Politique de gestion des données institutionnelles

de l'Université de Genève

UNIVERSITÉ DE GENÈVE

UNIVERSITÉ DE GENÈVE

Table des matières

UNIVERSITÉ DE GENÈVE

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 et 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	• *Description 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

Pour faciliter la lecture et la compréhension de ce document, l'ensemble des principes et règles en matière de gestion des données sont décrits et détaillés dans un document séparé (*Règles applicables en matière de gestion des données institutionnelles*).

UNIVERSITÉ DE GENÈVE

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.

Respect du 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

Documents officiels de l'UNIGE sur lesquels la politique s'appuie

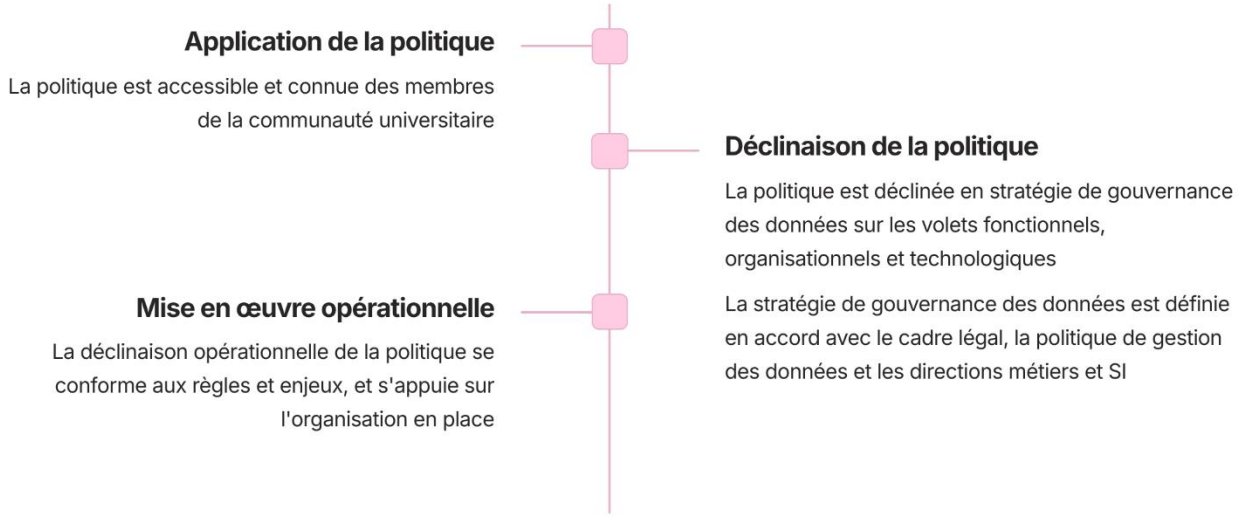
- Les documents officiels s'appliquant en particulier :
  - Règlement d'organisation de la gouvernance du système d'information (ROGSI) du 28 septembre 2023, disponible ici
  - La politique de protection des données personnelles, disponible ici
  - La politique de sécurité du système d'information, disponible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

La politique de gestion des données institutionnelles de l'UNIGE est appliquée, promue et respectée par l'ensemble de la communauté universitaire. Elle est accessible à toutes et tous et s'intègre dans une stratégie de gouvernance des données, alignée sur le cadre légal suisse et genevois, ainsi que sur les stratégies institutionnelles. Cette stratégie se décline selon des dimensions fonctionnelles, organisationnelles et technologiques, en tenant compte des usages de l'institution. La mise en œuvre opérationnelle repose sur une organisation technologique et humaine adaptée, s'appuyant sur les structures existantes pour garantir son application efficace et cohérente.

Les règles *AP03, AP04, AP05* décrivent les modalités d'application de la politique

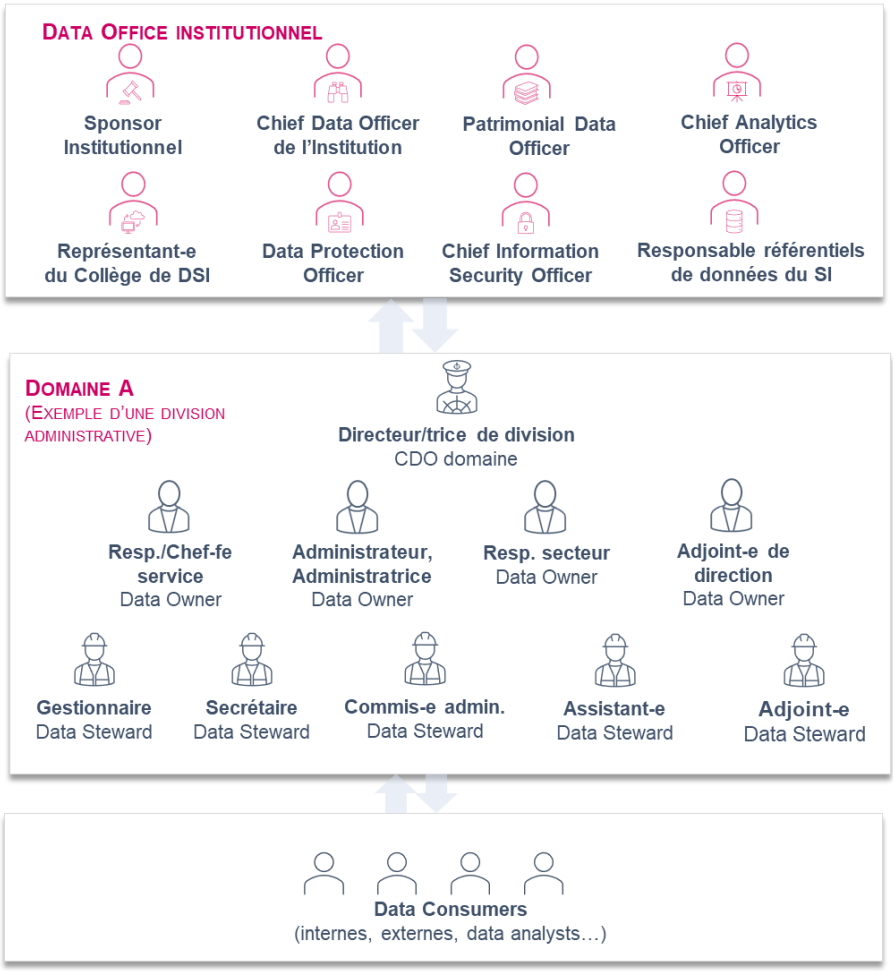


S'agissant des données de la recherche, se référer aussi à la *Politique institutionnelle sur la gestion des données de la recherche* pour des aspects plus spécifiques (Data management plan, responsabilité des chercheurs et chercheuses)

Organisation et gouvernance des données

Organigramme de gouvernance des données

La gouvernance des données suit un organigramme défini et connu de toutes et tous (*règle OD01*).



Le schéma ci-dessus illustre un exemple d'organisation au sein d'une division administrative. La distribution des casquettes suit l'organisation hiérarchique, ce qui n'est pas systématiquement le cas ailleurs et/ou dans une vision transverse des métiers.

Par exemple

Au sein de la Division de la formation et des étudiant-es, le responsable du service des immatriculations est le *Data Owner* pour les données de son périmètre d'activité. Les personnes rattachées à son service et qui traitent au quotidien des données et documents, en tant que *Data Stewards*, appliquent les règles et principes qu'il a fixés en matière de gestion des données.

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 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.

Rôles composant le Data Office institutionnel

Le/la CDO institutionnel est garant-e de la politique et de sa bonne application au sein de l'institution et s'appuie sur un collectif formant le Data Office (*règle OD02,OD03*).

Les rôles du Data Office couvrent la stratégie, la sécurité, la protection et la gestion des données dans l'organisation, chaque fonction ayant des responsabilités spécifiques pour assurer une gouvernance des données efficace et conforme.

1 Chief Data Officer (CDO) institutionnel

· 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 et des synergies entre domaines métier sur l'usage et la gestion des données

· Est garant-e des évolutions de la politique de gestion des données et de son application

2 Chief Information Security Officer (CISO)

· Définit et pilote le plan de sécurité des SI

· Conseille et forme les partenaires sur les risques et les mesures de protection

· Contrôle le respect des normes et des règles de sécurité

· Coordonne et supervise les actions de prévention et de réaction aux incidents de sécurité

3 Data Protection Officer (DPO)

· Propose et coordonne la mise en œuvre de la politique de protection des données personnelles

· Conseille et soutient sur les obligations et bonnes pratiques et s'assure de la conformité des traitements

· Coordonne l'établissement et la mise à jour du registre des activités de traitement 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

4 Représentant-e du Collège de DSI

· Met à disposition des outils SI sur lesquels s'appuie l'ensemble du cycle de vie des données (collecte, stockage, traitement, ...)

· Coordonne le déploiement des outils SI sur les périmètres concernés

· Encourage l'utilisation de ces outils SI afin d'assurer la montée en compétences des personnes concernées

5 Chief Analytics Officer (CAO)

· Centralise, coordonne et déploie les solutions d'analyse des données

· Conseille et accompagne les partenaires sur les enjeux de l'analytique

· Contrôle la qualité et la performance des données

6 Responsable référentiel de données du SI

· Organise le référencement des entités du SI pour en fournir une vision globale

· Identifie les responsable et les aide à définir les processus de revue et de mise à jour

· Fournit un support et des recommandations auprès des responsables métiers et IT

7 Patrimonial Data Officer (PDO)

· Conseille et soutient les métiers sur la gestion du cycle de vie des documents et données

· Coordonne l'établissement et la révision des règles de conservation

· Veille à l'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

Rôles clefs et actions – Mise en œuvre de la politique par domaine de données

Les règles *OD07, OD08, OD09, OD10* identifient les rôles et définissent les responsabilités dans la mise en œuvre de la politique de gestion des données institutionnelles au niveau d'un domaine

Stratégie

CDO Domaine

Garant-e de la politique et de sa bonne application au sein du domaine

- Définit et pilote la stratégie des données du domaine
- Définit et valide les usages de valorisation des données
- Est garant-e de l'efficacité de l'organisation pour la gouvernance des données de son domaine, des synergies entre parties prenantes sur l'usage et la gestion des données
- S'appuie sur les instances existantes (Data Office, COCSIM, CDO autres domaines)

Mise en oeuvre

Data Owners

Responsable métier d'un ou de plusieurs sous-domaines de données

- Est responsable de l'intégrité, de la qualité, de la classification et de l'usage des données
- Est garant-e de la définition et description fonctionnelle des données
- Fixe le cadre du cycle de vie des données et les processus associés
- Fait appliquer les règles de conservation (DUAL et sort final)
- Contrôle la conformité des usages des données et valide les demandes d'accès

Application

Data Stewards

Assure l'application des règles de gestion définies par le Data owner

- Maintient les référentiels à jour, met en qualité les données
- Gère un périmètre de données défini, sous contrôle du Data Owner
- Participe à la définition et construction des modèles de données
- Veille à la bonne application de la politique de protection des données et des règles de conservation des documents et données et de leur sort final

Par exemple

Le chef du service des aides financières en tant que *Data Owner* pour les données de son périmètre d'activité a mis en place un processus de mise en qualité des données comprenant un contrôle régulier du niveau de qualité (exactitude et complétude des informations). Les gestionnaires rattaché-es à son service, en tant que *Data Stewards*, appliquent les mesures visant à garantir un niveau de qualité des données suffisant (double contrôle des informations au moment de la saisie, par exemple). Par ailleurs, ces personnes ont la charge d'exécuter les listes de contrôle et de corriger les erreurs relevées.

Les points clefs de la politique et de son organisation

Les règles *OD04, OD05, OD06, OD08, OD11* décrivent le processus de revue de la politique institutionnelle, son découpage par domaine de données et la formation et les outils mis en œuvre

Revue régulière de la politique

Le/la CDO institutionnel révise la politique de gestion des données annuellement pour garantir sa mise à jour et sa conformité

Gouvernance déclinée par 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

Désignation du CDO Domaine

Sélection basée sur les aptitudes professionnelles et la connaissance de la politique de gestion des données

Les CDO domaines identifient les objets métiers et déclinent la gouvernance spécifique à leur domaine avec le soutien du Data Office

Comité de gouvernance du domaine

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. 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

Formation et outils

Des formations et outils spécifiques sur la gestion, la protection et la sécurisation des données sont mises en œuvre avec le soutien du Data Office

Par exemple

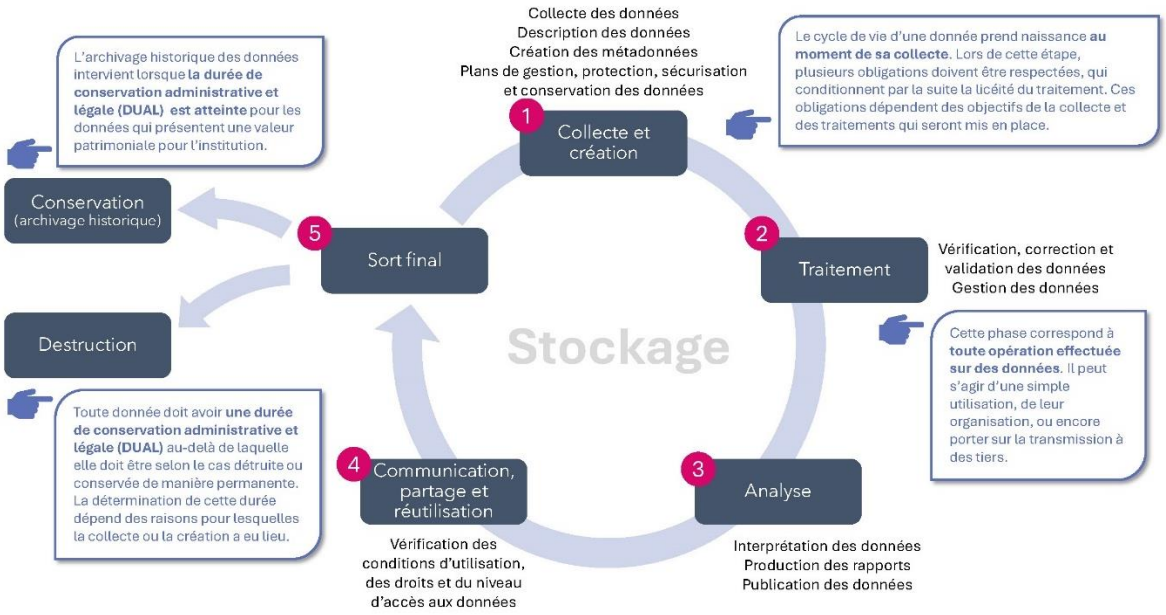
La Directrice de la division des ressources humaines, en tant que CDO domaine, propose d'organiser deux ou trois fois par an une séance dédiée au traitement des évolutions en matière de gestion des données au niveau de son domaine avec la participation des responsables de secteur (*Data Owners*). Ces moments d'échange, qui peuvent être intégrés à des séances existantes, permettent de discuter des problématiques liées à la gestion des données et de passer en revue les évolutions du cadre légal, du cadre institutionnel et du cadre technique.

La Directrice de la division de la formation et des étudiant-es, en tant que CDO domaine, veille à ce que les *Data Owners* et *Data Stewards* soient formé-es sur les bonnes pratiques et suivent les séances d'information et de sensibilisation à la gestion des données.

Cycle de vie, valorisation et sort final des données

La gestion du cycle de vie des données est un élément central de la politique de gestion des données institutionnelles. Elle vise à encadrer l'ensemble des étapes, de la création à l'archivage ou la destruction des données, en garantissant leur qualité, leur sécurité et leur accessibilité. Dès leur création/récolte, les données doivent être documentées et stockées selon des standards institutionnels et légaux afin d'en assurer l'intégrité et la réutilisation. Durant leur exploitation, des mécanismes de gouvernance doivent permettre de contrôler leur usage et leur partage dans le respect des cadres réglementaires et légaux, notamment en matière de protection des données sensibles. La conservation à long terme repose sur des stratégies adaptées, assurant la pérennité et la disponibilité des données pertinentes pour la recherche, l'enseignement et l'administration. Cette approche globale permet d'optimiser la valorisation des données tout en garantissant leur conformité aux exigences institutionnelles et éthiques.

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.

Pour plus d'informations ou en cas de questions :

- Sur la gestion des données de recherche https://www.unige.ch/researchdata/fr/accueil/
- Sur les services numériques https://catalogue-si.unige.ch/#filters=.cat__15&search=

Rôles clefs et actions – Cycle de vie des données

Les règles *CV01, CV02, CV03, CV04, CV05, CV06, CV07, CV08, CV09, CV10 et CV11* identifient les rôles et définissent les responsabilités des actions à mettre en œuvre en matière de cycle de vie des données (création/collecte, traitement, partage, conservation)

Stratégie	Mise en oeuvre	Application
CDO Domaine **Garant-e de la politique et de sa bonne application au sein du domaine** • Coordonne l'identification des rôles et responsabilités associés au cycle de vie des données • Détermine 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) • Est responsable de la bonne collaboration entre ces rôles	**Data Owners** **Responsable de la définition, de la gestion du cycle de vie, de la sécurisation et de la documentation des données** • Définit et documente le cycle de vie des documents et données dont il/elle est responsable • Assure l'amélioration continue du cycle de vie des données dont il/elle est responsable • Partage les processus de gestion avec les utilisateurs et utilisatrices (*Data Stewards*, *Data Consumers*) • Est garant de la qualité et de la traçabilité des données • Est responsable de statuer sur le partage des données et des conditions sous lesquelles ce partage est autorisé • Définit la durée de conservation des données et veille à la bonne application du sort final prévu • Participe aux campagnes de sensibilisation sur le cycle de vie des données et diffuse régulièrement le cadre d'utilisation des données	**Data Stewards** **Applique les principes de la gouvernance des données, notamment en matière de qualité, de conformité et de conservation** • Met en œuvre et fait respecter le cycle de vie et les processus de contrôle et de validation des données pour son domaine métier • Met à jour la documentation • Rappelle les principes liés à l'utilisation, au traitement et au stockage des données lors du partage avec des tiers • Applique 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 *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 points clefs du cycle de vie des données

Définition et Documentation

Les *Data Owners* sont responsables de la définition et de la documentation du cycle de vie de chaque ensemble de données sous leur responsabilité. Ce processus inclut la collaboration avec différentes expertises : CDO, CISO, DPO et PDO

Classification et Sensibilité

Les CDO Domaine, en partenariat avec le/la DPO et le/la CISO, déterminent le niveau de sensibilité de chaque ensemble de données et appliquent la classification appropriée

Accès et Partage

Le partage des données se fait en respect du cadre légal et des dispositions de l'UNIGE

En interne, le partage de données s'effectue en accord avec la législation, les règles de classification des données et les droits d'accès de la personne demandant l'accès aux données

⚠ Article 320 du code pénal (révélation des données soumises au secret de fonction)
Article 39 LIPAD (communication des données personnelles)
Articles 11, 12, 13 et 14 LArch (partage et consultation des archives historiques)

Amélioration Continue

Tous les processus liés au cycle de vie des données sont régulièrement revus et améliorés. Ceci vise à optimiser l'efficacité, la conformité et la sécurité.

⚠ Évaluation régulière de la qualité, de la fiabilité et de la sécurité des données
Mise en place d'actions correctives ou préventives

Mise en œuvre et Contrôle

Les *Data Stewards*, en collaboration étroite avec les utilisateurs finaux, mettent en œuvre et assurent le respect du cycle de vie défini, ainsi que les processus de contrôle et de validation des données

Utilisation des données

L'utilisation des données par les Data Consumers doit être connue et validée par les Data Owners L'accès aux données tient compte des règles et normes propres à chaque domaine

Conservation et Destruction

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 : élimination des documents et données ; versement des documents et données aux AAP pour leur conservation permanente

ⓘ 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

La documentation sur les données doit être accessible et partagée

La règle *CV09* décrit les actions d'accessibilité de l'information

- 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.
- 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 données doivent avoir une procédure d'autorisation et de révocation d'accès

La règle *CV11* décrit les actions d'accès aux données

- 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

Par exemple

Une équipe de recherche conduit une étude sur l'impact du changement climatique sur la biodiversité des zones humides. Les chercheurs et chercheuses collectent des données sur la température, l'humidité et la présence de certaines espèces animales et végétales.

- Dès la phase de conception du projet de recherche, les chercheurs/euses rédigent un Plan de gestion des données (DMP) décrivant le format des données, les standards utilisés, les modalités de stockage et de partage. Ils/elles suivent les principes FAIR en veillant à ce que les données soient bien documentées et réutilisables.
- Les données brutes sont stockées sur un serveur sécurisé avec des identifiants uniques et des métadonnées descriptives. Des procédures de sauvegarde et de gestion des versions sont mises en place.
- À la fin du projet, les données validées sont déposées dans un dépôt de données (*Data Repositories*) avec un DOI (digital object identifier) et des métadonnées détaillées.
- Grâce aux métadonnées standardisées et à l'utilisation de licences ouvertes , d'autres équipes de recherche peuvent exploiter ces données pour des analyses comparatives ou des modélisations.

UNIVERSITÉ DE GENÈVE

Sécurité et protection des données

La mise en œuvre de la politique de gestion des données institutionnelles de l'UNIGE pour le volet *Sécurité et protection des données* s'appuie sur la Politique de sécurité du système d'information et sur la Politique de protection des données personnelles, assurant ainsi un traitement conforme aux exigences légales et réglementaires. Les données sont classées selon leur sensibilité et leur criticité, ce qui permet d'adopter des mesures de protection adaptées aux risques associés. Les Data Owners et les CDO domaine ont la responsabilité d'assurer la traçabilité des données, de documenter leur classification et d'appliquer les mesures de sécurité définies par le CISO. Par ailleurs, les traitements de données personnelles doivent respecter des principes fondamentaux tels que la licéité, la proportionnalité et la finalité, garantissant ainsi les droits des personnes concernées. Enfin, un registre des activités de traitement est maintenu à jour afin d'assurer une transparence et un contrôle efficace des données gérées par l'institution.

Rôles clefs et actions – Sécurité et protection des données

Les règles *SP01, SP02, SP03, SP04, SP05, SP06, SP07, SP08* identifient les rôles et actions à mettre en œuvre pour garantir la sécurité et la protection des données

Stratégie	Mise en oeuvre	Application
CDO Domaine **Garant-e de la politique et de sa bonne application au sein du domaine** • Établit, 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 • Renseigne le Registre des activités de traitement des données personnelles • Fait appliquer les mesures de protection adaptées au niveau de sensibilité des données dont il/elle a la responsabilité, en collaboration avec le Data Owner	**Data Owners** **Responsable métier d'un ou de plusieurs sous-domaines de données** • Classifie les données de son domaine selon leur niveau de sensibilité • Établit la criticité et les exigences de traçabilité des données du domaine • Fait appliquer les mesures de protection adaptées au niveau de sensibilité des données dont il/elle a la responsabilité, en collaboration avec le CDO domaine	**Data Stewards** **Assure l'application des règles de gestion définies par le Data owner** • Applique et respecte les mesures de protection définies par le CDO domaine et le Data owner

ⓘ 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. Il tient à jour 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

Les points clefs des principes de sécurité et protection des données

Sécurité de l'information

Les données sont protégées à un niveau adéquat, adapté à leur niveau de sensibilité

En fonction de cette classification, les services numériques de l'UNIGE adaptés sont disponibles

Classification des données par niveau de sensibilité

La sensibilité de chaque information est déterminée et classée en niveau (sensibilité faible, moyenne, élevée)

Les Data Owners documentent et communiquent le niveau de sensibilité des données aux parties prenantes

Traçabilité des données

Les *Data Owners* assurent la traçabilité des données dont ils/elles ont la responsabilité et identifient les exigences métier de traçabilité des données

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

Principes de protection des données personnelles

La politique s'appuie sur la politique de protection des données personnelles de l'UNIGE. Les principes en matière de traitement des données personnelles (art. 35 nLIPAD) doivent être respectés ; ils contribuent au respect du droit à l'intégrité numérique de la personne concernée

Criticité des données

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

Registre des activités de traitement

Les CDO domaine, avec le support du DPO, déclarent et mettent à jour dans le Registre des activités de traitement (art. 43 nLIPAD) les traitements des données personnelles dont ils/elles sont responsables

Par exemple

Licéité du traitement
La division des ressources humaines traite les données des employé-es pour gérer les contrats et salaires. Ce traitement repose sur une base légale.

Proportionnalité et minimisation des données
Lorsqu'un-e étudiant-e demande une bourse, seules les informations financières nécessaires à l'évaluation de son éligibilité doivent être demandées, et non des données non pertinentes comme son historique médical.

Conservation et suppression des données
Les dossiers des membres du personnel doivent être conservés pendant une période définie, puis supprimés ou anonymisés.
Une épuration des documents et données contenus dans le dossier est réalisée périodiquement afin de ne conserver que ceux et celles qui sont encore utiles, sous l'angle administratif et légal.

Partage et transfert des données
Lors d'une collaboration ou d'une sous-traitance avec un tiers (art. 36C nLIPAD), le traitement n'est possible que si l'Etat concerné dispose d'une législation assurant un niveau de protection adéquat conformément à la liste établie par le Conseil fédéral

UNIVERSITÉ DE GENÈVE

Classification des informations et données en niveau de sensibilité

Sensibilité faible

Informations accessibles au public

📌 **Exemple** : Horaires des cours, événements institutionnels, informations du domaine public, annuaires des services administratifs, offres d'emploi, séances publiques, rapports d'activité, données de recherche publiées, etc.

? **Questions à se poser** :

- Ces données sont-elles destinées à un large public ?
  ✅ Oui
- Leur divulgation peut-elle causer un risque pour l'institution ou les individus concernés ?
  ❌ Non
- Sont-elles déjà disponibles sur le site web de l'université ou via des publications officielles ?
  ✅ Oui

💡 **Traitement** : Aucune restriction particulière, diffusion libre possible

Sensibilité moyenne

Accès restreint, usage interne

📌 **Exemple** : Dossiers étudiant-es et demandes d'immatriculation, dossiers et données des collaborateurs/trices, notes et e-mails internes, informations budgétaires internes, comptes-rendus de réunions, données de recherche non publiées, etc.

? **Questions à se poser** :

- Ces données contiennent-elles des informations à usage interne ?
  ✅ Oui
- Peuvent-elles être partagées librement en dehors de l'université ?
  ❌ Non
- Leur divulgation non autorisée pourrait-elle avoir un impact négatif sur l'université et son fonctionnement ?
  ✅ Oui

💡 **Traitement** : Accès limité à la communauté universitaire ou à un sous-ensemble de celle-ci, ou à des tiers clairement identifiés et légitimes

Sensibilité élevée

Accès restreint à un nombre limité de personnes

📌 **Exemple** : Certificats médicaux des étudiant-es et des employé-es, PV des séances à huis clos, analyses de prestations, sanctions administratives et pénales, assessment, données de santé, NAVS, données de recherche non anonymisables, collection (volume important) de données personnelles non sensibles, etc.

? **Questions à se poser** :

- Ces données concernent-elles des informations sensibles (santé, finances, donnée confidentielle) ?
  ✅ Oui
- Un accès non autorisé pourrait-il causer un préjudice à l'institution (juridique, financier, éthique) ou à la personne concernée ?
  ✅ Oui
- Existe-t-il des obligations légales strictes concernant leur protection et leur conservation ?
  ✅ Oui

💡 **Traitement** : Accès restreint aux seules personnes habilitées, mesures de protection particulière

Selon la nLIPAD, les données personnelles sensibles sont des 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,
4. des poursuites ou sanctions pénales ou administratives,
5. les données génétiques,
6. les données biométriques identifiant une personne physique de façon unique

Le niveau de sensibilité de ces données est donc élevé et elles doivent faire l'objet de mesures de protection particulières.

Pour plus d'informations ou en cas de questions :

- Sur la sécurité des données https://cybersecurite.unige.ch/
- Sur la protection des données personnelles https://www.unige.ch/donnees-personnelles/

Des questions à se poser

Licéité du traitement

- Ai-je une base légale pour traiter ces données ?
- Le traitement est-il nécessaire pour l'exécution d'une tâche publique ou d'un contrat ?
- Les personnes concernées sont-elles informées du traitement et de ses finalités ?

Proportionnalité et protection des données

- Les données collectées sont-elles strictement nécessaires à l'objectif poursuivi ?
- Peut-on anonymiser ou pseudonymiser certaines données pour limiter les risques ?
- L'accès aux données est-il limité aux seules personnes pour lesquelles elles sont nécessaires ?

Sécurité des données

- Est-ce que la sensibilité des données traitées a été déterminée ?
- Les données sont-elles stockées de manière sécurisée (chiffrement, accès contrôlé) ?
- En cas de transmission de données, est-ce fait de manière sécurisée (VPN, chiffrement) ?

Conservation et suppression des données

- Existe-t-il une durée de conservation clairement définie pour chaque type de données ?
- À l'issue de cette période, y a-t-il une procédure de suppression ou d'anonymisation ?
- Les données sont-elles stockées plus longtemps que nécessaire sans justification ?
- Les données doivent-elles être archivées en raison de leur valeur patrimoniale ?

Partage et transfert des données

- Si nous souhaitons partager ces données avec une autre entité, ce partage est-il légal, justifié et sécurisé ?
- Y a-t-il un accord formel (contrat, convention) régissant cet échange de données ?
- Les données restent-elles en suisse ou sont-elles transférées à l'étranger ?

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. Cette démarche s'inscrit dans une perspective progressive et sur le long terme qui nécessite un accompagnement du Data Office institutionnel et des services transverses pour mettre en œuvre la politique. Enfin 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 et historique de l'institution.

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 »[2]. 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.)[3].

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[4].

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

Données personnelles sensibles (au sens de la loi[5]) :

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,
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[6] 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.

[5] Selon L13347 du 3 mai 2024 modifiant la LIPAD

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

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 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.