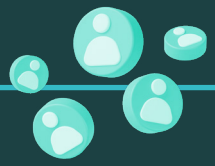
Règlement Général sur la Protection des Données (RGPD)

Le RGPD vise d'une part à protéger les données personnelles des usagers, et d'autre part à responsabiliser les organismes publics et privés qui traitent ces données personnelles.



ENTITÉS CONCERNÉES

Concerne toutes les entités publiques et privées qui traitent des données personnelles.

ENTRÉE EN VIGUEUR

En vigueur depuis mai 2018

PRINCIPALES OBLIGATIONS

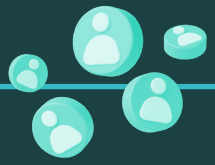
Impose des mesures de protection que les responsables de traitements de données personnelles et sous-traitants doivent mettre en place quand ils collectent, traitent, ou transfèrent des données personnelles.

AUTORITÉS DE CONTRÔLE

Autorité de Protection des Données (APD)

Directive NIS-1

Première initiative en matière de cybersécurité dans l'Union européenne, la Directive NIS-1 établit des obligations en matière de cybersécurité pour les opérateurs de services essentiels (OSE).



ENTITÉS CONCERNÉES

- Opérateurs de Services Essentiels (OSE) : secteurs de l'énergie, des transports, les banques et marchés financiers, de la santé, de l'eau et de l'infrastructure numérique.
- Fournisseurs de services numériques (FSN) : sites de e-commerce, cloud computing, et moteurs de recherche par exemple.

ENTRÉE EN VIGUEUR

- Adoptée par l'UE en 2016
- Transposée en 2019 dans le droit national belge par la loi NIS du 7 avril 2019.

PRINCIPALES OBLIGATIONS

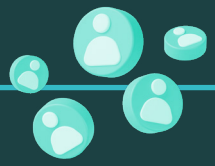
Obligation pour ces entités de prendre des mesures de sécurité minimales et de signaler les incidents majeurs. Elle énonce 23 règles réunies en 4 catégories : gouvernance, protection, défense et résilience

AUTORITÉS DE CONTRÔLE

- **Energie :** Ministère fédéral de l'Énergie
- **Transports :** Ministère fédéral de la Mobilité
- **Transports** (par voies d'eau accessibles aux navires maritimes) : Ministère fédéral compétent pour la Mobilité maritime
- **Finances** (établissements financiers) : Banque Nationale de Belgique (BNB)
- **Finances** (plates-formes de négociation financières) : Autorité des services et marchés financiers (FSMA)
- **Santé :** Ministère fédéral de la Santé publique
- **Infrastructures numériques :** Institut belge des services postaux et des télécommunications (IBPT)
- **Eau potable :** Comité national de sécurité pour la fourniture et la distribution d'eau potable.

Directive NIS-2

La Directive NIS-2 vient renforcer l'efficacité et de clarifier le champ d'application de la Directive NIS-1. Cette nouvelle directive couvre un plus grand nombre de secteurs.



ENTITÉS CONCERNÉES

- Liste des OSE et FSN de NIS-1
- Gestionnaires d'eaux usées et de déchets
- Fabricants de produits critiques (ex : produits médicaux)
- Services postaux et de messagerie
- Administrations publiques (à l'exception de la défense, sécurité nationale et publique et le système judiciaire).

ENTRÉE EN VIGUEUR

- Adoptée par l'UE en 2022
- En cours de transposition dans le droit belge

PRINCIPALES OBLIGATIONS

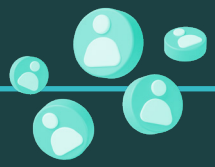
- Obligations de NIS-1
- Obligation d'effectuer des analyses de risques sur le potentiel et l'impact des incidents, puis mettre en place des mesures organisationnelles et techniques proportionnelles à ce risque.

AUTORITÉS DE CONTRÔLE

- Mêmes autorités de contrôle que pour NIS-1
- En attente de la transposition belge pour les autorités de contrôle des nouveaux secteurs concernés.

Artificial Intelligence Act (AI Act)

Face au développement de l'intelligence artificielle et à l'absence de cadre juridique sur cette matière, l'Union européenne a créé l'AI Act dans le but de développer les potentialités sociales et économiques de l'IA, tout en encadrant les risques qu'elle fait peser sur les droits fondamentaux.



ENTITÉS CONCERNÉES

- Principalement les fournisseurs
- Les mandataires, importateurs et distributeurs d'IA quand le fournisseur se trouve en dehors de l'UE.

ENTRÉE EN VIGUEUR

En cours d'adoption par l'UE.

PRINCIPALES OBLIGATIONS

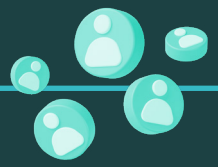
- Régulation de l'IA en fonction du risque qu'elle représente (de la liberté de commercialisation à la prohibition)
- Evaluation de conformité obligatoire pour les IA à haut risque.

AUTORITÉS DE CONTRÔLE

Pas d'autorité nationale désignée pour le moment.

Cyber Resilience Act (CRA)

Le CRA vise à protéger les consommateurs et les entreprises qui achètent ou utilisent des produits ou logiciels contenant un composant numérique, en fixant des règles communes en matière de cybersécurité tout au long de la vie des produits vendus.



ENTITÉS CONCERNÉES

- Principalement les fabricants et éditeurs de logiciels et de produits connectés
- Également les distributeurs de ces produits ou logiciels

ENTRÉE EN VIGUEUR

En cours d'adoption par l'UE.

PRINCIPALES OBLIGATIONS

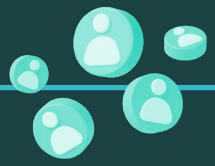
- Obligation de prise en compte des impératifs de cybersécurité dans la conception, développement et production de ces produits.
- Mise sur le marché des produits avec la documentation nécessaire quant à leur sécurité
- Diffusion de correctifs de sécurité, ou la mise en place de procédures de gestion des vulnérabilités tout au long de la vie du produit

AUTORITÉS DE CONTRÔLE

Pas d'autorité nationale désignée pour le moment.

Digital Operational Resilience Act (DORA)

Le Règlement DORA s'adresse tout particulièrement à la cybersécurité du secteur financier, et vise à renforcer la sécurité des systèmes numériques de ce secteur.



ENTITÉS CONCERNÉES

- Large éventail d'entités financières
- Prestataires de services TIC qui opèrent dans les services financiers dans l'UE

ENTRÉE EN VIGUEUR

- Adopté en 2022 par l'UE
- En cours d'implémentation, avec application en 2024.

PRINCIPALES OBLIGATIONS

- Assurer la cybersécurité adéquate de ces acteurs
- Mener des tests approfondis
- Assurer une gestion des risques adéquate (signalement d'incidents, politiques de gestion des risques et de continuité de l'activité).

AUTORITÉS DE CONTRÔLE

Banque Nationale de Belgique (BNB)