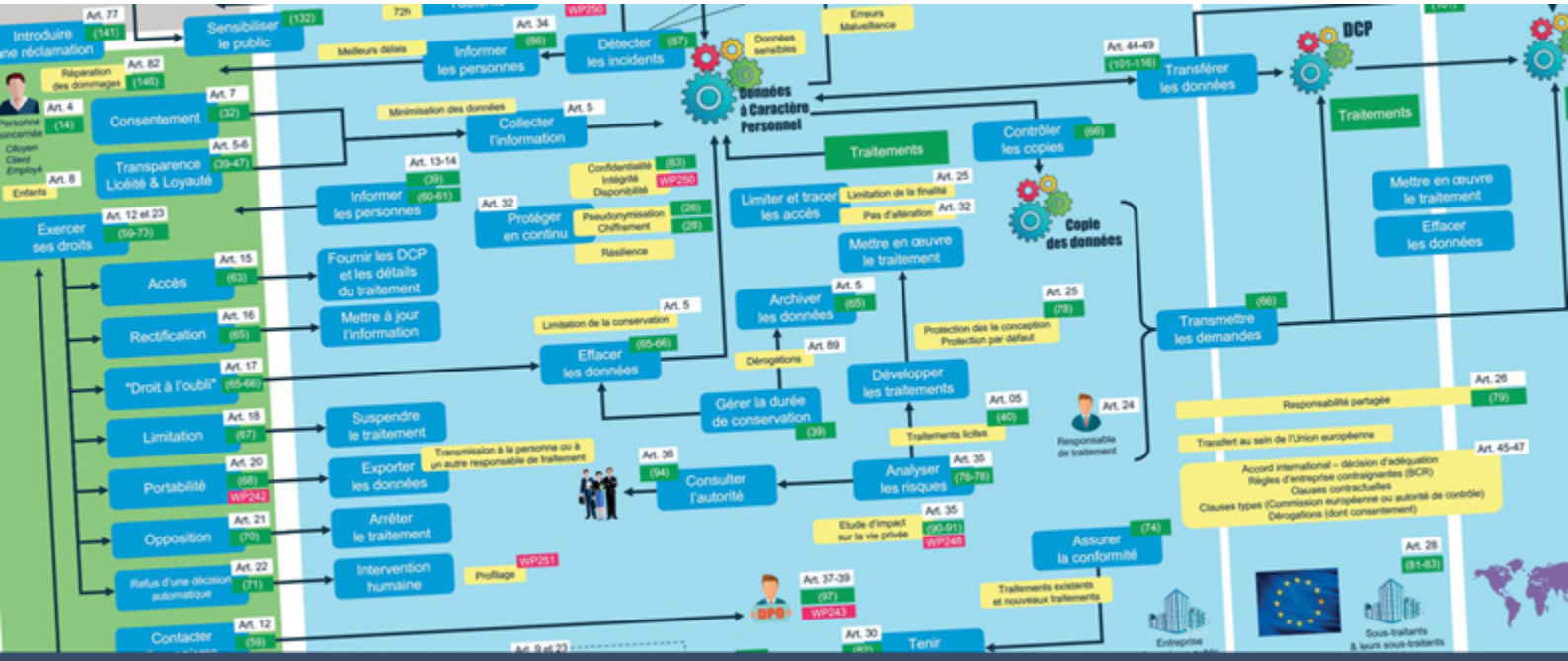
CLUSIF

LES GUIDES PRATIQUES DU CLUSIF - RGPD



LES RÉGLEMENTATIONS LIÉES À LA PROTECTION DES DCP

1. LE CONTEXTE

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

Depuis le principe posé dans la Déclaration universelle des droits de l'Homme, les institutions nationales et internationales n'ont eu de cesse de légiférer sur le sujet.

Cette mosaïque de lois et règlements devient alors complexe à appréhender pour les organisations, de plus en plus tournées vers l'international, notamment dans le cadre de partage ou de transferts de données personnelles.

2. LA RÉGLEMENTATION APPLICABLE EN UNION EUROPÉENNE ET EN FRANCE

La liste suivante n'est pas exhaustive et apporte un regard orienté pour les DPO et les RSSI concernés par la protection de la vie privée et la sécurité de l'information.

Sigle	Origine	Porteur	Titre
RGPD	Règlement européen (UE)	DPO	Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, couramment appelé « Règlement général sur la protection des données ». **[UE/2016/679]**
RGPD : Lignes directrices	CEPD / EDPB (UE)	DPO	RGPD : Lignes directrices, recommandations, bonnes pratiques du Comité Européen de la Protection des Données (CEPD) : https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_fr
POL-JUS	Directive européenne (UE)	DPO	Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, couramment appelée directive « Police-Justice ». [**UE/2016/680]**
NIS	Directive européenne (UE)	RSSI	Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, couramment appelée « Directive NIS ». **[UE/2016/1148]**
eIDAS	Règlement européen (UE)	RSSI	Règlement (UE) 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. **[UE/2014/910]**
DSP2	Règlement européen (UE)	RSSI	Directive (UE) 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur. **[UE/2015/2366]**
CYB-ACT	Règlement européen (UE)	RSSI	Règlement (UE) 2019/881 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, couramment appelé « Cyber Act ». **[UE/2019/881]**
E-Privacy	Règlement européen (UE)	DPO	Règlement (UE) 2019/881 concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »), couramment appelé « Règlement e-Privacy » – Non promulgué
LIL	Loi française (FR)	DPO	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, couramment appelée loi « Informatique et libertés » et son décret d'application n° 2019-536 du 29 mai 2019 à la suite de la mise en conformité avec le RGPD.

LCEN	Loi française (FR)	RSSI	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
RGS	Arrêté du 13 juin 2014 (FR)	RSSI	Référentiel Général de Sécurité, cadre règlementaire permettant d'instaurer la confiance dans les échanges électroniques au sein de l'administration et avec les citoyens : https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
PSSIE	Circulaire française Secteur public (FR)	RSSI	Circulaire du Premier ministre du 17 juillet 2014 portant sur la politique des systèmes d'information de l'Etat et fixant les règles de protection applicables aux systèmes d'information de l'État.
LPM	Loi française (FR)	RSSI	Loi n° 2018-607 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense.
DSP2 FR	Loi française (FR)	RSSI	Loi n° 2018-700 ratifiant l'ordonnance n° 2017-1252 du 9 août 2017 portant transposition de la directive 2015/2366 concernant les services de paiement dans le marché intérieur.
Santé	Cadre réglementaire (FR)	DPO et RSSI	Se référer au dossier technique du Clusif sur le sujet : https://clusif.fr/publications/le-traitement-des-donnees-de-sante/
Codes publics	Lois françaises (FR)	RSSI	Code civil, code pénal, code des relations entre le public et l'administration, code de la santé publique, code de la sécurité sociale, etc. : https://www.legifrance.gouv.fr/

Concernant l'articulation et la hiérarchisation des textes européens (règlement, directive) avec le droit français (loi, décret, arrêté, etc.), le document **« Vademecum juridique[1] »** du Clusif et de Cyberlex sera une aide précieuse.

3. SPÉCIFICITÉS DES ÉTATS MEMBRES DE L'UE

Un « règlement » est directement applicable et a un effet uniforme dans tous les États membres. Cependant, le RGPD autorise les États membres à légiférer différemment sur plus de 50 sujets dans leurs propres lois nationales sur la protection des données. D'où l'importance de consulter ces lois nationales en cas de transferts de données.

Etat	Site de l'autorité	Loi nationale (post RGPD)
Allemagne	https://www.bfdi.bund.de	L'Allemagne a adapté son cadre juridique au RGPD en adoptant la nouvelle loi fédérale allemande sur la protection des données (Bundesdatenschutzgesetz ou BDSG). Le BDSG est entré en vigueur avec le RGPD.

[1] https://clusif.fr/publications/vademecum-obligations-juridiques-liees-aux-systemes-dinformation/

Autriche	https://www.dsb.gv.at	La loi sur la protection des données (Datenschutzgesetz, DSG) tend à remplacer la précédente loi, DSG 2000. Elle prévoit la mise en œuvre des dispositions du RGPD et comprend également la transposition et la directive [UE/2016/680].
Belgique	https://www.autoriteprotectiondonnees.be	La « Data Protection Act » du 30 juillet 2018 relative à la protection des données. Elle prévoit la mise en œuvre des dispositions du RGPD et comprend également la transposition et la directive [UE/2016/680].
Bulgarie	http://www.cpdp.bg	La dernière rédaction du 26 février 2019 de la loi sur la protection des données personnelles est en cours.
Chypre	http://www.dataprotection.gov.cy	La loi 125(I)/2018 relative à la protection des personnes physiques contre le traitement des données à caractère personnel et à la libre circulation de ces données transpose certaines dispositions du RGPD en droit local, est entrée en vigueur le 31 juillet 2018.
Croatie	http://www.azop.hr	La « Loi » (ou « Act ») sur la mise en œuvre RGPD a été adoptée par le Parlement croate le 27 avril 2018 et est entrée en vigueur avec le RGPD.
Danemark	http://www.datatilsynet.dk	Le Danemark a adapté son cadre juridique au RGPD avec la « Danish Data Protection Act ». Elle est entrée en vigueur avec le RGPD et a remplacé la précédente loi danoise sur le traitement des données personnelles (loi n° 429 du 31/05/2000). La loi danoise sur la protection des données ne s'applique pas au Groenland et aux îles Féroé.
Espagne	http://www.agpd.es	La nouvelle loi fondamentale espagnole sur la protection des données et la garantie des droits numériques est entrée en vigueur le 7 décembre 2018 (« NLOPD »). Elle a abrogé l'ancienne loi organique 15/1999 (LOPD).
Estonie	http://www.aki.ee/et	La nouvelle loi sur la protection des données personnelles (PDPA) complète le RGPD. Des amendements au Code pénal ont été proposés pour permettre l'imposition en Estonie des amendes prévues dans le cadre du RGPD. Le nouveau PDPA est entré en vigueur le 15 janvier 2019.
Finlande	http://www.tietosuoja.fi	La Finlande a adopté une loi complémentaire de mise en œuvre du RGPD, la loi finlandaise sur la protection des données (Tietosuojalaki) (1050/2018), entrée en vigueur le 1er janvier 2019. D'autres lois clés concernent la confidentialité et la protection des données : loi sur les services de communication électronique (917/2014), loi sur la protection de la vie privée dans la vie professionnelle (759/2004).
France	https://www.cnil.fr	La France a mis à jour la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés suivant le RGPD. L'adoption du décret n° 2019-536 clarifie les règles de procédure de l'autorité française, la CNIL, et précise les droits des personnes concernées.
Grèce	http://www.dpa.gr	La loi grecque 4624/2019 a mis à jour l'ancienne loi 2472/1997 suivant les mesures légales d'application du RGPD et de la directive POL-JUS. La HDPA (Hellenic Data Protection Authority) est l'autorité grecque.
Hongrie	http://www.naih.hu	Le Parlement hongrois a mis en œuvre le RGPD en modifiant la loi CXII de 2011 sur le droit à l'autodétermination informationnelle et sur la liberté d'information. Depuis le 26 avril 2019, toutes les lois sectorielles ont également été modifiées suivant le RGPD.

Irlande	http://www.dataprivacy.ie	La loi irlandaise («DP Act») est entrée en vigueur le 25 mai 2018 et comprend certaines dérogations au RGPD, prévoit l'établissement d'une nouvelle commission de protection des données (DPC). La législation précédente continue de s'appliquer (sécurité et défense nationale) ainsi que pour les plaintes, infractions survenues avant le 25 mai 2018.
Italie	http://www.garanteprivacy.it	Le cadre juridique italien a été harmonisé avec le RGPD par le biais du décret législatif 101/2018, entré en vigueur le 19 septembre 2018, qui a modifié des dispositions du décret législatif 196/2003 (Testo Unico).
Lettonie	http://www.dvi.gov.lv	La loi sur le traitement des données personnelles est entrée en vigueur le 5 juillet 2018. Cette loi a fourni les conditions juridiques préalables à la mise en œuvre du RGPD et a remplacé la loi antérieure.
Lituanie	http://www.ada.lt	La mise en œuvre du RGPD a été réalisée au travers de la loi sur la protection des données, en vigueur depuis le 16 juillet 2018 (N° XIII-1426) et a remplacé la loi antérieure. La directive POL-JUS a été déclinée suivant la loi N° XIII-1435.
Luxembourg	http://www.cnpd.lu	La loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données (CNPD) et du régime général sur la protection des données a été promulguée le 1er août 2018. Elle a abrogé la précédente loi sur la protection des données (loi modifiée du 2 août 2002) et complète le RGPD au niveau national.
Malte	http://www.dataprotection.gov.mt	Le chapitre CAP 586 des lois de Malte (Data Protection Act) est la loi portant sur la protection des données. Elle a été promulguée en 2018. Elle possède actuellement 8 législations subsidiaires (S.L.586.04 : mineurs, S.L.586.10 : santé, S.L.586.01 : communication électronique, etc.). La loi de 2018 a abrogé et remplacé la précédente loi sur la protection des données (chapitre CAP 440). L'IDPC (Information and Data Protection Commissioner) est l'autorité maltaise en charge de la protection des données.
Pays-Bas	https://www.autoriteitpersoonsgegevens.nl	La loi néerlandaise de mise en œuvre du RGPD suit une approche politique neutre, ce qui signifie que les exigences de la précédente loi néerlandaise (Loi du 6 juillet 2000) sur la protection des données sont maintenues autant que possible dans le respect du cadre du RGPD. La Dutch Data Protection Authority (DPA) est l'autorité néerlandaise en charge de la protection des données.
Pologne	https://uodo.gov.pl	La loi sur la protection des données personnelles du 10 mai 2018 est entrée en vigueur le 25 mai 2018 (Journal of Laws of 2019, item 1781, «PDPA»). Une seconde loi apporte des amendements aux lois sectorielles (droit bancaire, assurances, droit du travail, etc.). Elle est entrée en vigueur le 4 mai 2019 (Journal of Laws of 2019, item 730 «Acte d'exécution»). UODO est l'autorité polonaise en charge de la protection des données.
Portugal	https://www.cnpd.pt	Le traitement des données personnelles est régi en sus du RGPD par la loi n° 58/2019 du 8 août qui garantit l'exécution du règlement au Portugal. Cependant, l'autorité de contrôle locale (CNPD) a publié la décision 494/2019 décidant de ne pas appliquer certaines dispositions de cette loi (car considérées comme étant en contradiction avec le RGPD). La loi n° 59/2019 contient elle la transposition des dispositions relatives à la directive POL-JUS.

République tchèque	http://www.uoou.cz	La nouvelle loi tchèque n° 110/2019 (ZZOÙ) sur le traitement des données personnelles est entrée en vigueur le 24 avril 2019. Cette loi a remplacé l'ancienne loi (n° 101/2000 Coll., telle que modifiée) et réglemente le traitement des données personnelles dans le cadre du RGPD et de la directive POL-JUS. Il régit également la compétence de l'autorité pour la protection des données personnelles (Czech DPA).
Roumanie	http://www.dataprotection.ro	La loi n°190/2018 sur les mesures d'application du règlement est devenue applicable le 31 juillet 2018. Elle modifie la loi précédente n° 102/2005 du 3 mai 2005. L'ANSPDCP est l'autorité en charge de la protection des données personnelles en Roumanie.
Royaume-Uni	https://ico.org.uk	Le RGPD est entré en vigueur au Royaume-Uni le 25 mai 2018, mais le Royaume-Uni a quitté l'UE le 31 janvier 2020. Le traité de retrait UE - Royaume-Uni prévoit une période de transition allant jusqu'à la fin de 2020 (sauf prolongation d'un commun accord). Pendant cette période, le droit de l'UE (y compris le RGPD) continue de s'appliquer directement au Royaume-Uni. Après la fin de la période de transition, le droit communautaire cessera de s'appliquer au Royaume-Uni. Parallèlement au RGPD et à la directive POL-JUS, le Royaume-Uni a préparé une nouvelle loi nationale sur la protection des données, la Data Protection Act 2018 («DPA»), en vigueur le 25 mai 2018.
Slovaquie	http://www.dataprotection.gov.sk	La Slovaquie a adopté la loi n° 18/2018 relative à la protection des données à caractère personnel et modifiant et complétant certains actes pour mettre en œuvre le RGPD. Elle est entrée en vigueur le 25 mai 2018.
Slovénie	https://www.ip-rs.si	La nouvelle loi slovène sur la protection des données (ZVOP-2) qui mettra en œuvre certains aspects du RGPD n'a toujours pas été adoptée. Actuellement, outre le RGPD, la ZVOP-1 reste applicable : plus précisément, les dispositions qui ne sont pas régies par le règlement et qui ne sont pas en contradiction avec celui-ci s'appliquent.
Suède	http://www.datainspektionen.se	La loi sur la protection des données (2018:218) et l'ordonnance sur la protection des données (2018:19) régit les aspects généraux de la protection des données lorsque le RGPD le permet. La loi est entrée en vigueur le 25 mai 2018. En plus de la loi suédoise sur la protection des données, un grand nombre de lois sectorielles ont été adoptées en Suède (santé, finances, énergie, environnement, éducation, etc.). Les amendements aux lois concernées sont entrés en vigueur le 1er janvier 2019.

Source : https://www.dlapiperdataprotection.com/index.html?c=FR&c2=&go-button=GO&t=law

4. LES TEXTES INTERNATIONAUX RELATIFS À LA PROTECTION DES DONNÉES

4.1. DUDH - Déclaration universelle des droits de l'Homme et CEDH

La Déclaration universelle des droits de l'Homme a été adoptée en 1948 par l'ONU.

L'article 12 de la DUDH stipule notamment que : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. » [2]

Peu après l'adoption de la DUDH, l'Europe a également affirmé ce droit dans la Convention européenne des droits de l'homme (CEDH), un traité établi en 1950 et juridiquement contraignant pour ses Parties contractantes. La CEDH dispose que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Toute ingérence d'une autorité publique dans l'exercice de ce droit est prohibée à moins que cette ingérence ne soit

[2] https://www.un.org/fr/universal-declaration-human-rights/

prévue par la loi, poursuive des intérêts publics importants et légitimes et soit nécessaire dans une société démocratique.

La CEDH dispose que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Toute ingérence d'une autorité publique dans l'exercice de ce droit est prohibée à moins que cette ingérence ne soit prévue par la loi, poursuive des intérêts publics importants et légitimes et soit nécessaire dans une société démocratique.

« Le droit au respect de la vie privée et le droit à la protection des données à caractère personnel sont étroitement liés. Ces deux droits diffèrent par leur formulation et leur portée. Le droit au respect de la vie privée consiste en une interdiction générale de toute ingérence, sous réserve de certaines conditions d'intérêt public de nature à justifier une ingérence dans certains cas. La protection des données à caractère personnel est considérée comme un droit moderne et actif, qui met en place un système de contrôles et de mises en balance afin de protéger les individus chaque fois que leurs données à caractère personnel sont traitées.[3] »

4.2. ONU

En 1990, les Nations Unies ont publié la Résolution 45/95 [4] qui contient une liste de principes de base pour la protection des données personnelles d'application mondiale, tels que leur exactitude, leur finalité, leur accès et leur non-discrimination. Les modalités de mise en œuvre des règles relatives aux fichiers informatisés de données à caractère personnel sont laissées à l'initiative de chaque État, dans le respect des orientations listées dans la résolution[5].

A la suite de l'essor des nouvelles technologies et aux révélations de l'affaire SNOWDEN concernant la surveillance de masse, l'ONU a adopté 2 résolutions en 2013 (A/RES/68/167, et A/C.3/69/L.26/Rev.1) liées à la vie privée. Celles-ci ont été révisées en 2016.[6]

Pour aller plus loin, et plus particulièrement à propos des données sensibles liées à la biométrie, l'ONU a défini un guide qui rappelle les différentes réglementations de données personnelles et émet des recommandations pour l'utilisation et le partage de la biométrie dans la lutte contre le terrorisme.[7]

En 2017, le Conseil de Sécurité de l'ONU adopte à l'unanimité la résolution 2396. Les États membres de l'ONU doivent élaborer et mettre en œuvre des systèmes de collecte de données biométriques dans le respect du droit interne et du droit international des droits de l'homme. Dans le cadre de la lutte contre le terrorisme, ces données pourront être échangées entre Etats, et avec Interpol et d'autres organismes internationaux compétents.[8]

4.3. OCDE

Le Conseil de l'Organisation de coopération et de développement économiques a réglementé le traitement des données à caractère personnel et le flux international de ces données en 1980 par un ensemble de lignes directrices concernant la protection de la vie privée et les mouvements transfrontaliers de données à caractère personnel.[9]

Ainsi, le Conseil de l'OCDE reconnaît déjà expressément que « les mouvements transfrontières de données à caractère personnel contribuent au développement économique et social » mais rappelle en même temps que « la législation nationale concernant la protection de la vie privée et les mouvements transfrontières des données personnelles peut empêcher ces mouvements transfrontaliers ».

L'OCDE, consciente de la nécessité d'accords de coopération internationaux et afin de permettre une meilleure coopération entre les autorités dans l'application des législations protégeant la vie privée a adopté en 2007 la recommandation relative à la coopération transfrontière dans l'application des législations protégeant la vie privée.[10]

Toutefois, l'efficacité des principes directeurs de l'OCDE est limitée : il s'agit de recommandations et elles ne sont donc pas juridiquement contraignantes, donc non exécutoires.

[3] https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_fr.pdf

[4] https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/567/42/IMG/NR056742.pdf

[5] http://hrlibrary.umn.edu/instree/french/Fq2grcpd.html

[6] https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1&Lang=F

[7] https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf

[8] https://www.un.org/press/en/2017/sc13138.doc.htm

[9] http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(98)12&docLanguage=Fr

[10] https://edps.europa.eu/sites/edp/files/publication/2013-09-09_oecd_guidelines_en.pdf

4.4. Conseil de l'Europe – Convention 108

Le Conseil de l'Europe adopte en 1981 la Convention de Strasbourg ou **Convention 108**[11] pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Elle étend ainsi la protection du citoyen et plus particulièrement son droit du respect de sa vie privée, en prenant en compte l'augmentation des flux de données personnelles au travers de traitements automatisés.

Ce fut le premier instrument international contraignant[12] qui a pour objet de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel, et qui réglemente les flux transfrontaliers des données.

Ce texte de 27 articles, modernisé depuis, est toujours en vigueur et a largement inspiré la directive européenne 95/46[13]/CE puis le RGPD. On notera ainsi les articles initiaux suivants :

Article 6 – Catégories particulières de données

Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénales.

Article 7 – Sécurité des données

Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés.

Article 12 – Flux transfrontières de données à caractère personnel et droit interne

1. Les dispositions suivantes s'appliquent aux transferts à travers les frontières nationales, quel que soit le support utilisé, de données à caractère personnel faisant l'objet d'un traitement automatisé ou rassemblées dans le but de les soumettre à un tel traitement.

2. Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre Partie.

3. Toutefois, toute Partie a la faculté de déroger aux dispositions du paragraphe 2 :

a) dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente;

b) lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe.

Du point de vue du DPO :

- L'article 6 rappelle les articles 9 et 10 du règlement définissant les données sensibles
- L'article 7 rappelle l'article 32 du règlement sur la sécurité des traitements.
- L'article 12 rappelle l'article 44 du règlement sur les transferts.
  On notera le changement de paradigme entre ces deux textes. Pour la Convention 108 « Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières […] », alors que le RGPD pose le principe suivant « ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant […]».

[11] https://rm.coe.int/compilation-final-version/168094ea73
[12] https://www.echr.coe.int/Documents/FS_Data_FRA.pdf
[13] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046

Avec l'évolution des réglementations en Europe, le Conseil de l'Europe et l'UE ont veillé à assurer la cohérence et la compatibilité entre leurs deux cadres juridiques. La Convention 108 a ainsi fait l'objet d'une modernisation en parallèle du travail sur le RGPD. La modernisation préserve le caractère général et flexible de la Convention et renforce son potentiel d'instrument universel pour le droit de la protection des données. Le processus de modernisation s'est achevé avec l'adoption d'un Protocole d'amendement de la Convention 108 le 10 octobre 2018 (Protocole STCE nº 223). Les articles précédemment cités ont été modifiés.[14]

Aujourd'hui, 55 pays[15] ont ratifié cette convention, dont l'ensemble des 47 États membres du Conseil de l'Europe. L'Uruguay est le premier pays non européen à y avoir adhéré en août 2013, suivi au fil des années par Maurice, le Sénégal, la Tunisie, le Cap Vert, le Mexique, l'Argentine et enfin le Maroc en septembre 2019.

4.5. OSCE - Organisation pour la Sécurité et la Coopération en Europe

L'OSCE compte 57 Etats participants en Amérique du Nord, en Asie centrale et en Europe. C'est la plus grande organisation de sécurité régionale du monde. Elle trouve ses origines dans la phase de détente du début des années 1970, lorsque la Conférence sur la sécurité et la coopération en Europe (CSCE) a été créée pour servir de forum multilatéral de dialogue et de négociation entre l'Est et l'Ouest.

Le RGPD est notamment donné en référence pour la protection de la vie privée et des données pour le déploiement et l'utilisation de l'IA (Intelligence artificielle).[16]

4.6. APEC - Asia Pacific Economic Cooperation CDE

L'APEC a été créée en 1989 et compte 27 pays actuellement dont le Canada, les Etats-Unis, le Chili, le Pérou, le Mexique, la Russie, les Philippines, l'Indonesie, le Vietnam, le Japon, l'Australie, la Nouvelle-Zélande.

Le cadre de protection de la vie privée de l'APEC est un ensemble de principes et de lignes directrices qui ont été créés afin d'établir des mesures efficaces de protection de la vie privée et évitent les obstacles à la circulation de l'information dans la région Asie-Pacifique. Il est conforme aux valeurs fondamentales des lignes directrices de l'OCDE sur la protection de la vie privée.

Le cadre actualisé (2015) s'inspire des concepts introduits dans les Lignes directrices de l'OCDE (2013) en tenant dûment compte des différentes caractéristiques juridiques et du contexte de la région APEC.

Le Privacy Framework est disponible sur la site de l'APEC.[17]

Le 23 aout 2019, l'APEC a proposé une vue des réglementations sur la protection de la vie privée avec un panorama de plusieurs framework dont le RGPD. [18]

4.7. Etats-Unis

La constitution américaine ne garantit pas le droit général au respect de la vie privée car ne se réfère pas explicitement au respect de la vie privée. Les 1er, 3e, 4e et 5e amendements offrent plusieurs formes de protection contre l'intrusion gouvernementale dans la vie des individus. Mais c'est surtout le 4e amendement qui protège les droits des citoyens « dans leurs personnes, leurs maisons, leurs papiers et leurs effets » qui fourni la principale référence constitutionnelle à la protection de la vie privée aux Etats-Unis.[19]

Ainsi, Dans l'affaire Schmerber c. Californie, en 1966, la Cour suprême a déclaré que *« [ ]la fonction primordiale du quatrième amendement est de protéger la vie privée et la dignité contre l'intrusion injustifiée de l'Etat »*.

Le droit à la vie privée, qui n'est pas constitutionnellement garanti, relève donc des législations des différents Etats et de leur application par les tribunaux.

[14] http://rm.coe.int/16808ac919

[15] https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/223/signatures

[16] https://www.osce.org/files/f/documents/9/f/456319_0.pdf

[17] https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf

[18] http://mddb.apec.org/Documents/2019/CTI/TPD2/19_cti_tpd2_009.pdf

[19] http://www.senat.fr/lc/lc33/lc3312.html#fn8

En 1974, est adopté le **Privacy Act**[20] (loi relative à la protection des données personnelles collectées et utilisées par le pouvoir exécutif). Celle loi ne concerne cependant que le secteur public et fait suite au Watergate et à la loi d'accès à l'information FOIA (Freedom of Information Act). Elle est fondée sur le principe du droit à l'information et oblige les agences fédérales à transmettre leurs documents.

Concernant le secteur privé, les Etats-Unis ne possèdent pas de cadre juridique général mais, depuis les années 1970, le Congrès a adopté plusieurs lois couvrant un secteur. On pourra citer par exemple le « video privacy protection act » de 1988 concernant la protection des clients de magasins de location de vidéos, loi toujours utilisée dans le cadre des plateformes de streaming. Le « Health Insurance Portability and Accountability Act (HIPAA) » de 1996 permet au ministère concerné de promulguer des réglementations sur le respect de la vie privée des dossiers médicaux. On pourra aussi citer le « Children's Online Privacy Protection Act » de 1998 qui limite l'utilisation des informations collectées par des sites Internet auprès d'enfants de moins de 13 ans.

A partir de 2001, les Etats-Unis ont connu un tournant concernant la protection de la vie privée en promulgant des lois sécuritaires en réponse à la lutte contre le terrorisme. Ainsi, Le **Patriot Act** (2011) a accordé de très larges pouvoirs aux agences de renseignement qui peuvent obtenir un mandat obligeant les opérateurs de téléphonie à fournir l'intégralité des métadonnées téléphoniques de leurs clients américains. Le **Freedom Act** (2015) a fait suite aux révélations d'Edward Snowden, mais il permet encore aux services de renseignement d'obtenir les métadonnées des opérateurs téléphoniques, en faisant des demandes au cas par cas. Le **Cloud Act**, Clarifying Lawful Overseas Use of Data Act (2018) rend légale la saisie de toutes données numériques, y compris les emails, stockées sur des serveurs américains, y compris à l'étranger. Les GAFAM et les entreprises du cloud, filiales comprises, doivent s'y conformer. De même pour les entreprises non américaines dès lors qu'elles sont sur le territoire américain.

4.7.1. Bouclier de protection des données Union européenne - États-Unis

Depuis 2000, la mise en place d'un cadre juridique adapté était devenue nécessaire face aux échanges de données sur internet, et pour répondre à la la directive 95/46/CE. Un accord entre l'UE et les États-Unis a alors encadré la transmission et l'usage des données personnelles par les entreprises qui exercent leur activité dans un cadre transatlantique, c'était le **Safe Harbor**[21] (« Sphère de sécurité »).

Ce 1er accord est alors invalidé par la CJUE le 6 octobre 2015[22]. La Cour considère que les États-Unis n'offrent pas un niveau de protection adéquat aux données personnelles transférées. Des négociations sont alors entreprises et un nouvel accord transfrontalier voit le jour, le **Privacy shield**[23]. Celui-ci connaitra le même sort après 4 ans d'existence, il est invalidé par la CJUE le 16 juillet 2020[24].

Les différentes lois sécuritaires, les révélations liées au programme de surveillance électronique PRISM[25] ainsi que les plaintes de ressortissants de l'UE ont eu un fort impact sur les différents accords transfrontaliers négociés entre l'UE et le département du commerce des États-Unis.

4.7.2. Cas de la Californie

L'article 1, section 1 de la Constitution californienne stipule que « Tout individu est par nature libre et indépendant et possède des droits inaliénables. Parmi ceux-ci se trouvent la jouissance et la défense de la vie et de la liberté, l'acquisition, la possession et la protection des biens, ainsi que la poursuite et l'obtention de la sécurité, le bonheur et le respect de la vie privée ». Cette section a été amendée et adoptée le 5 novembre 1974.

Depuis le 1er janvier 2020, le California Consumer Privacy Act (CCPA)[26] régit le droit des données personnelles des consommateurs Californiens (et uniquement ceux-ci). Contrairement au RGPD qui s'applique à toutes les organisations, le CCPA est plus limité et traite des entreprises qui font des affaires dans l'État de Californie et qui répondent à au-moins un des 3 critères suivants :

- de grande taille (dont le revenu dépasse les 25 millions de dollars annuels)
- à but lucratif (qui génèrent plus de 50 % de leur chiffre d'affaires via la vente de données)
- traitent de données massives (ont des informations sur au moins 50 000 consommateurs, ménages ou équipements).

Le texte californien prévoit de plus une amende maximum de 7 500 dollars et 750 dollars de dommages intérêts maximum par consommateur et par infraction.

Le texte exclue de son champ d'application les traitements des données par les services publiques et notamment le gouvernement fédéral, les États fédérés ou les administrations locales. Les données sensibles ne sont pas non plus évoquées. Enfin, aucune autorité de contrôle, de type CNIL, n'est formulée par le CCPA.

[20] https://www.justice.gov/opcl/privacy-act-1974

[21] https://www.cnil.fr/en/node/545

[22] http://www.assemblee-nationale.fr/14/europe/rap-info/i3740.asp#P83_9491

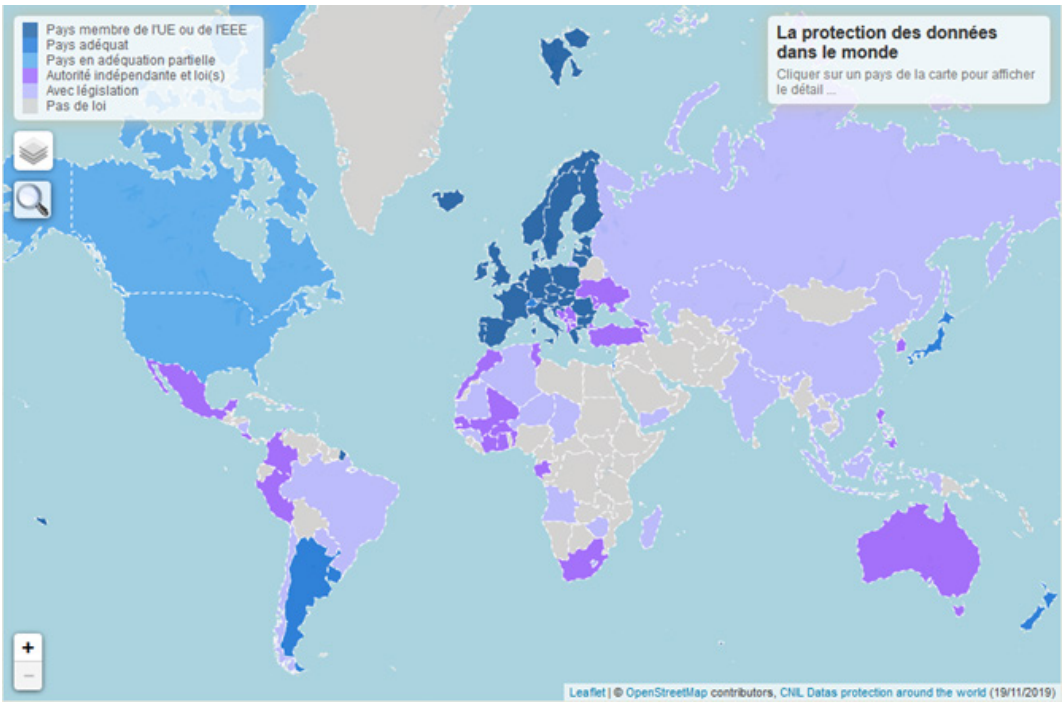
[23] https://www.cnil.fr/fr/le-privacy-shield

[24] https://www.cnil.fr/fr/invalidation-du-privacy-shield-la-cnil-et-ses-homologues-analysent-actuellement-ses-consequences

[25] https://www.cnil.fr/fr/affaire-prism-avis-du-g29-sur-la-surveillance-massive-des-citoyens-europeens

[26] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

5. EXTRATERRITORIALITÉ ET RESTE DU MONDE



Source CNIL - https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Etat	Site de l'autorité	Adéquation UE
27 Etats membres	Cf. §3 du document - Spécificités des Etats membres de l'UE	Totale : Membre de l'UE
Norvège	http://www.datatilsynet.no/ (Pays membre de l'EEE, l'espace économique européen, le RGPD s'applique)	Totale : Membre de l'EEE
Islande	http://www.personuvernd.is/ (Pays membre de l'EEE, l'espace économique européen, le RGPD s'applique)	Totale : Membre de l'EEE
Andorre	https://www.apda.ad/	Totale : Pays hors UE et EEE
Argentine	https://www.argentina.gob.ar/aaip/datospersonales/responsables/obligaciones	Totale : Pays hors UE et EEE
Guernesey	https://odpa.gg	Totale : Pays hors UE et EEE
Ile de Man	https://www.inforights.im/	Totale : Pays hors UE et EEE
Iles Féroé	http://www.dat.fo/	Totale : Pays hors UE et EEE
Israel	https://www.gov.il/en/departments/the_privacy_protection_authority	Totale : Pays hors UE et EEE
Japon	http://www.ppc.go.jp/en/	Totale : Pays hors UE et EEE

Jersey	https://jerseyoic.org/	Totale : Pays hors UE et EEE
Nouvelle-Zélande	https://www.privacy.org.nz/	Totale : Pays hors UE et EEE
Suisse	http://www.leprepose.ch/	Totale : Pays hors UE et EEE
Uruguay	http://www.datospersonales.gub.uy/	Totale : Pays hors UE et EEE
Canada	https://www.priv.gc.ca/fr/	Partielle
Etats-Unis	https://www.privacyshield.gov/ (Invalidation du Privacy Shield le 16 juillet 2020 par la CJUE : la CNIL et le CEPD procèdent actuellement à une analyse précise de l'arrêt)	Partielle
Etats-Unis – Californie *	California Consumer Privacy Act (CCPA) https://oag.ca.gov/privacy/ccpa (Invalidation du Privacy Shield le 16 juillet 2020 par la CJUE : la CNIL et le CEPD procèdent actuellement à une analyse précise de l'arrêt)	Partielle
Afrique du Sud	https://www.justice.gov.za/inforeg/docs.html	Autorité indépendante et loi(s) existante(s)
Albanie	https://www.idp.al/?lang=fr	Autorité indépendante et loi(s) existante(s)
Arménie	http://www.moj.am	Autorité indépendante et loi(s) existante(s)
Australie	https://www.oaic.gov.au/	Autorité indépendante et loi(s) existante(s)
Bénin	http://www.cnilbenin.bj/	Autorité indépendante et loi(s) existante(s)
Bosnie-Herzégovine	http://www.azlp.ba/Default.aspx?langTag=en-US	Autorité indépendante et loi(s) existante(s)
Burkina Faso	http://www.cil.bf/	Autorité indépendante et loi(s) existante(s)
Cap-Vert	https://www.cnpd.cv	Autorité indépendante et loi(s) existante(s)
Colombie	https://www.sic.gov.co/tema/proteccion-de-datos-personales	Autorité indépendante et loi(s) existante(s)
Corée du Sud	http://www.pipc.go.kr/cmt/main/english.do	Autorité indépendante et loi(s) existante(s)
Costa Rica	http://www.prodhab.go.cr/reformas/	Autorité indépendante et loi(s) existante(s)
Côte d'Ivoire	http://www.artci.ci/	Autorité indépendante et loi(s) existante(s)
Gabon	https://www.cnpdcp.ga/accueil2/	Autorité indépendante et loi(s) existante(s)
Géorgie	https://personaldata.ge/en	Autorité indépendante et loi(s) existante(s)
Ghana	http://www.dataprotection.org.gh	Autorité indépendante et loi(s) existante(s)
Gibraltar	http://www.gra.gi/	Autorité indépendante et loi(s) existante(s)

Hong-Kong	http://www.pcpd.org.hk/	Autorité indépendante et loi(s) existante(s)
Kosovo	http://www.amdp-rks.org	Autorité indépendante et loi(s) existante(s)
Macédoine	https://dzlp.mk/en	Autorité indépendante et loi(s) existante(s)
Mali	http://www.apdp.ml	Autorité indépendante et loi(s) existante(s)
Maroc	https://www.cndp.ma/fr/	Autorité indépendante et loi(s) existante(s)
Maurice	https://dataprotection.govmu.org/SitePages/Index.aspx	Autorité indépendante et loi(s) existante(s)
Mexique	http://inicio.ifai.org.mx/SitePages/English_Section.aspx	Autorité indépendante et loi(s) existante(s)
Moldavie	https://datepersonale.md/en/	Autorité indépendante et loi(s) existante(s)
Monaco	http://www.ccin.mc	Autorité indépendante et loi(s) existante(s)
Monténégro	http://www.azlp.me/index.php/en/home	Autorité indépendante et loi(s) existante(s)
Pérou	https://www.minjus.gob.pe/actividadesapdp/	Autorité indépendante et loi(s) existante(s)
Philippines	https://privacy.gov.ph/	Autorité indépendante et loi(s) existante(s)
Sénégal	http://www.cdp.sn/	Autorité indépendante et loi(s) existante(s)
Serbie	https://www.poverenik.rs/en	Autorité indépendante et loi(s) existante(s)
Tunisie	http://www.inpdp.nat.tn/	Autorité indépendante et loi(s) existante(s)
Turquie	https://www.kvkk.gov.tr/	Autorité indépendante et loi(s) existante(s)
Ukraine	http://www.ombudsman.gov.ua/en/page/zpd/	Autorité indépendante et loi(s) existante(s)
Algérie	https://www.joradp.dz/FTP/JO-FRANCAIS/2018/F2018034.pdf	Législation existante
Chine	https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021	Législation existante
Russie	http://rkn.gov.ru/eng/	Législation existante
Afghanistan		Pas de loi
Biélorussie		Pas de loi
Vatican		Pas de loi

Sources : Fichier CNIL du 22/10/2019 https://www.data.gouv.fr/fr/datasets/protection-des-donnees-personnelles-dans-le-monde/ et https://www.dlapiperdataprotection.com/ et https://www.ilo.org/dyn/natlex/natlex4.listResults?p_lang=fr&p_count=106244&p_classification=01.05

11 rue de Mogador
75009 Paris
France
Tel : +33 1 53 25 08 80
clusif@clusif.fr
https://clusif.fr

L'intégralité de la FAQ RGPD et la liste des membres qui y ont contribué sont consultables sur le site du Clusif www.clusif.fr/publications