Politique de gestion des données institutionnelles

de l'Université de Genève

Règles applicables en matière de gestion des données institutionnelles

UNIVERSITÉ DE GENÈVE

UNIVERSITÉ DE GENÈVE

Table des matières

1. Executive summary

La Politique de gestion des données institutionnelles de l'Université de Genève (UNIGE), ci-après « la Politique », s'inscrit dans une démarche institutionnelle de réduction des risques en matière de sécurité des données et de mise en conformité aux lois et règlements régissant l'usage des données (LIPAD, LArch, LRH, par exemple). La formalisation de principes et de règles de gestion en matière de cycle de vie, de valorisation et de protection/sécurité des données fournit un cadre institutionnel fort qui contribue au respect de la Charte d'éthique et de déontologie des hautes écoles universitaire et spécialisée de Genève et des directives institutionnelles en matière d'intégrité de la recherche. Cette ambition ancre ainsi la démarche au plus haut niveau en favorisant l'adhésion de toutes les parties. La présente politique répond également aux recommandations de l'audit du service d'Audit de l'État de Genève mené en 2021 sur la gouvernance des Systèmes d'Information (SI) de l'UNIGE. D'une part, cet audit a mis en avant la nécessité d'impliquer les responsables métiers (*Data owners*) lors du processus de classification des données dans les différents niveaux de sensibilité (pour une application de mesures de protection adéquates), d'autre part il souligne que cette classification doit s'articuler avec une politique de gestion globale, prenant en considération l'ensemble du cycle de vie des données et des documents, de la collecte à l'archivage ou destruction.

La mise en place d'une gouvernance des données au sein de l'UNIGE offre une multitude d'avantages qui vont de la conformité réglementaire à la maîtrise des données, en passant par l'optimisation des processus métiers et la valorisation des données produites dans le cadre des activités d'enseignement, de recherche, de service et de support. C'est en respectant et en appliquant les principes contenus dans cette politique que l'ensemble de la communauté universitaire pourra contribuer de manière significative à améliorer l'intégrité, la fiabilité et la sécurité des données et contribuer à la conservation du patrimoine scientifique, historique de l'institution.

Objectifs de la politique et bénéfices attendus

Les données traitées et produites par l'UNIGE sont de nature diverse et touchent des domaines d'activité variés (formation/étudiant-es, ressources humaines, finances, logistique, recherche, etc.). Les traitements opérés sur ces données et les usages qui en sont faits se doivent d'être conformes et appropriés en regard des exigences légales et règlementaires propres à chaque domaine, mais également en matière de sécurité de l'information.

La présente Politique s'inscrit dans une approche à long terme qui se veut saine en définissant les bonnes pratiques en matière de gestion des données. Elle vise à fournir à l'ensemble des parties prenantes des principes directeurs et des règles opérationnelles de mise en œuvre en vue de garantir une gestion efficiente des données. Par la mise en place d'une organisation autour de rôles clairement identifiés et dont les responsabilités sont assignées en fonction de compétences métiers fortes, elle doit contribuer non seulement à l'amélioration de la qualité des données, mais également à renforcer leur gestion efficiente et à assurer la protection des données sensibles.

Principaux bénéfices attendus par la mise en place d'une gouvernance des données

Responsabilités et gouvernance

Portée par le Secrétaire général de l'UNIGE, la Politique s'appuie sur les recommandations évoquées plus haut pour assurer une gestion des données responsable, efficace et maîtrisée au sein de l'Institution. Son application concrète consiste à :

- la constitution d'un Data Office institutionnel regroupant des rôles-clefs en matière de gestion des données au sein de l'institution. Ce nouvel organe permettra d'accompagner et de conseiller les métiers et les entités dans la mise en œuvre progressive de la politique. Il fournira par ailleurs une expertise transversale à la demande des entités et services qui souhaitent améliorer des processus existants, édictera des directives ou formera et sensibilisera le personnel.
- la mise en place d'une organisation structurée par domaine métier et fondée sur l'identification de rôles existants au sein de chaque domaine pour lesquels des responsabilités spécifiques seront attribuées. Cette organisation facilitera ainsi la gouvernance des données à tous les échelons de l'organisation.

Organisation de la politique de gouvernance des données

Le premier chapitre précise la portée du document et définit la terminologie employée. Les chapitres suivants décrivent les règles de cette politique et les directives associées. Elles sont regroupées selon les thématiques suivantes :

Application de la politique de gouvernance des données au sein de l'UNIGE	• *Principes d'application de la politique selon le cadre légal et sa déclinaison stratégique et opérationnelle*
Organisation et gouvernance des données	• *Description de l'organisation, de la comitologie, des rôles et des responsabilités de la gouvernance des données*
Cycle de vie, valorisation et sort final des données	• *Decriptions des rôles, responsabilités, principes et processus de gestion du cycle de vie des données, depuis leur collecte, en passant par leur référencement, jusqu'à leur sort final*
Sécurité et protection des données	• *Description des principes de sécurité et de protection des données et des responsabilités associées aux rôles identifiés dans la gouvernance des données*

Mesures de mise en œuvre

L'application de cette politique implique de définir et de mettre en place une déclinaison stratégique et opérationnelle par domaine métier. Pour ce faire, un set documentaire est mis à disposition des domaines métiers afin de les guider sur les actions opérationnelles à mettre en œuvre : il comprend une data map du domaine, l'affectation des rôles de *CDO domaine*, *Data Owners* et *Data Stewards* par sous-domaine et les actions opérationnelles de mise en œuvre. Ces actions sont découpées selon l'ordre des chapitres de la politique et peuvent être ajustées en fonction des spécificités propres à chaque domaine. Dans cette optique, le Data Office institutionnel fournit un appui à l'application de la Politique et accompagne la formalisation de nouveaux processus. La déclinaison opérationnelle est priorisée en fonction des besoins métiers exprimés, par exemple en fonction du risque sécuritaire, de la non-conformité d'un processus, ou d'un besoin d'optimisation des ressources.

La formation et la sensibilisation des personnes en charge de différents traitements de données (saisie, mise à jour, transmission, etc.) est un volet important du déploiement de la politique de gestion des données. Elle est conçue en tenant compte des spécificités des domaines métiers, rappelle le cadre légal auquel est soumise l'institution, présente les mesures de protection et de sécurité des données et promeut les bonnes pratiques simples et efficaces à mettre en œuvre au quotidien.

Politique adoptée par le rectorat le 29 octobre 2025

2. Portée et application de la politique de gouvernance des données au sein de l'UNIGE

Portée du document

La présente politique s'applique à l'ensemble des parties prenantes de l'Université qu'il s'agisse du corps étudiant[1], du corps professoral, du corps des collaborateurs et collaboratrices de l'enseignement et de la recherche, du personnel administratif et technique ou des partenaires et intervient à plusieurs échelles : individuelle, collective, facultaire, administrative et universitaire.

Ce document est diffusé et mis à disposition de la communauté universitaire afin d'être connu et respecté.

La présente politique de gestion des données institutionnelles prévaut sur toute politique de gestion des données antérieure.

Règle AP01 : La politique respecte le cadre légal et réglementaire en vigueur

- Le cadre légal et réglementaire s'applique quelle que soit la nature de la donnée et prévaut sur les directives UNIGE
- Cadre légal et réglementaire en vigueur :
  - Loi sur l'Université (LU) du 13 juin 2008
  - Statut de l'Université, entré en vigueur le 28 juillet 2011
  - Accord intercantonal universitaire (AIU) du 27 juin 2019
  - Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) du 5 octobre 2001
  - Règlement d'application de la Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (RIPAD) du 21 décembre 2011
  - Loi sur les archives publiques (LArch) du 1er décembre 2000
  - Règlement d'application de la Loi sur les archives publiques (RArch) du 21 août 2001
  - Loi sur la statistique fédérale (RS 431.01) et l'ordonnance du 30 juin 1993 concernant l'exécution des relevés statistiques fédéraux (RS 431.012.1)
  - Loi sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE) du 19 décembre 2003
  - Loi fédérale concernant le droit d'auteur et les droits voisins (LDA) du 9 octobre 1992
  - Toutes les lois métiers susceptibles d'avoir un impact sur le cycle de vie des données

Règle AP02 : La politique s'appuie sur les documents officiels de l'UNIGE

- Les documents officiels s'appliquant en particulier :
  - Règlement d'organisation de la gouvernance du système d'information (ROGSI) du 28 septembre 2023, disponible ici
  - La politique de protection des données personnelles, disponible ici
  - La politique de sécurité du système d'information, disponible ici
  - La politique de classification de l'information / des données, disponible ici

[1] Les principes présentés dans la présente politique s'appliquent également aux données utilisées dans le cadre de travaux pratiques et/ou de recherche conduits par des étudiant-es (enquêtes et récolte de données)

- La charte d'éthique et de déontologie des hautes écoles universitaire et spécialisée de Genève, disponible ici
- Les directives institutionnelles en matière d'intégrité dans la recherche, disponibles ici
- La politique Open Access, disponible ici
- La directive institutionnelle pour l'Archive ouverte UNIGE, disponible ici
- La politique institutionnelle sur la gestion des données de la recherche, disponible ici
- La politique de préservation des données de la recherche, disponible ici
- La politique de gestion des documents et des archives, en attente de validation

Règle AP03 : La politique doit être appliquée, promue et respectée par toutes et tous

- La politique de gestion des données est accessible et connue de l'ensemble des membres de l'UNIGE (corps professoral, collaborateurs et collaboratrices de l'enseignement et de la recherche, personnel administratif et technique, corps étudiant, etc.)

Règle AP04 : La politique est déclinée en Stratégie de gouvernance des données sur les volets fonctionnels, organisationnels et technologiques

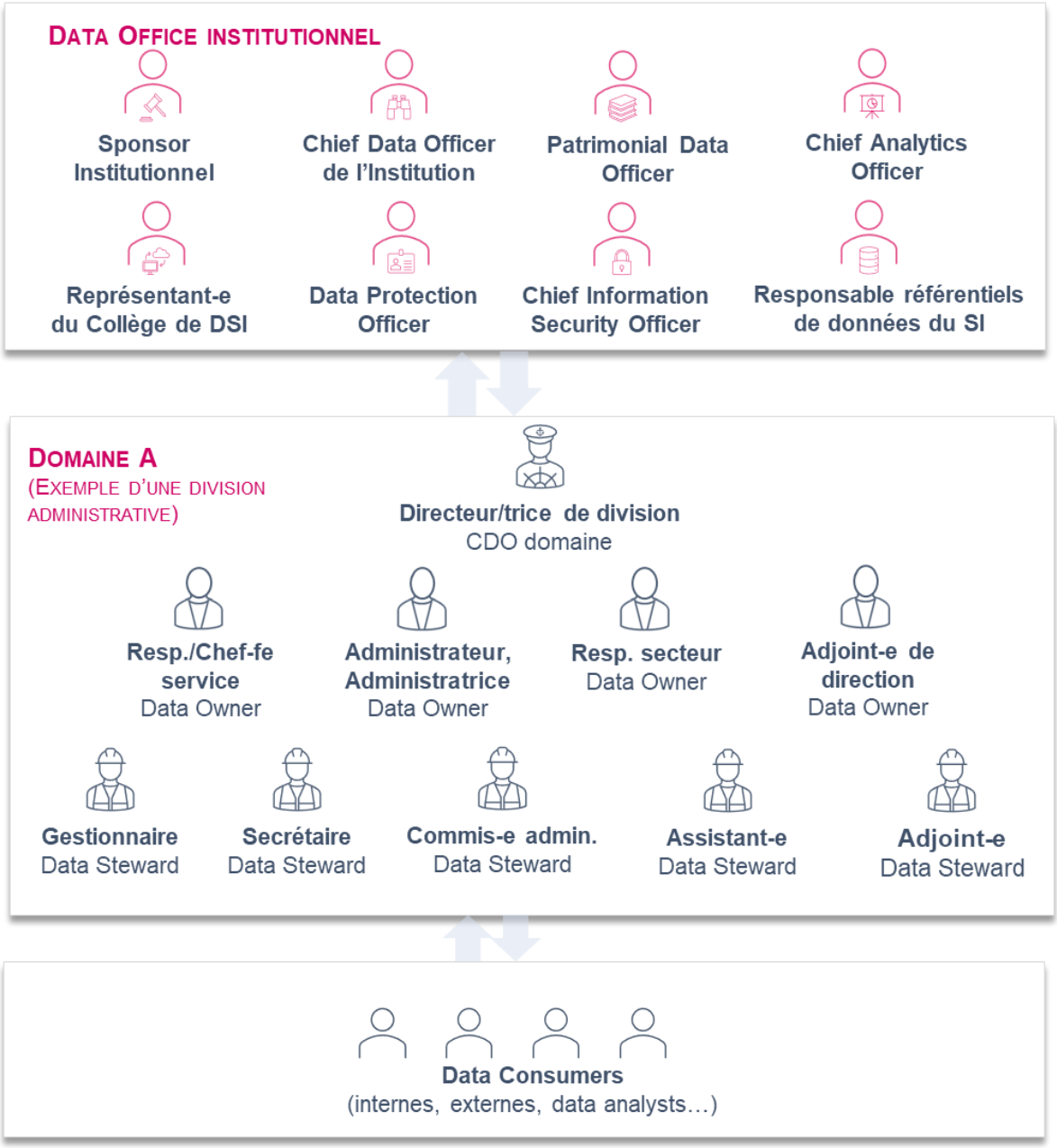
- La Stratégie de gouvernance des données est définie en accord avec :
  - Le cadre légal régissant les données en Suisse et dans le Canton de Genève,
  - La Politique de gestion des données institutionnelles,
  - Les Stratégies de l'UNIGE et des Directions Métiers et SI
- Elle est déclinée sur les volets fonctionnels, organisationnels et technologiques, en se basant sur les usages de valorisation et consultation de l'institution.

Règle AP05 : La politique repose sur la mise en œuvre opérationnelle d'une organisation technologique et humaine

- La déclinaison opérationnelle de cette politique se conforme aux règles décrites dans ce document et aux enjeux stratégiques définis
- Elle peut s'appuyer sur l'organisation déjà en place (ROGSI, Organisation Métier…)

3. Organisation et gouvernance des données

Règle OD01 : La gouvernance des données suit un organigramme défini et connu de toutes et tous



Cet organigramme illustre et formalise les multiples rôles clés au sein de l'UNIGE participant à la bonne gouvernance des données, que ce soit au niveau de leur collecte, de leur gestion, de leur mise à jour, de leur sécurisation ou de leur exploitation à des fins de prise de décision.

Il s'agit d'une recommandation de haut niveau, selon l'état de l'art. Une personne peut ainsi assumer un ou plusieurs rôles. Chaque domaine métier est tenu de s'organiser en conséquence et peut identifier les personnes ou groupe de personnes les plus à même d'occuper ces rôles. Les règles associées à chaque rôle sont décrites dans ce document et sa déclinaison opérationnelle s'appuiera en partie sur des rôles existants à l'UNIGE.

Règle OD02 : Le/la CDO institutionnel est garant-e de la politique et de sa bonne application au sein de l'institution

Le/la CDO institutionnel :

- Est nommé-e par le Rectorat
- Est responsable d'informer et de transmettre tout changement légal ou réglementaire aux CDO domaine
- Porte la vision et pilote la stratégie des données et sa mise en œuvre au sein de l'UNIGE
- S'assure de l'efficacité de l'organisation mise en place pour la gouvernance des données
- Est garant-e des évolutions de la politique de gestion des données et de son application
- S'assure des synergies entre domaines métier sur l'usage et la gestion des données
- Arbitre les activités liées à la gestion et à l'utilisation des données
- Définit un budget associé à la gouvernance des données

Règle OD03 : Le/la CDO institutionnel s'appuie sur un collectif formant le Data Office institutionnel

- Le/la *Chief Information Security Officer* (CISO)/Responsable de la Sécurité des Systèmes d'Information (RSSI) accompagne le/la CDO institutionnel sur la mise en œuvre de la stratégie de sécurité des données. Dans ce cadre, il/elle :
    - Est responsable de la définition et du pilotage du plan de sécurité des systèmes d'information
    - Conseille et forme les partenaires internes sur les risques et les mesures de protection
    - Contrôle le respect des normes et des règles de sécurité des données
    - Coordonne et supervise les actions de prévention et de réaction aux incidents de sécurité
- Le/la Data Protection Officer (DPO) accompagne le/la CDO institutionnel dans l'application de la politique de protection des données personnelles et :
    - Propose et coordonne la mise en œuvre de la politique en matière de protection des données personnelles au sein de l'UNIGE
    - Conseille et soutient les partenaires internes sur les obligations et les bonnes pratiques
    - Coordonne l'établissement et la mise à jour du registre des activités de traitement des données personnelles
    - S'assure de la conformité des traitements et contrôle le respect des principes en matière de protection des données personnelles
    - Est l'interlocuteur/trice privilégié-e des personnes concernées et du préposé cantonal (PPDT) pour tout ce qui a trait au traitement des données personnelles
- Le/la Représentant-e du Collège de DSI accompagne le/la CDO institutionnel sur l'outillage de la mise en œuvre de la politique de gestion des données et s'interface avec le Collège de DSI. Dans ce cadre il/elle :
    - Met à disposition des outils SI sur lesquels s'appuie l'ensemble du cycle de vie des données (stockage, traitement, collecte, …)
    - Coordonne le déploiement des outils SI sur les périmètres concernés, ainsi que l'infrastructure nécessaire à leur bon fonctionnement
    - Encourage l'utilisations de ces outils SI afin d'assurer la montée en compétences des personnes concernées

    - S'assure du maintien de ces outils SI en condition opérationnelle
- Le/la *Chief Analytics Officer* (CAO) accompagne le/la CDO institutionnel dans le processus d'alimentation et la valorisation des données institutionnelles. Dans ce cadre, il/elle :
    - Centralise, coordonne et propose le déploiement des solutions de mise à disposition (consultation) et d'analyse des données institutionnelles
    - Conseille et accompagne les partenaires internes sur les opportunités et les enjeux de l'analytique (collecte/alimentation, organisation, compilation et diffusion des données institutionnelles)
    - Contrôle le respect des standards de qualité et de performance des données institutionnelles, de leur alimentation à leur exploitation
- Le/la Responsable référentiel de données du SI accompagne le/la CDO dans la définition du cadre de gouvernance et de gestion des données numériques de référence. Dans ce cadre il/elle :
    - Organise le référencement des entités du SI afin d'en fournir une vision globale
    - Identifie les personnes en charge de sa mise à jour et définit avec elles les processus de revue et de mise à jour
    - Fournit un support et des recommandations auprès des responsables métiers et IT dans la mise en œuvre de la politique de gestion des données et des évolutions nécessaires
- Le/la *Patrimonial Data Officer* (PDO), en tant que responsable de la constitution, de la gestion et de la conservation des archives historiques de l'UNIGE, accompagne le/la CDO et les CDO domaines dans la gestion du cycle de vie des documents et données. À ce titre, il/elle :
    - Conseille et soutient les métiers sur les bonnes pratiques inhérentes à la gestion du cycle de vie des documents et données
    - Coordonne l'établissement, la mise à jour et la révision périodique des règles de conservation des documents et données qui définit notamment :
        - la durée d'utilité administrative et légale (DUAL) ;
        - le sort final (versement ou élimination)
    - Veille activement à la bonne application du sort final des documents et données
    - Gère les archives historiques dès leur versement et fait office d'interlocuteur/trice privilégié- e des Archives d'État de Genève

Règle OD04 : La politique est revue régulièrement selon un processus défini

- Le/la CDO institutionnel, au nom du Rectorat, est responsable de la politique de gestion des données
- Le Data Office institutionnel se réunit, à l'initiative du/de la CDO institutionnel, pour revoir la Politique de gestion des données en cas de nouvelle stratégie, de nouvelles lois ou de changements organisationnels
- La politique de gestion des données est revue annuellement afin de garantir sa mise à jour, sa conformité légale et son adéquation aux besoins métiers

Règle OD05 : La gouvernance des données est déclinée par domaine de données

- Le/la CDO institutionnel est responsable du découpage par domaine de l'institution
- Les CDO domaines identifient les objets métiers pour leur domaine

- La gouvernance des données est déclinée par domaine comme extension de cette politique. Le plan d'action de mise en œuvre par domaine ne doit pas entrer en contradiction avec la politique générale, ni soustraire les parties prenantes à des responsabilités contractuelles, légales ou sécuritaires
- Le plan de mise en œuvre de la politique de gestion des données du domaine est élaboré avec le soutien du Data Office institutionnel et l'ensemble des parties prenantes du domaine
- La déclinaison opérationnelle du domaine doit respecter tous les points énoncés dans cette politique de gestion des données

Règle OD06 : La désignation du/de la CDO domaine suit un processus défini

- Les personnes connaissant la donnée du domaine, sa définition et son cycle de vie, parce qu'elles la génèrent ou l'utilisent, désignent des personnes aptes à occuper le rôle de CDO domaine sur le périmètre du domaine concerné
- Le/la CDO institutionnel acte la désignation du CDO domaine
- Le choix du/de la CDO domaine est basé sur les aptitudes professionnelles et sur une connaissance de la politique de gestion des données

Règle OD07 : Les CDO domaine sont garant-es de la politique et de sa bonne application au sein de leur domaine

Les CDO domaine :

- Sont responsables de former et de transmettre tout changement légal aux personnes de référence du domaine
- Portent la vision et pilotent la stratégie des données au sein de leur domaine de données
- Définissent et valident les usages de valorisation des données du domaine
- S'assurent de l'efficacité de l'organisation mise en place pour la gouvernance des données
- Sont garant-es de l'application de la politique de gestion des données du domaine
- Garantissent les synergies entre les parties prenantes sur l'usage et la gestion des données au sein de leur domaine
- Peuvent s'appuyer sur les différentes instances en place (Data Office institutionnel, COCSIM, échanges avec les CDO des autres domaines) pour traiter des sujets spécifiques
- Sont accompagné-es par le/la DPO pour monter en compétence en ce qui concerne la protection des données personnelles et par le/la PDO pour ce qui est de la mise en œuvre du cycle de vie des documents et données (en particulier, la définition de la DUAL et l'application du sort final)

Règle OD08 : Une formation et des outils sont mis en œuvre

- Les CDO domaine s'assurent que les *Data Owners* bénéficient d'une formation spécifique sur la gestion, la protection et la sécurisation des données mise en œuvre par les DPO, CISO et CDO institutionnel
- Les *Data Owners* doivent actualiser leurs connaissances et leurs compétences en fonction de l'évolution des normes et des réglementations des données associées à leur périmètre

Règle OD09 : La responsabilité des données de chaque domaine est attribuée à un-e ou plusieurs Data Owners

- La nomination des *Data Owners* est basée sur leurs aptitudes professionnelles
- Les *Data Owners* sont nommé-es par les CDO domaine
- La nomination des *Data Owners* est documentée et communiquée à l'ensemble des parties prenantes
- Les *Data Owners* :
    - Sont responsables métier de l'intégrité, de la qualité, de la classification et de l'usage des données à l'intérieur de leur périmètre
    - Sont garant-es de la définition et description fonctionnelle des données
    - Fixent le cadre du cycle de vie des données et les processus de gestion associés
    - Sont responsables de faire appliquer les règles de conservation des documents et données (DUAL et sort final) et de contribuer à leur mise à jour par l'identification et le recensement des documents et données produits ou reçus dans leur périmètre
    - Contrôlent la bonne conformité des usages des données avec les règles définies et valident les demandes d'accès

Règle OD10 : Les Data Owners s'appuient sur des Data Stewards

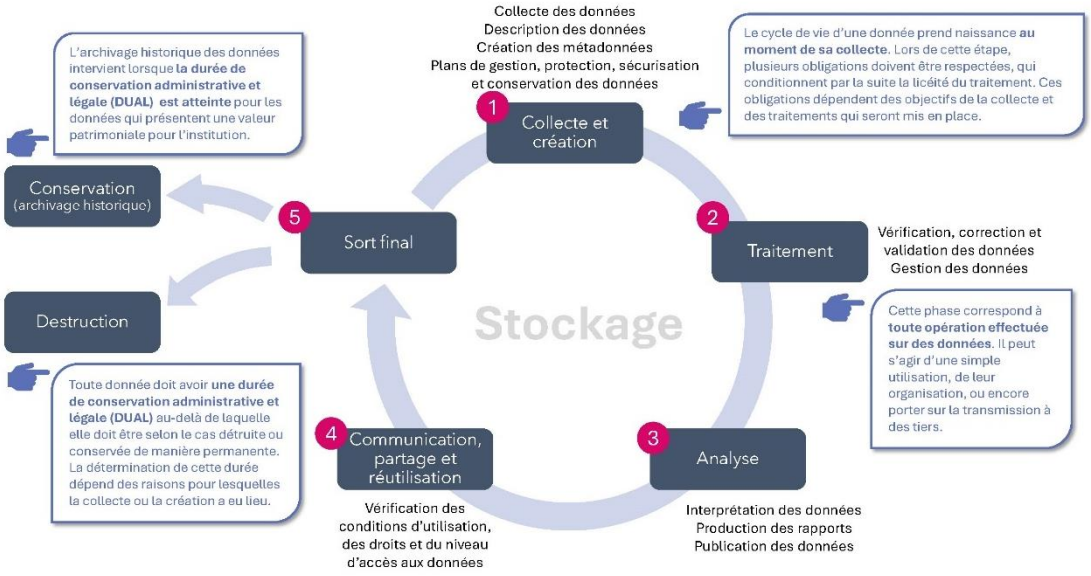
- Les *Data Owners* identifient des *Data stewards* pour les accompagner dans leurs tâches
- Les *Data Stewards* :
    - Maintiennent les référentiels à jour, assurent au quotidien la mise en qualité des données (à partir des règles définies par le/la *Data Owner*) et accompagnent les autres utilisateurs et utilisatrices sur leur usage
    - Gèrent un périmètre de données bien défini, sous le contrôle des *Data Owners*
    - Peuvent participer à la définition et à la construction des modèles de données
    - S'assurent de la bonne application de la politique de protection des données
    - S'assurent de la bonne application des règles de conservation des documents et données, et de leur sort final

Règle OD11 : La gouvernance des données par domaine relève d'un comité défini et connu de toutes et tous

- Chaque CDO domaine définit les acteurs et actrices du comité de gouvernance de leur domaine en s'appuyant sur les rôles et sachants data du domaine (*Data owners*, *Data stewards* notamment). Le/la CDO institutionnel peut être inclus à titre consultatif au Comité de gouvernance du domaine selon les besoins
- Le Comité de gouvernance du domaine arbitre les politiques locales, en particulier la cohérence avec la politique de gestion des données vis-à-vis des évolutions de la stratégie de l'institution
- Le Comité de gouvernance du domaine identifie des arbitrages à remonter au Data Office institutionnel

4. Cycle de vie, valorisation et sort final des données

Représentation des principales étapes du cycle de vie des données



Le schéma ci-dessus représente le cycle de vie des documents et données au sein de l'institution. La durée d'utilité administrative et légale (DUAL) et le sort final sont déterminés dès la collecte ou la création des documents et données selon le calendrier de conservation institutionnel. Au terme de la DUAL, les documents et données sont détruits ou archivés. Dans ce second cas, la politique de gestion des archives s'applique, sous la responsabilité du PDO. Les principes de sécurité et de protection des données s'attachent à l'ensemble du cycle de vie des données et de documents.

Règle CV01 : Les Data Owners définissent les principes et processus de gestion du cycle de vie des données du domaine

- Les *Data Owners* définissent et documentent le cycle de vie des documents et données dont ils/elles sont responsables. Pour ce faire, ils/elles sollicitent l'expertise des CDO, CISO, DPO (pour les données personnelles) et PDO (DUAL et sort final)
- Les *Data Stewards* sont responsables de mettre en œuvre et de faire respecter le cycle de vie et les processus de contrôle et de validation des données pour leur domaine métier, en collaboration avec les utilisateurs et utilisatrices des données
- Les *Data Stewards* sont responsables d'appliquer les règles de conservation des documents et données, ainsi que leur sort final (versement ou élimination), sous le contrôle et selon les modalités déterminées par le/la PDO
- Les CDO domaine déterminent le niveau de sensibilité et la classification des données en collaboration avec le/la DPO (données personnelles) et le/la CISO (politique de classification de l'information)
- Ces processus sont régulièrement revus dans une logique d'amélioration continue
- Les *Data Owners* s'assurent auprès de leur référent-e IT que les données devant être détruites du système d'information le soient

Règle CV02 : Les rôles et les responsabilités associés au cycle de vie des données doivent être respectés et impliqués lorsque nécessaire

- Les CDO domaine coordonnent l'identification des rôles et responsabilités associés au cycle de vie des données
- Parmi ces rôles, il convient d'identifier :
  - Les *Data Owners*, qui sont responsables de la définition, de la gestion du cycle de vie, de la sécurisation et de la documentation des données
  - Les *Data Stewards* qui appliquent les principes de la gouvernance des données, notamment en matière de qualité, de conformité et de conservation. Ils/elles veillent à ce que les données soient cohérentes, fiables et respectent les réglementations en vigueur
  - Les *Data Consumers* sont responsables de l'utilisation des données à des fins spécifiques. Ils/elles peuvent être des bénéficiaires internes ou externes accédant aux données via des rapports, des tableaux de bord, des applications ou pour des besoins d'analyse, d'interprétation, de mise à disposition et de valorisation (*Data Analyst*).
- Une personne au sein de l'organisation peut exercer différents rôles
- Les CDO domaine sont responsables de la bonne collaboration entre ces rôles

Règle CV03 : Les principes et processus de gestion des données doivent être partagés

Les *Data Owners* :

- S'assurent que ces principes sont accessibles aux utilisateurs et utilisatrices (*Data Stewards*, *Data Consumers*)
- Partagent ces processus avec les utilisateurs et utilisatrices (*Data Stewards*, *Data Consumers*)
- Participent aux campagnes de sensibilisation sur le cycle de vie des données et diffusent régulièrement le cadre d'utilisation des données dont ils/elles ont la responsabilité

Règle CV04 : Les Data Owners assurent l'amélioration continue du cycle de vie des données dont ils/elles sont responsables

- Les *Data Owners* évaluent régulièrement la qualité, la pertinence, la fiabilité et la sécurité des données tout au long de son cycle de vie
- Les *Data Owners* mettent en place des actions correctives ou préventives pour améliorer le cycle de vie des données et les processus de gestion associés

Règle CV05 : Les Data Owners sont garant-es de la qualité et de la traçabilité des données dont ils/elles sont responsables

- Les standards de qualité et de traçabilité des données doivent être définis en fonction des besoins et des objectifs du domaine métier par les *Data Owners*
- Les standards de qualité et de traçabilité doivent être respectés à chaque étape du cycle de vie des données

Règle CV06 : Les conditions d'utilisation et la valorisation des données s'appuient sur des services et principes transverses fournis et approuvés par l'Institution

- Pour chaque type de données, il convient de définir les besoins et les exigences en termes d'infrastructure, de sécurité, de qualité, d'interopérabilité et d'accessibilité
- Le Bureau des données institutionnelles et décisionnelles est responsable de fournir et de maintenir les services transverses nécessaires à la gestion, à l'accès et à l'exploitation des données au sein de l'institution avec le support de la DISTIC

Règle CV07 : L'utilisation des données par les Data Consumers doit être connue et validée par les Data Owners

- Pour chaque type de données, il convient de définir les objectifs associés en matière d'utilisation (contexte et finalité d'utilisation des données)
- Le niveau de qualité des données doit être suffisamment élevé pour permettre une utilisation adéquate et pertinente
- L'utilisation et la valorisation des données se font en accord avec les *Data Owners* des domaines concernés et en toute transparence
- L'accès aux données tient compte des règles et normes propres à chaque domaine
- L'utilisation et l'accès aux données dans le cadre de la recherche respectent les principes et valeurs de la science ouverte

Règle CV08 : Les Data Owners sont responsables de définir la durée de conservation des données sous leur périmètre et de veiller à la bonne application du sort final prévu

- La durée d'utilité administrative et légale (DUAL) des documents et données figurant dans le calendrier de conservation institutionnel est définie par les *Data Owners* avec l'aide du/de la PDO
- Le sort final des documents, données et métadonnées qui n'ont plus d'utilité administrative et légale est déterminé par le/la PDO et est inscrit dans le calendrier de conservation institutionnel. Deux cas de figure sont prévus :
    - L'élimination des documents et données ;
    - Le versement des documents et données aux AAP pour leur conservation permanente
- Les *Data Owners* sont responsables de faire appliquer le sort final des documents et données sous leur périmètre, sous le contrôle et selon les modalités déterminées par le/la PDO

Règle CV09 : La documentation sur les données doit être accessible et partagée

- Les *Data Owners* travaillent avec les personnes expertes du domaine pour proposer une définition de la donnée compréhensible par l'ensemble des parties prenantes. Cette définition et sa nomenclature doivent être précises et contextualisées
- Les *Data Owners* sont responsables de fournir les informations nécessaires à la documentation des données, notamment : définition, sensibilité, structure, droits d'accès, utilisation des données (stockage et application consommatrices), rôles, règles de conservation (DUAL et sort final)
- Les CDO Domaines, avec l'aide du Data Office institutionnel, fournissent aux *Data Owners* le moyen de documenter leurs données. Ce moyen constitue alors la seule source fiable et prévaut sur toute autre source de documentation des données

- Les *Data Owners* transmettent régulièrement au/à la responsable Référentiel SI la documentation élaborée en vue d'alimenter et de maintenir la cartographie des données à jour
- Les *Data Owners* s'assurent de la mise à jour de la documentation selon les évolutions de l'UNIGE (réorganisation, nouvelles stratégies, cadre légal…)
- Les *Data stewards* mettent à jour la documentation

Règle CV10 : Le partage des données respecte le cadre légal et les dispositions de l'UNIGE

- L'article 320 du code pénal s'applique dans le cadre de la révélation des données soumises au secret de fonction
- La communication des données personnelles, y compris au sein de l'institution, est régie par l'article 39 LIPAD
- Le partage et la consultation des archives historiques est régie par la Loi sur l'archivage public (LArch), et en particulier les art. 11, 12, 13 et 14, qui s'appliquent de façon coordonnée avec la Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD)
- Le partage des données, en interne UNIGE, s'effectue en accord avec la législation et :
    - Les règles de classification des données
    - Les droits d'accès de la personne demandant d'accéder aux données
- Le partage de la donnée peut nécessiter une demande d'accès préalable auprès du *Data Owner* responsable de cette donnée

Règle CV11 : Les données doivent avoir une procédure d'autorisation et de révocation d'accès formalisée

- Les *Data Owners* :
    - Sont responsables de statuer sur le partage en interne des données et des conditions sous lesquelles ce partage est autorisé
    - Définissent les règles d'accès aux données
    - Procèdent à la revue régulière des accès délivrés
    - Accordent ou non l'accès aux personnes ayant formulé une demande d'accès
    - Révoquent l'accès lorsque la situation d'une personne évolue (par exemple, évolution ou changement de fonction)
- Les demandes d'accès aux données et leur octroi doivent être tracées
- Le partage des données s'accompagne d'un rappel des principes liés à leur utilisation, leur traitement et leur stockage.

5. Sécurité et protection des données

Règle SP01 : La politique s'appuie sur la politique de sécurité du système d'information de l'UNIGE

- Les données sont protégées à un niveau adéquat, c'est-à-dire adapté à leur niveau de sensibilité
- La sensibilité de chaque information est déterminée et classée dans l'une des trois catégories suivantes :
    - Informations à sensibilité faible : publiques ou sans enjeu de confidentialité
    - Informations à sensibilité moyenne : pas accessibles au public ou dont la perte de confidentialité, d'intégrité ou de disponibilité pourrait avoir un impact négatif moyen pour l'UNIGE
    - Informations à sensibilité élevée : protégées légalement, juridiquement, contractuellement ou stratégiquement. La perte de confidentialité, d'intégrité ou de disponibilité pourrait avoir un impact négatif important pour l'UNIGE

  Les données privées sont des données personnelles sans lien avec l'UNIGE. Elles doivent rester du domaine privé.
- En fonction de cette classification, une liste des services numériques de l'UNIGE est disponible ici
- La politique de sécurité du Système d'information doit être disponible et à jour

Règle SP02 : La politique s'appuie sur la politique de protection des données personnelles de l'UNIGE

- Principes de protection des données personnelles

  Les domaines métiers sont tenus de respecter les principes suivants en matière de traitement des données personnelles (art. 35 LIPAD[2]), principes qui contribuent au respect du droit à l'intégrité numérique de la personne concernée (art. 21A Cst-GE) :

    - *Licéité (art. 35 al. 1 LIPAD)*
      Le traitement de données personnelles effectué par le domaine ne peut se faire que s'il est licite : il ne doit pas enfreindre une autre norme du droit suisse visant directement ou indirectement à protéger la personnalité
    - *Bonne foi et proportionnalité (art. 35 al. 2 LIPAD)*
      Le principe de proportionnalité doit être respecté à toutes les étapes du traitement, y compris au stade initial lorsqu'il est décidé de procéder ou non au traitement des données (principe d'évitement). Seules les données qui sont absolument nécessaires (principe de minimisation) et pertinentes pour atteindre l'objectif fixé peuvent être traitées. Le principe de minimisation s'applique également à l'accès aux données et à leur durée de conservation.
    - *Finalité et reconnaissabilité (art. 35 al. 3 LIPAD)*
      Les données collectées ne peuvent être traitées que pour une finalité déterminée, indiquée lors de leur collecte, découlant des circonstances ou prévue par la loi. Les données collectées doivent ensuite être traitées de manière compatible avec la finalité initiale. Par ailleurs, le but et les méthodes du traitement, ainsi que les catégories de

[2] Selon la L13347 du 4 mai 2024 modification la LIPAD

données collectées et traitées, doivent être globalement reconnaissables pour les personnes concernées.

- *Conservation, destruction, effacement et anonymisation (art. 35 al. 4 LIPAD)*
  Le domaine détruit, efface ou rend anonymes les données personnelles dès qu'elles ne sont plus nécessaires au regard des finalités du traitement, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi. Cela implique que le responsable du traitement fixe des délais de conservation.
- *Exactitude (art. 35 al. 5 et 6 LIPAD)*
  Quiconque traite des données personnelles doit s'assurer qu'elles sont exactes. Ce terme signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.

- Droits des personnes concernées

  Les CDO domaine mettent en œuvre les moyens leur permettant d'assurer les droits prévus par les articles 44 et suivants LIPAD pour les personnes concernées. En justifiant de leur identité, ces dernières sont notamment légitimées à :

  - Demander si nous traitons des données personnelles à leur sujet
  - Recevoir les informations nécessaires à la mise en œuvre de leurs droits en matière de protection des données personnelles. A leur demande, elles reçoivent notamment les informations suivantes :
    - le responsable du traitement;
    - les données personnelles traitées;
    - la finalité du traitement;
    - la durée de conservation des données personnelles, ou, si cela n'est pas possible, les critères pour fixer cette dernière;
    - les informations disponibles sur l'origine des données personnelles, dans la mesure où ces données n'ont pas été collectées auprès des personnes concernées;
    - le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont communiquées
  - Exiger à propos des données la concernant que nous :
    - Nous abstenions de procéder à un traitement illicite
    - Mettions fin à un traitement illicite et en supprimions les effets
    - Constations le caractère illicite du traitement
    - Nous abstenions de les communiquer à des personnes de droit privé à des fins d'exploitation commerciale.
  - Sauf disposition légale contraire, elles peuvent demander que nous :
    - Effacions ou détruisions les données personnelles qui ne sont pas nécessaires pour les finalités pour lesquelles elles ont été collectées;
    - Rectifions, complétions ou mettions à jour les données personnelles qui sont respectivement inexactes, incomplètes ou dépassées;
    - Fassions figurer, en regard des données personnelles dont ni l'exactitude ni l'inexactitude ne peuvent être prouvées, une mention appropriée, à transmettre également lors de leur communication éventuelle;
    - Nous abstenions de communiquer les données personnelles qui ne répondent pas aux exigences de qualité visées à l'article 35 LIPAD

- Nous publions nos décisions prises à la suite de leur requête ou la communiquions aux institutions ou tiers ayant reçu de notre part des données ne répondant pas aux exigences de qualité visées à l'article 35 LIPAD

Règle SP03 : Les Data Owners classifient les données de leur domaine selon leur niveau de sensibilité

- Les CDO domaine et les *Data Owners* utilisent l'échelle de classification qui distingue les données selon leur degré de sensibilité
- Les *Data Owners* documentent et communiquent le niveau de sensibilité des données aux parties prenantes

Echelle de classification du niveau de sensibilité des données

Sensibilité faible	Sensibilité moyenne	Sensibilité élevée
Les actifs sont classés comme à faible risque s'ils ne sont pas considérés comme à risque modéré ou élevé, et : 1. Les actifs sont destinés à la divulgation publique, ou 2. La perte de confidentialité, d'intégrité ou de disponibilité des actifs n'aurait aucun impact négatif sur la mission, la sécurité, les finances ou la réputation de l'UNIGE. Pour les données destinées au public, des garanties en termes d'intégrité et de disponibilité des données sont nécessaires.	Les actifs sont classés comme à risque modéré s'ils ne sont pas considérés comme à haut risque, et : 1. Les actifs ne sont généralement pas accessibles au public, ou 2. La perte de confidentialité, d'intégrité ou de disponibilité des actifs pourrait avoir un impact négatif limité sur la mission, la sécurité, les finances ou la réputation de l'UNIGE. L'accès à ce type d'actifs est limité à la communauté universitaire ou à un sous-ensemble de celle-ci, ou à des tiers clairement identifiés et légitimes.	Les actifs sont classés comme à haut risque si : 1. L'Université doit protéger les actifs en vertu d'une loi, d'un règlement, d'un contrat, d'une entente de confidentialité ou de par leur valeur stratégique 2. L'UNIGE est tenue de déclarer des accès inappropriés à ces données 3. La perte de confidentialité, d'intégrité ou de disponibilité des actifs pourrait avoir un impact négatif important sur la mission, la sécurité, les finances ou la réputation de l'UNIGE.

Règle SP04 : Les Data Owners établissent la criticité des données du domaine

- Les CDO domaine établissent, avec l'aide des *Data Owners*, le niveau de criticité cible des données du domaine en fonction des contraintes métier et des grilles d'impact en termes de disponibilité et intégrité des données
- Les Data Owners doivent documenter et communiquer le niveau de criticité des données dont ils/elles ont la responsabilité aux parties prenantes

Règle SP05 : Les Data Owners établissent les exigences de traçabilité des données de leur domaine

- Les *Data Owners* :
  - Assurent la traçabilité des données dont ils/elles ont la responsabilité
  - Documentent et communiquent le besoin en traçabilité des données dont ils/elles ont la responsabilité aux parties prenantes

- Identifient les exigences métier de traçabilité des données

Règle SP06 : Les CDO domaine renseignent le Registre des activités de traitement des données personnelles

- Les CDO domaine, avec le support du DPO, déclarent et mettent à jour dans le Registre des activités de traitement (art. 43 LIPAD) les traitements des données personnelles dont ils/elles sont responsables
- Les *Data Owners* fournissent notamment les informations suivantes :
  - L'identité du responsable du traitement (CDO domaine)
  - La dénomination, la base légale et la finalité du traitement
  - Une description des catégories des personnes concernées et des catégories des données personnelles traitées
  - Les catégories des destinataires
  - Le cas échéant, l'identité et les coordonnées des autres responsables du traitement et la répartition des responsabilités
- Les *Data Owners* se tiennent à disposition notamment pour fournir les informations additionnelles suivantes :
  - Le délai de conservation des données personnelles ou les critères pour déterminer leur durée de conservation
  - Les mesures techniques et organisationnelles en place pour protéger les données personnelles
  - En cas de communication de données personnelles à l'étranger, le nom de la corporation ou de l'établissement de droit public étranger destinataire
  - Le cas échéant, l'identité et les coordonnées des sous-traitants

Règle SP07 : Le CISO définit, met à disposition et maintient des mesures de protection des données applicables par niveaux de sensibilité et par étapes du cycle de vie des données

- Le CISO :
  - Définit des mesures de sécurité des données qui couvrent les aspects techniques, organisationnels et humains de la protection des données
  - Communique ces mesures de sécurité aux parties prenantes, notamment les CDO domaine et les *Data Owners*, et s'assure qu'elles sont respectées et contrôlées
  - Fournit une liste des outils numériques qui garantissent la sécurité des données selon leur niveau de sensibilité et des standards minimaux de sécurité pour les actifs du SI

Règle SP08 : Les CDO domaine et les Data Owners appliquent ou font appliquer les mesures de protection adaptées au niveau de sensibilité des données dont ils/elles ont la responsabilité

- Les CDO domaine et les *Data Owners* :
  - Identifient les mesures de protection nécessaires à chaque catégorie de données qu'ils/elles détiennent ou traitent
  - Appliquent ou s'assurent de l'application des mesures de protection applicables, notamment par les partenaires techniques

- S'appuient sur les standards minimaux de sécurité pour sélectionner les mesures de protection adaptées au niveau de sensibilité des données préalablement défini. Le CISO peut également être sollicité si des mesures particulières sont nécessaires
- Sollicitent l'avis du CISO pour toute question relative à la sécurité des données, notamment lors de l'évaluation des risques ou de la conception d'un nouveau système de gestion des données

Glossaire

a) Objets liés à la politique de gestion des données

Archives patrimoniales : ensemble des documents et données produits ou reçus dans le cadre des activités de l'UNIGE, quels qu'en soient la date, le type ou le support, et destinés à la conservation à long terme en raison de leur valeur archivistique - juridique, politique, économique, historique, sociale ou culturelle.

Catalogue de données : répertorie et décrit les ensembles de données au sein d'un domaine en fournissant aux utilisateurs et utilisatrices une vue d'ensemble des données disponibles, ainsi que des informations sur leurs définition, modèle, droits d'accès et utilisation potentielle.

Cartographie du SI : inventaire institutionnel des entités de données, des applications qui les exploitent, des technologies sous-jacentes offrant une vue d'ensemble des éléments collectés et de leurs traitements.

Cycle de vie : ensemble des étapes que franchit un document ou une donnée, de sa collecte ou de sa création jusqu'à sa conservation permanente ou à sa destruction.

Domaines de données métier : un domaine de données est un groupe de données liées par un thème, un sujet ou un contexte commun. Il peut avoir des sous-domaines plus précis sous la responsabilité d'un-e ou de plusieurs *Data Owners*, qui garantissent la qualité, la sécurité et la gouvernance des données de leur domaine.

Données de recherche : des « enregistrements factuels (chiffres, textes, images et sons), qui sont utilisés comme sources principales pour la recherche scientifique et sont généralement reconnus par la communauté scientifique comme nécessaires pour valider des résultats de recherche »[3]. Les données de recherche sont produites par la plupart des disciplines et domaines de recherche et leur format peut varier (documents, photographies, sondages/enquêtes, codes informatiques, bibliographies, bases de données, etc.)[4].

Donnée institutionnelle : un élément d'information est qualifié de donnée institutionnelle s'il est engendré par les opérations courantes et les activités académiques et administratives de l'UNIGE, s'il sert à la planification, la gestion, l'exploitation, le contrôle ou la vérification d'une entité organisationnelle, s'il porte sur un domaine de l'UNIGE (étudiantes et étudiants, personnel, finances, logistique, activités de recherche). L'usage des données institutionnelles peut être interne (données utilisées par le personnel de l'UNIGE dans le cadre de l'exercice de leur fonction), à usage restreint (contraintes légales – par exemple LIPAD –, réglementaires, éthiques, de sécurité), et à usage public. Ceci inclut également les documents, physiques ou numériques, produits, gérés et utilisés par l'institution.

Données personnelles : toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable[5].

Données personnelles sensibles (au sens de la loi[6]) : données personnelles sur :

1. les opinions ou activités religieuses, philosophiques, politiques ou syndicales,
2. la santé, la sphère intime ou l'origine raciale ou ethnique,
3. des mesures d'aide sociale,

[3] Principes et lignes directrices de l'OCDE pour l'accès aux données de la recherche financée sur fonds publics
[4] Identifier les données de recherche https://www.UNIGE.ch/researchdata/fr/planifier/identifier-donnees-de-recherche/
[5] Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD)
[6] Selon L13347 du 3 mai 2024 modifiant la LIPAD

4. des poursuites ou sanctions pénales ou administratives,
5. les données génétiques,
6. les données biométriques identifiant une personne physique de façon unique.

Durée d'utilité administrative et légale (DUAL) : durée pendant laquelle les documents et données doivent être conservés et rester accessibles pour des raisons administratives (DUA) et légales (DUL). Au terme de cette période, les documents et données sont soit éliminés, soit versés aux Archives administratives et patrimoniales (AAP).

Qualité : la qualité est le degré de conformité d'une donnée à un ensemble de critères définis au préalable, tels que la pertinence, l'exactitude, l'exhaustivité, la cohérence, l'actualité ou l'accessibilité. Elle permet de mesurer et d'améliorer la fiabilité, l'utilité et la crédibilité des données.

Référentiel de classement et de gestion des données et des documents : outil de pilotage des documents et des données qui associe le plan de classement et les règles de conservation. Le plan de classement structure l'organisation des documents et données de l'UNIGE en fonction de ses activités au sein de séries ; les règles de conservation assignent à chaque série une durée d'utilité administrative et légale (DUAL) et un sort final.

Sort final : résultat de l'évaluation de la valeur archivistique des documents et données selon laquelle les documents et données sont, au terme de leur durée d'utilité administrative et légale (DUAL), soit éliminés, soit versés aux Archives administratives et patrimoniales (AAP).

Traçabilité : capacité à connaître la composition, l'origine, le parcours et les transformations d'une donnée tout au long de son cycle de vie. La traçabilité permet de garantir la conformité, la sécurité et la fiabilité des données.

b) Rôles impliqués dans la gestion des données

CDO (*Chief Data Officer*) : le ou la CDO porte la vision et pilote la stratégie des données, en définit et en valide les usages de valorisation. Il/elle s'assure de l'efficacité de l'organisation mise en place pour la gouvernance des données et garantit l'application de la politique de gestion des données.

DPO (*Data Protection Officer*) : le ou la DPO[7] est responsable du maintien et de la bonne application de la politique de protection des données personnelles.

CISO (*Chief Information Security Officer*) : dans le cadre de cette politique le ou la CISO est responsable du maintien et de la bonne application de la politique de sécurité du Système d'information et de la politique de classification de l'information.

Représentant-e du Collège de DSI : est le point de contact privilégié du Collège de direction du SI et assure l'interface ainsi que la cohérence entre la politique institutionnelle de gestion des données et la gouvernance SI.

PDO (*Patrimonial Data Officer*) : est responsable de la constitution, de la gestion et de la conservation des archives patrimoniales de l'UNIGE ; à ce titre, il/elle accompagne le/la CDO institutionnel et les CDO domaines en ce qui concerne la gestion du cycle de vie des documents et données à travers la définition de leur durée d'utilité administrative et légale (DUAL) et de leur sort final.

CAO (*Chief Analytics Officer*) : est responsable de fournir un accès aux données institutionnelles à des fins de gouvernance et de prise de décision, en respect des principes de protection et de sécurité des données. Le/la CAO participe à la structuration des données et à la conception de modèles en vue de

[7] Conseillère ou conseiller LIPAD, selon art. 50 de la L13347 du 3 mai 2024 modifiant la LIPAD

leur exploitation. Il/elle accompagne les métiers et les conseille en matière de reporting institutionnel et d'exploitation de données à des fins statistiques.

Responsable référentiels des données du SI : met en place et tient à jour la cartographie des données du SI et offre une vue centralisée de ces dernières.

CDO Domaine (*Chief Data Officer Domaine*)**:** Les CDO Domaine déclinent et garantissent l'application de la politique de gestion des données de leur domaine. Les CDO Domaine en définissent et en valident les usages de valorisation, tout en s'assurant de l'efficacité de l'organisation mise en place dans leur domaine.

Data Owners : Les *Data Owners* sont responsables métier de l'intégrité, de la qualité, de la classification, de l'usage, de la conservation et de l'application du sort final des données au sein de leur périmètre. Les *Data Owners* sont responsables de la définition et de la description fonctionnelle de la donnée. Ils/elles mettent en œuvre et pilotent la gouvernance du cycle de vie des données et les processus de gestion associés.

Data Stewards : Les *Data Stewards* assurent l'application des règles de gestion définies par les *Data Owners*, gèrent un périmètre de données bien défini sous le contrôle des *Data Owners* et s'assurent de la bonne application de la politique de protection des données.

Data Consumers : les *Data Consumers* sont les utilisateurs et utilisatrices finales des données produites ou collectées par l'ensemble des entités. Les *Data Consumers* accèdent aux données selon leurs besoins et leurs droits d'accès, exploitent les données pour réaliser des analyses, des rapports, des tableaux de bord ou des applications et contribuent à l'amélioration de la qualité et de la valeur des données en signalant les anomalies ou les opportunités.