Recueil de règles pour une économie de données équitable

Le présent recueil de règles propose des instructions et des modèles pour faciliter la construction des réseaux de données.

Préface et modèles

Le recueil de règles pour une économie de données équitable est un guide pour les créateurs de réseaux de données. Les modèles d'accords et les autres outils facilitent la construction et l'adhésion à de nouveaux réseaux de données en mettant l'accent sur la transparence dans le partage de données.

Le présent recueil de règles contient:

- des modèles d'accord pour des règles légales, économiques, techniques et administratives
- une série de questions de contrôle
- des modèles de code de conduite

Ce recueil de règles comprend deux parties: **le contenu général dans la partie 1** et **des modèles modifiables dans la partie 2** (modèles sous fichiers Word et PDF). (publié le 12 juin 2023)

Versions précédentes

La version 2.0 du recueil de règles a été publié en finnois et en anglais.

Le premier Recueil de règles pour une économie de données équitable a été publié le 30 juin 2020 (version 1.1) en anglais. Le recueil a été mise à jour le 11 janvier 2021 (1.2), le 13 août 2021 (1.3) et le 20 avril 2022 (1.4). La version 1.2 a été publié en finnois (le 18 juin 2021) et en portugais (le 30 mars 2021). La version 1.4 a été publié en finnois et en anglais le 20 avril 2022. La version 2.0 a été publié en anglais le 31 août 2022 et en finnois le 7 décembre 2022.

La version 1.2 du recueil de règles a été publié en portugais "Manual para uma Economia Equitativa de Dados" (1.2 PDF, Word) par SPMS – Services partagés du ministère des Affaires sanitaires du Portugal le 10 mars 2021 et mis à jour le 30 mars 2021.

Le groupe de travail du recueil de règles

Le modèle de Recueil de règles a été créé par le groupe de travail du Recueil de règles sous le thème de l'économie de données équitable de Sitra.

Ont activement contribué au modèle de recueil de règles : Olli Pitkänen (editeur, 1001 Lakes Oy), Sami Jokela (1001 Lakes Oy), Marko Turpeinen (1001 Lakes Oy), Viivi Lähteenoja (1001 Lakes), Jyrki Suokas (Sitra), Juhani Luoma-Kyyny (editeur, Sitra), Saara Malkamäki (Sitra), Anna Wäyrynen (Sitra et Adesso Nordics Oy), Jorma Yli-Jaakkola (Borenius Attorneys Ltd et Lexia Attorneys Ltd), Otto Lindholm (Dottir Attorneys Ltd), Jani Koskinen (Université de Turku), Jussi Mäkinen (Industries technologiques de Finlande), Kai Kuohuva (TietoEVRY Oyj, Fortum Oyj), Jutta Suksi (VTT), Jari Juhanko (Aalto University), Kari Hiekkanen (Université Aalto), Antti Kettunen (TietoEVRY Oyj), Petri Laine (Hybrida), Kari Uusitalo (Business Finland), Pekka Mäkelä (Université de Helsinki), Meri Valtiala (The Human Colossus Foundation), Anna-Mari Rusanen (Ministère des Finances), et Sari Isokorpi (Medifilm Oy).

Le modèle opérationnel de la sécurité des données a été créé sur l'initiative de Digipooli (Industries technologiques de Finlande), l'organisation de la sécurité des services, ce avec le soutien de la NESA (Agence nationale de la sécurité de l'approvisionnement). Le modèle opérationnel de la sécurité des données a été développé par les experts de 1001 Lakes Oy, Olli Pitkänen, Sami Jokela et Marko Turpeinen et par le secrétaire du pool Digipooli, Antti Nyqvist. Les membres de Digipooli ont activement pris part au travail en présentant leurs points de vue dans les ateliers de travail et en commentant le modèle.

Les images 1–7: Topias Dean, Sitra

© Sitra 2022, Creative Commons 4.0 CC-BY
Citation recommandée: Sitra (2022), Rulebook for a Fair Data Economy / Sitra (2023) Recueil de règles pour une économie de données équitable, version 2.0

Table des matières

Recueil de règles pour une économie de données équitable 1

Préface et modèles 1

Partie 1: pourquoi et comment utiliser un recueil de règles? 5

1. Introduction à la Partie 1 5

1.1 Pourquoi et quand devriez-vous utiliser un recueil de règles pour partager des données 5

1.2 Guide de démarrage rapide : Comment commencer à travailler sur un recueil de règles pour le partage des données 8

1.3 Contexte et concepts-clés 9

2. Cadre contractuel 11

2.1 Introduction 11

2.2 Prémisses 13

3. Comment décrire votre réseau de données? 15

3.1 Perspective Affaires et opérations 15

3.2 Perspective Technique et sécurité 17

4. Modèle opérationnel de la sécurité des données pour les réseaux de données 19

4.1 Généralités 19

4.2 Processus de sécurité des données 20

4.3 Priorisation et étendue 21

4.4 Prise en compte de la protection des données 22

4.5 Orientation: identification du système, des exigences légales, des menaces et vulnérabilités 23

4.6 Aperçu des menaces liées à la sécurité 24

4.7 Identifier les menaces et vulnérabilités existantes 31

4.8 Évaluation des risques 32

4.9 État cible pour le réseau de données et les parties impliquées 33

4.10 Construction, contrôle et amélioration constante du modèle opérationnel de la sécurité des données pour les réseaux de données 33

4.11 Sources utilisées pour le modèle opérationnel de la sécurité des données 36

5. Principes éthiques: Valeurs partagées du réseau de données 38

5.1 Responsabilité et vérifiabilité 40

5.2 Prévention des dommages 41

5.3 Traitement justifié des données personnelles 41

5.4 Équité, justice et égalité 41

5.5 Approche centrée sur la personne 41

5.6 Vie privée 41
5.7 Sécurité 42
5.8 Durabilité et économie circulaire 43
5.9 Transparence 43
5.10 Amélioration continue 44
5.11 Support des individus 44
5.12 Communication 44

Partie 1: pourquoi et comment utiliser un recueil de règles?

1. Introduction à la Partie 1

1.1 Pourquoi et quand devriez-vous utiliser un recueil de règles pour partager des données

Ce modèle du recueil de règles a pour objet de fournir un manuel accessible et pratique sur la manière de créer un réseau de données et d'établir des conditions générales pour les ententes de partage des données. Le présent modèle de recueil de règles aidera les organisations à former de nouveaux réseaux de données, d'adopter des recueils de règles pour ces réseaux, et de promouvoir l'économie de données équitable en général. À l'aide de ce recueil de règles, les parties peuvent créer un réseau de données basé sur la confiance mutuelle qui partage une mission, une vision et des valeurs en commun.

Le recueil de règles aide également les fournisseurs de données et les utilisateurs de données à évaluer toute exigence imposée par la loi et les contrats applicables, outre le fait qu'elles orientent à adopter des pratiques promouvant l'utilisation des données et la gestion des risques. Toutefois, en dépit du modèle du recueil de règles, il est important de noter que les parties ont encore besoin de vérifier pour eux-mêmes que toutes les législations pertinentes, en particulier aux niveaux national et infranational, ainsi que législation spécifique régissant les données en question ont été prises en considération.

Il existe de nombreux avantages pour le partage des données. Ceci peut permettre aux utilisateurs des données d'avoir accès aux données pour des fins de développement de leurs produits et services. Partager les données permet aussi aux fournisseurs de données d'améliorer leurs produits ou services et de soutenir le développement à la valeur ajoutée ou des services de tierces parties. L'existence d'écosystèmes riches qui créent de nouveaux produits et services peuvent devenir très attractifs pour les utilisateurs.

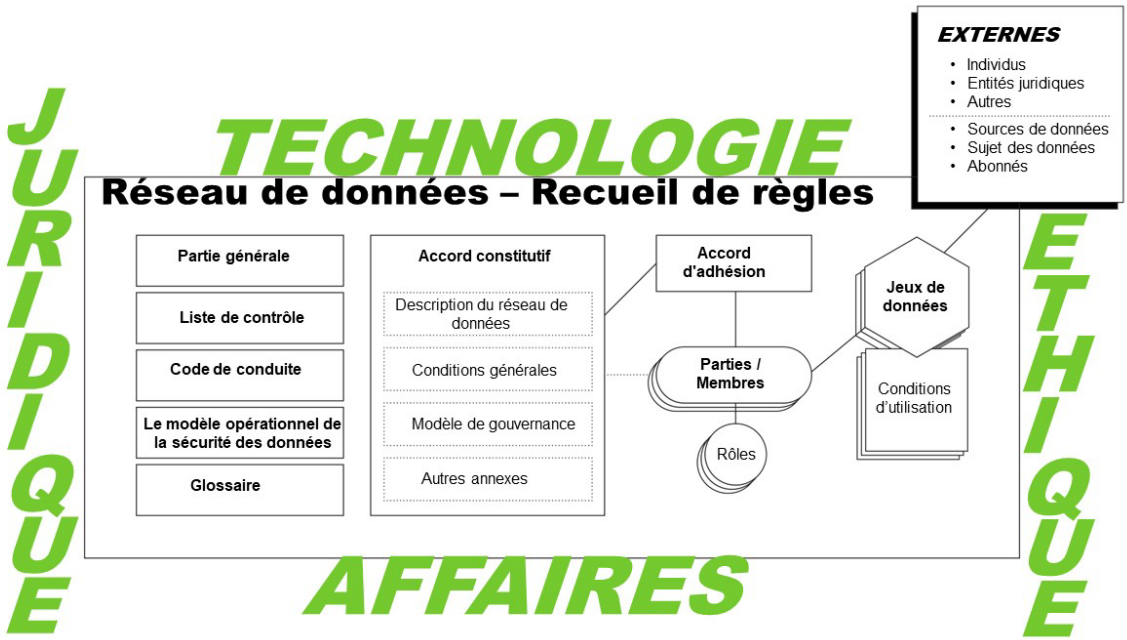
Une augmentation du nombre d'utilisateurs du service, quant à elle, encourage les développeurs et utilisateurs de nouveaux produits et services à adhérer à l'écosystème de données. Cet effet de réseau peut augmenter la valeur d'un service spécifique, voire même de la totalité de l'écosystème. En outre, partager les données peut faire baisser les coûts de collecte des données et permettre aux fournisseurs de données de combiner leurs bases de données avec des changements organisationnels minimum.

Les réseaux de données qui adoptent le modèle de recueil de règles doivent être équitables, loyaux et légitimes dans leur traitement des données. Ils doivent également être justes et impartiaux envers leurs membres, et d'assurer que les droits de tierces parties ne sont pas bafoués. Les données à caractère personnel doivent être traitées en conformité avec les réglementations européennes et les règlementations nationales en matière de protection des données applicables.

Les réseaux de données identifient et gèrent les risques associés au partage et au traitement des données tout en assurant l'exploitation de nouvelles possibilités offertes par les données. Ceci inclut également l'assurance de la conformité avec la législation sur la concurrence pertinente et que le réseau de données n'aura pas d'impact négatif sur la concurrence du marché ou sur les consommateurs. Les dispositions limitant l'accès au réseau sont particulièrement importantes à prendre en considération dans ce type d'évaluation.

Le présent Modèles de recueil de règles est publié avec la licence internationale Creative Commons Attribute 4.0 qui permet la reproduction et le partage de la documentation sous licence, ainsi que pour la production, la reproduction et le partage du matériel adapté. Les auteurs et éditeurs du Modèle de recueil de règles doivent être identifiés, et toute modification apportée au Modèle de recueil de règles doit être signalée.

L'image 1. Les relations entre les différentes parties d'un recueil de règles établies à partir de ce modèle.



Il est possible d'améliorer notoirement les affaires et les services publics en mettant mieux à disposition les données. Partager les données entre les organisations multiplie ces opportunités. Toutefois, il existe de nombreux obstacles qui empêchent le partage de données trans-organisationnel. Ceux-ci comprennent:

- le manque d'interopérabilité technique et sémantique;
- l'inaptitude à identifier adéquatement les différents acteurs;
- le manque de qualité des données;

- les problèmes culturels et attidunaux; les difficultés de comprendre les avantages du partage de données;
- risque liés à la perte de contrôle des données et des secrets commerciaux, à la violation des droits d'autrui, et à la protection des données;
- l'inaptitude à coordonner les écosystèmes de données et d'encourager et impliquer toutes les entités;
- l'inaptitude à définir le succès et à montrer la valeur à toutes les entités dans l'écosystème de données;
- l'inaptitude à créer une vision, une mission, un but et des valeurs en commun;
- l'inaptitude à identifier les rôles de chaque identité.

Le Modèle de recueil de règles vise à aider à supprimer ces obstacles. Il permet et améliore un partage de données plus équitable, plus simple et mieux sécurisé au sein des réseaux de données. Le recueil de règles basé sur ce modèle décrit les modèles de gouvernance, légaux, techniques que les utilisateurs de données utilisent pour se partager les données entre eux. Il est d'une importance cruciale de prendre en considération les principes éthiques, et en particulier, les exigences découlant de la vie privée des individus et de la protection des données.

Les conditions générales du Modèle de recueil de règles, ainsi que la majeure partie du glossaire, du Code de conduite, et les listes de contrôle dans les annexes du contrat sont les mêmes pour tous les réseaux de données qui utilisent le Modèle du recueil de règles de l'économie de données équitable. Seules les conditions spécifiques seront rédigées au cas par cas. Pour cette raison, il est plus facile et plus économiquement efficace de créer des réseaux et des écosystèmes car les recueils de règles de différents réseaux de données ont substantiellement une base similaire. Cela simplifie la collaboration et le partage de données entre les réseaux et facilite la participation de l'organisation à plusieurs réseaux de données. Les recueils de règles similaires garantissent des affaires équitables, durables et éthiques au sein d'écosystèmes de données, qui à leur tour permet un savoir-faire approfondi, la confiance et des pratiques communes de marché.

Afin d'être en mesure d'utiliser ses propres données et celles des autres, l'organisation a besoin de comprendre largement les perspectives économiques, juridiques, techniques et éthiques du partage de données. Elle doit en particulier reconnaître dans quel rôle elle agit dans le réseau de données, de quels traitement des données et capacités de raffinage elle a besoin d'avoir, et quelles sont les exigences minimum pour prendre part au réseau de données. Les quatre rôles principaux des acteurs au sein d'un réseau de données sont :

1. **Fournisseur de données**: une ou plusieurs sources qui fournit le réseau avec les données. (Remarque; dans les versions précédentes du modèle de recueil de règles pour les réseaux de données, le terme «Source de données» est utilisé au lieu de Fournisseur de données.)
2. **Fournisseur de services**: un ou plusieurs «raffineurs» de données qui combinent les flux de données, raffinent les données, et les fournissent à autrui. Fournissent des services aux utilisateurs finaux ou en tant que sous-traitant à d'autres Fournisseurs de services.
3. **Utilisateurfinal**: un ou plusieurs individus ou organisations pour lesquels un Fournisseur de services a développé ses services. Consomme, utilise et accède à la valeur qui est créée dans l'écosystème de données.

4. **Opérateur d'infrastructure**: un ou plusieurs acteurs qui fournissent la gestion de l'identité, la gestion du consentement, l'enregistrement, ou les services de gestion du service pour le réseau de données.

De la manière reconnue par la Loi européenne sur la gouvernance des données (DGA), on attend des fournisseurs de services d'intermédiation des données de jouer un rôle clé à l'avenir dans l'économie européenne des données. Un intermédiaire de données peut fournir des services pour faciliter l'agrégation et l'échange de données en quantités importantes. Les intermédiaires de données offrant leurs services qui mettent en relation les différents acteurs ont le potentiel de contribuer à une centralisation efficace des données, ainsi qu'à une facilitation de l'échange de données bilatéral. Les intermédiaires qui sont indépendants à la fois des parties qui délivrent des données et de celles qui font usage de ces données ont un rôle de médiateur (facilitateur) dans l'émergence de nouveaux écosystèmes fondés sur les données, indépendants de tout acteur unique détenant une forte puissance sur le marché.

Les réseaux de données, tels que décrits dans le recueil de règles, peuvent également inclure des acteurs qui fournissent des services d'intermédiation de la donnée. Il est cependant essentiel de garder à l'esprit que chacun des membres du réseau de données peut opérer dans de multiples rôles simultanément ou changer de rôle avec le temps. Les fournisseurs de services et les opérateurs d'infrastructure sont des candidats naturels pour être des intermédiaires de données indépendants en conformité avec la Loi sur la gouvernance des données (DGA). Néanmoins, il est à noter qu'ils ne sont pas toujours indépendants, mais les fournisseurs de données et les utilisateurs finaux peuvent occasionnellement fournir aussi des services ou exploiter l'infrastructure.

Veuillez également noter que dans un contexte plus élargi, les Fournisseurs de données peuvent obtenir des données de parties externes, les Abonnés, qui reçoivent des données à partir du réseau de données conformément aux Conditions d'utilisation du jeu de données bien qu'ils ne soient pas des parties de l'Accord constitutif. Le point de départ est que le recueil de règles soit ouvert et public, point requis par le principe de transparence et la législation sur la protection des données. Cependant, les parties spécifiques au réseau d'un recueil de règles contiennent également des règles confidentielles qui ne sont pas divulguées en dehors du réseau de données.

1.2 Guide de démarrage rapide : Comment commencer à travailler sur un recueil de règles pour le partage des données

Par quoi commencer?

Si vous voulez initier un réseau de données basé sur le recueil de règles, suivez les étapes suivantes:

1. Lisez entièrement cette introduction (Partie I) pour vous familiariser avec les diverses dimensions du modèle de recueil de règles.
2. Lisez entièrement la section Modèle du recueil de règles (Partie II). Votre point de départ peut dépendre des compétences des participants de votre équipe de base : experts en

enjeux commerciaux, experts juridiques, experts en technologie, experts en éthique. Vous travaillerez sur ces questions de manière itérative et étendrez votre réseau avec davantage de parties prenantes au fur et à mesure que votre version du recueil de règles progressera.

3. Remplissez la description du réseau, aussi bien la partie Affaires & Opérations que la partie Technologie & Sécurité. Lisez attentivement et répondez aux listes de contrôle du modèle de recueil de règles dans les annexes du contrat pour déterminer la manière de mettre en œuvre votre version de recueil de règles.
4. Vérifiez si vous voulez ajouter davantage de termes au glossaire ou modifier les définitions existantes.
5. Lisez soigneusement les parties contractuelles et décidez comment vous voulez les compléter, et quelles conditions doivent être modifiées dans votre cas.
6. Demandez aux membres fondateurs de signer l'accord constitutif et de commencer à partager les données. Les nouveaux membres peuvent rejoindre le réseau de données en signant l'accord d'adhésion. Le réseau de données est gouverné conformément au modèle de gouvernance.
7. Donnez-nous votre commentaires sur les types de modifications et amendements que vous avez faits au recueil de règles et sur la manière dont nous pourrions améliorer ces modèles.

1.3 Contexte et concepts-clés

Les recueils de règles sont des outils important pour une économie de données équitable et pour le partage de données en général. Pour tirer le meilleur profit du processus d'élaboration du recueil de règles et de son éventuel mise en œuvre et utilisation, il est important de comprendre le contexte plus vaste des recueils de règles.

Une économie de données équitable propose la poursuite simultanée de deux objectifs : donner aux individus le contrôle de leurs données et maximiser l'utilisation des données. Une économie de données équitable peut servir les intérêts des individus, les fournisseurs de services existants et les ré-utilisateurs de données semblables, basés sur la portabilité des données et le consentement. Les avantages sociaux du partage des données reposant sur la permission comprend la croissance économique, la responsabilisation individuelle et de vastes avantages sociaux. (Une feuille de route pour une économie de données équitable, Sitra)

En se tenant à ces objectifs, le recueil de règles pour une économie de données équitable est un outil de gouvernance des réseaux de données nécessaires pour maximiser l'utilisation des données et pour les aligner sur les considérations éthiques permettant aux individus de contrôler les données personnelles les concernant. Ce recueil de règles est formé d'un guide (Partie 1) et d'une série de modèles (Partie 2) qui peuvent être modifiés, adoptés, et utilisés pour les besoins d'un réseau de données spécifique.

Le partage de données requiert un certain nombre de règles - qui peut et doit faire quoi, avec quelles données, etc. Le partage bilatéral de données est relativement simple comparé à un partage de données en réseau multilatéral, et ses règles sont communément fixées par un contrat entre les deux parties qui gouvernent les conditions du partage. Quand un nombre plus élevé de

parties décide de partager des données entre elles, une forme de gouvernance plus complexe est appropriée.

Un recueil de règles est une collection de documents qui peuvent être utilisés ensemble pour gouverner un réseau de données, par lequel nous entendons un arrangement pour le partage de données. Plus précisément, un réseau de données est un réseau comprenant un ensemble de plus de deux parties qui se partagent des données entre elles. Le but des réseaux de données et de partager des données entre les parties de manière responsable et licite pour que tout le monde en tire profit.

Il y a plusieurs concepts importants liés, et se chevauchant en partie avec les réseaux de données. Un espace de données est « un écosystème de données fédéré au sein d'un domaine d'application particulier et basé sur des politiques et règles partagées » (Principes de conception pour les espaces de données – Exposé de position). Les réseaux de données particuliers peuvent faire partie de ces espaces de données plus vastes et spécifiques au domaine dans lesquels ils sont connecté d'une certaine manière définie avec d'autres réseaux ou méthodes de partage des données.

Les écosystèmes de données, d'autre part, sont des systèmes de données complexes et interdépendants, incluant, mais sans s'y limiter, les espaces de données et les réseaux de données pouvant être gouvernés par des recueils de règles.

Finalement, il existe tout un nombre de termes pour décrire soit les *rôles* ou les *entités* qui sont les parties des accords de partage des données. Dans ce recueil de règles, nous utilisons «fournisseur de données» pour toute personne naturelle ou juridique qui fournit (ou permet la fourniture) de données pour d'autres parties dans le réseau de données. Les autres termes utilisés dans d'autres contextes pour ce rôle sont «source de données», «détenteur de données», «détenteur des droits sur les données»; ou «personne concernée» en parlant exclusivement de personnes physiques. En outre, nous utilisons «source de données» pour des *systèmes techniques* spécifiques qui contiennent ou génèrent les données qui sont partagées (par. ex. un capteur).

Notez que les modèles d'accord figurant dans le présent recueil de règles comprennent des définitions supplémentaires, juridiquement contraignantes de certains termes qui sont utilisés dans l'accord. Si ce qui est indiqué ci-dessus et les définitions dans les définitions de contrat sont en contradiction, les définitions de l'accord prévaudront juridiquement.

2. Cadre contractuel

2.1 Introduction

Le cadre contractuel définit par le modèle du recueil de règles consiste des parties suivantes:

Accord constitutif

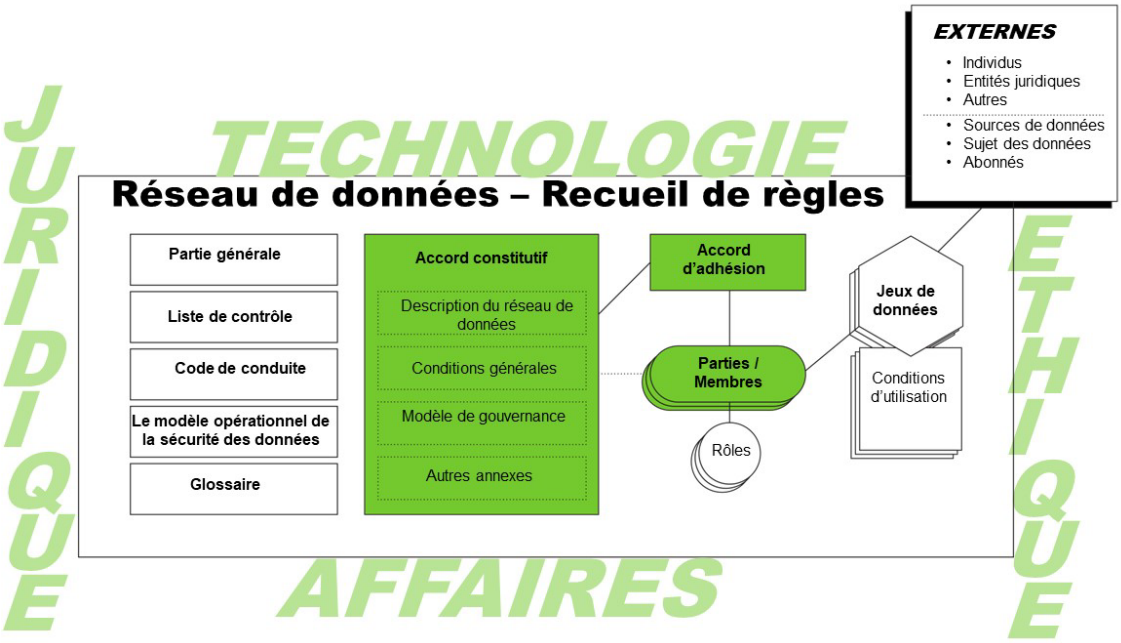
- Conditions générales
- Modèle de gouvernance
- Description du réseau de données
  - Annexe Affaires et opérations
  - Annexe Technologie et sécurité
- Accord d'adhésion

Conditions d'utilisation du jeu de données

- Description du réseau de données
  - Partie Affaires
  - Partie technologie

Les membres du Réseau de données sont les parties de l'Accord constitutif, soit directement (les membres fondateurs) ou via l'Accord d'adhésion.

L'image 2. Position du cadre contractuel dans l'ensemble du recueil de règles



Les réseaux de données sont créés dans le cadre de l'Accord constitutif, qui est conclu par et entre les membres fondateurs du réseau de données. Les conditions générales sont comprises dans l'Annexe de l'accord constitutif.

Bien que l'intention visée par les Conditions générales est de servir de solution de base universelle pour différents réseaux de données, la réalité est que chaque réseau de données demandera des modifications spécifiques à apporter aux conditions générales. Á cet effet, le modèle d'Accord constitutif inclut une section réservée aux dérogations des Conditions générales que les membres fondateurs doivent réviser et modifier afin de s'assurer que le cadre contractuel convient à leur réseau de données. En tant que tels, les contenus finaux de différents accords constitutifs des réseaux de données et leurs annexes divergent sont censés se différer sensiblement.

Nous recommandons aux membres fondateurs de ne pas modifier le document contenant les Conditions générales, mais d'inclure plutôt toute modifications pertinentes en tant que dérogations à l'Accord constitutif. Ceci permettra aux membres d'identifier aisément les modifications qui ont été faites, sans avoir à comparer le document original des conditions générales avec la version modifiée.

Les membres fondateurs peuvent permettre à de nouveaux membres d'adhérer au réseau de données dans le cadre de l'Accord d'adhésion. Lorsque le réseau de données est établi pour autoriser ce type d'accès, les membres fondateurs doivent décrire les critères d'adhésion applicables pour les nouveaux membres dans l'Accord constitutif. De plus, les membres fondateurs doivent considérer s'ils doivent définir les critère et le processus pour accepter de nouveaux membres dans le réseau de données dans l'Annexe du modèle de gouvernance, ensemble avec les autres sujets liés au cadre de gouvernance qui doivent être prises en considération pendant toute la durée du cycle de vie du réseau de données.

L'Annexe du modèle de gouvernance présume que chaque membre désigne un représentant pour être au service du Comité directeur. Le mandat du Comité directeur a été défini au sens large pour faciliter la collaboration entre les membres et pour organiser l'administration du réseau de données de la manière appropriée au niveau stratégique. Ceci inclut, par ex., un mandat pour modifier l'Accord constitutif par une majorité qualifiée des représentants du Comité directeur.

Les Conditions générales ont pour objet de servir d'outil pendant la phase opérationnel d'un réseau de données. D'un côté, créer un réseau de données peut impliquer des investissements de projet de matériels communs par les membres fondateurs, alors que d'un autre côté, créer un réseau de données pourrait nécessiter de part des membres de réaliser des actions individuelles. Tout accord de projet potentiel de la sorte noué par et entre les membres fondateurs doit être conclu séparément, dans lequel les membres fondateurs sont ouverts à accueillir de nouveaux membres dans le réseau de données à un stade ultérieur, leur contribution pour couvrir les coûts de projet doivent être convenus dans l'Accord constitutif et dans tout Accord d'adhésion.

De plus, les membres doivent également définir tout engagement à durée déterminée pour le partage des données au sein du réseau de données, par ex., lorsque les membres cherchent à

recouvrir tout investissement, qu'ils ont fait dans le but d'établir le réseau ou, alternativement, lorsqu'ils exigent la réciprocité en partageant des données.

Les Conditions d'utilisation du jeu de données ont pour objet de fournir un modèle aux fournisseurs de données afin de définir les Conditions générales détaillées qui sont applicables au(x) Jeu(x) de données que le fournisseur de données respectif rend accessible au sein du réseau de données. Si le fournisseur de données permet la redistribution des données à toute tierces parties, le fournisseur de données devrait aussi définir toute condition spécifique applicable aux Conditions d'utilisation du jeu de données que les membres doivent inclure dans leur accord avec telles tierces parties en ce qui concerne la redistribution des données y afférent.

En utilisant les Conditions générales, les parties conviennent de s'y conformer, à moins que les parties décident expressément de déroger aux Conditions générales dans l'Accord constitutif. Les Conditions d'utilisation du jeu de données, d'autre part, sont supposées être définies pour chaque jeu de données par le fournisseur de données qui rend les données disponibles dans le réseau de données.

Les rôles identifiés pour les membres du réseau de données dans les conditions générales incluent :

- **Fournisseur de données** (rend les données disponibles dans le réseau de données);
- **Fournisseur de services** (traite les données pour fournir les services liés et redistribue les données, comme l'anonymisation, la pseudonymisation ou la combinaison des données);
- **Utilisateur final** (utilise les données dans ses affaires); et
- **Opérateur** (fournit les services pour faciliter les opérations du réseau, comme la fourniture de données IPV, la gestion des identités, connexions et/ou contrats).

De plus, le rôle de **l'utilisateur final tierce partie** a été identifié pour toute tierce partie qui reçoit des données de la part des fournisseurs de données lorsque le fournisseur respectif a permis une telle transmission des données.

Il convient de noter que les parties individuelles peuvent assumer plusieurs rôles au sein d'un réseau de données, et d'un autre côté, les réseaux de données ne requièrent pas nécessairement tous les rôles. Par exemple, le rôle de l'opérateur ou du fournisseur de service ne sont pas forcément pertinents si les parties échangent des données entre elles et utilisent les données dans leurs affaires respectives. D'autre part, les données peuvent passer par plusieurs fournisseurs de services dans certains réseaux de données avant que les utilisateurs finaux ou les tierces parties les reçoivent et les utilisent.

2.2 Prémisses

Aussi bien les données partagées dans différents réseaux de données et les Conditions générales qui sont applicables aux données peuvent grandement varier. Comme il n'est pas faisable de définir une bibliothèque exhaustive de termes et de conditions qui couvrirait tous les scénarios

possibles, ce modèle de recueil de règles contient un simple ensemble de prémisses que les auteurs ont supposé pour le modèle de cadre contractuel.

- Le fournisseur de données peut décider séparément pour chaque jeu de données, quelles parties ont accès aux données;
- sauf accord contraire défini par le fournisseur de données dans les Conditions d'utilisation du jeu de données ou convenu par les membres, le fournisseur de données a le droit d'utiliser les données gratuitement;
- la fourniture de données au sein du réseau de données ne constitue pas un transfert des droits de propriété intellectuelle;
- les données peuvent être redistribuées uniquement par les membres du réseau, mais les fournisseurs de données peuvent autoriser la redistribution des données à de tierces parties dans le cadre des conditions d'utilisation du jeu de données applicables;
- les membres sont autorisés à redistribuer les matériaux dérivés á de tierces parties, sujettes à d'éventuelles exigences supplémentaires concernant les droits de propriété intellectuelle, et les informations confidentielles;
- Si les données impliquent des données à caractère personnel, le destinataire des données par défaut devient responsable du traitement;
- le Fournisseur de données indemnise les autres parties contre les réclamations selon lesquelles ses données, qui sont soumises à des frais, enfreignent les droits de propriété intellectuelle ou les Informations confidentielles dans le pays du fournisseur de données;
- les membres sont autorisés à utiliser les données après l'expiration de l'Accord constitutif, auquel cas l'Accord constitutif demeure valide au-delà de l'expiration, excepté si l'Accord constitutif résilié en raison d'une violation substantielle de la Partie; et que
- le fournisseur de données est autorisé à réaliser des audits liés à ses données.

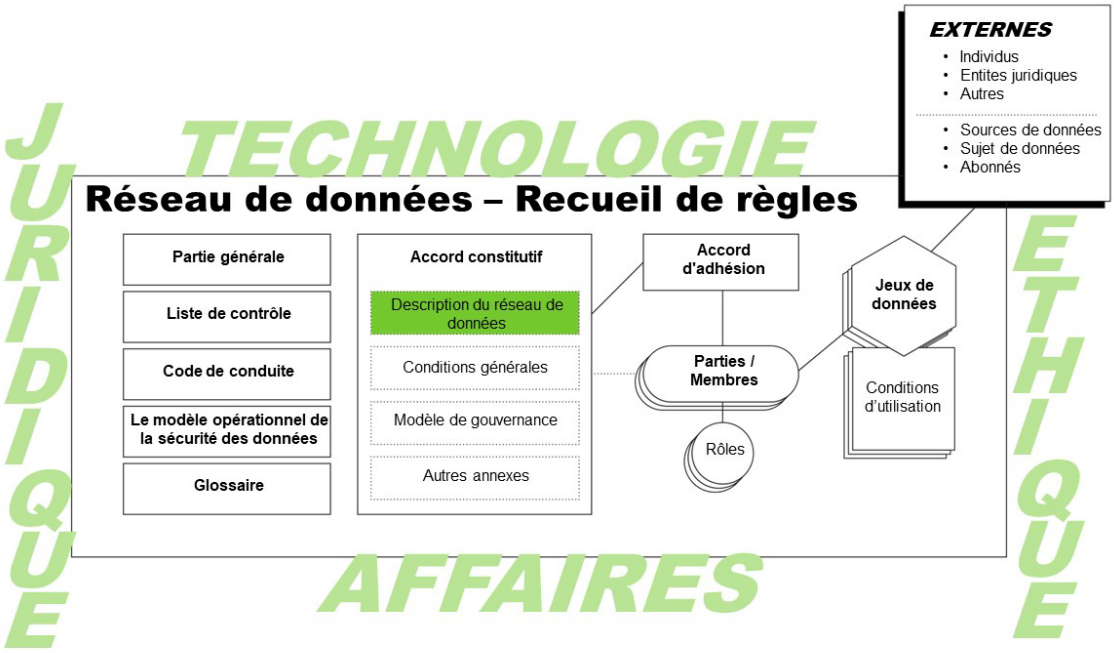
En termes de processus, les membres doivent analyser soigneusement leurs besoins et objectifs par rapport aux principes énoncés ci-dessus. Si nécessaire, les membres du réseau de données concerné peuvent souhaiter modifier ces principes au cas par cas, soit au niveau du réseau de données en indiquant toute dérogation nécessaire aux Conditions générales dans l'Accord constitutif et/ou en définissant un modèle plus détaillé pour les Conditions d'utilisation du jeu de données spécifiques au réseau de données.

De plus, chaque fournisseur de données doit définir, dans le cadre établi pour chaque réseau de données, les conditions qui s'appliquent à leurs données. En outre, des conditions plus détaillées peuvent être ajoutées afin de s'adapter à des modèles d'affaires différentes et plus polyvalents, par example, un cadre pour le traitement des données personnelles. Les membres du réseau de données peuvent également avoir besoin d'ajouter un mécanisme qui facilite le transfert de données, également aux tiers.

3. Comment décrire votre réseau de données?

Cette partie de l'Accord constitutif décrit le réseau de données. Il est formé de deux sous-parties: Affaires et opérations ainsi que Technique et sécurité.

L'image 3. Description de la position du cadre contractuel dans l'ensemble du recueil de règles



3.1 Perspective Affaires et opérations

3.1.1 Introduction

La partie Affaires & opérations rassemble les décision-relatives aux affaires et opérations soulevées via les questions et réponses de la liste de contrôle du recueil de règles et autrement pendant la conception de l'écosystème.

La partie Affaires & Opérations est divisée en deux sous-parties principales : le canevas écosystème de données et les questions qui l'accompagnent définissent le résumé de haut-niveau et la structure pour des aspects économiques du réseau de données, et les chapitres subséquents fournissent des informations plus approfondies pour la conception des affaires qui ne s'insère pas dans le cadre du canevas lui-même. D'autres documents liés à la conception (contrats, présentations, etc.) peuvent être ajoutés pour fournir un niveau supplémentaire de détails pour le réseau de données, si celui-ci est disponible et nécessaire.

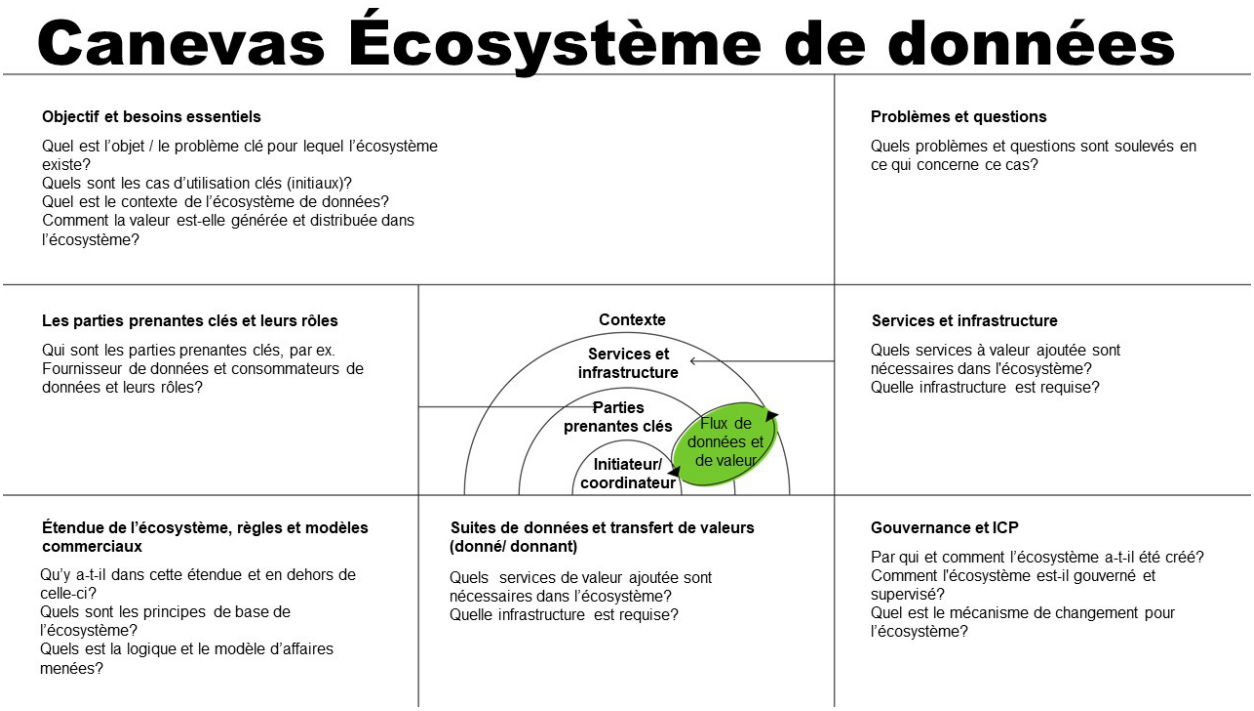
3.1.2 Canevas Écosystème de données.

Le canevas Ecosystème de données suivantes est un résumé de haut-niveau de la conception des affaires pour le réseau de données. La liste de contrôle du recueil de règles Affaires et opérations (section 4.6.1.3) aide à délimiter le contenu de chacun des champs du canevas.

Les réponses couvrent les catégories suivantes :

- **But et objectifs:** Principale raison d'être pour le réseau de données
- **Rôles et responsabilités:** Nommer les intervenants clés, leurs rôles et responsabilités.
- **Logique d'affaires et valeur des données:** Échange de valeurs et modèles d'affaires qui sont rendus possibles par l'écosystème de données.
- **Gouvernance:** Mécanismes pour prendre des décisions au niveau du réseau de données, administrer et superviser ses opérations.
- **Services de données et infrastructure:** Composants ajoutant la valeur requise exigé du réseau de données.

L'image 4. Canevas Écosystème de données



3.2 Perspective Technique et sécurité

3.2.1 Introduction

Le modèle Technique et sécurité rassemble les décisions techniques et de sécurité pendant la conception de l'infrastructure et du système pour l'écosystème de données. La liste de contrôle aide à identifier et à définir les besoins techniques communs et leurs caractéristiques principales.

Le modèle est actuellement une espèce de boîte vide, mais il fournit les sujets qui doivent être couverts et discutés pendant la conception de la solution technique. Le modèle sert de document maître pour les spécifications d'infrastructure, ainsi que pour répartir les tâches entre les systèmes de participants et l'infrastructure commune. D'autres éléments techniques liés à la conception peuvent être ajoutés pour fournir un niveau de détails plus élevé pour le réseau de données, si celui-ci est disponible et nécessaire.

3.2.2 Aperçu de la solution technique

La condition préalable pour la conception technique est d'avoir au moins une compréhension initiale des besoins communs, des parties et rôles impliqués, ainsi que des exigences pour la solution commune. L'outil de liste de contrôle vise à soutenir le processus, ainsi qu'à identifier les prescriptions techniques détaillées. Lorsque les parties seront parvenues à une compréhension initiale commune sur les besoins, les parties et la fonctionnalité de base commune, documentez également une brève introduction pour la partie technique.

3.2.3 Questions centrales sur la sécurité

La condition préalable pour l'opération du réseau de données est une compréhension commune et d'un état d'esprit documenté sur les risques (en matière de sécurité), les pratiques et les solutions liées su réseau de données. Quelles perspectives de sécurité le partage de données apporte-t-il au réseau de données, telles que les normes et politiques de sécurité des informations d'entreprise existantes ? Quelques aspects à prendre en considération :

- Quelle est la base commune de la solution technique liée à la sécurité et à la vie privée?
- Comment la sécurité des données est-elle assurée pour les données partagées à travers l'ensemble du réseau de données?
- Quels fonctionnalités de sécurité de protection de la vie privée sont nécessaires dans la solution commune et parmi les participants, et comment ceux-ci seront mis en œuvre et gérés ? Quelles activités communes sont requises?
- Quels sont les références et normes à utiliser pour la sécurité dans le réseau de données?

Toutes les questions relatives à la sécurité ne sont pas forcément convenues conjointement, mais chaque partie du réseau de données est responsable de s'assurer que la sécurité est mise en œuvre et que les conditions exigences envers les autres parties et le réseau sont remplies.

La solution n’est pas uniquement statique, et le modèle opérationnel doit aussi prendre en compte les points liés au contrôle et à l’amélioration de la sécurité. Le chapitre suivant aborde plus en détail les aspects liés à la sécurité.

4. Modèle opérationnel de la sécurité des données pour les réseaux de données

4.1 Généralités

Les présentes instructions énoncent les principes de développement du modèle opérationnel de la sécurité des données pour les réseaux de données, conformément auquel le réseau de données veille au traitement sécurisé des données. Les besoins en matière de sécurité des données peuvent varier considérablement dans les différents réseaux, il est donc important de modifier le modèle opérationnel au cas par cas et le mettre à jour suffisamment fréquemment. Plus les données partagées sont précieuses ou plus les violations liées à la sécurité des données peuvent créer des dommages, plus le réseau devrait investir dans une sécurité des données de haute qualité.

Dans les réseaux de partage des données, la confiance entre les parties impliquées est la clé du succès. À cet égard, un niveau de sécurité des données adéquat constitue un élément clé crucial. Les règles du réseau doivent être élaborées de manière à soutenir une niveau de confiance suffisant. Les membres du réseau peuvent, dans une certaine mesure, se partager les responsabilités entre eux, mais pas les externaliser dans leur intégralité.

Dans ce contexte, il est également á noter que les compétences et la volonté d'assumer des risques peut différer entre les parties. Á cet égard, il est aussi important que le modèle opérationnel de la sécurité des données soit basé sur des points de vue convenus conjointement sur quels niveaux de risque ou de risques résiduels sont acceptables après les mesures de préventions des risques et comment ceux-ci doivent être partagés.

La sécurité des données doit être prise en compte dès le départ, déjà au moment de la planification des opérations, et elle doit être comprise comme étant une activité continue à travers tout le cycle de vie du partage des données. Tout comme la protection des données personnelles doit être incluse dès la conception et par défaut (article 25 du RGPD), il peut également être impossible ou du moins très onéreux d'ajouter la sécurité des données après-coup.

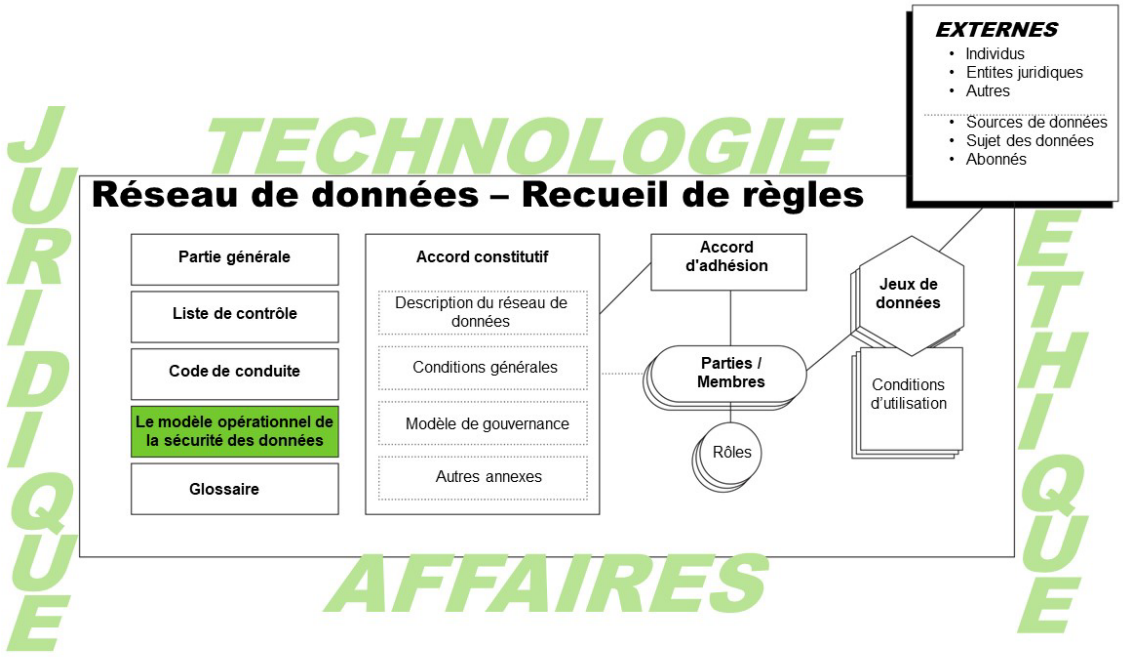
Sauf accord contraire, le modèle opérationnel de la sécurité des données ne fait pas partie intégrante de l'Accord constitutif du réseau de données. Pour ces raisons, il est important que les droits et obligations importants pour la sécurité des données dans lesquels les membres du réseau veulent s'engager soient inclus séparément dans les accords. Une attention doit être accordée à ce point en passant en revue les questions de sécurité de la liste de contrôle ci-dessous et pour élaborer un modèle opérationnel de la sécurité des données pour le réseau de données.

Les lignes directrices pour le modèle opérationnel de la sécurité des données a été créé sur l'initiative de Digipooli (Industries technologiques de Finlande) de l'organisation de la sécurité des services, et avec le soutien de la NESA (Agence nationale de la sécurité de l'approvisionnement).

Les lignes directrices ont été préparées par les experts Olli Pitkänen, Sami Jokela et Marko Turpeinen de 1001 Lakes Oy et par Antti Nyqvist, secrétaire du pool Digipooli. Le workshop

organisé pour développer les lignes directrices a impliqué des membres de Digipool, des sociétés de nombreux différents secteurs et des représentants d'universités et d'organisations.

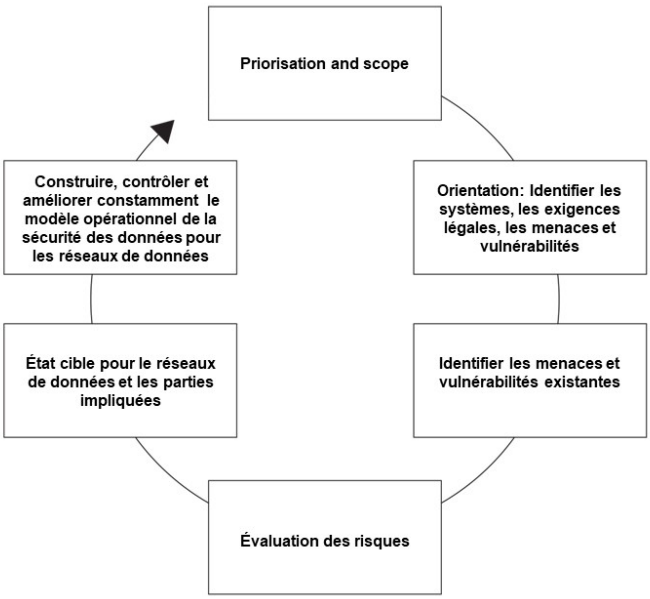
L'image 5. Modèle opérationnel de la sécurité des données dans un recueil de règles en tant qu'entité.



4.2 Processus de sécurité des données

Le diagramme suivant montre dans un format simplifié le processus de développement du modèle opérationnel de la sécurité des données pour les réseaux de données, ou, en bref, le processus lié à la sécurité des données, décrit ci-dessous.

L'image 6. Processus de développement du modèle opérationnel de la sécurité des données pour les réseaux de données, ou, par ex., le processus de la sécurité des données.



4.3 Priorisation et étendue

Les membres fondateurs du réseau de données doivent nommer un comité de travail impliquant des représentants de tous les membres fondateurs pour préparer un modèle opérationnel de sécurité des données. La première tâche du comité de travail est de définir l'environnement opérationnel. En ce qui concerne le réseau de données, ceci peut être fait simplement en se référant á des éléments de la partie Affaires du recueil de règles sur la pertinence de la sécurité des données, si ce règles ont déjà été élaborées.

Après cela, vous devez limiter ce qui est inclut dans l'étendue de la sécurité des données couverte par le recueil de règles. Le point essentiel est d'attirer l'attention sur le partage des données et sur les activités comme celles de réseau. Dans ce contexte, il peut ne pas être nécessaire de résoudre d'autres problèmes liés à la sécurité, qui peuvent être importants en tant que tels.

Le comité de travail doit également se prononcer sur l'objet de la protection: les données couvertes par le recueil de règles, conformément à l'Accord constitutif dans le cadre contractuel du recueil de règles, ou autre chose?

4.4 Prise en compte de la protection des données

Si les données contiennent des données à caractère personnel, la législation sur la protection des données doit être appliquée. La législation principale est le règlement général sur la protection des données (RGPD) de l'UE, qui est applicable à l'ensemble du traitement des données personnelles. De plus, selon la situation, les dispositions nationales relatives à la protection des données personnelles couvrant des secteurs spéciaux peuvent aussi être applicables. Par exemple, en Finlande, selon le type de données concernées, la loi sur la protection de la vie privée dans la vie professionnelle (759/2004) doit être prise en compte dans les sujets liés à la supervision technique des employés et du Code de la société d'information (917/2014) en ce qui concerne les messages transmis et les services de la valeur ajoutée.

Pour davantage d'informations
Pour davantage d'informations, voir Korpisaari, Pitkänen, Warma-Lehtinen: Uusi tietosuojalainsäädäntö. (en finnois; Nouvellle législation sur la protection des données) Alma Talent, Helsinki 2018.

Dans le RGPD, les données à caractère personnel font référence à toute information se rapportant à une personne physique identifiée ou identifiable, c.-à-d., une **personne concernée**. Étant donné que la définition des données à caractère personnel est vaste, il est généralement raisonnable de présumer que les données peuvent inclure des données personnelles, même si ceci n'est pas évident. C'est uniquement si la personne qui traite les données peut être entièrement certaine que les données ne contiennent aucune donnée personnelle, que la législation sur la protection des données peut être ignorée.

L'article 24 du RGPD est une disposition générale sur les responsabilités du responsable du traitement de données. Cet article prévoit quel type de mesures le responsable du traitement doit mettre en œuvre afin de s'assurer et d'être en mesure de prouver que le traitement des données personnelles est réalisé tel que requis par le Règlement. La disposition comprend à la fois les obligations d'agir avec précaution et l'obligation de démontrer quels types de mesures ont été mis en œuvre pour assurer un traitement licite.

L'article 32 contient des dispositions spécifiques sur la sécurité des données. Conformément à cet article, le responsable du traitement et le sous-traitant doivent mettre en place des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité approprié au risque.

Garantir que la protection des données est dûment gérée offre souvent des avantages importants et un atout concurrentiel pour le responsable du traitement, alors que dans le cas inverse, négliger la protection des données peut devenir très coûteuse. La mise en œuvre, la récupération et les dommages liés à la protection des données peuvent avoir un impact sur le montant de toute amende administrative imposée conformément à l'article 83 du RGPD.

Dans les réseaux de données, une attention particulière doit être apportée au fait, qu'en principe, les données personnelles puissent être collectées uniquement pour des finalités déterminées, explicites et légitimes, et elle ne doivent pas être traitée par la suite d'une manière incompatible avec ces finalités. Ceci peut être un problème si les différentes parties ont des besoins différents pour le traitement des données personnelles et si ces besoins changent avec le temps. Pour cette raison, il faut accorder de l'attention aux finalités d'utilisation des données personnelles dès la mise en place du réseau de données.

Il est bonne chose, en règle générale, que le recueil de règles soit préparé de telle manière que les finalités d'utilisation des données qui y sont définies soient suffisamment précises et explicites pour la finalité légale du traitement des données à caractère personnel et que la finalité du traitement ne doive pas être définie séparément en ce qui concerne aux données personnelles. S'il existe de nombreux types de données à partager, il peut ne pas être possible de définir les finalités spécifiques de l'utilisation en détail pour la totalité des données concernées. Au lieu de cela, il faut accorder de l'attention à différents types de données personnelles.

Si un ensemble de critères rationnels et couramment utilisés pour l'anonymisation des données peut être trouvé, il peut être utilisé pour exempter ces données des obligations de la législation sur la protection des données, car les données anonymisées ne peuvent plus être reliées à une personne physique.

Pour plus d'informations
Pour plus d'informations, voir, par ex., le Bureau du Médiateur européen de la protection des données (Finlande): Données pseudonymisées et anonymisées

Il peut également être possible d'utiliser le réseau de données pour remplir l'obligation de rapporter les atteintes à la sécurité des données (stipulé par RGPD), dans la mesure où les obligations pertinentes ont été inclues dans l'Accord constitutif du recueil de règles. Par exemple, il peut être convenu que les personnes concernées peuvent soumettre des demandes d'informations à n'importe quelle partie du réseau ou à la partie la plus visible du point de vue des personnes concernées, qui les transmet au responsable du traitement approprié, ou que les informations sont fournies de manière centralisée par une partie du réseau au nom de toutes les parties. Toutefois, il est à noter qu'un tel arrangement ne doit pas compromettre les droits des personnes concernées et qu'ils ont toujours le droit d'avoir affaire le responsable du traitement approprié.

4.5 Orientation: identification du système, des exigences légales, des menaces et vulnérabilités

Lorsque tous les sujets couverts par la sécurité des données en conformité avec le recueil de règles ont été priorisés et spécifiés, les objectifs de la sécurité des données doivent être définis et les méthodes de gestion au moyen des quelles ils peuvent être atteints doivent être passés en revue. Nous reviendrons à la manière dont les méthodes de gestion sont définies plus en détail ci-dessous.

Les membres fondateurs doivent **définir les objectifs de la totalité du réseau de données** en ce qui concerne la sécurité des données, et les parties individuelles doivent **définir leurs propres objectifs** en ce qui concerne le réseau de données. Selon le type de données partagées et le secteur dans lequel les parties opèrent, il peut être nécessaire d'appliquer la législation spéciale, dont les exigences doivent être prises en compte. Au total, de telles dispositions spéciales peuvent être trouvées dans des centaines de réglementations spécifiques pour chaque secteur. Par exemple, en Finlande, la loi qui réglemente le traitement automatisé des données à caractère personnel du client dans les services de soins sanitaires et sociaux contient davantage de dispositions détaillées sur le traitement des données personnelles du client.

Une fois les objectifs définis, il est possible d'identifier quelles méthodes de gestion de la sécurité des données sont adaptées pour le réseau de données concerné. Une définition plus détaillée des méthodes de gestion sera réalisée aux stades ultérieurs du processus. Les méthodes de gestion de la sécurité des données peuvent être divisées en trois catégories : moyens administratifs, techniques et physiques.

Les moyens administratifs sont liés à la gestion des risques, à la documentation de la sécurité des données, à la sécurité personnelle et à la formation. Les moyens techniques sont mis en place en utilisant soit des logiciels soit du matériel hardware. Ceux-ci peuvent inclure la gestion centralisée des journaux, les pares-feux, les systèmes de détection d'intrusion (IDS), les systèmes de prévention d'intrusion (IPS), et les systèmes de gestion des identités et des accès. Les moyens physiques de la gestion de la sécurité des données, d'un autre côté, font référence à la protection des ressources et du personnel par des moyens comme des barrières, serrures, éclairage et caméras de surveillance.

Il est important de prendre en considération tous les différents moyens de gestion de la sécurité des données qui permettent d'assurer que le réseau de données peut atteindre un niveau suffisant de sécurité des données. De multiples couches de contrôle doivent être créées autour de l'objet protégé pour atteindre une protection multicouche.

Il convient de souligner qu'à ce stade, les méthodes variées de gestion de la sécurité des données disponibles ne sont qu'explorées de manière générale. Il est conseillé au réseau de données et aux organisations impliquées de sélectionner les meilleures méthodes de gestion convenables à leur situation spécifique, uniquement après avoir procédé au processus d'évaluation des risques de sécurité décrit ci-dessous.

4.6 Aperçu des menaces liées à la sécurité

Dans le modèle de déploiement local traditionnel des applications, les donnée sensible de chaque organisation restent à l'intérieur de l'organisation et sont soumises à ses politiques de sécurité physique, logique, personnelle et de contrôle d'accès. Toutefois, le modèle cloud communément utilisé par les réseaux de données enregistre les données en dehors des limites de l'organisation. Pour cette raison, les vérifications de sécurité supplémentaires doivent être menées pour assurer la sécurité des données et pour prévenir les atteintes à la sécurité des données causées par des failles de la sécurité des données ou des employés malveillants.

Les informations sur les menaces actuelles à la sécurité des données peuvent être trouvées, entre autres, sur les sites web de l'Agence européenne pour la cybersécurité (ENISA) et des autorités nationales de sécurité de l'information.

Le cloud computing peut utiliser des ensembles de matériel et de logiciels provenant de divers réseaux informatiques à travers le monde. Il permet un partage de données coût-efficace et plus rapide. Ceci a été identifié par les criminels qui exploitent des virus et autres programmes malveillants (maliciels) pour des fins visant le vol de données sensibles, les perturbations de services, ou l'endommagement des réseaux informatiques en nuage des entreprises.

Selon IBM Security, globalement, le total des coûts moyens de chaque violation de données s'élève à USD 4.24 millions. En Scandinavie, le coût total moyen par violation de données est légèrement inférieur, à USD 2.67 millions. Il a fallu une moyenne de 287 jours pour identifier et minimiser la violation de sécurité des données. Plus il faut du temps pour identifier la violation, plus les coûts sont élevés. Le coût d'une violation de données ayant un cycle de vie de moins de 200 jours était inférieur de près d'un tiers à celui d'une violation de données qui a duré plus de 200 jours.

Par la suite, voici quelques tendances importantes ayant un impact sur la sécurité des données :

1. L'interdépendance entre les processus sociaux et les systèmes d'information augmente
2. De nouvelles interdépendances entre les organisations de l'État émergent
3. Les questions liées à la sécurité de l'information s'internationalisent
4. La nécessité de gérer les informations privées ou confidentielles et les apparitions publiques dans les environnements TIC augmente
5. La protection des données à caractère personnel devient un enjeu politique de plus en plus important
6. Il devient de plus en plus difficile de veiller à l'exactitude des informations
7. L'exactitude des informations devient de plus en plus importante
8. La collecte de données augmente
9. L'intégration d'informations provenant de différentes sources augmente
10. La traçabilité des personnes et des biens augmente
11. Les actions malveillantes à l'encontre des systèmes d'information augmente
12. Les questions relatives à la qualité et la sécurité sont de plus en plus prises en compte dans le développement de logiciels
13. Les systèmes automatisés/autonomes sont de plus en plus utilisés pour assurer la sécurité
14. La disponibilité de l'information augmente à mesure que les ressources d'information publiques s'ouvrent
15. Les intérêts commerciaux orientent les acteurs à restreindre l'accès aux ressources d'information confidentielles
16. La gouvernance de l'accès aux ressources informationnelles dans les organisations devient plus difficile

Dans ce qui suit, les menaces relatives à la sécurité de l'information sont discutées en particulier de la perspective sur la manière dont elles affectent le partage des données dans les réseaux de données.

4.6.1 Utilisation des données d'une manière incompatible avec l'objet

Les données peuvent également être utilisées pour des fins non convenues dans l'Accord constitutif ou dans les Conditions d'utilisation du jeu de données, ou bien non prises en compte dans le recueil de règles. Cela peut soulever des problèmes que le fournisseur de données n'a pas pris en compte mais sur lesquels il s'est engagé. Typiquement, ceci implique un préjudice subi (par ex., les données révèlent certains sujets que la partie ne veut pas partager) ou le fait qu'une autre partie développe ses affaires sur ces données sans donner de compensation suffisante au fournisseur de données. Un autre sous-ensemble à cela est la construction et l'utilisation de modèles pour remplacer les données.

4.6.2 Fuites de données

Les données peut se retrouver chez une mauvaise partie, délibérément ou involontairement. Ceci peut avoir lieu par le biais d'une erreur de TI (proche des menaces traditionnelles liées à la sécurité des données) ou par une partie transmettant les informations, une sous-catégorie ou un modèle de données érigé á partir des données d'un tiers. Dans les fuites de données, les erreurs faites par les utilisateurs et l'incompétence jouent souvent un rôle essentiel. Ceux-ci peuvent être réduites par l'éducation et la formation, tel que décrit ci-dessous. Les fuites de données peuvent aussi avoir lieu de telle manière que les données ont été utilisées pour des fins d'enseignement de l'intelligence artificielle, dans le cadre duquel quelques informations confidentielles sont restées dans le modèle IA, et peuvent ainsi avoir été divulguées à des personnes extérieures via le modèle.

4.6.3 Responsabilité relative aux données

Intégrité des données. Les données ne correspondent pas à ce qui a été convenu, sont incorrectes, ou ont été modifiées. Ceci implique essentiellement des questions liées à la responsabilité : qui est responsable si les données ne correspondent pas à ce qui a été convenu ou présumé, ou si elles ont été modifiées. Les questions liées aux responsabilités sont discutées plus largement dans le cadre contractuel du recueil de règles, en particulier, dans les sections 3 Responsabilités à rôle spécifiques, 5 Responsabilités générales et 11 Responsabilités et les exceptions et spécifications potentielles les concernant dans l'Accord constitutif et les Conditions d'utilisation du jeu de données.

Outre ce qui est indiqué précédemment, les questions liées à la responsabilité des données comprennent des responsabilités imprévues, telles de nouvelles responsabilités surprenantes liées aux données, concernant le traitement des données personnelles, qui émergent via les interprétations développées par les autorités, alors que la manière d'interpréter la législation en matière de protection des données trouve simplement sa forme. Par définition, il est difficile de

prendre de telles éventualités en compte, mais dans une certaine mesure, il est possible de prendre position, à savoir qui assumera leur responsabilité dans les accords.

4.6.4 Partage accidentel de données

Tous les événements de perte de données ne sont pas l'œuvre de cybercriminels sophistiqués. En réalité, un nombre surprenant de violations de données sont causées par les propres employés d'une entreprise qui partagent accidentellement, perdent ou gèrent mal des données sensibles. Il est courant que les employés partagent, autorisent l'accès, perdent ou traitent fautivement des informations précieuses, soit accidentellement ou parce qu'ils ne sont pas conscients des pratiques de sécurité. Il est également malheureusement courant que les employés traitent avec négligence les appareils sur lesquels des données sont stockées, les oublient dans des lieux publics ou les stockent sans protection adéquate. Par exemple, selon le rapport publié par Shred-it en 2018, 40% des violations de la sécurité des données sont causées par de tels comportements. Ce problème majeur peut être résolu par la formation des employés et des autres utilisateurs, mais aussi par d'autres mesures, telles que la technologie de prévention des pertes de données (DLP) et l'amélioration des contrôles d'accès.

Exemple 1
Le carnet électronique d'un employé d'une entreprise de services a été volé. Le carnet volé contenait les prénoms, noms, sexes, adresses et dates de naissance de plus de 100 000 clients. Après-coup, il s'est avéré impossible de déterminer entièrement le contenu de toutes les données qui ont été perdues. L'accès au disque dur de l'appareil n'était pas protégé par un mot de passe. Quelques données ont pu être restaurées à partir des sauvegardes quotidiennes.

Exemple 2
Le département RH d'un bureau de l'administration publique a envoyé un e-mail sur les formations à venir aux personnes inscrites comme chercheurs d'emploi. Un fichier contenant des données personnelles de tous ces chercheurs d'emploi (nom, e-mail, adresse postale, code d'identification personnelle) était joint à cet e-mail. Plus de 60.000 personnes ont été concernées.

Les gens font des erreurs, et atténuer les risques associés á ces erreurs est d'une importance critique pour protéger la confidentialité des données. Les données de l'entreprise sont l'un des actifs les plus précieux que toute entreprise contrôle, et elles doivent être protégées en conséquence. Tout simplement, l'accès aux données devrait être un système qui minimise l'exposition et réduit les risques d'utilisation abusive.

Une autre menace de sécurité liée à aux personnes concerne les opportunités limitées de l'équipe de cybersécurité de l'organisation de superviser tous les risques. Les administrateurs système sont souvent débordés lorsqu'ils tentent de protéger des informations sensibles. Ceci laisse les entreprises exposées, et devrait davantage les inciter à mettre en place une système automatisé quand possible, sans oublier que l'automatisation en elle-même comprend des risques variés.

4.6.5 Hameçonnage et ingénierie sociale

Les attaques d'ingénierie sociale sont un vecteur principal utilisé par les agresseurs qui veulent avoir accès aux données sensibles. Ils impliquent de manipuler ou d'inciter des individus à fournir des informations privées ou à accéder à des comptes privilégiés.

Le phishing ou l'hameçonnage est une forme courante d'ingénierie sociale. Il s'agit des messages qui apparaissent d'une source fiable, mais qui sont en fait envoyées par un agresseur. Lorsque les victimes se laissent faire, et fournissent par exemple des informations privées ou cliquent sur un lien malveillant, les agresseurs peuvent compromettre leur appareil ou avoir accès au réseau de la société.

Les courriels de phishing sont en hausse. En même temps, les nouvelles technologies et l'accessibilité accrue des informations rend ces attaques encore plus sophistiquées, et augmente la probabilité d'intrusion des agresseurs dans vos systèmes TI. En dépit des meilleurs efforts déployés dans le domaine, ces messages malveillants se retrouvent dans les boîtes de messagerie électronique des employés. Gérer ce trafic et fournir les outils aux employés, les éduquer et les former à se défendre contre ces menaces sera d'une importance critique.

Les adresses e-mails et les mots de passe, en particulier, font l'objet d'une grosse demande parmi les cybercriminels. Ce sont les données volées en premier lieu dans les cas de violation de données. Étant donné que ces informations peuvent être utilisées pour déployer d'autres attaques, encore plus diversifiées, chaque société doit être consciente de la manière dont ses propres informations peuvent être utilisées à son encontre.

Exemple 3

Le service client d'une société de télécommunications reçoit un appel d'une personne qui se fait passer pour un client. Il demande à la société de changer son adresse e-mail à laquelle les informations de facturation client sont envoyées. L'employé du centre de contact confirme l'identité du client en lui posant des questions personnelles, tel que requis par les procédures de la société. L'appelant fournit correctement le numéro fiscal et l'adresse postale demandés (car il a accès aux informations). Après confirmation, l'opérateur effectue la modification demandée, et à partir de ce moment-là, les factures sont envoyées à la nouvelle adresse e-mail.

Cette procédure ne requiert pas de notification à l'ancienne adresse e-mail. Le mois suivant, le client légitime contacte la société pour demander pour quelle raison il ne reçoit plus les données de facturation à son adresse e-mail et nie avoir demandé don changement d'adresse e-mail. La société s'aperçoit plus tard que les informations ont été envoyées à un mauvais utilisateur et annule donc cette modification.

4.6.6 Menaces internes

Les menaces internes sont les employés qui, par inadvertance ou intentionnellement, menacent la sécurité des données d'une organisation. Il existe trois types de menaces internes :

- Intrus non malveillants – ce sont des initiés qui peuvent causer des dommages accidentellement, par négligence ou incompétence.
- Intrus malveillants – il s'agit d'initiés qui essayent activement de dérober des données ou de causer préjudice à l'organisation pour en tirer un profit personnel.
- Intrus compromettants – ce sont des initiés qui ne sont pas conscients que leurs comptes ou identifiants ont été compromis par une attaque externe. L'attaquant peut alors réaliser une activité malveillante, tout en prétendant être un utilisateur légitime.

Lorsque les entreprises déterminent leurs risques liés à la cybersécurité, ils pensent en premier lieu aux tiers malveillants. En effet, les cybercriminels jouent un rôle prédominant dans certaines fuites de données, mais les employés de la société en promulguent beaucoup d'autres.

Le rapport de Verizon (2019) sur les menaces internes a mis en évidence que 57% des violations de bases de données comprennent les menaces internes et la majorité, 61%, de ces employés n'occupent pas de postes de direction lorsqu'ils compromettent les données du client.

La corruption constitue une forme de menace interne. Les données de la société et la propriété intellectuelle sont toutes les deux étonnamment précieuses, et dans certains cas, les employés peuvent-être corrompus pour révéler ces informations. Par exemple, en 2018, Amazon a accusé plusieurs employés d'avoir participé à un système de corruption qui compromettait les données des clients, et en 2019, on s'est aperçu que les employés d'AT&T recevaient des pots-de-vin pour implanter des logiciels malveillants sur le réseau de la société. Évidemment, la corruption n'est pas le moyen le plus accessible de perpétuer un système de données, mais, en particulier pour les sociétés dont la valeur repose sur leur propriété intellectuelle, ceci peut représenter un grave danger pour la sécurité des données.

Exemple 4
Pendant la période de préavis, un employé de l'entreprise copie les informations concernant les affaires à partir de la base de données de la société. L'employé n'a le droit d'accéder à ces données que pour l'exercice de ses fonctions. Des mois plus tard, après avoir démissionné de son poste, il utilise les données ainsi obtenues (informations de contact de base) pour saisir de nouvelles données de traitement. En tant que responsable de traitement, il a l'intention de contacter les clients de la société pour les attirer dans ses nouvelles affaires.

4.6.7 Attaques rançongiciel

Les faux logiciels de décodage et de protection ransonware contamine les appareils de la société et crypte les données, et les rend inutilisables sans clé de décodage. Les agresseurs affichent un message de rançon pour demander un paiement permettant de remettre la clé, mais dans la plupart des cas, payer la rançon ne sert à rien et les données sont perdues.

Le coût des attaques de rançongiciels a plus que doublé en 2019, et cette tendance continuera certainement à l'avenir. De nombreuses attaques de rançongiciels commencent par des courriels de phishing envoyés aux employés et d'autres communications malveillantes qui ont des conséquences dévastatrices.

De nombreux types de ransomwares peuvent se propager rapidement et contaminer de grandes parties du réseau de la société. Si une organisation n'effectue pas des sauvegardes régulières, ou si le virus ransomware arrive à infecter les serveurs de sauvegarde, il n'y aura peut-être aucun moyen de récupération.

Exemple 5

Une attaque ransomware est ciblée contre les systèmes informatiques d'une petite entreprise industrielle, et les données y figurant sont cryptées. La société s'était elle-même chargée de crypter les données à l'avance afin que toutes les informations auxquelles le programme ransomware a accès soient déjà cryptées, et que la clé de décodage ne soit pas compromise dans cette attaque. Pour cette raison, l'agresseur a uniquement accès aux données cryptées.

La société a recours à l'expertise d'une société extérieure de cybersécurité pour examiner ce cas. Tous les journaux d'e-mails sortants et les autres suites de données sont disponibles. Après avoir analysé les journaux et les données collectées par le systèmes d'observation de la société, un examen interne soutenu par la société de cybersécurité dresse avec certitude que l'agresseur a seulement crypté les données sans avoir accès à leur contenu. Les données personnelles touchées par la violation concernent les clients et les employés de la société, au total, quelques dizaines de personnes. La copie de sauvegarde est facilement accessible, et les données sont récupérées quelques heures après l'attaque.

Cette atteinte à la protection des données n'a aucune conséquence sur les opérations quotidiennes de la société. Il n'y a aucun délai pour les paiements des employés ou le traitement des demandes des clients.

Exemple 6
Le serveur d'une entreprise de transport public est exposé à une attaque ransomware et l'agresseur crypte les données sur le serveur. Un examen interne révèle que l'agresseur n'a pas seulement crypté les données, mais en a aussi retiré pour son compte. Les données compromises comprennent des données personnelles des clients et des employés, ainsi que de milliers de gens qui utilisent les services de la société (par ex., pour acheter des billets en ligne). Outre les données personnelles de base, la violation des données porte sur les numéros de cartes d'identité et sur les informations financières, comme les informations de carte de crédit. Il y a une base de données sur les sauvegardes, mais l'agresseur les crypte également.

4.6.8 Pertes de données dans le cloud

De nombreuses organisations transfèrent les données sur le cloud pour faciliter le partage et la collaboration. Toutefois, lorsque les données passent sur le cloud, il est plus difficile de contrôler et prévenir la perte de données. Les utilisateurs ont accès aux données à partir de leurs appareils personnels et via des réseaux non sécurisés. Il est facile de partager un fichier avec des parties non autorisées, soit accidentellement, soit de manière malveillante.

4.6.9 Mauvaises pratiques en matière de mot de passe

L'étude menée par Thomas et al a permis de conclure que 1.5% de toutes les informations de connexion sur Internet sont vulnérables aux attaques de bourrage d'informations d'identification qui utilisent des informations volées pour infliger de nouvelles attaques au réseau informatique d'une entreprise. De nombreux identifiants de connexion ont été compromis lors des atteintes aux données précédentes, et comme les gens ont des mots de passe répétés ou faciles á deviner, les informations peuvent être utilisées pour avoir accès aux données de la société si le réseau n'est pas sécurisé.

Pour cette raison, les meilleures pratiques comme demander de mettre à jour les mots de passe en tant que routine sont simples, mais une manière importante pour prévenir ce genre de menace (voir les instructions de Traficom).

4.7 Identifier les menaces et vulnérabilités existantes

Une fois les objectif en matière de sécurité définis et les méthodes de gestion identifiées, il est recommandable d'**évaluer et de documenter la situation actuelle**. À cet égard, la situation est sensiblement différente si les données sont déjà partagées entre les parties d'une certaine manière, comparé à une situation dans laquelle le partage de donnée est juste sur le point de commencer.

Comment la sécurité des données est-elle assurée actuellement dans l'étendue selon laquelle les données sont déjà partagées entre les parties? Qu'est-ce qui va changer du point de vue de la perspective de la sécurité des données lorsque les données sont partagées en conformité avec la partie Technique et la partie Affaires du recueil de règles précité?

À ce sujet, il convient également de prendre en compte les exigences légales et l'étendue selon laquelle les réglementations internationales, au niveau de l'UE, et les dispositions nationales dans les différents pays sont pris en considération. En règle générale, les réglementations sur la partage des données sont fortement harmonisées au sein de l'UE. Par exemple, le Règlement général sur la protection des données (RGPD), ainsi que les autres réglementations de l'UE appliquées sous forme de règlementation, sont en vigueur dans tous les pays membres de l'UE et de l'EEE.

D'autre part, il peut y avoir de grosses différences sur la manière dont les directives de l'UE ont été mises en œuvre dans la législation des différents États membres, par exemple. Si les données sont partagées à l'extérieur de l'UE et de l'EEE, vous devez être préparé à la possibilité que la législation diffère complètement ou, en particulier, que le transfert des données personnelles ne puisse pas être permis sans arrangements spéciaux.

La question clé est de savoir si les données sont partagées directement entre les parties ou si les données sont conservées quelque part dans un répertoire central d'où chaque partie peut les retirer. Ceci a également un impact essentiel sur l'attribution des exigences de gestion de la sécurité des données aux bonnes parties. Une option peut être d'utiliser un opérateur de type séquestre, une tierce partie fiable, qui gérera certaines obligations contre une rémunération.

4.8 Évaluation des risques

Tel que décrit ci-dessus, le réseau de données et ses participants doivent identifier **les menaces et vulnérabilités liés à la sécurité**. Ensuite, ils **évaluent la sévérité** des risques en déterminant le degré de probabilité de chaque menace et l'étendue du dommage au cas où la menace se concrétise.

Dans les réseaux de données, l'évaluation des risques est placée en premier lieu sous la responsabilité des Membres fondateurs, mais dans la pratique, ils doivent aussi confier cette tâche au comité de travail sur la sécurité susmentionné. À nouveau, il faut accorder une attention toute particulière à la perspective de l'ensemble du réseau de données.

La sévérité des risques peut apparaître très différemment du point de vue de l'ensemble du réseau de données et de la perspective d'une partie individuelle. Néanmoins, chaque partie impliquée est responsable de chaque évaluation des risques selon sa propre perspective.

La sévérité du risque est le produit de la probabilité et l'étendue du dommage. Étant donné qu'il n'est pas facile d'attribuer une valeur numérique pour la probabilité ou l'étendue du dommage, dans la pratique, le meilleur moyen est souvent d'avoir recours à une classification, telle une approche en trois phases, lors de leur évaluation, et de placer ensuite les risques sur une matrice

où un axe représente la probabilité et une autre l'étendue du dommage. Ceci aide à voir quels risques sont les plus sérieux et qui demandent le plus d'attention.

La gestion des risques fait référence aux processus et pratiques qui peuvent être utilisées pour identifier, évaluer et atténuer les risques et pour attribuer les responsabilités pour ces mesures. Il est recommandé que le réseau de données définisse des méthodes opérationnelles communes pour l'évaluation des risques dans la mesure où elles portent sur l'opération du réseau. Le modèle opérationnel de la sécurité des données comprend des définitions adéquates pour la gestion des risques de tous les domaines de l'ensemble du réseau.

4.9 État cible pour le réseau de données et les parties impliquées

Après avoir évalué les risques, les Membres Fondateurs peuvent se mettre d'accord sur l'**état cible de la sécurité de l'information** pour l'ensemble du réseau de données et ses membres individuels. Considéré l'étendue selon laquelle les parties veulent rendre l'état cible juridiquement contraignant, il est nécessaire de les modalités et conclusions contraignantes de l'Accord constitutif, de l'Accord d'adhésion ou les Conditions d'utilisation du jeu de données.

Le réseau doit avoir une intention commune concernant le niveau des risques et l'étendue des mesures. Ceci peut requérir un nombre considérable de négociations et de coordination des objectifs, en particulier, si les niveaux d'exigence en matière de connaissances, d'expertise et de sécurité varient parmi les participants du réseau. Selon la nature du réseau de données, l'état cible est documenté en décrivant, par exemple, ce que le réseau de données vise à atteindre dans les domaines suivants :

1. Politiques en matière de sécurité des données
2. Sûreté et sécurité du personnel
3. Gestion des données à protéger
4. Contrôle d'accès
5. Chiffrement
6. Sécurité physique et environnementale
7. Sécurité opérationnelle
8. Sécurité des communications
9. Acquisition, développement et maintenance de systèmes
10. Relations avec les fournisseurs
11. Gestion des incidents de sécurité
12. Aspects de la sécurité des données liés à la gestion de la continuité des affaires
13. Conformité

4.10 Construction, contrôle et amélioration constante du modèle opérationnel de la sécurité des données pour les réseaux de données

Après avoir défini l'état cible, **un modèle opérationnel de la sécurité des données** pour soutenir la réalisation, la maintenance et l'amélioration constante de l'état cible sera élaboré. Selon le réseau de données, il inclut les thèmes comme:

1. Organisation de la sécurité des données

Selon la taille, les opérations et l'objectif du réseau de données, il peut s'avérer approprié d'établir un sous-groupe de comité directeur conformément au Modèle de gouvernance afin de s'assurer que la sécurité de l'information, et la réalisation, la maintenance et le développement de son état cible, ou pour attribuer ces tâches au comité directeur ou de confier la responsabilité de celles-ci à certaines personnes désignées, par exemple. Une définition de ce caractère contraignant pour les parties doit habituellement être intégrée au Modèle de gouvernance ou à l'Accord constitutif et/ou d'adhésion.

Dans le cadre de l'organisation de la sécurité des données, les responsabilités concernant qui réagit si des risques se matérialisent et de quelle manière doivent être définies. Ceci comprend non seulement les mesures immédiates pour limiter et remédier aux dommages, mais aussi la communication et l'apprentissage de ce qui est arrivé.

Le RGPD contraint généralement les parties impliquées à signaler toutes les violations de données à caractère personnel à l'ombudsman chargé de la protection des données, et dans certains cas, aussi les personnes touchées. En règle générale, une notification doit être faite à l'ombudsman pour la protection des données dans les 72 heures suivant la découverte de la violation de la sécurité des données. Ceci est un délai si court qu'il est bon de planifier à l'avance comment réagir à une violation de la sécurité des données et de le signaler, afin qu'il ne soit pas nécessaire de commencer à y songer une fois l'incident arrivé.

2. Engagement de la direction envers la sécurité des données. Qui/quel organe assume la direction envers le réseau de données?

Assurer l'engagement de la direction est essentiel pour le modèle opérationnel de la sécurité des données. Pour cette raison, les Membres fondateurs doivent identifier la personne ou la partie qui est dans une position de leader concernant la sécurité des données dans le réseau de données et s'assurer de leur engagement à atteindre l'état cible.

3. Comment la sécurité des données est-elle mesurée?

Le réseau de données doit convenir des indicateurs mesurant la sécurité des données. Quels indicateurs sont principalement utilisés selon le type de paramétrage réseau des données? Les indicateurs doivent être définis de telle manière à être reliés aux objectifs fixés précédemment, que les parties peuvent avoir une influence sur ceux-ci par le biais de leurs propres mesures et qu'ils sont particulièrement significatifs en terme de risques évalués comme étant les plus sérieux ci-dessus.

4. Quel type d'audits et d'examens sont menés dans le Réseau de données?

Afin de construire la confiance, le processus de sécurité des données doit être suffisamment transparent. En particulier, il vaut la peine d'investir dans une gestion des risques transparente du réseau.

Afin d'assurer la sécurité des données, on peut aussi convenir que les parties ont le droit d'auditer et d'examiner les systèmes et installations de chaque autre partie. Si de tels audits ou examens sont jugés nécessaires, une clause doit être intégrée dans l'Accord constitutif, l'Accord d'adhésion, les Conditions d'utilisation du jeu de données ou le Modèle de gouvernance qui oblige les parties qui peuvent être assujetties à de telles mesures de permettre l'accès à leurs systèmes et installations. Le terme doit être sans ambiguïté et clair de manière à ce qu'il n'y ait aucun doute sur qui il concerne, sur ce que l'audit ou l'examen se concentre, qui peut le réaliser, qui est responsable des coûts occasionnés et à quel type d'obligations de confidentialité la partie exécutante est soumise.

5. Documentation sur le modèle de sécurité des données du réseau de données

Le modèle opérationnel de sécurité des données pour le réseau de données doit être intégré dans le recueil de règles du réseau de données. Généralement, c'est un document similaire au Code de conduite qui décrit la compréhension mutuelle entre les parties, mais qui n'est pas une partie de l'Accord constitutif juridiquement contraignante. Pour cette raison, toutes les obligations qui doivent être juridiquement contraignantes doivent être inscrites séparément dans les sections pertinentes de l'Accord constitutif ou ses annexes. Il est également possible d'inclure la totalité du modèle opérationnel de la sécurité des données en tant qu'annexe contraignante de l'Accord constitutif. Toutefois, ceci peut rendre le modèle d'opération trop rigide alors qu'il doit être possible de le réformer et maintenir d'une manière flexible.

En ce qui concerne la documentation, il est important de noter que l'article 30 du RGPD exige de maintenir un registre des activités de traitement des données personnelles. Celui-ci doit également être mis à la disposition de l'autorité de contrôle, à sa demande, pour permettre d'évaluer le caractère licite des activités de traitement. De plus, conformément à l'article 5, le responsable de traitement a généralement l'obligation d'être en mesure de prouver la conformité avec le Règlementation (*reddition de comptes*) à tout moment.

6. Amélioration constante: comment assurer la continuité de la sécurité des données et le développement du processus?

À mesure que le réseau de données se développe, que les opérations changent et que de nouvelles parties apportent de nouveaux besoins au réseau, il est important de s'assurer que la sécurité des données reste au niveau souhaité et que le processus de sécurité des données du réseau de données est continuellement amélioré. Il est recommandé d'intégrer séparément dans le Modèle de gouvernance la manière dont le modèle opérationnel de la sécurité des données est examiné et mis à jours aux intervalles convenus.

7. Changement des finalités d'utilisation des données et leur gestion

Les finalités d'utilisation des données sont définies dans l'Accord constitutif ou dans les Conditions d'utilisation du jeu de données. Ceci est essentiel pour la mise en œuvre de 1) la limitation de la finalité de la protection des données et 2) les droits d'accès aux données.

La limitation de la finalité de la protection des données en conformité avec le Règlement général sur la protection des données (**RGPD**) restreints les fins pour lesquelles le responsable du traitement peut utiliser les informations collectées sur les personnes. La limitation de la finalité comprend deux aspects importants : les données à caractère personnel doivent être collectées pour des finalités spécifiées, explicites et légitimes (spécification de la finalité), et ne doivent pas être traitées par la suite de manière incompatible avec ces finalités (utilisation compatible). La limitation de la finalité n'interdit pas que les données collectées pour un objectif défini ne puisse être traitée pour d'autres fins, tant que ceci n'est pas incompatible avec l'objectif initial. Ce principe vise, d'une part, à protéger les attentes légitimes des personnes concernées par rapport au traitement des données personnelles les concernant, et d'autre part, à permettre l'utilisation des données personnelles par la suite, dans certaines limites.

Toutefois, en ce qui concerne les droits d'utilisation, la question essentielle est de savoir à quelles fins le titulaire des droits, tel que le titulaire des droits d'auteur, des droits du producteur ou du droit aux données fondé sur la protection des secrets d'affaires, a autorisé l'utilisation des données. Normalement, ils n'ont pas les droits d'utilisation à d'autres fins.

En d'autres termes, la règle de base est que les données ne peuvent pas être utilisée pour des finalités autres que celles spécifiées. Toutefois, les circonstances changent, de nouveaux besoins peuvent faire surface pour les parties du réseau en ce qui concerne les données, et les nouvelles parties qui rejoignent le réseau peuvent introduire avec eux de nouveaux besoins qui ne pouvaient pas être anticipés. Pour cette raison, il peut y avoir de bon motifs pour changer les fins d'utilisation. Lorsque ce besoin se manifeste, on doit déterminer la manière selon laquelle ceci peut être réalisé en conformité avec la législation sur la protection des données, en demandant aux personnes leur consentement pour traiter leurs données à caractère personnel pour de nouvelles fins, par exemple. D'un autre côté, il est généralement nécessaire de négocier sur les conditions d'utilisation qui peuvent être reformulées avec le détenteur de ces droits, si le détenteur dispose du droit de veto sur les nouvelles fins et qu'elles n'entrent pas dans le champ de l'ancienne définition.

4.11 Sources utilisées pour le modèle opérationnel de la sécurité des données

Orientations EDPB 01/2021 sur les Exemples concernant la notification de violation des données

Forbes: 10 risques liés à la sécurité des données qui pourrait avoir un impact sur votre entreprise en 2020.

Sécurité IBM. Rapport 2021 sur les coûts d'une violation des données 2021

Imperva. Sécurité des données.

Päivi Korpisaari, Olli Pitkänen, Eija Warma-Lehtinen. Uusi tietosuojalainsäädäntö. (en finnois; Nouvellle législation dur la sdécurité des données) Alma Talent, Helsinki 2018.

Olli Pitkänen, Risto Sarvas, Asko Lehmuskallio, Miska Simanainen, Vesa Kantola, Mika Rautila, Arto Juhola, Heikki Pentikäinen, Ossi Kuittinen. Informations supplémentaires sur les tendances relatives à la sécurité. Projet de recherche Kasi, programme de recherche Tekes sur la sûreté et la sécurité, rapport final, Mars 11, 2011

Olli Pitkänen. Tietosuojasäädösten muutostarve (en finnois; Besoin de changer la loi sur la protection des données), Bureau du premier ministre, 41/2017

Olli Pitkänen, Päivi Korpisaari, Rauno Korhonen. Miten kansallista lainsäädäntöämme pitää muuttaa EU:n yleisen tietosuoja-asetuksen vuoksi? (en finnois; Comment la législation nationale finlandaise devrait être amendée en raison du règlement RGPD ?) In Korpisaari (ed.) Annuaire de la loi sur les communications 2016, Forum Iuris, 2017

Subashini, Subashini, et Veeraruna Kavitha. Une étude sur les questions relatives à la sécurité sur les modèles de prestation de services de cloud computing. Journal des applications réseau et informatique 34.1 (2011): 1–11

M. Swathy Akshaya et G. Padmavathi. Taxonomy of Security Attacks and Risk Assessment of Cloud Computing. J. D. Peter et al. (eds.), Advances in Big Data and Cloud Computing, Advances in Intelligent Systems and Computing, 2019

Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh et Elie Bursztein. Protéger les comptes contre les détournements des identifiants avec un service de notification de violation du mot de passe. Compte-rendu du symposium sur la sécurité USENIX 2019.

5. Principes éthiques: Valeurs partagées du réseau de données

Le modèle éthique assiste pour prospecter et améliorer l'aspect éthique du réseau de données, et des activités et organisations qui en font partie. Le Code de conduite intégré ne constitue pas un code d'éthique standardisé pour tous les cas de figure, étant donné que les organisations et réseaux– qui veulent l'utiliser– sont certainement très différentes selon le contexte et d'autres raisons variées.

Par conséquent, étant donné que différents réseaux de données peuvent utiliser le présent recueil de règles, ce code ne peut pas être considéré comme une liste suffisante, mais comme une liste de questions nécessaires à prendre en compte. Cela signifie que des codes plus détaillés et spécifiques ou d'autres guides d'éthique devraient être pris en considération et examinés, en se basant sur les demandes de réseaux de données ou d'organisations spécifiques qui mettent en œuvre le présent Code de conduite.

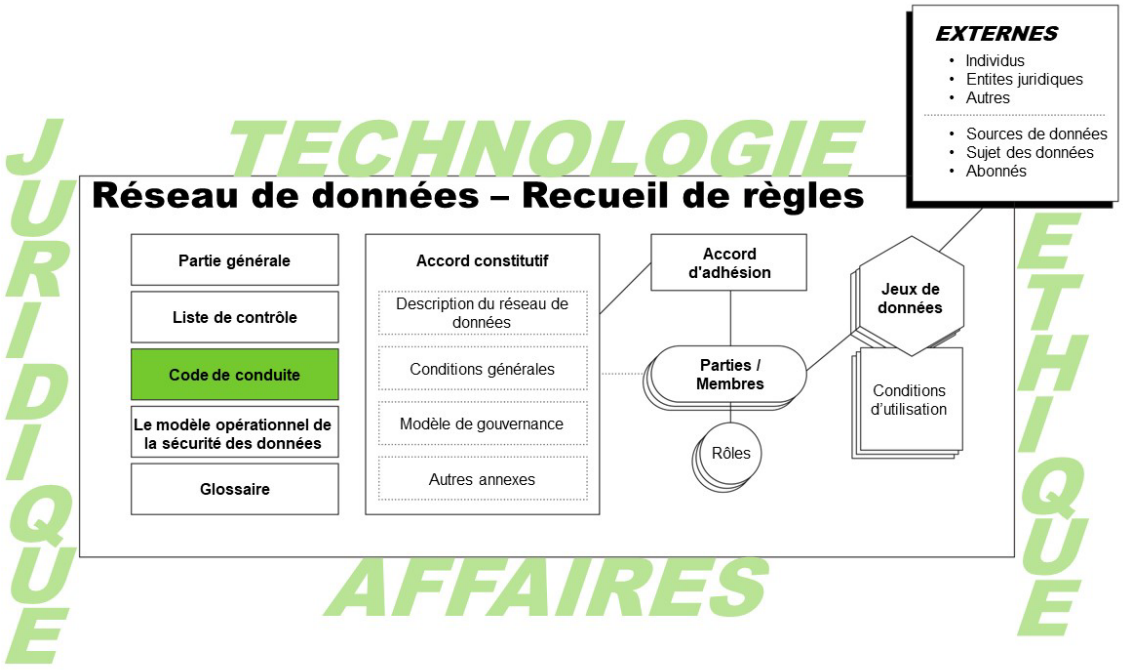
Les exigences en matière de codes éthiques sont différentes en fonction du type d'informations utilisées et la cible d'utilisation peut également soulever des préoccupations éthiques différentes. Par exemple, lors de l'utilisation d'informations sur la santé, les codes de déontologie médicale doivent être pris en compte. Par contre lorsque les données traitées au sein d'un réseau de données ne comprennent aucune donnée personnelle, l'accent doit être mis sur le respect, par exemple, des droits de propriété intellectuelle.

Le code d'éthique ne devrait pas être perçu comme un moyen de restreindre les acteurs d'un réseau de données, mais plutôt comme un ensemble de normes communément acceptables qui rendent la coopération plus pratique en fixant la direction des règles plus détaillées définies par les organisations qui le mettent en place. Le code n'est pas un obstacle. Comme les lois, il aide à créer la confiance dans le réseau de données, qui est nécessaire pour obtenir de véritables profits et de nouvelles opportunités commerciales. Le présent Code de conduite repose sur le respect entre les différentes parties prenantes, une communication transparente et sur l'ambition de trouver des valeurs qui soient communément acceptables.

Le code en lui-même n'a pas de valeur intrinsèque, mais une valeur instrumentale. Le principal est que l'organisation ait un véritable but d'améliorer ses procédures et politiques de manière plus éthique. Le simple suivi mécanique des codes vaut mieux que de ne pas les suivre. Cependant, l'objectif devrait changer la culture de l'organisation de telle manière à placer l'aspect éthique dans les actions quotidiennes, afin que les changements viennent de l'intérieur – et non de l'extérieur. Dans ce cas, le changement est durable et aidera l'organisation à répondre aux exigences que la société lui impose à juste titre.

Agir de manière éthique n'est pas simplement un facteur de coût, mais une possibilité pour des affaires résilientes.

L'image 7. Code de conduite du modèle de recueil de règles.



Il existe un consensus parmi les théoriciens normatifs du pluralisme culturel selon lequel le dialogue représente la clé pour garantir une relation juste entre différents groupes. L'éthique du discours est un outil applicable pour introduire différents points de vue dans le cadre d'une communication constructive, et ainsi, de permettre un discours plus transparent et rationnel. L'éthique du discours fournit un mécanisme pour prendre en considération les différents points de vue sur la morale et les intuitions des partie prenantes.

Toutefois, le Code de conduite ne met pas l'accent sur les théories éthiques. Au lieu de cela, le code a pour objectif d'aborder le thème du point de vue des praticiens et de fournir des outils conceptuels et analytiques pour évaluer les raisons sur la base de laquelle il est possible de répondre à la question «que devons-nous faire?». Ceci est réalisé en présentant les valeurs jugées comme importantes pour l'économie de données, ainsi que pour proposer un modèle de maturité (voir la section suivante) qui peut être utilisé dans l'analyse de l'état des affaires dans une organisation et par conséquent dans la recherche de manières d'amélioration et de développement.

Les valeurs suivantes se sont avérées importantes dans le recherche menée pendant le projet IHAN. Pour atteindre l'objectif d'une utilisation équitable des données, ces valeurs doivent être observées et respectés dans les pratiques quotidiennes.

Sources et autre matériel sur l'éthique

James, M. R. (2003). Communicative Action, Strategic Action, and Inter-Group Dialogue. Journal européen de théorie politique, 2(2), 157–182.

Stahl, B. C. (2012). Moralité, éthique, et réflexion: A categorization of normative IS research. Journal of the Association for Information Systems,13(8):636–65.

Code d'éthique ACM (PDF) est un code d'éthique qui fournit des aperçus pour les professionnels de l'informatique et les dirigeants concernant la prise en compte des questions d'éthique dans la pratique.

Orientation éthiques pour une IA de confiance par le Groupe d'Experts de haut-niveau sur IA mis en place par la Commission européenne.

Canevas éthique des données (PDF) fourni par ODI (Open Data Institute) qui met l'accent sur l'aide à identifier et gérer questions éthiques liées à l'utilisation des données.

Une éthique pour les grosses données (PDF): Trouver l'équilibre entre les profits économiques et les Big Data dans le contexte politique de l'UE

5.1 Responsabilité et vérifiabilité

Les membres du réseau de données sont responsables de leurs actes, et ils doivent être en mesure de donner des raisons satisfaisantes à cela. Cela signifie que tous les acteurs sont censés suivre le recueil de règles du réseau de données et en particulier son contrat. Tous les contrats doivent également suivre les principes du Code de conduite et du recueil de règles du réseau de données. La responsabilité a lieu envers les membres du réseau de données, mais aussi envers les parties prenantes externes, par exemple les personnes physiques, dont les données personnelles peuvent être traitées dans le réseau de données.

Les opérations au sein du réseau de données doivent également être vérifiables, par ex., un auditeur doit être en mesure de réaliser un examen exhaustif des données traitées dans le réseau de données. Par conséquent, les registres de membres, les journaux et les documents sur le traitement des données sont bien organisés et complets, leur personnel est transparent dans ses démarches avec l'auditeur, et les membres ont un bon système pour le contrôle interne, la sécurité et la documentation concernant le traitement des données.

5.2 Prévention des dommages

Tous les acteurs du réseau de données doivent éviter de causer du tort, mais plutôt se concentrer à créer de la valeur (directe ou indirecte) pour l'ensemble du réseau de données et toutes les personnes touchées par les actions au sein du réseau de données.

5.3 Traitement justifié des données personnelles

Les données à caractère personnel doivent être traitées sur une base licite et équitable, comme sur un consentement informé de l'individu, en conformité avec un contrat noué avec l'individu, une obligation légale, un intérêt vital de l'individu, dans l'intérêt public, ou aux fins d'intérêts légitimes, à condition que les intérêts et droits et libertés fondamentaux de l'individu ne soient pas menacés, en particulier lorsque l'individu est un enfant.

5.4 Équité, justice et égalité

Tous les acteurs du réseau de données doivent promouvoir l'équité, la justice et l'égalité entre les individus. L'équité signifie que chacun est traité avec respect, indépendamment de son contexte ou statut socio-économique. De même, les bénéfices (économiques et autres) doivent être équilibrés entre toutes les parties prenantes de telle manière que les individus qui sont la source de données ne soient pas vus comme de simples ressources exploitables.

Pour garantir une utilisation équitable de leurs informations, les individus disposent de véritables possibilités de comprendre et contrôler leurs données personnelles qui sont collectées, transférées et traitées dans le réseau de données.
Le règles et la structure du réseau de données sécurise les bénéfices et attentes légitimes de toutes les parties. Ceci nécessite une structure de pouvoir équilibrée dans le réseau de données et une gouvernance transparente orientée sur le consensus.

5.5 Approche centrée sur la personne

Les gens vivent dans des environnements différents, et ils ont des expériences vécues personnelles de leur propre existence. Ils doivent être respectés et encouragés. Cela signifie que les individus doivent être considérés et traités comme des acteurs actifs ayant la possibilité de faire leurs propres choix dans le réseau de données. Ils doivent être capables de garder entièrement et effectivement leur autodétermination. De plus, leurs besoins et souhaits devraient être pris en compte au lieu de les réduire à de simples objets ou sujets.

5.6 Vie privée

La vie privée figure parmi les points centraux de l'économie des données. Pour cette raison, la vie privée doit être respectée et protégée. Le réseau de données est basé sur l'utilisation d'informations, qui requièrent beaucoup de confidentialité, étant donné que ces informations

peuvent être sensibles et privées. Ainsi, cela signifie que les données personnelles doivent être traitées de manière licite, équitable et de manière transparente par rapport aux individus.

Les données personnelles doivent être collectées pour des finalités spécifiées, explicites et légitimes et ne pas être traitées par la suite de manière incompatible avec ces fins. Seules les données personnelles qui sont adéquates, pertinentes et limitées au strict nécessaire par rapport aux fins énoncées, peuvent être traitées.

Les organisations ne collectent pas les informations personnelles dont ils n'ont pas besoin. Toutes les données personnelles qui sont traitées doivent être nécessaires pour l'utilisation spécifique. Les membres du réseau de données prennent des mesures raisonnables pour s'assurer que les données personnelles sont correctes et à jour. Les données personnelles ne doivent être conservées plus longtemps que ce qui est nécessaire pour les fins pour lesquelles ces données sont traitées.

Pour assurer l'intégrité et la confidentialité de la vie privée, les données personnelles doivent être traitées d'une manière qui garantir la sécurité des données, y compris la protection contre le traitement non autorisé ou illicite et contre les pertes accidentelles, la destruction ou le dommage, en utilisant des moyens techniques ou organisationnels appropriés.

Pour préserver l'intégrité, la confidentialité et la disponibilité des données, les organisations ont besoin de développer et mettre en œuvre un cadre politique sur la sécurité de l'information. En fusionnant les jeux de données, il faut veiller plus soigneusement à la protection de la vie privée que normalement. L'anonymisation des données est recommandable, si elle est possible.

Toute organisation doit également être responsable, par ex. elle doit être en mesure de prouver sa conformité avec les principes susmentionnés. Ainsi, le traitement des données personnelles doit être planifié et documenté. Il doit exister des procédures claires et documentées pour collecter, conserver, utiliser et distribuer les données.

Pour les données collectées, il doit y avoir un plan de cycle de vie clairement documenté où la collecte, l'archivage et l'éventuelle suppression des données sont décrites. Les éléments pertinents du plan de cycle de vie sont disponibles pour les fournisseurs de données et les individus qui sont liés aux données.

5.7 Sécurité

Tous les membres du réseau de données sont responsables de la sécurité de leur collecte, usage, conservation, partage et autre traitement des données. Cela signifie que des solutions et processus de sécurité adaptés sont utilisés et aussi que les points relatifs au contrôle, à la réparation et aux rapports sur la sécurité soient conçus comme il se doit.

Les données à caractère personnel doivent être sécurisés de la manière appropriée, et les risques liés aux droits et libertés des individus doivent être analysés. Toutes les actions techniques, organisationnelles et personnelles nécessaires doivent être mise en place afin de minimiser les

menaces liées à la sécurité des individus dont les informations sont traitées. Compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature, de l'étendue, du contexte et des finalités du traitement ainsi que du risque de probabilité et de gravité variables pour les droits et libertés des personnes, tous les membres du réseau informatique doivent mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque.

De même, les violations de données doivent être traitées sans délai. Lorsque la violation de données à caractère personnel est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques, le membre responsable du réseau de données communique la violation de données à caractère personnel à la personne concernée sans retard injustifié.

5.8 Durabilité et économie circulaire

Tous les membres du réseau des données sont orientés et encouragés à développer et déployer des solutions durables pour être en harmonie avec une économie circulaire plus durable. Les membres mettront en œuvre le réseau de données de manière à rendre ses opérations plus durables et circulaires, tout en réduisant ses externalités négatives sur l'environnement, le climat, et sur les ressources naturelles.

5.9 Transparence

Le réseau de données est basé sur la coopération et le respect des sources d'information. La transparence est importante pour développer la confiance. Les données doivent être traitées de manière licite, équitable et transparente. Toute information destinée au public ou aux individus doit être concise, d'accès facile et à compréhension aisée, exprimée dans un langage clair et simple, et, en outre, le cas échéant, une visualisation sont utilisés.

Ceci ne signifie pas que les informations sont ouvertes à tout le monde sans restrictions. Au lieu de cela, cela signifie que tous les membres du réseau de données doivent savoir (quand/si possible), quelles données sont offertes sur le réseau de données et selon quelles exigences pour promouvoir la transparence du réseau. Pour soutenir une économie en temps réel, les membres du réseau de données ne détiennent pas forcément les données, mais les partagent dès que possible.

Il faudrait éviter l'utilisation d'un jargon juridique inutile. Si on demande à un individu de donner son consentement ou d'accepter un accord, ceci doit être présenté d'une manière facilement distinguable des autres éléments, sous une forme intelligible et facilement accessible, et utiliser un langage simple et clair. De plus, des informations honnêtes doivent être fournies aux individus pour comprendre quelles données les concernant ont été collectées et la manière dont elles sont traitées.

5.10 Amélioration continue

Les questions éthiques varient et les différentes questions peuvent se manifester au cas par cas. Ainsi, l'évaluation éthique doit être un processus continu dans l'organisation, il y doit y avoir un support institutionnel pour cela. Pour cette raison, la gestion du membre du réseau doit supporter les employés de l'organisation en s'assurant qu'ils disposent de réelles opportunités pour faire respecter, promouvoir, et observer les principes du Code de conduite.

L'éthique est mise en œuvre dans les actions quotidiennes des individus ou n'est pas du tout mise en œuvre, car seul l'individu peut prendre cette décision morale. Toutefois, sans le support institutionnel pour les décisions éthiques, il existe un risque accru de conduite contraire á l'éthique, étant donné que les individus n'ont pas l'autonomie leur permettant de prendre des décisions morales.

5.11 Support des individus

Tous les membres du réseau de données doivent soutenir les individus à (a) obtenir des informations sur l'utilisation de leurs informations personnelles, (b) comprendre les informations, pratiques, contrats, et leurs conséquences, et (c) participer, contribuer, et influencer les systèmes et pratiques en utilisant les informations personnelles de ces individus. L'objectif est d'assurer que si les individus ont besoin d'informations ou ont des demandes justifiées d'Informations, ils bénéficieront du support nécessaire (orientations, aide personnelle etc.) par des moyens transparents. L'accent doit être mis dans la création d'un moyen à faible barrière pour vérifier la surexploitation des informations personnelles pour les individus auprès desquels elles sont directement collectées, ou reçues d'une autre manière.

5.12 Communication

Une communication appropriée est fondamentale à travers le cercle de vie du réseau de données. Elle est essentielle pour les individus, les organisations, et la société dans l'ensemble. Chacun d'eux a besoin, en plus de contenus et de délais différents, de canaux de communication et de manières appropriés. Les principes éthiques mentionnés ci-dessus sont également mis en pratique avec la communication. De plus, la communication est le moyen de démontrer l'engagement de l'organisation dans celles-ci. La gestion a une responsabilité spéciale d'articuler, d'appliquer et de soutenir la culture et les processus de l'organisation qui reflètent les principes du présent Code de conduite.