FICHE DE RÉVISION

Module : Règlementation — RGPD, ISO, Conformité

Formation : Pilotage et Animation de la Cybersécurité

⚖️ 1. Introduction au RGPD

> **Objectif :** Comprendre les fondements juridiques de la protection des données personnelles

▸ Contexte et champ d'application

Le Règlement Général sur la Protection des Données (RGPD / GDPR) est entré en vigueur le 25 mai 2018. Il s'applique à tout organisme traitant des données personnelles de résidents européens, quel que soit son lieu d'établissement.

Périmètre	Précision
Qui est concerné ?	Tout responsable de traitement ou sous-traitant traitant des données de personnes de l'UE
Qu'est-ce qu'une donnée personnelle ?	Toute information permettant d'identifier directement ou indirectement une personne (nom, email, IP, biométrie…)
Données sensibles (Art. 9)	Santé, origine raciale, opinions politiques, religion, orientation sexuelle, données biométriques
Autorité de contrôle (France)	CNIL (Commission Nationale de l'Informatique et des Libertés)

▸ Les 7 principes fondamentaux du RGPD (Art. 5)

Principe	Signification
1. Licéité, loyauté, transparence	Le traitement repose sur une base légale ; les personnes sont informées
2. Limitation des finalités	Les données sont collectées pour des fins déterminées, explicites et légitimes
3. Minimisation des données	Seules les données strictement nécessaires sont collectées
4. Exactitude	Les données doivent être exactes et tenues à jour
5. Limitation de la conservation	Les données ne sont pas conservées plus longtemps que nécessaire
6. Intégrité et confidentialité	Mesures techniques et organisationnelles appropriées pour sécuriser les données
7. Responsabilité (Accountability)	Le RT doit démontrer sa conformité à tout moment

▸ Bases légales du traitement (Art. 6)

- Consentement explicite et libre de la personne concernée
- Exécution d'un contrat auquel la personne est partie
- Obligation légale à laquelle le responsable est soumis
- Sauvegarde des intérêts vitaux de la personne
- Mission d'intérêt public ou exercice de l'autorité publique
- Intérêts légitimes du responsable (sauf si intérêts de la personne prévalent)

▸ Droits des personnes concernées

Droit	Description	Délai de réponse
Accès (Art. 15)	Obtenir une copie des données traitées	1 mois (+ 2 mois si complexe)
Rectification (Art. 16)	Corriger des données inexactes ou incomplètes	1 mois
Effacement (Art. 17)	Droit à l'oubli — suppression des données	1 mois
Opposition (Art. 21)	S'opposer à un traitement fondé sur l'intérêt légitime	Immédiat
Portabilité (Art. 20)	Récupérer ses données dans un format structuré et lisible	1 mois
Limitation (Art. 18)	Geler le traitement sans effacer les données	1 mois

▸ Obligations clés pour les organismes

Obligation	Détail
Registre des traitements (Art. 30)	Inventaire de tous les traitements : finalité, base légale, durée, destinataires, mesures de sécurité
Analyse d'Impact (AIPD / DPIA)	Obligatoire pour les traitements à risque élevé (profilage, données sensibles à grande échelle)
Privacy by Design & by Default	Intégrer la protection des données dès la conception et paramétrer la confidentialité maximale par défaut
DPO (Art. 37-39)	Obligatoire pour les organismes publics, les traitements à grande échelle de données sensibles
Notification de violation (Art. 33-34)	À la CNIL sous 72h ; aux personnes concernées sans délai si risque élevé
Transferts hors UE (Art. 44-49)	Nécessitent des garanties : décision d'adéquation, clauses contractuelles types (CCT), BCR

▸ Sanctions (Art. 83)

Niveau	Montant maximum	Exemples d'infractions
Niveau 1	10 M€ ou 2 % du CA mondial	Manquements organisationnels : registre, DPO, AIPD
Niveau 2	20 M€ ou 4 % du CA mondial	Violations des principes fondamentaux, droits des personnes, transferts illicites

2. Règlementation et Sécurité de l'Information

> **Objectif :** Identifier les liens entre la règlementation cyber LPM, NIS2, DORA, CRA, sécurité et gestion des risques

Vue d'ensemble des textes réglementaires majeurs

Texte	Origine	Entrée en vigueur	Périmètre
LPM 2024	France	2024	Opérateurs d'Importance Vitale (OIV) et Services Essentiels
NIS2	Union Européenne	Oct. 2024	Entités essentielles & importantes dans 18 secteurs critiques
DORA	Union Européenne	Jan. 2025	Secteur financier : banques, assurances, prestataires TIC
CRA (Cyber Resilience Act)	Union Européenne	2026-2027	Fabricants de produits connectés (hardware et software)
RGS	France (ANSSI)	Permanent	Systèmes d'information des autorités administratives de l'État

LPM 2024 — Loi de Programmation Militaire

Volet	Détail
Qui ?	OIV (secteurs vitaux : énergie, eau, télécoms, santé, transports, finance…) et Opérateurs de Services Essentiels (OSE)
Obligations de détection	Déploiement de sondes qualifiées ANSSI pour la détection des cyberattaques
Signalement d'incidents	Notification obligatoire à l'ANSSI en cas d'incident de sécurité significatif
Qualification ANSSI	Recours à des prestataires qualifiés (PDIS, PRIS, hébergeurs SecNumCloud)
Contrôles et sanctions	Audits imposés par l'ANSSI, mesures coercitives en cas de manquement

Directive NIS2 — Network and Information Security

NIS2 élargit considérablement le périmètre de NIS1 (2016) en couvrant 18 secteurs et en renforçant les obligations.

Catégorie	Entités Essentielles (EE)	Entités Importantes (EI)
Exemples de secteurs	Énergie, transports, santé, eau, infrastructures numériques	Poste, gestion des déchets, industrie, alimentaire
Taille (indicative)	Grandes entreprises (> 250 ETP ou > 50 M€ CA)	Moyennes entreprises (50-250 ETP)
Supervision	Proactive (contrôle ex ante)	Réactive (contrôle ex post, sur incident)
Sanctions max.	10 M€ ou 2 % du CA mondial	7 M€ ou 1,4 % du CA mondial

Mesures de sécurité imposées par NIS2 (Art. 21)

- Gouvernance : responsabilité des dirigeants, formation cyber des organes de direction
- Gestion des risques : analyse et traitement formalisé des risques cyber
- Sécurité de la chaîne d'approvisionnement : évaluation des prestataires et fournisseurs
- Gestion des incidents : détection, signalement à l'autorité compétente sous 24h (alerte précoce), 72h (notification) et 1 mois (rapport final)
- Continuité d'activité : PCA, PRA, gestion des sauvegardes

- Chiffrement et authentification multifacteur obligatoires

▸ DORA — Digital Operational Resilience Act

DORA s'applique au secteur financier européen (banques, assureurs, prestataires de services de paiement, plateformes de cryptoactifs…) et à leurs prestataires TIC critiques.

Pilier DORA	Contenu
1. Gouvernance des risques TIC	Cadre de gestion des risques TIC approuvé par la direction, rôles et responsabilités définis
2. Gestion des incidents TIC	Classification, notification aux autorités (DORA impose des délais précis), rapport post-incident
3. Tests de résilience opérationnelle	Tests réguliers : TLPT (Threat-Led Penetration Testing) pour les entités critiques
4. Risques liés aux tiers (TIC)	Registre des contrats TIC, clauses contractuelles obligatoires, surveillance des prestataires critiques
5. Partage d'informations	Encouragement au partage de renseignements sur les cybermenaces entre entités financières

▸ CRA — Cyber Resilience Act

Aspect	Détail
Périmètre	Tout produit avec éléments numériques vendu dans l'UE : IoT, logiciels, systèmes industriels connectés
Obligations fabricants	Security by design, mises à jour de sécurité pendant 5 ans minimum, documentation des vulnérabilités
Notification de vulnérabilités	Signalement à l'ENISA sous 24h pour les vulnérabilités activement exploitées
Marquage CE	Conformité CRA requise pour obtenir le marquage CE (accès au marché européen)
Sanctions	Jusqu'à 15 M€ ou 2,5 % du CA mondial

▸ Articulation entre textes réglementaires et gestion des risques

Réglementation	Lien avec la gestion des risques cyber
RGPD	Exige une AIPD pour les traitements à risque élevé ; impose des mesures de sécurité proportionnées aux risques
NIS2	Impose une approche formelle de gestion des risques ; la méthode EBIOS Risk Manager est recommandée
DORA	Cadre de gestion des risques TIC obligatoire, appétit au risque défini par la direction
LPM	Qualification des prestataires réduisant le risque de chaîne d'approvisionnement
ISO 27005	Norme de référence pour la gestion des risques SI, alignée avec toutes les réglementations ci-dessus

3. Normes et Conformité — ISO 27001 & ISO 27005

Objectif : Découvrir les normes de sécurité et leur articulation avec la règlementation

La famille de normes ISO 2700x

Norme	Intitulé	Rôle dans le SMSI
ISO 27001	Système de Management de la Sécurité de l'Information (SMSI)	Norme de certification — exigences à satisfaire
ISO 27002	Code de bonnes pratiques en sécurité de l'information	Guide de mise en oeuvre des 93 mesures de sécurité (Annexe A de 27001)
ISO 27005	Gestion des risques liés à la sécurité de l'information	Méthodologie de gestion des risques, en soutien à 27001
ISO 27017	Sécurité pour les services Cloud	Mesures additionnelles pour les environnements Cloud
ISO 27018	Protection des données personnelles dans le Cloud	Complément RGPD pour les sous-traitants Cloud

ISO 27001 — Structure SMSI et cycle PDCA

ISO 27001 est organisée selon la structure harmonisée (High Level Structure) commune à toutes les normes de management ISO. Elle repose sur le cycle d'amélioration continue PDCA.

Phase PDCA	Chapitres ISO 27001	Actions clés
PLAN — Planifier	Chap. 4 à 8	Contexte, parties prenantes, périmètre, politique de sécurité, analyse des risques, objectifs, mesures (Annexe A)
DO — Réaliser	Chap. 8	Mise en oeuvre des mesures de sécurité, gestion opérationnelle, sensibilisation, formation
CHECK — Contrôler	Chap. 9	Audits internes, revues de direction, mesure des performances, surveillance des indicateurs
ACT — Améliorer	Chap. 10	Traitement des non-conformités, actions correctives, amélioration continue du SMSI

Les 4 thèmes et 93 mesures de l'Annexe A (ISO 27002:2022)

Thème	Nb. de mesures	Exemples de mesures
Organisationnelles	37 mesures	Politique de sécurité, gestion des actifs, relations fournisseurs, réponse aux incidents
Liées aux personnes	8 mesures	Sensibilisation, formation, processus disciplinaire, travail à distance
Physiques	14 mesures	Contrôle des accès physiques, protection des équipements, sécurité des supports
Technologiques	34 mesures	Contrôle d'accès logique, chiffrement, journalisation, gestion des vulnérabilités, sécurité réseau

Processus de certification ISO 27001

- Étape 1 — Définition du périmètre SMSI : quels actifs, processus, sites sont couverts ?
- Étape 2 — Analyse des risques (via ISO 27005) : identification des actifs, menaces, vulnérabilités, impacts
- Étape 3 — Déclaration d'Applicabilité (DdA) : liste des 93 mesures applicables ou exclues + justification
- Étape 4 — Mise en oeuvre des mesures et formation des équipes
- Étape 5 — Audit interne et revue de direction
- Étape 6 — Audit de certification par un organisme accrédité (étape 1 documentaire + étape 2 sur site)
- Surveillance annuelle + recertification tous les 3 ans

▸ ISO 27005 — Gestion des risques SI

ISO 27005 fournit la méthodologie de gestion des risques qui alimente le SMSI. Elle est compatible avec ISO 31000 (gestion des risques généraliste) et avec les méthodes françaises EBIOS Risk Manager (ANSSI).

Étape ISO 27005	Description
1. Établissement du contexte	Définir le périmètre, les critères d'acceptation du risque, l'appétit au risque de l'organisation
2. Identification des risques	Recenser les actifs, les menaces pesant sur eux, les vulnérabilités exploitables et les impacts potentiels
3. Estimation des risques	Évaluer la vraisemblance et l'impact de chaque risque ; obtenir une valeur de risque brut
4. Évaluation des risques	Comparer les risques aux critères d'acceptation ; prioriser le traitement
5. Traitement des risques	Choisir une option : Réduire / Accepter / Transférer / Éviter ; définir un plan de traitement
6. Acceptation des risques résiduels	Validation formelle par la direction des risques non traités ou partiellement traités
7. Communication et surveillance	Reporting régulier, réévaluation périodique des risques, gestion des événements déclencheurs

▸ Options de traitement des risques

Option	Description	Exemple concret
🔽 Réduire	Mettre en oeuvre des mesures pour diminuer la probabilité ou l'impact	Déployer un MFA pour réduire le risque de compromission de compte
✅ Accepter	Décider de tolérer le risque car son coût de traitement est supérieur à l'impact potentiel	Accepter le risque de panne ponctuelle d'un service non critique
🔄 Transférer	Reporter le risque sur un tiers (assurance, sous-traitant)	Souscrire une assurance cyber, externaliser l'hébergement chez un prestataire qualifié
🚫 Éviter	Supprimer l'activité ou le système qui génère le risque	Renoncer à connecter un système SCADA à Internet

▸ Articulation ISO 27001/27005 avec les réglementations

Réglementation	Convergence avec ISO 27001 / 27005
RGPD	La DPIA s'appuie sur une démarche d'analyse de risques proche d'ISO 27005 ; Privacy by Design = Annexe A mesures de contrôle d'accès et chiffrement

NIS2	Exige un cadre de gestion des risques formalisé : ISO 27001 est reconnu comme référence pour démontrer la conformité NIS2
DORA	Le cadre de risques TIC de DORA s'aligne sur la structure du SMSI ISO 27001 (gouvernance, mesures, audits, amélioration continue)
LPM / RGS	L'homologation RGS repose sur une démarche similaire à ISO 27001 ; la qualification ANSSI référence ISO 27001

📌 Mémo Récapitulatif — À Retenir

RGPD — Données Personnelles	Règlementations Cyber	ISO 27001 / 27005
• 7 principes Art. 5 (CIA + accountability) • 6 bases légales (consentement, contrat…) • DPO obligatoire si données sensibles à grande échelle • AIPD si traitement à risque élevé • Violation → CNIL sous 72h • Sanction max : 20 M€ ou 4 % CA	• NIS2 : 18 secteurs, EE + EI, Art. 21 • LPM : OIV, sondes ANSSI, qualification • DORA : 5 piliers dont TLPT et risque tiers TIC • CRA : Security by design, maj 5 ans, marquage CE • NIS2 signalement : 24h → 72h → 1 mois • ISO 27001 alignée sur toutes ces réglementations	• SMSI = PDCA (Plan-Do-Check-Act) • Annexe A : 93 mesures en 4 thèmes • DdA : justifier l'exclusion ou l'inclusion des mesures • ISO 27005 : Identifier → Estimer → Traiter • 4 options de traitement : Réduire / Accepter / Transférer / Éviter • Recertification ISO 27001 tous les 3 ans