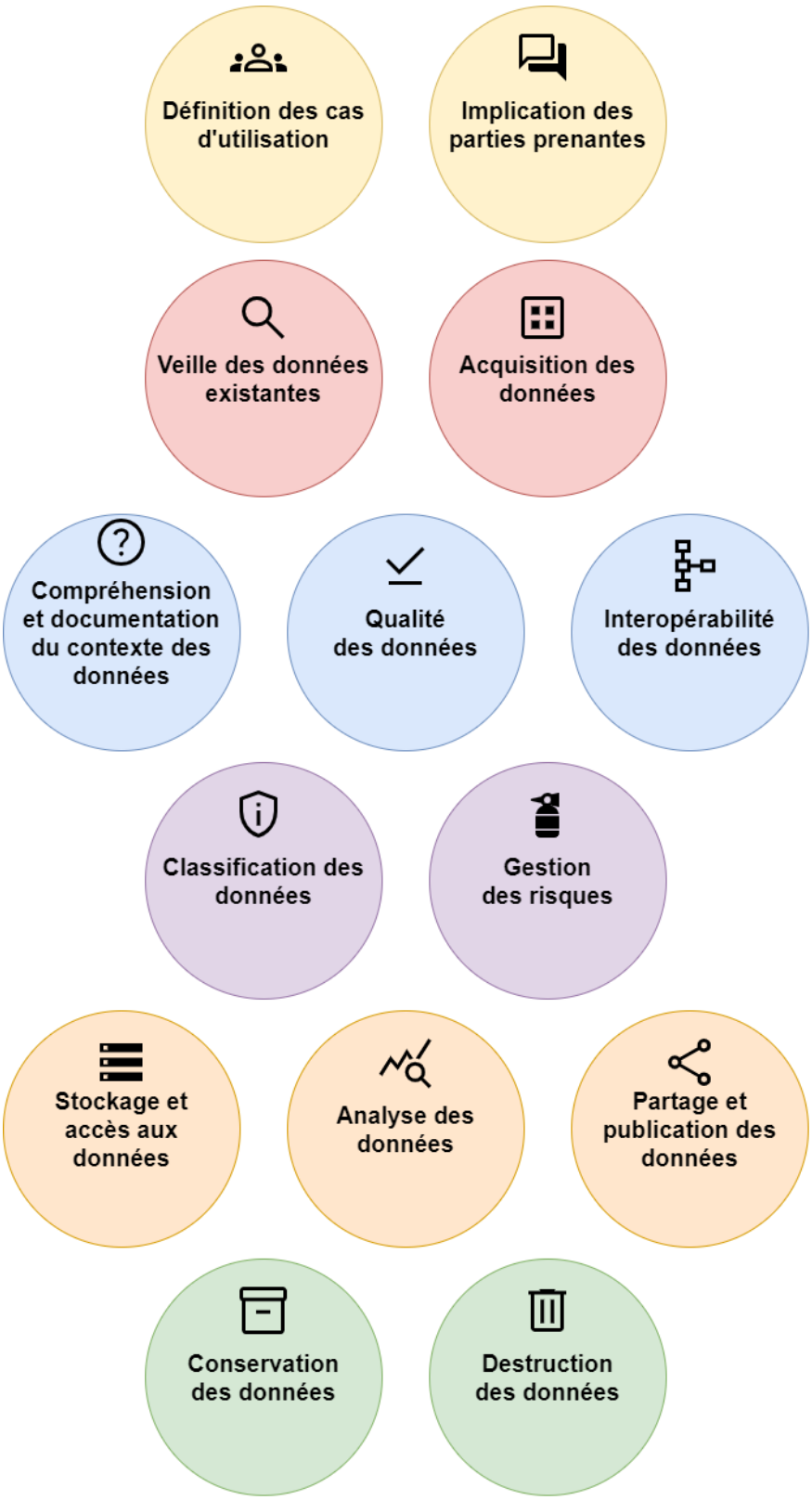
Les composantes d'une fiche de cas d'utilisation



1. Intitulé de la thématique des tactiques.
2. Activités, compétences ou outils de gestion en place favorisant l'application des tactiques.
3. Cote associée au thème et composée d'un numéro.
4. Principes associées au thème parmis ceux retenus par l'Université.
5. Colonne pour les tactiques fondamentales.
6. Colonne pour les tactiques opérationnelles.
7. Les tactiques fondamentales sont identifiées par une cote de deux numéros séparés par un point. Le premier numéro est celui associé au thème dont elles découlent.
8. Les tactiques opérationnelles sont identifiées par une cote de trois numéros séparés par des points.Les deux premiers numéros de la cote sont ceux de la tactique fondamentales dont elles découlent.
9. Résultats atteignables lorsque l'ensemble des tactiques énumérées dans le tableau sont mises en oeuvre.

Figure 2 Composantes d'une fiche de cas d'utilisation.

Les thèmes de la gestion des données



Matrice des tactiques opérationnelles appliquées au cycle de vie des données

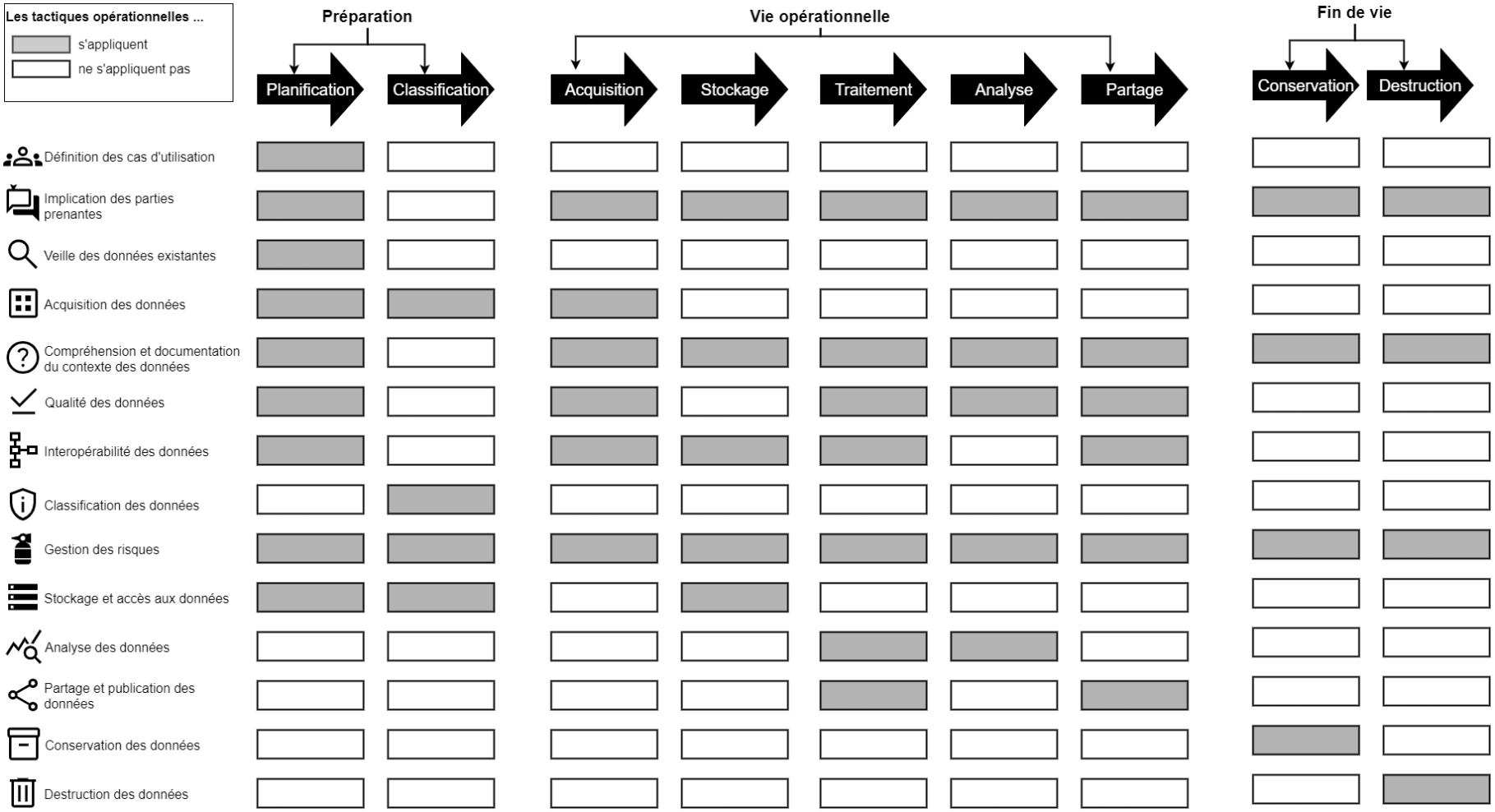
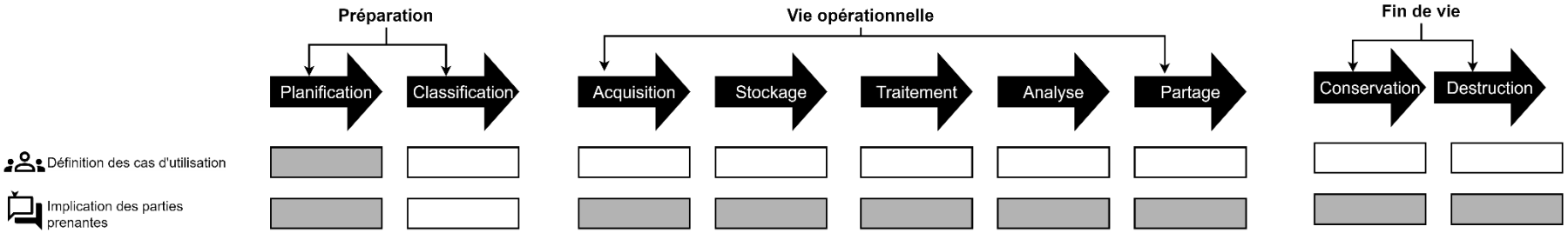


Figure 3 Matrice des tactiques opérationnelles appliquées au cycle de vie des données.

Fiches de cas d’utilisation des données

DÉFINITION DES CAS D’UTILISATION	IMPLICATION DES PARTIES PRENANTES
Ce thème vise à assurer que vous mobilisez vos données pour combler des besoins et prendre des décisions. Et que vous définissez clairement les conditions de succès du cas d’utilisation envisagé (qu’il soit exploratoire ou non).	Ce thème vous aide à établir la confiance, à atténuer les dommages et à améliorer la pertinence des données tout au long d’un cas d’utilisation.



01 - DÉFINITION DES CAS D'UTILISATION	**CONDITIONS FAVORABLES** • Supervision et vision stratégique • Plan de communication

PRINCIPES CLÉS	**FONDAMENTALE**	**OPÉRATIONNELLE**
Principe 1 Principe 2	**Tactique 1.1** En impliquant toutes les parties prenantes concernées, documenter les valeurs générales que votre unité ou votre partenariat cherche à générer par l'utilisation des données et comment celles-ci contribuent à la gestion ou à la mission de l'Université.	**Tactique 1.1.1** Explorer le ou les besoins auxquels le cas d'utilisation tente de répondre en incluant une analyse des parties prenantes et le contexte d'affaires afin de déterminer la décision à prendre. Étudiez les méthodes qui ont été utilisées jusqu'à maintenant, y compris les solutions non numériques. Documentez ce que vous avez appris avec des mots simples et clairs. **Tactique 1.1.2** Identifier le ou les résultats souhaités du cas d'utilisation, les indicateurs de succès et les conditions favorables à leur réussite. **Tactique 1.1.3** Démontrer que le ou les résultats souhaités et le processus du cas d'utilisation soutiennent la gestion ou la mission de l'Université, conformément à sa définition. **Tactique 1.1.4** Questionner l'utilité d'une intervention basée sur les données pour répondre au besoin. Si c'est le cas, réfléchissez au type de données nécessaires pour atteindre les objectifs du cas d'utilisation et aux limites potentielles de ces données. **Tactique 1.1.5** Questionner l'utilité d'une intervention basée sur l'intelligence artificielle. Si vous décidez d'y recourir, identifier les avantages et les risques d'y recourir dans le cadre de votre cas d'utilisation.
	Tactique 1.2 Intégrer les valeurs générales et les objectifs associés à l'utilisation des données dans de robustes processus organisationnels de suivi et d'évaluation.	**Tactique 1.2.1** Lorsque le cas d'utilisation s'arrête (achevé ou non), évaluer l'initiative ou le projet et ses résultats, en regard de ce qui était prévu, et partager les leçons apprises.
		RÉSULTATS

	• Être transparent sur les défis que vous relevez et conscient des risques encourus par l'unité, des groupes ou des personnes. • Mobiliser (de manière réfléchie, planifiée et structurée) les données comme moyen de répondre aux besoins réels et pour identifier des solutions plus efficaces et plus justes.

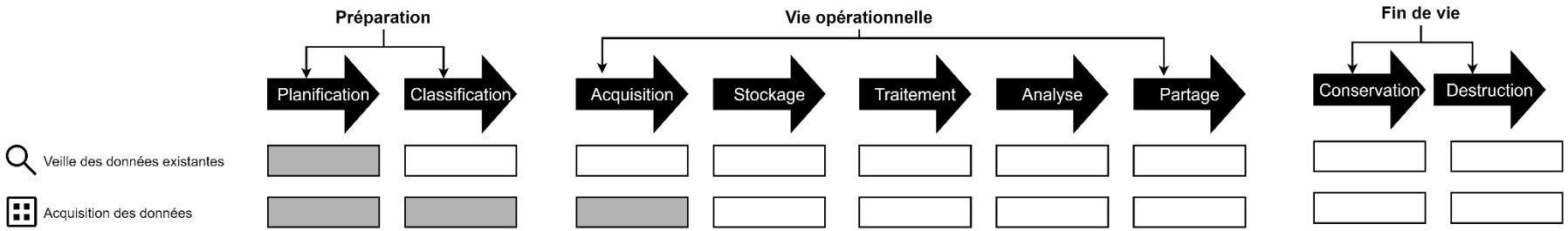
IMPLICATION DES PARTIES PRENANTES	**CONDITIONS FAVORABLES** • Compétences et formations • Supervision et vision stratégique • Culture des données claires et partagée • Plan de communication	
PRINCIPES CLÉS Principe 1 Principe 2	**FONDAMENTALE**	**OPÉRATIONNELLE**
	Tactique 2.1 Publier (sur un site Web, par exemple) et diffuser par tout moyen susceptible d'atteindre les parties prenantes de la gestion des données en utilisant un format lisible et facile à comprendre. Expliquer clairement comment un individu peut vous donner des retours ou poser des questions sur votre gestion des données, et comment vous allez les traiter. S'assurer que ces informations restent à jour.	**Tactique 2.1.1** Établir une stratégie inclusive sur la manière d'engager et de consulter toutes les parties prenantes concernées ou susceptibles d'être concernées par les décisions liées aux données tout au long du cas d'utilisation, le cas échéant (en mettant l'accent sur l'engagement et la consultation en amont du cas d'utilisation en question).
	Tactique 2.2 Élaborer un processus pour le traitement des plaintes et les enquêtes liées aux questions de confidentialité des renseignements personnels et le communiquer publiquement.	**Tactique 2.2.1** Traiter toutes les plaintes selon la procédure de gestion des incidents de confidentialité.
	RÉSULTATS • Renforcer la confiance du public en faisant preuve de transparence quant à vos pratiques de gouvernance des données et en valorisant l'opinion du public dans le processus décisionnel. • Prendre des décisions éclairées grâce à une meilleure compréhension des attentes et des besoins divers du public. • Respecter les principes de la Charte canadienne du numérique. • Améliorer la qualité de vos données en vous appuyant sur l'intelligence collective, ainsi que sur une diversité de points de vue, d'opinions et d'expertises.	

VEILLE DES DONNÉES EXISTANTES

Ce thème vous aide à découvrir les données existantes qui peuvent soutenir votre cas d'utilisation.

ACQUISITION DES DONNÉES

Ce thème s'applique si vous avez besoin de nouvelles données pour soutenir votre cas d'utilisation.



VEILLE DES DONNÉES EXISTANTES	**CONDITIONS FAVORABLES** • Supervision et vision stratégique • Outils et techniques	
PRINCIPES CLÉS Principe 1 Principe 2	**FONDAMENTALE**	**OPÉRATIONNELLE**
	Tactique 3.1 Tenir à jour le catalogue de tous les actifs de données à valeur stratégique détenus par votre unité ou votre partenariat, y compris les données ouvertes.	**Tactique 3.1.1** Évaluer si les jeux de données existants et disponibles dans le catalogue peuvent suffire pour le cas d'utilisation.
	RÉSULTATS • Disposer d'une vision complète et facilement accessible des données qui ont une valeur stratégique pour votre unité ou votre partenariat.	

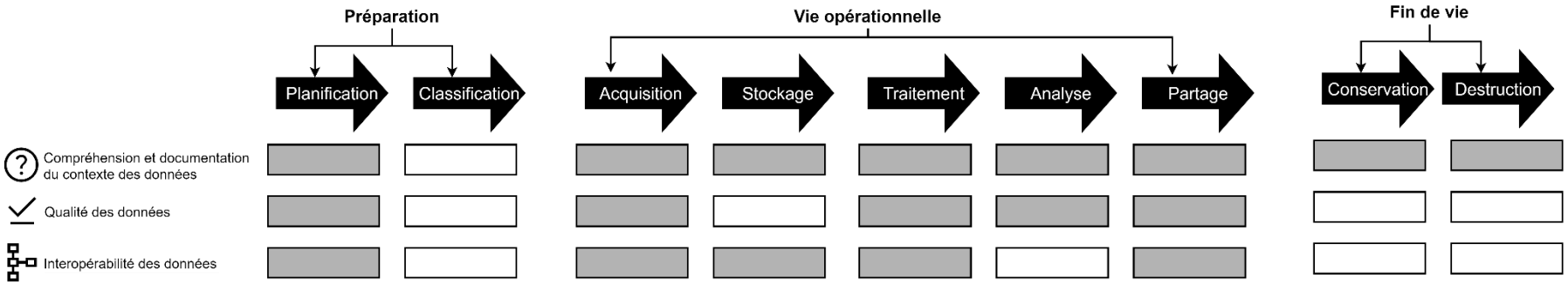
ACQUISITION DES DONNÉES	**CONDITIONS FAVORABLES** • Supervision et vision stratégique • Compétences et formation • Expertise légale • Plan de communication	
PRINCIPES CLÉS Principe 1 Principe 2	**FONDAMENTALE**	**OPÉRATIONNELLE**
	Tactique 4.1 Définir une stratégie d'acquisition des données qui concilie la pertinence des données (dont la capacité à rendre compte du contexte) avec les avantages des processus de minimisation des données.	**Tactique 4.1.1** Prévoir acquérir des données significatives et nécessaires pour atteindre les objectifs établis par le cas d'utilisation. **Tactique 4.1.2** Évaluer si l'acquisition des renseignements personnels (y compris les données ventilées) est absolument nécessaire pour atteindre efficacement les objectifs du cas d'utilisation. **Tactique 4.1.3** Déterminer une stratégie pour garantir que les nouvelles données saisies sont représentatives des groupes ou personnes concernées par le cas d'utilisation.
	Tactique 4.2 Rediriger vers la politique de confidentialité des données, accessible à toutes les personnes concernées, qui consigne des règles en termes simples pour protéger les renseignements personnels et sensibles pendant tout le cycle de vie des données	**Tactique 4.2.1** Appliquer les tactiques **8.2.1** et **9.1.2** avant de saisir des renseignements personnels ou des données sensibles. **Tactique 4.2.2** Évaluer si vos méthodes de saisie de données vous permettent d'obtenir un consentement manifeste, libre et éclairé à des fins déterminées et légitimes de la part des personnes concernées et, dans le cas contraire, réévaluez votre stratégie d'acquisition des données. **Tactique 4.2.3** Exiger du tiers qui saisira les données en votre nom de signer un accord de confidentialité (le cas échéant) et un accord de niveau de service avec des conditions d'utilisation définies.
	Tactique 4.3 Pour l'acquisition de données en utilisant une solution technologique, rédiger et publier les termes et conditions d'utilisation de celle-ci en termes clairs et simples et accessibles à tous les utilisateurs.	**Tactique 4.3.1** Si votre solution technologique comprend des fonctionnalités qui permettent l'identification, la localisation ou le profilage des individus, informer les par tous les moyens possibles de l'utilisation de cette technologie et des moyens, le cas échéant, proposer leur de désactiver les fonctionnalités d'identification, de localisation ou de profilage. **Tactique 4.3.2**

		S'assurer que, par défaut, les paramètres de votre solution technologique offrent le plus haut niveau de confidentialité sans aucune intervention de la personne concernée.
	RÉSULTATS • Utiliser des données utiles et adaptées aux besoins tout en minimisant les risques et les coûts environnementaux. • Assurer la conformité légale dans la collecte des renseignements personnels. • Protéger les droits fondamentaux à l'ère numérique, comme le consentement et le droit à la vie privée. • Construire la confiance des utilisateurs et encourager l'adoption des solutions technologiques.	

COMPRÉHENSION ET DOCUMENTATION DU CONTEXTE DES DONNÉES	QUALITÉ DES DONNÉES	INTEROPÉRABILITÉ DES DONNÉES

Ces trois thèmes, qui s'appliquent autant aux jeux de données existants que futurs, permettent d'avoir des données qui sont compréhensibles et prêtes à être utilisées dans tout système accepté et par tout utilisateur autorisé, ce qui assure leur capacité à répondre aux fins prévues et d'être mises en valeur.

Plus particulièrement, les deux premiers thèmes suscitent la confiance des parties prenantes en leur offrant de la documentation retraçant de manière transparente les décisions prises au sujet des données et les critères de qualités applicables. Bien qu'il faille privilégier l'application des tactiques appartenant à ces thèmes dès l'étape de la planification, elles peuvent également être appliquées à d'autres étapes du cycle de vie des données.



COMPRÉHENSION ET DOCUMENTATION DU CONTEXTE DES DONNÉES	**CONDITIONS FAVORABLES** • Outils techniques • Compétences techniques	
PRINCIPES CLÉS Principe 1 Principe 2 Principe 3 Principe 4 Principe 5	**FONDAMENTALE**	**OPÉRATIONNELLE**
	Tactique 5.1 Adopter des pratiques normalisées pour référencer et accéder aux métadonnées associées aux données qui sont sous votre responsabilité.	**Tactique 5.1.1** Veiller à ce que les métadonnées soient documentées conformément aux normes définies et accessibles dans un format lisible par les machines. **Tactique 5.1.2** Documenter les décisions pertinentes qui impactent les données à chaque étape de leur cycle de vie.
	Tactique 5.2 Participer à la mise à jour du glossaire de données et de l'ontologie de l'Université.	**Tactique 5.2.1** Ajouter les définitions des variables clés des données au glossaire des données. **Tactique 5.2.2** Ajouter les expressions et leur définition à l'ontologie de l'Université.
	RÉSULTATS • Assurer une compréhension cohérente des données afin qu'elles soient utilisées de manière appropriée. • Minimiser tout risque de malentendu sur les données et leur signification. • Augmenter la confiance dans les données pour l'ensemble des parties prenantes.	

<table>
<tr><td>✓
QUALITÉ DES DONNÉES</td><td colspan="2">CONDITIONS FAVORABLES
Outils techniques
Compétences techniques</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="2">PRINCIPES CLÉS

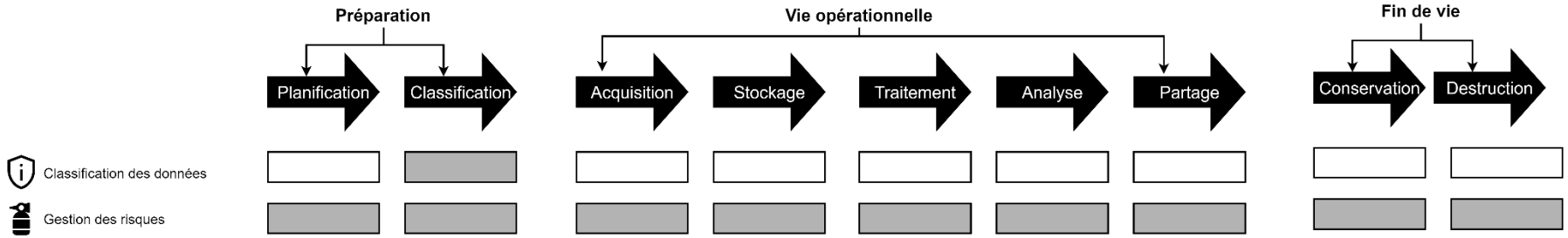
Principe 1
Principe 2
Principe 3
Principe 4</td><td>FONDAMENTALE</td><td>OPÉRATIONNELLE</td></tr>
<tr><td>Tactique 6.1
Définir et documenter les standards et les normes de qualité appropriées, applicables à divers ensembles de données utilisés au sein de votre unité ou de votre partenariat.</td><td>Tactique 6.1.1
Déterminer et documenter les standards et les normes de qualité des données les plus appropriées pour le cas d’utilisation en question.

Tactique 6.1.2
Évaluer et vérifier que les données du cas d’utilisation répondent aux exigences de qualité et partagez les résultats de l’évaluation avec les parties prenantes concernées.</td></tr>
<tr><td></td><td colspan="2">RÉSULTATS
S’assurer que les données sont utiles pour les fins déterminées.
Augmenter la confiance dans les données pour l’ensemble des parties prenantes.</td></tr>
</table>

<table>
<tr><td> 
INTEROPÉRABILITÉ DES DONNÉES</td><td colspan="2">CONDITIONS FAVORABLES
• Outils techniques
• Compétences et formation
• Supervision et vision stratégiques
• Plan de communication</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="4">PRINCIPES CLÉS

Principe 1
Principe 2
Principe 3</td><td>FONDAMENTALE</td><td>OPÉRATIONNELLE</td></tr>
<tr><td>Tactique 7.1
Adopter des conventions de nommage cohérentes pour les variables des jeux de données dont vous êtes responsables.</td><td>Tactique 7.1.1
Nommer vos variables de données avec les identifiants uniques et les codes standard identifiés aux tactiques 6.1.1 et 6.1.2</td></tr>
<tr><td>Tactique 7.2
Décrire comment les données structurées doivent être organisées dans un format ordonné.</td><td>Tactique 7.2.1
Suivre les étapes nécessaires pour transformer, corriger et formater vos données selon les normes définies.</td></tr>
<tr><td>Tactique 7.3
Privilégier les données ouvertes comme intrant et extrant des systèmes d’information.</td><td></td></tr>
<tr><td colspan="2">RÉSULTATS
• S’assurer que vos données sont prêtes à être utilisées.
• Soutenir l’intégration, l’interopérabilité et la portabilité des données.
• Combiner et croiser les données.
• Assurer une compréhension cohérente des données afin qu’elles soient utilisées de manière appropriée.</td></tr>
</table>

CLASSIFICATION DES DONNÉES	GESTION DES RISQUES
Ce thème vous aide à identifier les types de données en votre possession, ainsi que leur niveau de sensibilité.	Ce thème vous aide à identifier les risques associés aux différents types de données.



CLASSIFICATION DES DONNÉES	**CONDITIONS FAVORABLES** • Compétences et formation • Expertise légale • Culture des données claire et partagée	
PRINCIPES CLÉS **Principe 1** **Principe 2**	**FONDAMENTALE**	**OPÉRATIONNELLE**
	Tactique 8.1 Appliquer les lignes directrices de classification de la sécurité de l'information de l'Université de Montréal.	**Tactique 8.1.1** Conformément aux lignes directrices (voir tactique 8.1) classer les données que vous envisagez d'utiliser en fonction du niveau de sensibilité, d'ouverture et d'autres catégories d'intérêt.
	Tactique 8.2 Documenter et assurer le suivi des modifications et des amendements aux exigences légales affectant la classification des données tout au long du cycle de vie.	**Tactique 8.2.1** S'assurer de bien répondre à toutes les exigences de conformité (à la loi, aux tactiques de ce cadre, et à toutes autres conditions d'usages et d'accès) pour les données, le cas échéant.
	RÉSULTATS • Améliorer vos processus de gestion des risques et de sécurité des données. • Identifier les types de données détenues par votre unité ou votre partenariat et qui peut y avoir accès. • Assurer la conformité légale de votre gestion des données.	

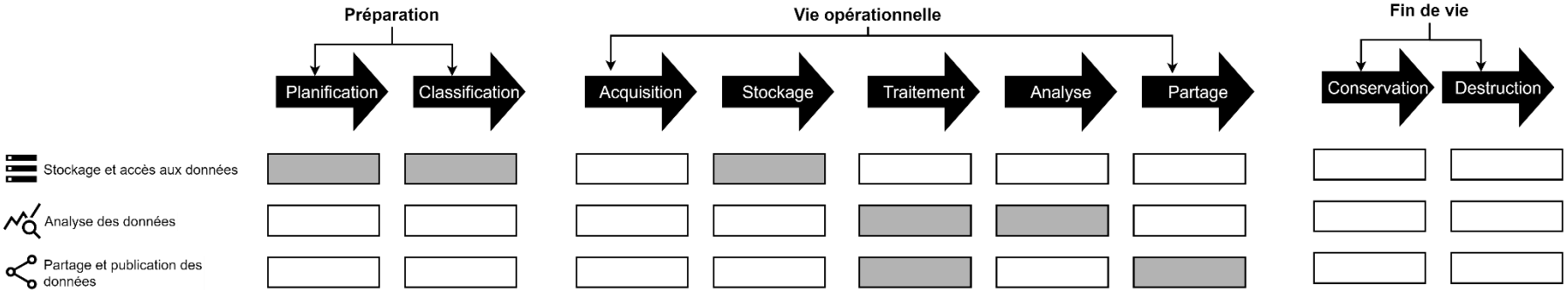
<table>
<tr><td> 
GESTION DES RISQUES</td><td colspan="2">CONDITIONS FAVORABLES
Compétences et formation
Expertise légale
Culture des données claire et partagée</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="3">PRINCIPES CLÉS

Principe 1
Principe 2</td><td>FONDAMENTALE</td><td>OPÉRATIONNELLE</td></tr>
<tr><td>Tactique 9.1
Élaborer des lignes directrices sur 1) la manière d’évaluer les risques qui pourraient nuire aux données et aux systèmes d’informations et 2) la manière d’atténuer ces risques de manière proactive.</td><td>Tactique 9.1.1
Identifier les risques pour le cas d’utilisation des données.

Tactique 9.1.2
Réaliser une évaluation des facteurs relatifs à la vie privée avant de prendre des décisions concernant la collecte ou le partage de données personnelles ou sensibles.

Tactique 9.1.3
Si possible, mettre en place des stratégies appropriées tout au long du cycle de vie des données pour atténuer les risques identifiés et, dans le cas contraire, réévaluer la stratégie de votre cas d’utilisation.</td></tr>
<tr><td>Tactique 9.2
Appliquer les directives de l’Université de Montréal relatives aux incidents de confidentialité et de sécurité des données.</td><td></td></tr>
<tr><td colspan="2">RÉSULTATS
Comprendre les risques associés à l’utilisation des données et atténuer les préjudices potentiels.
Gérer efficacement les incidents de confidentialité et de sécurité des données.</td></tr>
</table>

STOCKAGE ET ACCÈS AUX DONNÉES	ANALYSE DES DONNÉES	PARTAGE ET PUBLICATION DES DONNÉES
Ce thème garantit que les données sont stockées et accessibles de manière sécuritaire et responsable tout en réduisant les coûts environnementaux du stockage des données.	Ce thème soutient la découverte d'informations utiles comme moyen d'atteindre les objectifs fixés par chaque cas d'utilisation.	Ce thème vise à favoriser la circulation transparente d'informations pour la communauté universitaire et le grand public ainsi que les possibilités de collaboration permettant de mobiliser davantage les données pour le bien commun, dans le respect des droits fondamentaux collectifs et individuels à l'ère numérique.



STOCKAGE ET ACCÈS AUX DONNÉES	**CONDITIONS FAVORABLES** • Compétences techniques • Outils techniques • Culture des données claires et partagées	
PRINCIPES CLÉS **Principe 1** **Principe 2**	**FONDAMENTALE**	**OPÉRATIONNELLE**
	Tactique 10.1 Établir une stratégie qui aligne les besoins de stockage des données avec des dispositions de mécanismes d'accès fonctionnels et contrôlés.	**Tactique 10.1.1** Définir des conditions claires d'accès aux données pour toutes les parties prenantes et les tiers. **Tactique 10.1.2** Attribuer des autorisations ou des privilèges par rôle et configurez l'accès de manière à minimiser le besoin de copies inutiles d'un même ensemble de données.
	Tactique 10.2 Intégrer une liste de contrôle d'accès comme fonctionnalité à votre solution technologique.	
	Tactique 10.3 Établir une politique de conservation des données complète et adaptée à vos besoins.	**Tactique 10.3.1** Adopter des pratiques limitant le stockage. Vous ne devriez pas conserver les données plus longtemps que ce qu'il est nécessaire pour répondre aux fins prévues [qui sont légitimes et explicites]. Pour les données dont le potentiel de réutilisation est reconnu (se référer à la tactique 13.1.1). **Tactique 10.3.2** Intégrer vos données dans les règles de gestion des documents, en tenant compte des étapes de classification, de gestion des risques et de collecte des données.
	Tactique 10.4 Élaborez un plan d'intervention et de continuité des activités du système d'information en cas de violation potentielle des données ou des systèmes informatiques.	**Tactique 10.4.1** Prévoir des sauvegardes de données pour vous assurer de pouvoir les récupérer en cas de panne du système informatique. **Tactique 10.4.2** Prendre des mesures raisonnables pour minimiser le risque de préjudice causé par une violation de données et pour empêcher que des incidents similaires se reproduisent. **Tactique 10.4.3**

		Enregistrer les violations de données dans le registre des incidents (voir la tactique 9.2) et informer toutes les parties prenantes concernées d'un incident.
	Tactique 10.5  S'assurer que les tiers qui soutiennent vos besoins en matière de stockage, d'archivage et de destruction respectent les exigences énoncées dans les accords de niveau de service.	
	RÉSULTATS • Assurer que les données sont disponibles pour un accès futur (et décourager la création de copies). • Protéger les données contre les accès non autorisés et atténuer les risques comme les fuites de données, les pertes de données ou les pannes de système. • Minimiser la consommation énergétique de votre stockage de données en gardant votre base de données propre et facilement repérable.	

ANALYSE DES DONNÉES	**CONDITIONS FAVORABLES** • Compétences techniques • Supervision et vision stratégique	• Remise en question et apprentissage

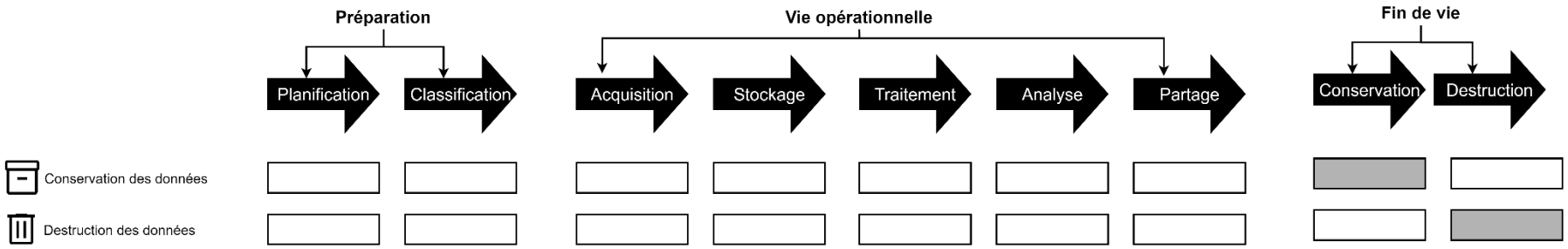
PRINCIPES CLÉS	**FONDAMENTALE**	**OPÉRATIONNELLE**
Principe 1 Principe 2	**Tactique 11.1** Documenter les différents types d'analyse de données utilisés au sein de votre **unité** ou de votre partenariat, à l'interne ou à l'aide d'un tiers. Précisez les exigences du cas d'utilisation à remplir lors de la réalisation des analyses (p.ex. documentation des traitements et des analyses effectués, reproductibilité, audits, engagement des parties prenantes) et les limites de chaque type d'analyse.	**Tactique 11.1.1** Déterminer les techniques d'analyse appropriées pour votre cas d'utilisation. **Tactique 11.1.2** Documenter les aspects pertinents du processus d'analyse de votre cas d'utilisation pour permettre la reproductibilité et les audits. **Tactique 11.1.3** Avant la publication et en règle générale, obtenir une boucle de rétroaction sur votre processus d'analyse de votre cas d'utilisation et vos résultats en présentant les analyses et leurs conclusions de manière claire et exploitable à l'ensemble des parties prenantes concernées. **Tactique 11.1.4** Exiger du tiers qui analysera les données en votre nom de signer un accord de confidentialité et un accord de niveau de service avec des conditions de service définies, notamment en demandant une transparence totale concernant le processus d'analyse. Prendre des dispositions pour vous assurer de pouvoir vérifier l'analyse et le bien-fondé des conclusions, avant de vous appuyer sur celles-ci.
	RÉSULTATS • Assurer que les personnes peuvent examiner minutieusement les résultats des algorithmes ou des calculs et comprendre la logique et le raisonnement qui sous-tendent les décisions relatives aux données qui les concernent. • Améliorer votre analyse des données en vous appuyant sur les perspectives et les connaissances de toutes les parties prenantes. • Responsabiliser les fournisseurs tiers qui analysent les données pour vous. • Permettre la reproductibilité et les audits des processus analytiques.	

PARTAGE ET PUBLICATION DES DONNÉES	**CONDITIONS FAVORABLES** • Compétences techniques • Outils et techniques • Culture des données claire et partagée	
PRINCIPES CLÉS **Principe 1** **Principe 2**	**FONDAMENTALE**	**OPÉRATIONNELLE**
	Tactique 12.1 Se référer à la tactique **4.2** (politique de confidentialité des données) qui consigne également les règles à suivre pour protéger les renseignements personnels et sensibles lors de l'étape du partage et de la publication.	**Tactique 12.1.1** Appliquer la tactique **8.2.1** avant de partager vos données. **Tactique 12.1.2** Appliquer la tactique **9.1.2** avant de partager vos renseignements personnels et sensibles; puis s'assurer de ne pas partager des données qui pourraient générer des préjudices individuels ou publics (au-delà des éventuelles mesures de protection de la vie privée). **Tactique 12.1.3** Avant de publier ou de partager des données, déterminer les techniques appropriées pour protéger les données et minimiser les risques de réidentification. **Tactique 12.1.4** Si vous divulguez des informations personnelles, vous devez d'abord conclure une entente de partage des données avec la personne, l'organisation ou le partenariat à qui elles sont divulguées, stipulant clairement les conditions d'utilisation et d'accès aux données. **Tactique 12.1.5** Lorsqu'applicable, les données autochtones doivent être retournées, en utilisant les formats appropriés, aux communautés autochtones concernées. Les personnes doivent également pouvoir demander et obtenir l'accès à leurs renseignements personnels.
		Tactique 12.2.1 Appliquer les énoncés d'orientation pour les données ouvertes du Gouvernement du Québec.
	RÉSULTATS	

	• Assurer la conformité légale dans la divulgation de données sensibles ou personnelles. • Protéger les droits fondamentaux à l'ère numérique, comme le consentement et le droit à la vie privée. • Être transparent quant aux attentes et obligations et assurer une bonne relation entre partenaires. • Garantir que les personnes ou les groupes concernés par des données personnelles conservent un niveau d'accès, de contrôle et de propriété sur les ensembles de données qui les concernent directement.

CONSERVATION DES DONNÉS	DESTRUCTION DES DONNÉES

Les deux thèmes suivants vous aident à gérer la fin du cycle de vie des données, en reconnaissant que les données sous-utilisées qui ont encore de la valeur doivent être stockées de manière plus sécuritaire, intentionnelle et durable, tandis que d'autres données doivent être détruites pour des raisons éthiques, juridiques ou opérationnelles.



<table>
<tr><td> 
CONSERVATION DES DONNÉES</td><td colspan="2">CONDITIONS FAVORABLES
• Supervision et vision stratégique
• Outils et techniques
• Expertise légale</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="3">PRINCIPES CLÉS

Principe 1
Principe 2</td><td>FONDAMENTALE</td><td>OPÉRATIONNELLE</td></tr>
<tr><td>Tactique 13.1
En complément des tactiques 10.3 et 8.1, développer et documenter un processus d’archivage décrivant les étapes nécessaires à la conservation des données.</td><td rowspan="2">Tactique 13.1.1
En suivant les directives de conservation des données, surveiller l’activité sur votre jeu de données et sa pertinence pour des cas d’utilisation futurs afin de déterminer s’il doit être archivé.</td></tr>
<tr><td>Tactique 13.2
En complément des tactiques 10.1 et 10.3, s’assurer que les données peuvent être extraites des archives au besoin et déterminez qui peut accéder aux données archivées.</td></tr>
<tr><td></td><td colspan="2">RÉSULTATS
• Conserver des données qui détiennent un potentiel de réutilisation significatif tout en respectant un budget de stockage raisonnable.</td></tr>
</table>

<table>
<tr><td> 
DESTRUCTION DES DONNÉES</td><td colspan="2">CONDITIONS FAVORABLES
Expertise légale
Outils et techniques</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="3">PRINCIPES CLÉS

Principe 1
Principe 2</td><td>FONDAMENTALE</td><td>OPÉRATIONNELLE</td></tr>
<tr><td>Tactique 14.1
En complément des tactiques 10.3 et 8.1, développer et documenter un processus de destruction décrivant les étapes nécessaires à la destruction des données.</td><td>Tactique 14.1.1
Le cas échéant, fixez un rappel pour la destruction des données en fonction de des règles de gestion des documents.

Tactique 14.1.2
S’assurer de la destruction irrécupérable de toutes les copies d’un jeu de données qui doit être détruit.</td></tr>
<tr><td colspan="2">RÉSULTATS
Minimiser la consommation énergétique de votre stockage de données en gardant votre base de données propre.
Respecter les conditions de conservation, le cas échéant, associées à vos données.
Protéger le droit à la vie privée.</td></tr>
</table>

Informations complémentaires

	PRÉCISIONS	LE SAVIEZ-VOUS ?	RESSOURCES UTILES
DÉFINITION DES CAS D'UTILISATION		En comparant les données avec les autos, on peut mieux comprendre certains points clés : conduire ne consiste pas seulement à éviter d'avoir des contraventions, et gouverner des données va au-delà de la conformité légale, pour aussi faire des données vos alliées dans l'atteinte de vos objectifs. La vision stratégique en gouvernance des données est aussi importante qu'un GPS indiquant la direction. Le responsable de la gouvernance des données est à la conduite, mais doit prendre en compte d'autres parties prenantes (comme un conducteur fait attention aux piétons, vélos, bus ...). Il est aussi intéressant de soulever les enjeux d'une société basée sur l'auto, que sur les données, et négocier ce que le bien commun signifie. L'objectif et le processus sont au moins aussi importants que les données. Par exemple, les données désagrégées sont essentielles à l'approche intersectorielle ADS+, mais peuvent aussi renforcer la stigmatisation des communautés si elles ne sont pas accompagnées d'un « processus dont l'objectif est de réduire le racisme et l'oppression systémiques et d'établir l'équité. » - Bureau du Commissaire des droits de la personne en Colombie-Britannique. (2020). *Collecte de données démographiques désagrégées en Colombie-Britannique : La perspective grand-mère*. https://bchumanrights.ca/wp-content/uploads/DD_Report_2020_French_FINAL.pdf	Consulter le site dédié à la protection des renseignements personnels de l'Université de Montréal pour en savoir plus, à https://vie-privee.umontreal.ca/accueil/
	(Tactique 1.1.3) Le modèle de capacité d'affaires, développé par l'équipe d'architecture, aide à démontrer comment un cas d'utilisation des données supporte la mission de l'Université.	Une capacité est une aptitude à faire quelque chose. Une capacité d'affaires est une capacité qu'une organisation possède pour atteindre un objectif. Un cas d'utilisation des données, pour qu'il soit utile à une organisation, doit pouvoir être lié à une capacité d'affaires.	TOGAF publie un guide sur le modèle de capacité d'affaires. https://pubs.opengroup.org/togaf-standard/business-architecture/business-capabilities.html
	(Tactique 1.1.5) Lorsque l'intelligence artificielle participe à un processus de prise de décision automatisée, le principe de responsabilité de la	Le principe de responsabilité stipule que « Dans tous les domaines où une décision qui affecte la vie, la qualité de la vie ou la réputation d'une personne doit être prise, la	La Déclaration de Montréal pour un développement responsable de l'intelligence artificielle énonce un ensemble de principes qui guident votre réflexion.

	Déclaration de Montréal pour un développement responsable de l'intelligence artificielle devrait s'appliquer.	décision finale devrait revenir à un être humain et cette décision devrait être libre et éclairée ». Dilhac, M.-A., Abrassart, C., & Voarino, N. (2018). *La Déclaration de Montréal IA responsable* (R. A. Normand & F. Girard, Trad.). Université de Montréal. https://declarationmontreal-iaresponsable.com/la-declaration/	
 **IMPLICATION DES PARTIES PRENANTES**	**(Tactique 2.1)** La diffusion de nos politiques et pratiques pertinentes en gouvernance des données inclut la publication des coordonnées de la personne responsable des pratiques en matière de confidentialité des renseignements, ainsi que des informations sur la manière dont une personne ou un groupe peut accéder à ses données personnelles. Plus largement, cette exigence légale est une occasion de soutenir l'engagement des parties prenantes sur la gouvernance et l'utilisation des données. **(Tactique 2.2)** La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels exige que les organisations mettent en place un processus de traitement des plaintes et répondent à une demande d'accès ou de rectification par la personne concernée dans un délai de 20 jours. (RLRQ, c A-2.1, art 98| Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. (s.d.). CanLII. https://www.canlii.org/fr/qc/legis/lois/rlrq-c-a-2.1/derniere/rlrq-c-a-2.1.html#art98) **(Tactique 2.2.1)** Les étapes pour traiter les plaintes liées aux questions de confidentialité des données personnelles peuvent inclure d'enregistrer et d'examiner la plainte, d'effectuer les changements ou corrections nécessaires et d'aviser la personne ayant déposé la plainte de sa résolution.	Votre équipe et vos partenaires profiteront aussi d'une documentation claire de la gouvernance des données. Ce guide de l'OBVIA présente 7 enjeux d'utilisation des technologies sur des populations marginalisées: exacerbations des inégalités préexistantes; stigmatisation avec la collecte de grandes quantités de données potentiellement sensibles; enjeu pour les personnes allophones; exclusion des populations; exclusion indirecte des populations; enjeu de confiance et d'acceptabilité sociale; enjeu de qualité et d'intégrité des données. D'où l'importance de « consulter les populations concernées et les organismes qui les représentent afin de déterminer les besoins et priorités » ainsi que de la « participation des acteurs et des groupes concernés au processus d'analyse et d'interprétation des données ». - *Petit guide sur les angles morts des réponses technologiques à la pandémie de COVID-19*. (s. d.). International Observatory on the Societal Impacts of AI and Digital Technology. https://observatoire-ia.ulaval.ca/petit-guide-angles-morts-covid/	Charte canadienne du numérique.- Canada, G. du. (2023, mars 13). *Charte canadienne du numérique* [Pages de renvoi]. Innovation, Sciences et Développement économique Canada. https://ised-isde.canada.ca/site/innover-meilleur-canada/fr/charte-canadienne-numerique-confiance-dans-monde-numerique Ressource pour commencer avec les règles pour l'accessibilité des contenus Web (WCAG) (NB la publication du standard WCAG 2.2 est prévue pour 2023). - Initiative (WAI), W. W. A. (2023). *What's New in WCAG 2.2 Draft*. Web Accessibility Initiative (WAI). https://www.w3.org/WAI/standards-guidelines/wcag/new-in-22/ Procédure de Gestion des Incidents de confidentialité (Université de Montréal. (2022). *Procédure de Gestion des Incidents de confidentialité*. https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/Renseignements_personnels/Procedure_incidents_confidentialite_final.pdf)

	PRÉCISIONS	LE SAVIEZ-VOUS ?	RESSOURCES UTILES
VEILLE DES DONNÉES EXISTEN-TES	**(Tactique 3.1)** Les mises à jour du catalogue des données doivent être intégrées dans le flux de travail. **(Tactique 3.1)** Le catalogue de données peut également contenir des liens vers des sources de données externes qui pourraient présenter un intérêt futur, mais qui ne sont pas encore en votre possession.	Pour que le catalogue des données soit utile et utilisé, pensez à intégrer dans vos habitudes de travail des mises à jour régulières. Le catalogue permet de repérer tant les données internes, qu'ouvertes et partagées (Gagnon-Turcotte, S., Sculthorp, M., & Coutts, S. (2021). *Les partenariats de données numériques : Mettre les bases d'une gouvernance de données collaborative dans l'intérêt du public,* Nord Ouvert. p.46), même si elles ne sont pas accessibles à tous. La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (anciennement le projet de loi 64) met à jour une vingtaine de lois provinciales, dont principalement la Loi sur la protection des renseignements personnels dans le secteur privé, ainsi que la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. La sobriété numérique et le respect du droit à la vie privée invitent à la minimisation de la collecte des données. Cette dernière est facilitée par une veille des données existantes. Pourtant, la tendance est plutôt à la prolifération du numérique, qui induit une augmentation de 9% de la consommation d'énergie. Cela est dû à 55% par son utilisation et à 45% pour sa production. (The Shift Project. (2020). *Déployer la sobriété numérique*. The Shift Project. https://theshiftproject.org/wp-content/uploads/2020/10/Deployer-la-sobriete-numerique_Rapport-complet_ShiftProject.pdf).	OpenDataFrance publie un guide sur les données ouvertes qui inclut une section importante sur les aspects environnementaux. (OpenDataFrance. (2022). *Greendata. Pour un impact maitrise des données*. https://opendatafrance.fr/. https://opendatafrance.gitbook.io/greendata-pour-un-impact-maitrise-des-donnees/greendata/preface-et-remerciements)

 **ACQUISITION DES DONNÉES**	**(Tactique 4.1.2)** Une approche ADS+ nécessite souvent d'obtenir des données personnelles ventilées par rapport à un sous-groupe en particulier (p.ex. une communauté immigrante). L'existence même de ces données est un risque pour cette communauté, qui est la mieux placée pour décider si ce risque vaut la peine d'être pris ou non.	Le rapport The Limits to Digital Consent (en anglais) partage 6 découvertes quant aux limites du consentement, notamment que le modèle actuel est dépassé, qu'il combine un fort potentiel de nuisance avec l'indifférence des décisionnaires, que tout le monde est en danger, que le stockage local des données n'est pas plus sûr pour les personnes et que les concepteurs de plateformes auraient intérêt à se considérer comme de potentiels mauvais acteurs.- Diehm, C., Smith, K., Elliott, A., & Bullen, G. (2021). *The Limits to Digital Consent : Understanding the risks of ethical consent and data collection for underrepresented communities* (v. 1). Simply Secure, The New Design Congress. https://simplysecure.org/resources/The_Limits_to_Digital_Consent_FINAL_Oct2021.pdf « Le statut d'emploi et le revenu, par exemple, prédiraient l'intensité d'usage des technologies, mais aussi des traces d'activités en ligne. » Cela mène à une sous-représentation. (*Petit guide sur les angles morts des réponses technologiques à la pandémie de COVID-19*. (s. d.). International Observatory on the Societal Impacts of AI and Digital Technology. P.11 https://observatoire-ia.ulaval.ca/petit-guide-angles-morts-covid/) Selon la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, le consentement doit répondre aux 5 critères suivants: manifeste, libre, éclairé, donné à des fins spécifiques, et d'une durée nécessaire à la réalisation des fins auxquelles il a été demandé. (*Critères de validité d'un consentement*. (s. d.). Gouvernement du Québec. https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/consentement/validite-dun-consentement) Les données ouvertes peuvent être une source de données intéressantes pour certains cas d'utilisation.	Ce guide du RGPD pour développeur donne notamment des indications pour minimiser la collecte de renseignements personnels. (CNIL. (s. d.). *Guide RGPD pour l'équipe de développement* [Github]. https://lincnil.github.io/Guide-RGPD-du-developpeur/#Fiche_n%C2%B07%C2%A0:_Minimiser_les_donn%C3%A9es_collect%C3%A9es) Le site Équité, diversité et inclusion de l'Université de Montréal énonce des actions qui sont soutenues par une utilisation responsable des données. (*Équité, diversité et inclusion—Université de Montréal*. (s. d.). https://www.umontreal.ca/diversite/) Deux guides qui contiennent des ressources intéressantes : Le Open Data Handbook, https://opendatahandbook.org/guide/fr/what-is-open-data/ et https://opendatafrance.gitbook.io/kit-de-ressources-odf/ de OpenDataFrance.

	PRÉCISIONS	LE SAVIEZ-VOUS ?	RESSOURCES UTILES
COMPRÉHENSION ET DOCUMENTATION DU CONTEXTE DES DONNÉES	**(Tactique 5.1)** Certains éléments standard que l'on trouve dans les métadonnées comprennent : l'origine, l'emplacement, les définitions des variables de données, les personnes qui ont participé à son cycle de vie, les choix qui ont été faits dans le traitement et l'analyse, la façon de citer le jeu de données, etc.) (source) **(Tactique 5.1.2)** Compléter et tenir à jour la Fiche de cas d'utilisation des données permet de documenter les décisions prises pendant tout le cycle de vie des données. **(Tactique 5.2.1)** Ajouter les définitions des variables clés des données au glossaire des données, c'est-à-dire uniquement celles qui sont significatives ou utiles pour vous et vos partenaires. Habituellement, elles servent à l'intelligence d'affaires ou pour les rapports.	Le but d'un glossaire des données est d'améliorer la compréhension et l'utilisation des données à travers votre unité. Il devrait donc être unique. À ne pas confondre avec les dictionnaires de données, plus techniques et dépendants des systèmes d'information. (Askham, N. (2016, mai 1). Ask the Data Governance Coach : What is a Data Glossary? *TDAN.Com*. https://tdan.com/ask-the-data-governance-coach-what-is-a-data-glossary/19752) Les variables des données sont parfois aussi appelées métadonnées, champs, nom de la colonne ou de la ligne, selon le logiciel utilisé.	Fiche de cas d'utilisation des données.
QUALITÉ DES DONNÉES	**(Tactique 6.1)** Il existe de nombreux standards et normes de qualité des données. Elles constituent de bons points de départ.	Selon l'article du Harvard Business Review "Only 3% of Companies' Data Meets Basic Quality Standards" publié en 2017, en moyenne, 47 % des données nouvellement créés comportent au moins une erreur critique (p. ex., une erreur ayant une incidence sur le travail). (Nagle, T., Redman, T. C., & Sammon, D. (2017, septembre 11). Only 3% of Companies' Data Meets Basic Quality Standards. *Harvard Business Review*. https://hbr.org/2017/09/only-3-of-companies-data-meets-basic-quality-standards) La confiance envers les données est perçue par les utilisateurs lorsque le producteur applique des normes, des standards et publie les exigences de qualité s'appliquant aux données.	Statistique Canada définit 6 dimensions principales de la qualité des données : pertinence, exactitude, actualité, intelligibilité, cohérence et accessibilité (Statistiques Canada (Réalisateur). (2020, septembre 23). *Qualité des données en six dimensions* [Vidéo]. https://www.statcan.gc.ca/fr/afc/litteratie-donnees/catalogue/892000062020001). Voir aussi la trousse sur la qualité des données (Statistiques Canada. (2017, septembre 27). *Trousse de la qualité des données*. Statistiques Canada. https://www.statcan.gc.ca/fr/trousse-qualite-donnees)
INTEROPÉRABILITÉ DES DONNÉES	**(Tactiques 7.1.1 et 7.2.1)** Si un jeu de données existant n'est pas correctement standardisé, faire une notification pour la(les) personne(s) responsable(s) du jeu de données des changements requis.	La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* exigera, dès septembre 2024, que si une personne en fait la demande, les organisations soient tenues de communiquer les renseignements personnels informatisés recueillis auprès de cette personne dans un format technologique structuré et communément utilisé. (source) Selon le SRIDAIL, « Un organisme public doit privilégier des formats adaptés aux renseignements demandés, ouverts et interopérables. De manière générale, des formats ouverts	Les principes FAIR peuvent vous aider dans l'atteinte des objectifs d'interopérabilités des données.(Statistiques Canada (Réalisateur). (2022, mai 24). *Principes des données FAIR : Qu'entend-on par FAIR?* [Vidéo]. https://www.statcan.gc.ca/fr/afc/litteratie-donnees/catalogue/892000062022002) Gouvernement du Québec. (2023). Droit à la portabilité. (Gouvernement du Québec. (2023, juin 22). *Droit à la portabilité*. Gouvernement du Québec. https://www.quebec.ca/gouvernement/travailler-

		de type CSV, XML ou JSON sont adaptés à la portabilité. En revanche, un format difficile à traiter, comme une image, un PDF ou un format dont l'utilisation implique l'acquisition d'un logiciel ou d'une licence payante, n'est pas considéré comme étant un format technologique structuré et couramment utilisé. » Si vous prévoyez rendre vos données ouvertes, des mesures doivent être prises pour permettre la réutilisation.	gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/acces-aux-renseignements-personnels/titre-par-defaut) Conseil du Trésor. (2018). Énoncés d'orientation pour les données ouvertes. Gouvernement du Québec. https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/gouvernement_ouvert/orientations_donnees_ouvertes.pdf Le Open Data Handbook, https://opendatahandbook.org/guide/fr/what-is-open-data/

	PRÉCISIONS	LE SAVIEZ-VOUS ?	RESSOURCES UTILES
CLASSIFICATION DES DONNÉES	**(Tactique 8.1)**. À l'Université de Montréal, Le niveau de risque et le degré de sensibilité sont particulièrement importants pour classifier les données. D'autres classifications importantes liées à la souveraineté des données comprennent les données autochtones et les données d'intérêt général. **(Tactique 8.1.1)** Ce processus de classification doit prendre en considération les questions relatives à la souveraineté collective des données, comme la souveraineté des données par les communautés autochtones. **(Tactique 8.2)** Une attention particulière doit être accordée aux renseignements personnels ou sensibles lors de la phase de collecte, d'analyse et de divulgation. **(Tactique 8.2)** La veille du cadre législatif est une activité collective partagée par les membres du Forum des intendant[e]s.	Selon la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, un renseignement personnel est sensible lorsque, par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée. (Commission d'accès à l'information du Québec. (s. d.). *Renseignements sensibles*. https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/renseignements-sensibles/) La *Charte québécoise des droits et libertés* garantit le droit à la vie privée (Charte des droits et libertés de la personne, Pub. L. No. C-12. https://www.legisquebec.gouv.qc.ca/fr/document/lc/c-12). La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* vise à protéger les renseignements personnels (qui peuvent être publics ou privés).	Consultez les Lignes directrices en matière de protection des renseignements personnels à l'intention des membres du personnel de l'UdeM. Il est possible de traiter différemment les données dépersonnalisées et les personnelles. Cependant, le Bureau du Commissaire des droits de la personne en Colombie-Britannique recommande qu'une même attention soit portée aux données désagrégées, qu'elles soient personnelles ou dépersonnalisées (Bureau du Commissaire des droits de la personne en Colombie-Britannique. (2020). *Collecte de données démographiques désagrégées en Colombie-Britannique : La perspective grand-mère*. https://bchumanrights.ca/wp-content/uploads/DD_Report_2020_French_FINAL.pdf pages 7-8). En effet, les avancées technologiques rendront de plus en plus facile la réidentification de données. La Commission d'accès à l'information du Québec offre un espace évolutif pour en savoir plus sur la modernisation des lois sur la protection des renseignements personnels au Québec (Loi modernisant des dispositions législatives en matière de protection des renseignements personnels). NB Gardez en tête que selon votre contexte vous pourriez être

			dans l'obligation de respecter d'autres obligations légales, réglementaires ou contractuelles. - Commission d'accès à l'information du Québec. (s. d.). *Renseignements sensibles*. https://www.cai.gouv.qc.ca/espace-evolutif-modernisation-lois/thematiques/renseignements-sensibles/ Lignes directrices en matière de protection des renseignements personnels à l'intention des membres du personnel (annexe à la fin du document). Division des archives et de la gestion de l'information (DAGI). (2023). *Lignes directrices en matière de protection des renseignements personnels à l'intention des membres du personnel*. Université de Montréal. https://secretariatgeneral.umontreal.ca/public/secretariatgeneral/documents/Renseignements_personnels/lignes_directrices_PRP_final.pdf
GESTION DES RISQUES	**(Tactique 9.1.1)** Pour bien identifier les risques, assurez-vous de vous poser les questions suivantes: le cas d'utilisation pourrait-il générer de nouveaux préjudices pour les individus ou la société? Le cas d'utilisation pourrait-il bénéficier ou nuire de manière inéquitable à certaines populations par rapport à d'autres? D'autres risques courants comprennent les incidents liés à la confidentialité des données, les violations de la sécurité, l'utilisation de données erronées ou inexactes et l'agrégation ou la corrélation de jeux de données incompatibles. **(Tactique 9.1.3)** Cette tactique invite à mitiger les risques identifiés notamment dans d'autres tactiques (4.1.2, 8.2.1, 9.1.1, 9.1.2, 11.1.3, 12.1.2, 12.1.3, 12.1.4, 14.1) et aussi dans une certaine mesure (4.2.3, 6.1.2, 10.4.3, 11.1.4). À noter que d'autres tactiques consistent déjà à la mise en place de la mitigation (10.1.1, 10.4.1, 10.4.2).	Une évaluation des facteurs relatifs à la vie privée évalue l'impact qu'un projet, initiative ou politique pourraient avoir sur la vie privée des personnes ; soit lors de la planification, soit au moment d'envisager un changement important. Cela permet de communiquer efficacement les risques pour la vie privée aux parties prenantes et notamment aux décisionnaires, ainsi que de formuler des recommandations. Ainsi, cette évaluation vise une prise de décision éclairée pour respecter le droit à la vie privée.	L'UdeM met à votre disposition un outil pour évaluer les facteurs relatifs à la vie privée (Université de Montréal. (n.d.). *Évaluer les facteurs relatifs à la vie privée (ÉFVP)*. Vie privée - Université de Montréal, https://vie-privee.umontreal.ca/evaluer-les-facteurs-relatifs-a-la-vie-privee-efvp/) Ressources en cybersécurité de l'Université de Montréal (*Cybersécurité*. (n.d.). Technologies de l'information - Université de Montréal, https://ti.umontreal.ca/cybersecurite/)

	PRÉCISIONS	LE SAVIEZ-VOUS ?	RESSOURCES UTILES
STOCKAGE ET ACCÈS AUX DONNÉES	**(Tactique 10.1)** Cette stratégie devrait inclure un protocole pour configurer l'accès aux jeux de données, en tenant compte du rôle de l'utilisateur et du type de données. **(Tactique 10.1.2)** Sans être une règle systématique, vous pouvez suivre le principe du moindre privilège, c'est-à-dire qu'un utilisateur doit recevoir le niveau d'accès minimal nécessaire pour effectuer une tâche ou un travail. **(Tactique 10.3)** Cette politique de conservation des données doit établir dans un langage simple des règles de gestion des documents qui identifie les durées minimale et maximale de conservation et de retrait des données à des fins juridiques et opérationnelles. Elle couvre donc l'archivage et la destruction des données. **(Tactique 10.3.2)** Cette tactique prévoit l'intégration des règles de gestion des données. Pour ce faire, il est important de prendre en considération les étapes de classification, de gestion des risques et de collecte des données. **(Tactique 10.5)** Le plan de continuité du système d'information planifie notamment pour la sauvegarde (redondance) des données et la reprise après un incident.	Les durées de conservation des données seront définies dans les règles de gestion maintenues par la DAGI. Même si la cause principale d'une violation de données précise peut être variée (p. ex. vol opportuniste, piratage ciblé, inattention d'un[e] employé[e]), toute organisation peut réduire les causes sous-jacentes (p. ex. capacités et attention du personnel, adéquation des mesures de protection, règles d'accès, quantité et sensibilité des données détenues, gouvernance et suivi). (Organisation For Economic Co-operation And Development. (2013). *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf) L'établissement de consignes concernant des mots de passe robustes, des mises à jour régulières, etc. sont autant de mesures raisonnables permettant de minimiser le risque de préjudice causé par une violation de données. Les sauvegardes de données sont utiles en cas « de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques ». (Assistance et prévention du risque numérique au service des publics. (2019, novembre 13). *Pourquoi et comment bien gérer ses sauvegardes ?* [Cybermalveillance.gouv.fr]. Assistance aux victimes de cyber malveillance. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes) Notez que les mêmes lois de protection des données s'appliquent aux données originales et à leur(s) copie(s). Le nombre d'auteurs de cybermenace est en hausse et ceux-ci deviennent de plus en plus sophistiqués.	S'assurer que seules les personnes autorisées peuvent accéder aux données fait partie du modèle des « Cinq éléments de sécurité » (Five Safes), reconnu au niveau international : Données sécuritaires, Projets sécuritaires, Personnes fiables, Installations sécuritaires, Produits sécuritaires. (Petitgand, C. (2022, août 5). Le modèle des Cinq éléments de sécurité pour guider l'accès aux données sensibles. *Data Lama*. https://datalama.ca/le-modele-des-cinq-elements-de-securite-pour-guider-lacces-aux-donnees-sensibles/) Cet article Wikipédia présente plusieurs méthodes de déduplication des données (en anglais, point de vue technique). Data deduplication. (2023). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Data_deduplication&oldid=1164069938 En plus de l'élaboration d'un plan d'intervention, il est aussi possible d'élaborer un plan de continuité des activités. Les bénéfices de cette démarche sont listés dans cette courte présentation, accompagnée d'un guide plus complet (le cadre est plus large que la seule cybersécurité). *Faire son plan de continuité des affaires en tant qu'entreprise*. (s. d.). Gouvernement du Québec. https://www.quebec.ca/securite-situations-urgence/urgences-sinistres-risques-naturels/entreprise Selon la directive relative à la continuité des affaires (10.65), la DPS conseille et accompagne les unités.(*Plan de contingence et de continuité des affaires*. (s. d.). Direction de la prévention et de la sécurité - Université de Montréal. https://dps.umontreal.ca/gestion-des-urgences/plan-de-contingence-et-de-continuite-des-affaires/) Règles de gestion des documents de l'Université de Montréal.(*Règles de gestion*. (s. d.). Archives et gestion de l'information - Université de Montréal. https://archives.umontreal.ca/gestion-de-documents/regles-de-gestion/)

			Directive sur l'utilisation de l'infonuagique (10.54) de l'Université de Montréal.(*Utilisation de l'infonuagique*. (2022)
ANALYSE DES DONNÉES	**(Tactique 11.1)** Comme certaines décisions basées sur des analyses de données auront des conséquences concrètes dans la vie des personnes, il est crucial de pouvoir expliquer la logique et le raisonnement qui sous-tendent ces décisions. Si ce n'est pas possible, vous pouvez chercher d'autres méthodes d'analyse qui permettent un degré d'explicabilité approprié. **(Tactique 11.1.2)** Les aspects importants de l'analyse à documenter peuvent inclure, sans s'y limiter, les descriptions des données prises en compte dans l'analyse, des techniques d'analyse de leur contenu ou de leur composante quantitative (ou techniques statistiques), des algorithmes et des hypothèses d'analyse mobilisés, ainsi que des résultats. **(Tactique 11.1.4)** Pour vérifier le bien-fondé des conclusions des analyses effectuées par un tiers, vous pouvez vous assurer d'avoir les capacités à l'interne, établir un partenariat avec une organisation de confiance pour vérifier le travail, ou même créer une liste de fournisseurs de confiance vérifiés et dont la qualité d'analyse est fiable.	L'approche partenariale de la recherche a les caractéristiques suivantes : • être centrée sur les communautés ; • reposer sur un partage équitable du pouvoir décisionnel tout au long du projet avec la communauté ; • proposer un processus et des résultats utiles à la communauté. Elle permet de produire de nouvelles connaissances de manière plus robuste et d'outiller la communauté pour résoudre des enjeux sociaux pressants. (Community Based Research Canada. (s. d.). *Approach*. CBRCanada. https://www.communityresearchcanada.ca/approach , en anglais).	Concernant des analyses quantitatives : 7 étapes vers plus de transparence dans la pratique statistique (en anglais) : (1) la visualisation des données ; (2) la quantification de l'incertitude inférentielle ; (3) l'évaluation des choix de prétraitement des données ; (4) la présentation de modèles multiples ; (5) la participation de plusieurs analystes ; (6) l'interprétation modeste des résultats ; et (7) le partage des données et du code. (Les constats sont assez généraux pour être utiles en dehors des sciences sociales et comportementales.) Wagenmakers, E.-J., Sarafoglou, A., Aarts, S., Albers, C., Algermissen, J., Bahník, Š., van Dongen, N., Hoekstra, R., Moreau, D., van Ravenzwaaij, D., Sluga, A., Stanke, F., Tendeiro, J., & Aczel, B. (2021). Seven steps toward more transparency in statistical practice. *Nature Human Behaviour*, *5*(11), Article 11. https://doi.org/10.1038/s41562-021-01211-8 PRP (directive sur les tiers).
PARTAGE ET PUBLICATION DES DONNÉES	**(Tactique 12.1.1)** La décision de partager ou non un jeu de données doit également prendre en compte s'il sera utilisé à des fins compatibles à celles pour lesquelles les données ont été collectées initialement. Elle doit aussi être alignée avec le principe de la mobilisation des données pour le bien commun selon sa définition. **(Tactique 12.1.3)** Les techniques pour protéger les données personnelles et minimiser les risques de ré-identification peuvent inclure la rédaction de chiffres ou de noms commercialement sensibles, la pseudonymisation, l'anonymisation ou l'agrégation d'informations personnelles, ainsi que l'application du principe de « confidentialité programmée » pour les solutions technologiques. **(Tactique 12.1.4)** Au-delà d'assurer une protection des	Il y a deux familles de techniques pour anonymiser les données: la randomisation et la généralisation. Comment vérifier l'efficacité de l'anonymisation? En vérifiant qu'il n'est pas possible d'isoler un individu dans le jeu de données (l'individualisation); de relier entre eux des ensembles de données distincts concernant un même individu (la corrélation); ni de déduire, de façon quasi certaine, de nouvelles informations sur un individu (l'inférence). (CNIL. (2020, mai 19). *L'anonymisation de données personnelles*. https://www.cnil.fr/fr. https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles) Les fondements d'un partenariat de données numériques réussi sont la création d'un climat de confiance propice à la collaboration et le recherche d'un impact social positif dans	Ce rapport donne d'importantes recommandations pour établir des partenariats numériques. Il est pensé pour le contexte québécois, sans rentrer dans les détails de la rédaction d'un contrat de partage de données. (Les partenariats de données numériques. (Gagnon-Turcotte, S., Sculthorp, M., & Coutts, S. (2021). *Les partenariats de données numériques : Mettre les bases d'une gouvernance de données collaborative dans l'intérêt du public* (p. 106). Nord Ouvert.) Les principes de PCAP® des Premières Nations : https://fnigc.ca/fr/les-principes-de-pcap-des-premieres-nations/

	données personnelles et sensibles, les ententes de partage de données peuvent être utilisées afin que les données contenant des informations sur l'environnement ou l'environnement bâti, par exemple, soient systématiquement mobilisées pour le bien commun.	l'intérêt du public. (Gagnon-Turcotte, S., Sculthorp, M., & Coutts, S. (2021). *Les partenariats de données numériques : Mettre les bases d'une gouvernance de données collaborative dans l'intérêt du public* (p. 106). Nord Ouvert.) La redistribution des données est importante dans le contexte des données ouvertes. Assurez-vous, selon le cas, d'appliquer la licence pertinente à vos jeux de données.	CARE Principles for Indigenous Data Governance : https://www.gida-global.org/care Conseil du Trésor. (2018). Énoncés d'orientation pour les données ouvertes. Orientations en matière de gestion des ressources informationnelles (gouv.qc.ca) Conseil du Trésor. (2018). *Énoncés d'orientation pour les données ouvertes*. Gouvernement du Québec. https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/gouvernement_ouvert/orientations_donnees_ouvertes.pdf Le Open Data Handbook, https://opendatahandbook.org/guide/fr/what-is-open-data/

	PRÉCISIONS	LE SAVIEZ-VOUS ?	RESSOURCES UTILES
CONSERVATION DES DONNÉES	**(Tactique 13.1)** Pour rappel, les tactiques **8.1** et **10.3** sont mises en place pour l'ensemble de l'Université. Vous devez vous appuyer sur ces deux tactiques fondamentales, autrement dit les lignes directrices de classification de la sécurité de l'information et la politique de conservation des données, pour la conception de votre processus d'archivage des données afin de vous assurer de leur application au sein de votre unité. **(Tactique 13.2)** Il est possible que le type d'accès aux données s'élargisse une fois qu'elles sont archivées et après une période donnée. Prenez en compte cette possibilité ainsi que les tactiques **10.1** et **10.3** pour déterminer qui peut avoir accès aux données archivées et à quel moment des changements du niveau d'accès sont applicables. La conservation des données se fait sous réserve du calendrier, ainsi que des clauses contractuelles avec les parties prenantes, le cas échéant.		Consultez les Règles de gestion des documents de l'Université. (*Règles de gestion*. (s. d.). Archives et gestion de l'information - Université de Montréal. https://archives.umontreal.ca/gestion-de-documents/regles-de-gestion/) Manuel de préservation numérique de la coalition pour la préservation numérique (en français), et le guide d'utilisation du manuel (en anglais, Digital Preservation Coalition. (s. d.). *How to use the Handbook—Digital Preservation Handbook*. Digital Preservation Handbook. https://www.dpconline.org/handbook/introduction/how-to-use-the-handbook)

 DESTRUCTION DES DONNÉES	(**Tactique 14.1**) La tactique 10.3 s'applique à l'ensemble de l'Université. Vous devez vous appuyer sur la politique de conservation des données pour la conception de votre processus de destruction des données afin de vous assurer de son application au sein de votre unité. La destruction des données se fait sous réserve du calendrier, ainsi que des clauses contractuelles avec les parties prenantes, le cas échéant.		Consultez les Règles de gestion des documents de l'Université. (*Règles de gestion*. (s. d.). Archives et gestion de l'information - Université de Montréal. https://archives.umontreal.ca/gestion-de-documents/regles-de-gestion/)

Ceci est la première itération du G*uide de gestion des données* de l'Université de Montréal. Dans un esprit d'évaluation et d'amélioration en continu, ce document sera amené à évoluer. Vous pouvez contribuer à le façonner ! Veuillez nous adresser vos questions, commentaires, retours ou idées à l'adresse courriel suivante : gdo@umontreal.ca.

Quelle est la prochaine étape de votre parcours de la gouvernance des données ?

Évaluer où vous en êtes dans la mise en œuvre des tactiques avec l'outil d'auto-évaluation de la gouvernance des données.