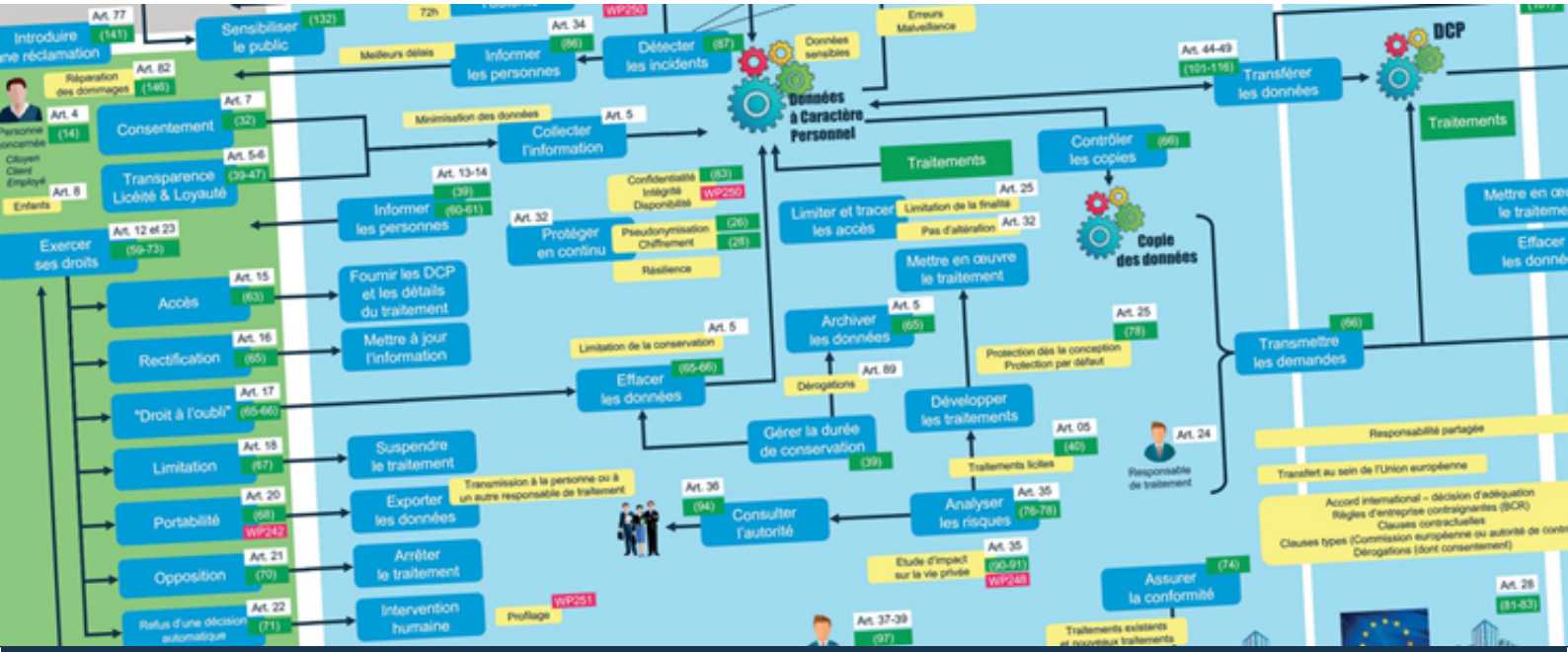
CLUSIF

LES GUIDES PRATIQUES du CLUSIF



LES NORMES EN MATIÈRE DE PROTECTION DES DCP

1. Contexte

La protection de la vie privée est une préoccupation majeure pour les entreprises, dont les obligations se doivent d'être rapidement mises en œuvre pour limiter les risques et protéger notre vie privée dans le monde numérique.

Le règlement européen, *via* l'article 40, encourage l'adoption de codes de conduite destinés à contribuer à sa bonne application. Ces codes doivent tenir compte de la spécificité des différents secteurs de traitement de données et des besoins spécifiques des micros, petites et moyennes entreprises.

Le considérant 77 précise, lui : *« Des directives relatives à la mise en œuvre de mesures appropriées et à la démonstration par le responsable du traitement ou le sous-traitant du respect du présent règlement, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques visant à atténuer le risque, pourraient être fournies notamment au moyen de codes de conduite approuvés, de certifications approuvées et de lignes directrices données par le comité ou d'indications données par un délégué à la protection des données. »*

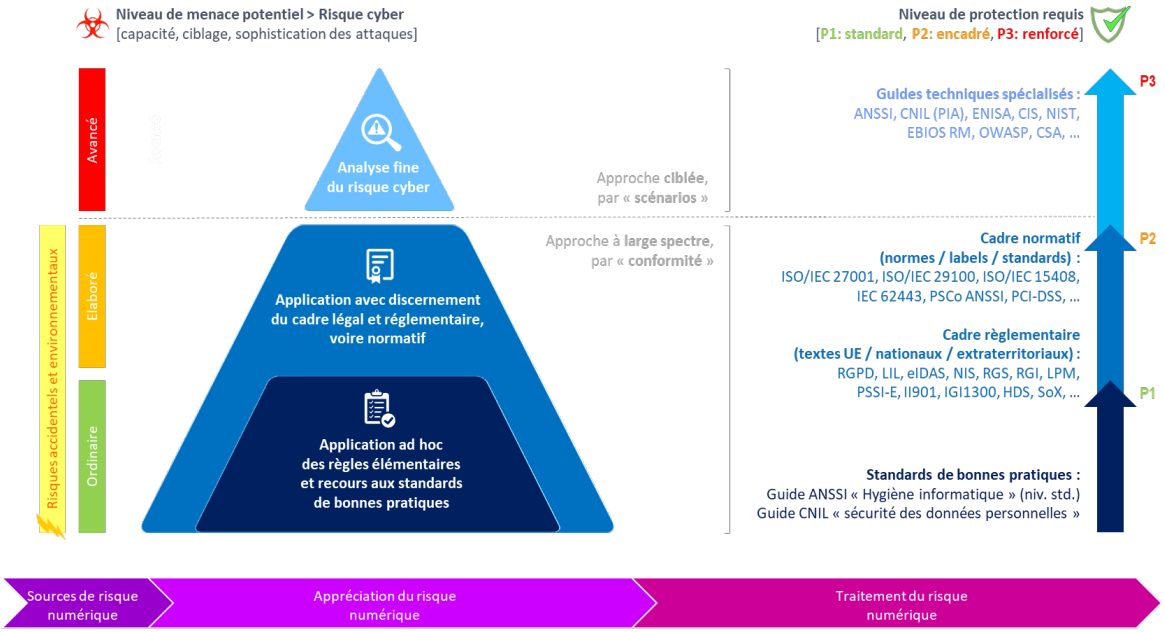
Du point de vue du RSSI :

❑ Peuvent être précisées dans des codes de conduite élaborés par les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants, *« les mesures et les procédures visées aux articles 24 et 25 et les mesures visant à assurer la sécurité du traitement visées à l'article 32 »* (RGPD, art.40, 2, h).

❑ Protection des données dès la conception et par défaut : *« Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément attestant du respect des exigences énoncées aux paragraphes 1 et 2 du présent article. »* (RGPD, art. 25, 3)

2. La mise en conformité via l'approche par les risques

Pourtant, et malgré les risques encourus en cas de non-respect de la réglementation, beaucoup d'entreprises ont besoin d'être accompagnées. Les normes sont là pour aider les entreprises à respecter les lois et règlements, quelle que soit la juridiction où elles opèrent. Mais entre les différents textes de lois, règlements, normes et standards, il est important de prioriser ses actions et de rester pragmatique en mettant en place une démarche globale d'amélioration continue.



Source : Société CONIX à partir d'EBIOS RM

3. Les normes et standards relatifs à la protection de la vie privée

3.1. Guides et normes (tous secteurs)

Sigle	Type de référentiel	Emetteur	Titre	Champ d'application
SEC-DP	Guide	CNIL	La sécurité des données personnelles (v2018)	Protection vie privée
HYG-INF	Guide	ANSSI	Hygiène informatique (v2.0) - règles de niveau standard	Sécurité informatique
Avis-CEPD	Guide	CEPD	Les lignes directrices du CEPD relativement au RGPD	Protection vie privée
HYG-INF	Guide	ANSSI	Hygiène informatique (v2.0) - règles de niveau renforcé	Sécurité informatique
ISO-27001	Norme internationale	ISO/IEC	Systèmes de management de la sécurité de l'information [ISO/IEC 27001:2013]	Sécurité de l'information

ISO-27002	Norme internationale	ISO/IEC	Code de bonne pratique pour le management de la sécurité de l'information [ISO/IEC 27002:2013]	Sécurité de l'information
ISO-27701	Norme internationale	ISO/IEC	Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices [ISO/IEC 27701:2019] (anciennement projet de norme ISO-27552)	Protection vie privée
ISO-29100	Norme internationale	ISO/IEC	Cadre privé [ISO/IEC 29100:2011]	Protection vie privée
ISO-29101	Norme internationale	ISO/IEC	Architecture de référence de la protection de la vie privée [ISO/IEC 29101:2018]	Protection vie privée
ISO-29134	Norme internationale	ISO/IEC	Lignes directrices pour l'évaluation d'impacts sur la vie privée [ISO/IEC 29134:2017]	Protection vie privée
ISO-29151	Norme internationale	ISO/IEC	Code of practice for personally identifiable information protection [ISO/IEC 29151:2017]	Protection vie privée
ISO-27005	Norme internationale	ISO/IEC	Gestion des risques liés à la sécurité de l'information [ISO/IEC 27005:2018]	Management des risques
ISO-31000	Norme internationale	ISO/IEC	Management du risque – Lignes directrices [ISO/IEC 31000:2018]	Management des risques
OWASP 2017	Guide	OWASP	Les 10 vulnérabilités Web les plus importantes : OWASP Top 10 2017	Sécurité de l'information sur le Web
EBIOS RM	Méthode	ANSSI	Méthode d'appréciation et de traitement des risques numériques	Management des risques

3.2. Spécificités sectorielles ou technologiques

Sigle	Type de référentiel	Emetteur	Titre	Champ d'application
CSA-BD-SP	Guide méthodologique	CSA	Big data - Security and privacy handbook	Sécurité et Protection vie privée en Big Data
ISO-27018	Guide	ISO/IEC	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [ISO/IEC 27018:2019]	Protection vie privée en cloud
ISO-27017	Guide	ISO/IEC	Code of practice for information security controls based on ISO/IEC 27002 for cloud services [ISO/IEC 27017:2015]	Sécurité de l'information en cloud
ISO-27550	Guide	ISO/IEC	Privacy engineering for system life cycle processes [ISO/IEC TR 27550:2019]	Protection dès la conception et par défaut
ISO-18370	Framework	ISO/IEC	ISO 18370 (2016) : Blind digital signatures [ISO/IEC 18370-1:2016]	Signatures et chiffrement
ISO-29191	Framework	ISO/IEC	Requirements for partially anonymous, partially unlinkable authentication [ISO/IEC 29191:2012]	Protection vie privée et authentification

ISO-20889	Guide	ISO/IEC	ISO 20889 (2018) : Privacy enhancing data de-identification techniques [ISO/IEC 20889:2018]	Protection vie privée et anonymisation
ISO-24745	Guide	ISO/IEC	Protection des informations biométriques [ISO/IEC 24745:2011]	Protection de données biométriques
ISO-27032	Guide	ISO/IEC	Guidelines for cybersecurity [ISO/IEC 27032:2012]	Cybersécurité
ISO-27035	Norme internationale	ISO/IEC	Gestion des incidents de sécurité de l'information — Partie 1 : Principes de la gestion des incidents et Partie 2 : Lignes directrices pour planifier et préparer une réponse aux incidents [ISO/IEC 27035:2016]	Gestion des incidents

3.3. Travaux de normalisation en cours

ISO-27030	Guide	ISO/IEC	Guidelines for security and privacy in Internet of Things (IoT)	Sécurité et Protection vie privée en IoT
ISO-27045	Framework	ISO/IEC	Big data security and privacy – Processes	Sécurité et Protection vie privée en Big Data
ISO-20547-4	Guide	ISO/IEC	Big data reference architecture -- Part 4: Security and privacy	Sécurité et Protection vie privée en Big Data
ISO-23244	Guide	ISO/IEC	Blockchain and distributed ledger technologies – Overview of privacy and personally identifiable information (PII) protection	Protection vie privée en Blockchain
ISO-27555	Guide	ISO/IEC	Establishing a PII deletion concept in organizations	Protection vie privée
ISO-27556	Framework	ISO/IEC	User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences	Protection vie privée
ISO-27570	Guide	ISO/IEC	Privacy guidelines for smart cities	Protection vie privée en Smart Cities
ISO-29184	Norme internationale	ISO/IEC	Online privacy notices and consent	Protection vie privée
ISO-29190	Framework	ISO/IEC	Privacy capability assessment model	Protection vie privée
ISO-31700	Norme internationale	ISO/IEC	Privacy by design for consumer goods and services	Protection vie privée

Sources :

https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
https://www.iso.org/fr/news/ref2419.html
https://normalisation.afnor.org/actualites/protection-donnees-personnelles-guide-afnor-recense-normes-incontournables/
https://marketing.afnor.org/fr/normalisation/guide-eprivacy
https://www.iso.org/fr/committee/45306.html
https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_fr