

IX.2323 / IX.2423 – Protection des données personnelles

INFORMATIONS GENERALES

Titre du module : Protection des données personnelles

Identifiant du module : IX.2423

Responsable du module : Ali ALLAOUA

ECTS : 4

Quantité de travail moyenne par élève : 100h dont 42 encadrées

Travail en équipe : oui

Mots clés : protection de la vie privée, protection des données à caractère personnel, DPD (Délégué à la Protection des Données), DPO (Data Protection Officer), RGPD (Règlement Général sur la Protection des Données)

PRESENTATION

Nos systèmes d'information informatisés stockent et traitent chaque seconde à une vitesse hallucinante des volumes sans cesse croissants d'informations relatives à des citoyens et à leur vie de moins en moins privée. En France, depuis 1978, une loi encadre l'utilisation de ces données et a créé une autorité administrative indépendante : la CNIL.

Au niveau européen, depuis 2018, un nouveau règlement (le Règlement Général sur la Protection des Données ou RGPD) met de nouvelles balises légales par rapport à ce qui est permis ou interdit. Ce RGPD crée une nouvelle fonction, celle du Délégué à la Protection des Données (DPD, ou DPO, pour Data Protection Officer) qui est le garant de la protection des données personnelles traitées par l'organisme qui l'emploie. Ce module présente une introduction au métier de DPD en passant par l'historique et ontologie de la protection de la vie privée, les socles de base pour la protection juridique des données (RGPD, convention 108, Article 8 CEDH...), le champ d'application de la loi, les cookies, la sécurité des données et la jurisprudence française. Il expose les principes de base et la déontologie que tout informaticien appelé à concevoir un logiciel ou un ordinateur manipulant des données sur les personnes physiques se doit de connaître et de respecter.

OBJECTIFS PEDAGOGIQUES

- Connaître et comprendre les principes de licéité du traitement, de limitation des finalités, de minimisation des données, d'exactitude des données, de conservation limitée des données, d'intégrité, de loyauté, de confidentialité et de responsabilité.
- Identifier la base juridique d'un traitement et l'applicabilité du cadre légal.
- Identifier des mesures de sécurité adaptées aux risques et à la nature des opérations de traitement.
- Identifier les violations de données personnelles nécessitant une notification à l'autorité de contrôle et celles nécessitant une communication aux personnes concernées.
- Identifier les enjeux liés aux traitements des données personnelles dans la mise en œuvre de technologies basées sur des algorithmes (intelligence artificielle, blockchain)
- Gérer les relations avec les autorités de contrôle, en répondant à leurs sollicitations et en facilitant leur action (instruction des plaintes et contrôles de la CNIL en particulier).
- Réaliser des audits périodiques afin d'identifier les sources de risques et les impacts potentiels.
- Élaborer des stratégies de protection des données conformément aux principes de protection des données du RGPD.

- Analyser l'impact relatif à la protection des données (Data Protection Impact Assessment (DPIA)).
- Être en mesure de coordonner les activités de sensibilisation à la protection des données personnelles au sein d'une organisation.
- Implémenter les principes de "Privacy by Design" et " Privacy by Default" dans le cycle de vie des produits et des services.
- Créer des chartes éthiques entourant la conception, la mise en place et l'usage des données personnelles.

Prérequis

- Notions de base en réseaux (IR.1101), et en développement web (II.1101 / II.1201).

Contenu/programme

Concepts

Le Délégué à la Protection des Données (DPD, ou DPO, pour Data Protection Officer) est le garant de la protection des données personnelles traitées par l'organisme qui l'emploie. Il maîtrise à la fois les outils et pratiques informatiques et l'environnement juridique, en particulier le Règlement Européen RGPD (en vigueur depuis le 25 mai 2018). Il élabore, au sein d'un organisme, une politique de protection des données personnelles, veille au respect des obligations légales, et s'assure en particulier que toutes les précautions sont prises pour préserver la sécurité des données personnelles et la légalité de leur traitement. Il exerce en toute indépendance par rapport à la Direction Générale et est en contact avec tous les métiers de l'organisme, et assure la relation avec la CNIL.

Ce module présente une introduction au métier de DPD en passant par

- Historique et ontologie de la protection de la vie privée
- Les socles de base pour la protection juridique des données (RGPD, convention 108, Article 8 CEDH,...)
- Le champ d'application de la loi : données à caractère personnel, traitement, responsable de traitement, sous-traitant, données sensibles et pouvoir des forces de police
- Les enjeux liés à la protection des données dans les secteurs à risque (santé, banque, assurance, etc.)
- Les enjeux liés à la protection des données personnelles dans les traitements algorithmiques
- Les cookies : fonctionnement, légalité, utilité et finalité
- La sécurité des données, exigences légales et gestion des failles et des attaques
- Statut, pouvoir et jurisprudence de la CNIL
- La jurisprudence française.

Outils utilisés par l'enseignant/intervenant

- Privacy-Friendly Firefox Add-ons

Outils utilisés par l'apprenant

- Privacy-Friendly Firefox Add-ons

MODALITES PEDAGOGIQUES

Méthodes d'apprentissage

La première partie de ce module est composée d'une série de cours et de conférences par des experts du domaine. Elle abordera les aspects juridiques, économiques et financiers des enjeux associés à la protection des données personnelles dans le cadre de la transformation numérique des entreprises. La deuxième partie de ce module abordera les aspects plus techniques de la sécurisation des systèmes d'information et des traitements algorithmiques au regard des principes édictés par la CNIL et les directives européennes. Une analyse d'impact d'un traitement de données à risque sera réalisée dans le cadre de travaux pratiques de groupe.

Modalités d'évaluation

L'évaluation de ce module repose sur :

- Évaluation collective (50 %) : Une activité en groupe où les élèves réaliseront une analyse d'impact sur un traitement de données personnelles à risque (vidéosurveillance, systèmes biométriques, etc.)
- Évaluation individuelle (50 %) : QCM et cas pratique pendant la période d'examen

Langue de travail

Bien que la langue de travail soit le français, certaines ressources bibliographiques peuvent être en anglais.

BIBLIOGRAPHIE, WEBGRAPHIE, AUTRES SOURCES

- « Les Algorithmes font-ils la loi » - Aurélie JEAN - Octobre 2021- Editions de L'Observatoire
- « L'Homme nu » - Marc DUGAIN et Christophe LABBÉ- Septembre 2016 – Robert Laffont
- « Contre atlas de l'intelligence artificielle » - Kate CRAWFORD- Mars 2022- ZULMA ESSAIS
- « RÉSEAUX SOCIAUX & CIE » Le commerce des données personnelles – Avril 2013- Franck LEROY-Actes Sud
- <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>
- <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Rapport, C. N. I. L. « Comment permettre à l'homme de garder la main. » Les enjeux éthiques des algorithmes et de l'intelligence artificielle (2017)
https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
- Rapport, C. N. I. L. « A votre écoute : Exploration des enjeux éthiques, techniques et juridiques des assistants vocaux » (2020)
https://www.cnil.fr/sites/default/files/atoms/files/cnil_livre-blanc-assistants-vocaux.pdf
- Rapport et propositions de recommandations sur le « Profilage et la Convention 108+ du Conseil de l'Europe »
<https://rm.coe.int/t-pd-2019-07fin-fr-rapport-profilage-2770-2878-8993-1-final-clean-2755/1680a0925b>
- Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FRA&toc=OJ%3AL%3A2022%3A333%3ATOC

- Proposition de règlement du parlement européenne et du conseil établissant des règles harmonisées concernant l'intelligence
<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021PC0206>