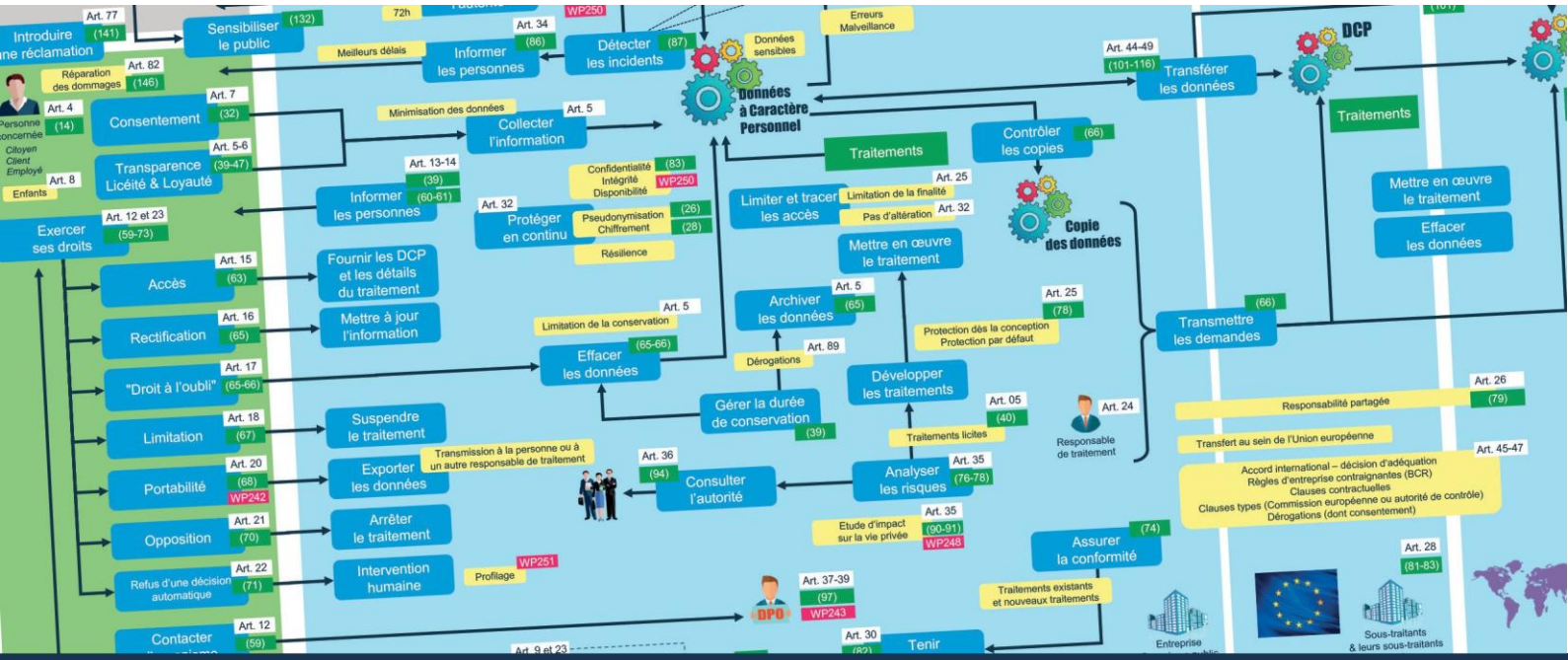
LES FICHES PRATIQUES du CLUSIF - RGPD



QU'EST-CE QUI CHANGE AVEC LE RGPD ?

Le règlement vient garantir un respect plus large et plus effectif des données à caractère personnel, bien que les grands principes restent les mêmes.

Le règlement renforce les droits des citoyens européens et leur donne plus de contrôle sur leurs données personnelles. Il simplifie les formalités pour les entreprises et leur offre un cadre juridique unifié avec la mise en place d'une législation unique dans l'Union européenne.

Le règlement permet :

- Pour le citoyen, un **renforcement des droits existants, notamment en lui permettant de disposer d'informations complémentaires sur le traitement de ses données mais également de les obtenir sous une forme claire, accessible et compréhensible.** Le droit à l'oubli est conforté et un nouveau droit à la portabilité est prévu, rendant ainsi plus effective la maîtrise de ses données par la personne. Les mineurs font également l'objet d'une protection particulière ;
- Pour les entreprises et organismes, une **simplification des formalités, la possibilité d'un interlocuteur unique pour toutes les autorités de contrôle européennes** et la mise à disposition d'une boîte à outils de conformité dont certains seront nouveaux (ex : code de conduite, certification). Ces outils pourront être modulés en fonction du risque sur les droits et libertés des personnes (ex : tenue d'un registre, consultation des autorités de contrôle, notification des violations de données). Le règlement européen impose également une **sécurité renforcée des traitements** ;
- Pour les autorités de contrôle, une affirmation de leurs compétences dès lors qu'il existe un établissement sur le territoire de l'Union ou que leurs citoyens sont affectés par le traitement, mais également un renforcement de leurs pouvoirs, notamment répressifs avec la possibilité de prononcer des sanctions administratives pouvant aller jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise concernée. Surtout, les « CNIL » européennes pourront désormais prononcer des décisions conjointes, aussi bien pour constater la conformité d'un organisme que pour prononcer une sanction. Cette intégration européenne renforcera ainsi la protection des personnes et la sécurité juridique pour les entreprises.

Les principales évolutions résultant du règlement sont résumées ci-après.

D'un régime déclaratif, à un régime d'auto-contrôle continu pour démontrer / documenter la conformité, notamment via :

(i) Le recensement des traitements ;
(ii) L'analyse d'impact si nécessaire ;
(iii) Les mesures techniques et organisationnelles selon les risques que représentent les traitements.

Avant le règlement	Avec le règlement
- Déclaration des traitements par le responsable de traitement, sauf en cas de dispense : - Demande d'autorisation CNIL ; - Déclaration normale ou simplifiée CNIL (sauf désignation d'un CIL qui tiendra un registre).	- Cartographie des traitements par le responsable de traitement et le sous-traitant ; - Établissement obligatoire d'un registre des traitements (*RGPD, Art. 30*) ; - Formalités déclaratives préalables résiduelles pour les traitements les plus risqués (*RGPD, C89, Art. 36, 46*, lois nationales…) ; - Adopter le « réflexe » données personnelles : *Accountability*, *Protection by design* (*RGPD, Art. 24, 25*), rôle du Délégué à la Protection des Données.

Vers une responsabilisation de tous les acteurs des traitements de données, impliquant de revoir les contrats entre les différents acteurs :

Avant le règlement	Avec le règlement
- Responsabilité endossée par le responsable de traitement en cas de non-respect de la réglementation ; - Amendes administratives par la CNIL jusqu'à 300 000 € (3 000 000 € avec la Loi pour une République Numérique).	- Tous les acteurs sont responsables (*RGPD, Art. 26, 28, et 82*) : o Responsabilité conjointe des traitements ; o Le sous-traitant est aussi responsable (sécurité et confidentialité des données + obligation de collaborer) ; - Des sanctions à la hauteur des enjeux prononcées par une autorité de contrôle européenne : jusqu'à 4% du chiffre d'affaires mondial ou 20 000 000 € (*RGPD, Art. 83*).

Plus de droits pour les personnes concernées :

Avant le règlement	Avec le règlement
Les personnes physiques bénéficient de droits : - d'interrogation, d'accès et d'opposition à leurs données personnelles ; - de voir leurs données rectifiées, complétées, mises à jour, verrouillées ou effacées si nécessaire ; - de définir leurs directives données personnelles après leur décès (spécificité de la loi française).	Renforcement des droits des personnes physiques (*RGPD, Art. 12 à 23*) : - Droit à l'oubli, à la limitation des traitements, à la portabilité des données ; - Droits de refus d'une décision individuelle automatisée fondée sur un traitement de données, y compris le profilage ; - Droit d'être consulté (en cas d'analyse d'impact) et de recevoir une notification (en cas de violation de données) ; - Actions de groupe pour faire cesser le traitement, mais pas pour obtenir réparation dans la Loi Française…

Les outils de mise en conformité :

Avant le règlement	Avec le règlement
- Site internet et décisions de la CNIL ; - Labels CNIL[1] ; - Packs de conformité sectoriels de la CNIL[2] ; - Rapports annuels de la CNIL[3].	- Codes de conduite par secteur, approuvés par les autorités de contrôle (*RGPD, Art. 40*) ; - Certifications et labels par des organismes de certification ou par les CNIL (*RGPD, Art. 42*)[4] ; - Guides et logiciel PIA de la CNIL ; - (…)

[1] https://www.cnil.fr/fr/les-labels-cnil
[2] https://www.cnil.fr/fr/packs-de-conformite
[3] https://www.cnil.fr/fr/mediatheque/rapports-annuels
[4] Il faut cependant noter que ces certifications ne sont pas encore disponibles.