Aspects juridiques, éthiques et déontologiques et sécurité des systèmes d'information

ECS1004-NBIN_

Domaine : **Sciences économiques et de gestion** Grade académique : **Bachelier de spécialisation en business data analysis - Namur**
Niveau de certification : **6** Cycle : **Premier Cycle** Année académique : **2026-2027** (Q1)

CRÉDITS ECTS	VOLUME HORAIRE
5	**50 h**

PRÉREQUIS	CO-REQUIS
Aucun	*Aucun*

IMPLANTATION	DIRECTEUR DE DÉPARTEMENT DU DOMAINE	RESPONSABLE DE L'UE	ENSEIGNANTS INTERVENANTS
Département économique de Namur	Sylvie Delwiche	Philippe VAN GOETHEM	—

PROGRAMME D'ÉTUDES

Programme	Bloc	Caractère
IE-Bachelier de spécialisation en business data analysis	1	Obligatoire

Partie 1 Contribution de l'UE au profil d'enseignement du programme et acquis d'apprentissage spécifiques (AAS) sanctionnés par l'évaluation

CONTEXTUALISATION

L'unité d'enseignement fait partie du programme, B1.

Elle contribue au profil d'enseignement de Bachelier de Spécialisation en Business Data Analysis.

ACQUIS D'APPRENTISSAGE SPÉCIFIQUES (AAS)

Acquis d'apprentissage spécifiques communs de cette UE

Cette unité d'enseignement vise à permettre à l'étudiant :

• D'identifier les principes et règles juridiques encadrant les entreprises, les professions libérales el es services publics dans le cadre des missions du Business Data Analys ;

• D'adopter une attitude éthique et de respecter les règles déontologiques ;

• De développer une approche responsable, critique et réflexive des pratiques professionnelles ;

• D'appliquer les dispositions légales et de mettre en œuvre les procédures respectant les aspects juridiques, éthiques et déontologiques relatifs à la profession de conseil, notamment :

• D'identifier les principes fondamentaux de protection et de sécurisation des données et d'identifier les risques et les menaces encourus,

• D'identifier les principes des droits fondamentaux afin de répondre adéquatement aux personnes concernées et aux autorités chargées de la surveillance des traitements de données

• D'identifier ses besoins de développement professionnel et de s'inscrire dans une démarche de formation permanente.

Aspects juridiques, éthiques et déontologiques

Face à une situation issue de la vie professionnelle courante en disposant ou en ayant accès à la documentation qu'il s'est constituée,

• D'appliquer, en les justifiant, les principes juridiques, éthiques et déontologiques qui encadrent les entreprises, les professions libérales et les services publics ;

• De caractériser les types de données au regarde des différents textes juridiques et d'en préciser les exigences de protection.

Principes de base de sécurité des données et S.I.

Face à une situation issue de la vie professionnelle courante en disposant ou en ayant accès à la documentation qu'il s'est constituée,

• D'identifier les risques et les menaces liées à la procédure d'exploitation des données et de formuler des solutions de remédiation proportionnées et adéquates au regard des textes juridiques.

OBJECTIFS DE DÉVELOPPEMENT DURABLE

Document annexe à la fiche UE accessible via un lien explicitant en quoi le programme d'études s'inscrit dans une politique de développement durable. Une ou plusieurs UE spécifique(s) pourraient être ciblée(s) dans cette annexe.

Partie 2 Description de l'unité d'enseignement

OBJECTIFS

Identifier et d'expliquer les enjeux sociétaux, les technologies, les risques et les principes essentiels en sécurité des systèmes.

CONTENU

Aspects juridiques, éthiques et déontologiques

L'étudiant sera capable :

En disposant ou en ayant accès à la documentation mise à disposition en respectant les consignes communiques par chaque enseignant.

• D'acquérir et d'appliquer les principes fondamentaux de la déontologie liée à la gestion de données ;

• D'utiliser les principaux textes juridiques notamment en matière de :

• Droits relatifs à la protection des données à caractère personnel (RGPD),

• Droits relatifs aux responsabilités et aux contrats informatiques,

• Droits relatifs à la propriété intellectuelle,

• Droits relatifs à la lutte contre la cybercriminalité et cybersécurité,

• Développer une méthodologie de veille juridique relative à ces aspects,

• Réglementation relative au développement, et à l'utilisation, de systèmes et modèles d'IA en Europe

• D'identifier les différents types de données et de préciser les exigences de protection quant à leur récolte, leur traitement, leur conservation (stockage, archivage, ...), leur communication, ainsi que leur destruction au regard des différents textes juridiques.

Principes de base de sécurité des données et S.I.

L'étudiant sera capable :

En disposant ou en ayant accès à la documentation qu'il s'est constituée,

• D'appréhender les principes fondamentaux de sécurité dans l'entreprise (confidentialité – intégrité – disponibilité) ;

• D'appréhender des principes spécifiques de sécurité des systèmes d'information (anonymisation et pseudonymisation des données, classification des données...) ;

• D'appréhender des principes et des méthodes d'analyse de risques dans le traitement de données : scénarios redoutés, matrice impact X, probabilités de survenance, contremesures...

SOURCES ET RÉFÉRENCES

AJED : Slides et, le cas échéant, textes légaux mis à disposition sur Moodle.

PSDSI :Slides du cours disponibles sur Moodle.

SUPPORTS DE COURS

Activité d'apprentissage	Support
ABIN1004A — Aspects juridiques, éthiques et déontologiques	Slides mises à disposition sur le site du cours et le cas échéant, textes légaux mis à disposition par les enseignants. L'existence de ces supports ne dispense pas l'étudiant de la prise de note en cours. L'étudiant n'est pas autorisé à faire usage de l'intelligence artificielle, tant pour la réalisation des exercices que lors de l'évaluation.
ABIN1004B — Principes de base de sécurité des données & S.I.	Slides du cours disponibles sur Moodle.

Partie 3 Méthodologie mise en œuvre et éventuel découpage de l'UE

DESCRIPTION DES ACTIVITÉS D'APPRENTISSAGE (AA) AU REGARD DE LEUR STATUT

Activité d'apprentissage	Heures	Langue d'enseignement	Langue d'évaluation
ABIN1004A — Aspects juridiques, éthiques et déontologiques	25 h	Français	Français
ABIN1004B — Principes de base de sécurité des données & S.I.	25 h	Français	Français

MÉTHODES D'ENSEIGNEMENT ET D'APPRENTISSAGE

Activité d'apprentissage	Méthodes d'enseignement et d'apprentissage
ABIN1004A — Aspects juridiques, éthiques et déontologiques	Participation active des étudiants, notamment par : La réalisation d'exercices permettant de mobiliser les textes de référence et d'appliquer les règles juridiques pertinentes et Des discussions collectives. Le cours asynchrone sera dédié à un temps d'étude pour les étudiants en vue de l'évaluation et sera suivi d'un temps de questions/réponses (30 min), à distance.

Activité d'apprentissage	Méthodes d'enseignement et d'apprentissage
ABIN1004B — Principes de base de sécurité des données & S.I.	Le cours alternera entre différentes méthodes : Ex-cathedra, Contenus multi-médias : lectures, vidéos, podcasts, ..., Travaux de groupes, Recherches individuelles, Travaux pratiques sur machines, ... Les cours asynchrones seront dédiés au suivi des épreuves intégrées.

DÉTERMINATION DE LA COHÉRENCE PÉDAGOGIQUE EN CAS DE REGROUPEMENT D'AA FAISANT L'OBJET D'UNE ÉVALUATION DISTINCTE

Les deux activités d'apprentissage de cette UE contribuent à un objectif commun : permettre au futur Business Data Analyst d'exploiter les données de manière responsable, en respectant les exigences juridiques, éthiques et déontologiques et en tenant compte des risques de sécurité.

L'activité « Aspects juridiques, éthiques et déontologiques » apporte les repères nécessaires pour identifier les règles applicables aux pratiques professionnelles et les exigences de protection des différents types de données, depuis leur collecte jusqu'à leur destruction. Elle développe également la capacité à justifier ses choix au regard des droits des personnes, des responsabilités professionnelles et des principes éthiques.

L'activité « Principes de base de sécurité des données et S.I. » complète cette approche par l'identification des risques et des menaces liés au traitement des données et par l'étude des mesures permettant d'assurer leur confidentialité, leur intégrité et leur disponibilité. Elle aborde notamment la classification des données, l'anonymisation, la pseudonymisation et l'analyse des risques.

L'articulation entre les deux activités permet à l'étudiant de relier les exigences de protection aux mesures de sécurité à envisager, puis d'en apprécier la pertinence et la proportionnalité. Bien que les évaluations soient distinctes, les deux activités concourent ainsi aux acquis d'apprentissage communs de l'UE : analyser une situation professionnelle, justifier les exigences applicables et proposer des solutions de protection adaptées.

Partie 4 Évaluation de l'unité d'enseignement

STRUCTURE DU DISPOSITIF GÉNÉRAL D'ÉVALUATION (EN LIEN AVEC LE PROGRAMME D'ÉTUDES)

Évaluation intégrée : non.

MÉTHODOLOGIE DE CONSTRUCTION DE LA NOTE FINALE DE L'UE

L'UE comporte deux activités d'apprentissage.

- **Aspects juridiques, éthiques et déontologiques : examen écrit, pondéré à 50 % de la note finale de l'UE ;**
- **Principes de base de sécurité des données et S.I. : examen écrit, pondéré à 50 % de la note finale de l'UE ;**

La note finale de l'UE est obtenue par la moyenne pondérée de ces deux évaluations.

LA PONDÉRATION DE L'ÉVALUATION DE L'UE À DES FINS DE DÉLIBÉRATION LORS DU CALCUL DE LA MOYENNE

Au sein du programme d'études, lors du calcul de la moyenne, la pondération de l'évaluation de l'unité d'enseignement est effectuée sur base des crédits affectés à cette unité d'enseignement et évalués

MODALITÉS D'ÉVALUATION PAR ACTIVITÉ D'APPRENTISSAGE

Activité d'apprentissage	Modalités d'évaluation
ABIN1004A — Aspects juridiques, éthiques et déontologiques	Évaluation Q2-Q3 : 100 % Examen écrit comprenant des questions de connaissances juridiques et des questions d'applications (par la résolution de cas pratiques). Pour la détermination du degré de maitrise, il sera tenu compte des critères suivants : Niveau de précision : la clarté, la concision, la rigueur au niveau de la terminologie, des concepts et des techniques/principes/modèles Niveau de cohérence : la capacité à établir avec pertinence une majorité de liens logiques pour former un ensemble organisé Niveau d'intégration : la capacité à s'approprier des notions, concepts, techniques et démarches en les intégrant dans son analyse, son argumentation, sa pratique ou la recherche de solutions Niveau d'autonomie : la capacité de faire preuve d'initiatives démontrant une réflexion personnelle basée sur une exploitation des ressources et idées en interdépendance avec son environnement. *Attention : l'ensemble des parties doit être présenté pour obtenir une cotation. En cas d'absence à une des épreuves, aucune note globale ne pourra être attribuée. Langue d'évaluation : français.*

Activité d'apprentissage	Modalités d'évaluation
ABIN1004B — Principes de base de sécurité des données & S.I.	Évaluation Q2-Q3 : 100% Examen écrit. Pour la détermination du degré de maitrise, il sera tenu compte des critères suivants : Niveau de précision : la clarté, la concision, la rigueur au niveau de la terminologie, des concepts et des techniques/principes/modèles Niveau de cohérence : la capacité à établir avec pertinence une majorité de liens logiques pour former un ensemble organisé Niveau d’intégration : la capacité à s’approprier des notions, concepts, techniques et démarches en les intégrant dans son analyse, son argumentation, sa pratique ou la recherche de solutions Niveau d’autonomie : la capacité de faire preuve d’initiatives démontrant une réflexion personnelle basée sur une exploitation des ressources et idées en interdépendance avec son environnement. *Attention : l'ensemble des parties doit être présenté pour obtenir une cotation. En cas d'absence à une des épreuves, aucune note globale ne pourra être attribuée. Langue d'évaluation : français.*

MODALITÉS CONCRÈTES D'ÉVALUATION

Une mention sur la fiche informera les étudiants du fait que les précisions sur les épreuves seront disponibles sur Moodle au plus tard 6 semaines avant l'évaluation.