Panorama national et international des labels relatifs aux données personnelles

Claire Levallois-Barth, Delphine Chauvet

Levallois-Barth, C., Chauvet, D.

«Panorama national et international des labels relatifs aux données personnelles»

dans **Signes de confiance – l'impact des labels sur la gestion des données personnelles** (Chapitre 5, pages 64 à 90).
Coordonné par Claire Levallois-Barth, Chaire Valeurs et Politiques des Informations Personnelles (France), Janvier 2018.

Livre disponible en version électronique sur http://www.informations-personnelles.org/
Une version papier est également disponible : ISBN 978-2-9557308-4-3

Panorama national et international des labels relatifs aux données personnelles

Parmi la centaine de signes de confiance que nous avons retenus, certains emploient le terme de « label », d'autres celui de « certification » ou de « marque »[1]. Si on constate une hétérogénéité entre les différents signes de confiance extérieurs délivrés par différents types d'entités (5.1.), il n'en reste pas moins vrai que les procédures présentent des similitudes (5.2.).

5.1. Des labels nombreux et hétérogènes

Nous avons répertorié une centaine de labels, nationaux, européens et américains. Cet aperçu comprend 75 labels délivrés en Europe et 22 en Amérique du Nord (États-Unis et Canada) et Japon. On constate que ***des entités labellisatrices multiplient la création de labels*** différents. Certains labels disparaissent à peine créés, d'autres semblent répondre à un simple effet d'annonce. D'où la difficulté à rendre compte de façon exhaustive d'un panorama des labels en matière de protection des données personnelles.

1 Voir Chapitre 2, section 2.4, page 32.

L'une des explications à cette multiplication des labels est sans doute à rechercher du côté des différents métiers disposant de compétences pour créer un référentiel sur les données personnelles et apprécier la concordance entre les critères définis et les pratiques de l'entité qui souhaite être labellisée. On compte notamment des consultants, des juristes et avocats spécialisés, des auditeurs travaillant entre autre dans le cadre des certifications ISO, des informaticiens en ce qui concerne la sécurité des données ou l'informatique en nuage, des personnes issues du marketing et de la communication, et des économistes. Chaque spécialité va ainsi orienter son type de signe de confiance à la fois selon le domaine couvert et selon les objectifs poursuivis.

Pour autant, il est possible de constituer un panorama en retenant certaines caractéristiques concernant le périmètre géographique, le champ d'application et le type d'entités qui délivrent un label en matière de données personnelles.

Des labels essentiellement délivrés par des organismes allemands

En premier lieu, on note une répartition géographique inégale. Ainsi, l'Allemagne et les États-Unis sont les plus importants créateurs de labels. Sur 75 labels recensés en Europe, on compte, sans prétendre à l'exhaustivité :

1. 41 labels en Allemagne
2. 9 en France dont 4 labels délivrés par la CNIL
3. 4 en Espagne et en Suisse
4. 3 en Italie et aux Pays-Bas
5. 2 au Royaume-Uni
6. 1 en Autriche, en Belgique, au Danemark et au Luxembourg
7. 5 labels de dimension européenne

On compte par ailleurs 22 labels en dehors de l'Europe (États-Unis, Canada et Japon).

En Europe, c'est l'Allemagne qui a développé le plus de labels (voir la liste des labels dans le Tableau 4, page 68 et suivantes), à la fois pour des raisons juridiques et culturelles. Si ce pays encadre strictement la protection de la vie privée et des données personnelles, notamment pour des raisons historiques, l'explication est aussi à rechercher du côté de la structure juridique de cet État fédéral. En effet, chaque Land a la possibilité d'édicter sa propre loi en matière de protection des données personnelles. Par exemple, la loi du 9 février 2000 du Land Schleswig-Holstein a introduit une possibilité de certification par l'autorité de protection des données de ce Land, l'*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (ULD).

À l'échelon fédéral, une disposition juridique adoptée en 2001, la Section 9a de la loi fédérale sur la protection des données, prévoit qu'« *afin d'améliorer la protection des données et la sécurité des données, les fournisseurs de systèmes de traitement de données et de programmes et les organismes chargés du traitement des données peuvent faire examiner et évaluer leurs stratégies de protection des données et leurs installations techniques par des évaluateurs indépendants et approuvés, et peuvent publier le résultat de la vérification. Les exigences détaillées relatives à l'examen et à l'évaluation, la procédure,*

(suite page 78)

Organisme	*Nom du label*	*Objet*	*Type d'organisme*	*Site web*
Adel	ADEL (*Algorithm Data Ethics Label*)	Services/ Algorithmes	Privé	www.adel-label.com
Cloud Confidence	Certification Cloud Confidence	Services/ Cloud	Association	www.cloudconfidence.eu
CNIL	Label CNIL Formations	Services / Formations	Public Autorité de contrôle Données personnelles	www.cnil.fr
	Label CNIL Audit de traitements	Services/ Audit		
	Label CNIL Coffre-fort numérique	Produits/ Coffre-fort numérique		
	Label CNIL Gouvernance Informatique et Libertés	Procédures		
FEVAD (Fédération du e-commerce et de la vente à distance)	Marque de confiance FEVAD	Services/ Commerce électronique	Association	www.fevad.com
FNTC (Fédération des Tiers de Confiance du numérique)	Label E-Vote	Services / Vote électronique	Association	www.fntc-numerique.com
France IT	Label Cloud	Services/ Cloud	Association	www.label-cloud.com

Tableau 3. Labels délivrés par des organismes français

Organisme	*Nom du label*	
ADCERT Privacy Audit GmbH	ADCERT-geprüfter Datenschutz	
Althammer & Kill GmbH & Co	Geprüfter Datenschutz	
	Zertifizierter Datenschutz	
a.s.k. Datenschutz	a.s.k. compagnysecure	
	a.s.k. websecure	
BNT GmbH	Geprüfter Datenschutz	
Check 11 - GDD-Fachgruppe Externe Daten-schutzbeauftragte	Datenschutzzertifikat Check11	
Conformity Trust GmbH	Trust in Privacy	
Datenschutz cert GmbH	Zertifikat für Auftragsdatenverarbeitung	
	Zertifikat für das Datenschutz-Management - Priventum	
	Gütesiegel IPS (internet privacy standards)	
Deutscher Dialogmarketing Verband e. V.	QuLS-Siegel Listbroker QuLS-Siegel Datenverarbeitung QuLS-Siegel Lettershop, QuLS-Siegel Adressverlag QuLS-Siegel Fulfillment	
DQS Deutsche Gesellschaft zur Zertifizierung von Management-systemen GmbH	DQS-Gütesiegel Datenschutz Plus	
	DQS-Gütesiegel Datenschutz	
DSZ Datenschutz Zertifizierungs-gesellschaft mbH	Datenschutzsiegel	

Tableau 4. Labels délivrés par des organismes allemands

Objet	*Type d'organisme*	*Site web*
Procédures, produits et services	Privé	www.adcert.eu
Procédures, produits et services	Privé	www.althammer-kill.de
Procédures, produits et services	Privé	www.bdsg-externer-datenschutzbeauftragter.de
Services / Sites web		
Procédures, produits et services	Privé	www.bntgmbh.de
Personnes / Experts Données personnelles	Association	externer-datenschutz.de
Procédures, produits et services	Privé	www.conformitytrust.de
Procédures, produits et services	Privé	www.datenschutz-cert.de
Procédures		
Services/Services en ligne		
Procédures, produits et services	Privé	www.ddv.de
Procédures	Privé	www.dqs.de
Procédures, produits et services	Privé	www.dsz-audit.de

(source : https://stiftungdatenschutz.org/aufgaben/zertifizierung, février 2017)

Organisme	*Nom du label*	
ePrivacy GmbH	ePrivacySeal	
	ePrivacyApp	
editco GbR	IT-Security- und Datenschutz-Audit	
EuroPriSe GmbH	EuroPriSe (European Privacy Seal)	
Datenschutz Mecklenburg-Vorpommern	Privacy Seal Gütesiegel Datenschutz Mecklenburg-Vorpommern	
GDD (Gesellschaft für Datenschutz und Datensicherheit)	Zertifizierung der Datenschutzqualifikation	
GDI Gesellschaft für Datenschutz und Informationssicherheit mbH	GDI - zertifizierter Datenschutz	
GenoTec GmbH	Datenschutz-CheckUp mit Zertifikat	
Greeneagle certification GmBH	Datenschutzkonform	
	Geprüfte Auftragsdaten- verarbeitung	
IITR (Institut für IT-Recht) GmbH	Datenschutz-Status Qualifizierter Datenschutz	
INOIS (Institut für organisatorische Informationssysteme)	Zertifizierter Datenschutz	
Interev GmbH	Geprüfter Datenschutz durch Interev	

Objet	*Type d'organisme*	*Site web*
Procédures, produits et services	Privé	www.eprivacy.eu
Services/ Applications mobiles		
Procédures, produits et services		
Produits, services/sites web	Public avec les autorités de contrôle Données personnelles puis privé depuis 2014	www.european-privacy-seal.eu
Procédures et produits	Public Autorité de contrôle Données personnelles en lien avec EuroPriSe	
Personnes/ Expert Données personnelles	Association	www.gdd.de
Procédures, produits et services	Privé	www.gdi-mbh.eu
Procédures, produits, services et personnes	Privé	www.geno-tec.de
Procédures, produits et services	Privé	www.greeneagle-certification.de
Procédures, produits et services	Privé	www.iitr.de/zertifizierung.html
Procédures, produits et services	Privé	www.inois.de/leistungsspektrum/zertifizierung
Procédures, produits et services	Privé	www.interev.de

Organisme	*Nom du label*	
Legitimis GmbH	Statement of Compliance	
MediaTest digital GmbH	Trusted App	
Privacy Stiftung	ADV Compliance Checked	
SCHUFA Holding AG	SCHUFA-DatenschutzSiegel	
Tacticx GmbH	Geprüfter Datenschutz	
Tekit Consult Bonn GmbH (TÜV Saarland Gruppe)	TÜV Geprüfter Datenschutz	
Trusted Shops GmbH	Trusted Shops	
TÜV Informationstechnik GmbH	TÜVIT-Zertifikat Trusted Site Privacy	
TUV Rheinland	Data Privacy Certification for Companies	
TÜV SÜD sec-IT GmbH	S@fer-shopping	
TÜV SÜD sec-IT GmbH	Zertifizierte Auftrags-datenverarbeitung	
Verband für Berater, Sachverständige und Gutachter im Gesundheits- und Sozialwesen e.V.	VBSG-Datenschutzsiegel	
ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)	Datenschutz-Gütesiegel	

Objet	*Type d'organisme*	*Site web*
Procédures	Privé	www.legitimis.de
Services/ Applications mobiles	Privé	www.mediatest-digital.com
Procédures, produits et services	Privé	www.privacy-stiftung.de
Procédures, produits, services et personnes	Privé	www.schufa.de
Procédures, produits et services	Privé	www.tacticx.de
Procédures, produits et services	Privé	www.tekit.de/zertifizierung/
Procédures/ Commerce électronique	Privé	www.trustedshops.com
Procédures, produits et services/ sites internet	Privé	www.tuvit.de
Procédures	Privé	www.tuv.com
Procédures/ Commerce électronique	Privé	www.safer-shopping.de www.tuev-sued.de/sec-it
Procédures	Privé	www.tuev-sued.de www.tuev-sued.de/sec-it
Procédures	Association	www.vbsg.org
Procédures, produits et services	Public Autorité de contrôle Données personnelles	www.datenschutzzentrum.de

Origine	Organisme	Nom du label
Autriche	Handelsverband	TrustMark Austria
Belgique	BeCommerce	Label Becommerce
Danemark	E-handelsfonden	E-maerket
Espagne	APEP (Asociación Profesional Española de Privacidad)	APEP-CertifiedPrivacy
Espagne	Confianza Online	Confianza Online
Espagne	ISMS Forum Spain	CDPP (Certified Data Privacy Professional)
Espagne	Seriedad Online	Seriedad Online
Italie	Bureau Veritas (Italie)	Certificazione del Personale Data Protection Officer
Italie	KHC (Know How Certification)	Certificazione data protection officer e privacy consultant
Italie	TÜV Italia/TÜV SUD GROUP	Certificazione di privacy officer e consulente della privacy
Luxembourg	EuroCloud Europe a.s.b.l.	EuroCloud Self Assessment EuroCloud Star Audit
Pays-Bas	Alliander NV	Data Privacy and Security certification
Pays-Bas	Thuiswinkel	Thuiswinkel Waarborg
Pays-Bas	Veiligheidsbranche	Keurmerk Particulier Onderzoekbureau
Royaume-Uni	Comodo CA Limited	Comodo Secure
Royaume-Uni	The Market Research Society	Fair Data
Suisse	APPD (Association des Professionnels de la Protection des Données)	CAPD (Certificat d'Aptitude à la Protection des Données)
Suisse		CIPD (Certificat d'Implémentation de la Protection des Données)
Suisse	SQS (Association Suisse pour Systèmes de Qualité et de Management)	Good Priv@cy
Suisse		SQS-OCPD (OCPD:2014; avant OCPD:2008)

Tableau 5. Labels délivrés par des organismes établis dans d'autres pays européens

	Objet	Type d'organisme	Site web
	Services / Commerce électronique	Association	www.handelsverband.at
	Services / Commerce électronique	Association	www.becommerce.be
	Services / Commerce électronique	Association	www.emaerket.dk www.emaerket.dk/english
	Personnes / Experts Données personnelles	Association	www.apep.es
	Services / Commerce électronique	Association	www.confianzaonline.es
	Personnes / Experts Données personnelles	Association	www.ismsforum.es
	Services / Sites web	Privé	www.seriedadonline.es
	Personnes	Privé	www.bureauveritas.it
	Personnes / Experts Données personnelles	Privé	www.khc.it
	Personnes / Experts Données personnelles	Privé	www.tuv.it
	Services / Cloud	Association	www.eurocloud-staraudit.eu
	Produits / Compteurs intelligents	Privé	www.alliander.com
	Services / Commerce électronique	Association	www.thuiswinkel.org
	Procédures / Investigation des agences de détectives privés	Association	www.veiligheidsbranche.nl
	Services / Sites web	Privé	www.comodo.com
	Procédures / Études de marché	Association	www.fairdata.org.uk
	Personnes / Experts Données personnelles	Association	www.appd.ch
	Personnes / Experts Données personnelles	Association	www.appd.ch
	Procédures et produits	Association	www.sqs.ch
	Procédures et produits	Association	www.sqs.ch

Origine	Organisme	Nom du label
États-Unis/ Canada	AICPA (American Institute of Certified Public Accountants) et CICA (Canadian Institute of Chartered Accountants)	WebTrust
Canada	Deloitte et Ryerson University	Privacy by design Certification
États-Unis	Better Business Bureau	BBB Accredited Business Seal or the Web
États-Unis	BuySAFE Inc.	Buysafe Guaranteed Shopping
États-Unis	CSA (Cloud Security Alliance)	CSA STAR (Security, Trust and Assurance Registry)
États-Unis	ESRB (Entertainment Software Rating Board)	ESRB Privacy Certified
		ESRB Privacy Certified for Kids
		ESRB Privacy Certified for Mobile
États-Unis	Gigya, Inc.	Gigya's Social Privacy Certification
États-Unis	Google	Trusted Store
États-Unis	IAPP (International Association of Privacy Professionnals)	Certified Information Privacy Professional (CIPP)
		Certified Information Privacy Manager (CIPM)
		Certified Information Privacy Technologist (CIPT)
États-Unis	McaFee Secure	McaFee Secure
États-Unis	PRIVO (Privacy Vaults Online, Inc.)	Privo Privacy Certified
		PRIVO's Safe Harbor Privacy Assurance Program Seal
États-Unis	TRUSTArc	TRUSTe Certification APEC
		TRUSTe Certification Enterprise Privacy certification
		TRUSTe Certification TRUSTed Data
		TRUSTe Certification TRUSTed Downloads
		TRUSTe Certification Children's Privacy
Japon	JIPDEC (Japan Institute for Promotion Of Digital Economy and Community)	PrivacyMark System

Tableau 6. Labels délivrés par des organismes situés en dehors de l'Europe

Objet	*Site web*
Services / Audits	www.webtrust.org
Procédures et produits	www2.deloitte.com/ca/en/pages/risk/articles/Privacybydesign.html
Services / Sites web	www.bbb.org
Services / E-commerce	www.buysafe.com
Services / Cloud	www.cloudsecurityalliance.org cloudsecurityalliance.org/star/
Services / Sites web	www.esrb.org et www.esrb.org/privacy.asp
Services / Applications mobiles, sites web et jeux vidéo en ligne pour les enfants	www.esrb.org
Services/ Applications mobiles	
Services / Sites internet et applications mobiles	www.gigya.com
Services / E-commerce	www.google.com/trustedstores/
Personnes / Experts Données personnelles	www.iapp.org/certify/cipp
	www.iapp.org/certify/cipm
	www.iapp.org/certify/cipt/
Services/Sites internet	www.mcafeesecure.com/
Services/Sites web, jeux, applications pour les enfants	www.privo.com
Procédures et produits	
Procédures	www.trustarc.com/privacy-certification-standards/
Procédures	
Services / publicité en ligne	
Services / Logiciel	
Services/ Enfants de moins de 13 ans	
Procédures	www.privacymark.org

(cas les plus connus – liste non exhaustive)

Organisme	*Nom du label*	*Objet*	*Type d'organisation*	*Site web*
EMOTA (European Multichanel and Online Trade Association)	Label de confiance de l'EMOTA	Services / Commerce électronique	Association	europeantrustmark.eu/fr
Ecommerce Europe	Ecommerce Europe Trustmark	Services / Commerce électronique	Association	www.ecommerce-europe.eu
EDAA (European Interactive Digital Advertising Alliance)	Trust Seal	Services / Publicité en ligne	Association	www.edaa.eu
	OBA Certification (Online Behavioural Advertising)	Service / Publicité comportementale		
European Schoolnet	eSafety Label.eu	Services / Écoles	Association	www.esafetylabel.eu

Tableau 7. Labels de dimension européenne

la sélection et l'approbation des évaluateurs sont stipulées dans une loi distincte. »[2] En pratique, cette loi spécifique n'a pas été adoptée. Aujourd'hui, 41 schémas de certification sont proposés en Allemagne. Seuls deux labels sont délivrés par les autorités de contrôle, les autres étant délivrés par des entités privées et visant à implémenter le cadre légal au-delà (cf. Chapitre 6).

2 Traduit librement de l'anglais : "*In order to improve data protection and data security, suppliers of data processing systems and programs and bodies conducting data processing may have their data protection strategies and their technical facilities examined and evaluated by independent and approved appraisers, and may publish the result of the audit. The detailed requirements pertaining to examination and evaluation, the procedure and selection and approval of the appraisers shall be stipulated in a separate act*", Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html. Source en anglais : https://databeskyttelsesdag.files.wordpress.com/2017/01/dk_privacy-seals-and-certifications_2017-2.pdf.

En dehors de l'Union européenne (voir Tableau 6, page 76), l'offre de labels, marques et sceaux s'est fortement développée aux États-Unis. Les plus connus sont TRUSTe, avec ses différents programmes fournis désormais par TrustArc et portant notamment sur les principes définis par la Coopération économique pour l'Asie-Pacifique (*Asia-Pacific Economic Cooperation* – APEC), la publicité en ligne ou la protection des enfants de moins de 13 ans, le *Better Business Bureau* (BBB) qui s'adresse aux sites web des entreprises établies aux États-Unis et au Canada et se conformant au *BBB Code of Business Practices*, l'*Entertainment Software Rating Board* (ESRB) et son *Privacy Online Seal*, et enfin *WebTrust*.

Certains proposent à leurs clients des programmes visant à intégrer les dispositions du RGPD, comme TrustArc et PRIVO.

Des labels délivrés dans des domaines et secteurs variés

De manière générale, le marché des labels ne compte pas ou peu de labels généraux applicables à l'ensemble des secteurs. En effet, il se focalise sur :

- les ***produits***, avec notamment le label « Coffre-fort numérique » délivré en France par la CNIL

- les ***services***, comme les applications mobiles (*ePrivacyApp* de l'entité allemande ePrivacy GmbH) et l'informatique en nuage (*CSA STAR* de l'entité américaine *Cloud Security Alliance*)

- les ***processus***, comme *Good Priv@cy* de l'association suisse pour les systèmes de Qualité et de Management (SQS) et *Datenschutz-CheckUp mit Zertifikat* de l'entreprise allemande GenoTec Gmbh

- la ***formation***, qui peut être dispensée sur des textes nationaux et européens (label CNIL « Formation »)

    - à des experts spécialisés en matière de données personnelles : en Espagne avec *Certified Data Privacy Professional* (CDPP) de l'organisme ISMS Forum Spain, en Italie avec *Certificazione del personale-Privacy* de l'organisme *Know How Certification* (KHC), et aux États-Unis avec *Certified Information Privacy*

Professional (CIPP) de l'*International Association of Privacy Professionnals* (IAPP)

- mais aussi, de façon plus spécifique, à une profession comme les détectives privés (aux Pays-Bas avec le label *Keurmerk Particulier Onderzoekbureau* de l'organisme *Veiligheidsbranche*)

- ***Les audits,*** avec un label CNIL spécifique (cf. Chapitre 6)

De fait, les labels concernent ***des secteurs multiples et variés***, ainsi qu'en témoignent les domaines suivants :

- le ***commerce électronique*** : la marque danoise *E-maerket*, le label *BeCommerce* en Belgique, *Trusted Shops* en Allemagne ou le *European Trustmark label* délivré par Ecommerce Europe

- la ***publicité en ligne*** : *OBA Certification* de l'entreprise allemande Privacy GmbH

- le ***cloud computing*** : *CSA STAR* délivré par la *Cloud Security Alliance* aux États-Unis, le label « Cloud » de France IT

- les ***sondages*** : *Fair Data* délivré par *The Market Research Society* au Royaume-Uni

- les ***sites web*** et les jeux en ligne accessibles aux mineurs : *Privo Privacy Certified* délivré par Privo aux États-Unis

- les ***réseaux sociaux*** : *Gigya's SocialPrivacy Certification* de Gigya aux États-Unis

- les ***écoles*** : *eSafety Label* de l'*European Schoolnet* délivré au niveau européen

Des labels délivrés par des entités de natures diverses

Les labels sont délivrés par des entités de différentes natures. En Europe, il s'agit d'***organismes privés*** (56%). On observe aussi des labels créés par des ***associations spécialisées*** (34,66%) dans un domaine déterminé.

► Par exemple, l'association française Cloud confidence délivre un label sur l'informatique en nuage. À ce titre, ses membres sont composés de fournisseurs de *cloud*, de prestataires de services, d'experts mais aussi d'utilisateurs.

La particularité d'un label délivré par une association est que le candidat doit en règle générale adhérer à l'association pour être labellisé. Par ailleurs, on observe que les labels liés au secteur du commerce électronique sont généralement délivrés par des associations de professionnels regroupant des e-commerçants et des prestataires.

► Tel est le cas du label espagnol *Confianza Online* ou du label belge *BeCommerce*.

Il existe des labels délivrés par des ***organismes publics*** (9,33%). Plus précisément, ceux que nous avons retenus sont délivrés par des autorités nationales de protection des données. Il en va ainsi de la France (CNIL), et de deux Länder allemands : le Schleswig-Holstein et le Mecklembourg-Poméranie.

Si les labels sont délivrés soit par des entités publiques, soit par des entités privées, le schéma donnant lieu à leur délivrance peut revêtir ***une nature mixte***, fonction de la nature et du degré d'intervention des autorités publiques. Ainsi, on distingue les schémas :

- directement gérés par les autorités publiques, typiquement les labels délivrés par la CNIL, ou qui revêtent une valeur légale

- dit d'auto-régulation auxquels les autorités apportent leur soutien sans intervenir directement (par exemple les labels privés TÜV IT et TÜV Rheinland, SQS, DEKRA, MRS/Fair Data, *Trusted shops* ou OBA)

- dit de corégulation où les autorités publiques sont parties prenantes pour élaborer les exigences et/ou participer à la gestion opérationnelle ou financière, notamment EuroPriSe

Le cas de la Suisse qui présente un schéma de certification semi-public est emblématique : l'autorité de protection, le Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT), participe aux procédures d'accréditation, de contrôle et de révocation des organismes de certification. Précisément, il s'agit des organismes qui délivrent des certifications pour les produits et procédures de traitements des données en application de l'Ordonnance Suisse sur les Certifications en matière de Protection des Données (OCPD) adoptée par le Conseil fédéral Suisse[3]. Par exemple, l'association Suisse pour les Systèmes de Qualité et de Management (SQS) est accréditée pour délivrer la certification OCPD:2014. Elle délivre par ailleurs le label « Good Priv@cy ».

5.2. Des schémas de labellisation présentant de fortes similarités

Les schémas donnant lieu à la délivrance d'un label présentent tous ***un référentiel***, ***une procédure d'évaluation***, ***un logo***, ***une procédure de vérification*** *a posteriori*, ainsi qu'***une procédure de résolution des conflits***. Leur but est de délivrer une attestation de conformité. Comme le fait remarquer Eric Lachaud, cela n'est pas typique à la protection des données[4]. Cet auteur démontre que « *la certification des données personnelles est une forme de certification comme une autre* » présentant des similarités en ce qui concerne à la fois les composantes et la procédure.

Un référentiel

Le terme de référentiel étant employé par la CNIL, nous utilisons ici cette notion, qui est définie par l'article L 433-3 du code de la consommation comme étant « *un document technique définissant les caractéristiques que doit présenter un produit, un service ou une combinaison de produits et de services, et les modalités de contrôle de la conformité*

3 Conformément à l'article 11, alinéa 2 de la loi fédérale suisse sur la protection des données du 19 juin 1992 (modifiée en dernier lieu le 1er janvier 2014) (CH301).

4 Lachaud, E. (2017). The General Data Protection Regulation and the rise of certification as a regulatory instrument. Computer Law & Security Review.

à ces caractéristiques. L'élaboration du référentiel de certification incombe à l'organisme certificateur qui recueille le point de vue des parties intéressées. » De manière générale, un référentiel fixe donc des caractéristiques, autrement appelées critères, exigences, spécifications ou normes. Ces caractéristiques, qui doivent être impérativement respectées, déterminent le périmètre des activités visées par le label, définissent les critères à respecter et fixent les valeurs pour chaque critère. Parfois, elles précisent le degré d'écart qu'un évaluateur peut accepter pour ces valeurs.

Dans le domaine des données personnelles, le référentiel s'appuie sur des sources diverses, juridiques ou non. Son contenu s'inscrit dans un continuum allant d'un référentiel très complet à des exigences pour le moins succinctes.

Tout d'abord, les spécifications se basent sur des ***obligations légales***, la directive 95/46/CE Protection des données et le RGPD, ainsi que les législations nationales. Tous les labels ne reprennent pas forcément l'ensemble des principes de protection des données personnelles définis dans ces textes mais ils se réfèrent toujours aux principaux (licéité, proportionnalité, finalité, transparence).

Les différents labels délivrés par Datenschutz cert GmbH sont fondés sur la loi fédérale allemande de protection des données, ceux délivrés par la CNIL sur la loi Informatique et Libertés et désormais le RGPD.

- Afficher un label qui garantit la conformité à une réglementation pose question car, par définition, la réglementation est obligatoire. Son non-respect expose le contrevenant à des sanctions. À cet égard, « *présenter les droits conférés au consommateur par la loi comme constituant une caractéristique propre à la proposition faite par le professionnel* » peut être considéré comme une pratique commerciale réputée déloyale[5].

5 Annexe 1 point 10 de la directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil, JOUE, n° L 149, 11 juin 2005, p. 22.

Les exigences peuvent également s'appuyer sur les ***recommandations de l'autorité de contrôle***[6].

- La conformité du label français « E-vote » délivré aux prestataires de vote par Internet par la FNTC à la loi Informatique et libertés a été attestée par la CNIL dans une délibération du 17 mars 2016[7].

- En Suisse, les certifications *GoodPriv@cy* et OCPD:2014 délivrées par l'Association Suisse pour les Systèmes de Qualité et de Management (SQS) ont notamment pour référentiel les directives du Préposé sur les exigences minimales qu'un système de gestion de la protection des données doit remplir[8].

Le référentiel peut aussi se référer à des normes internationales, en particulier celles établies par l'Organisation internationale de normalisation (*International Organization for Standardization* – ISO). Une norme est ici entendue comme un « *document, établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné* »[9]. Son respect est volontaire.

En matière de protection des données personnelles, on trouvera des labels dont les critères sont créés en partie à partir d'une interprétation des normes[10] :

6 Délibération n° 2010-371 du 21 oct. 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, JORF, 24 novembre 2010.

7 Délibération n° 2016-071 du 17 mars 2016 portant avis sur un projet de label « E-vote » présenté par la Fédération des tiers de confiance, JORF, 28 avril 2016.

8 Préposé fédéral à la protection des données et à la transparence (PFPDT): directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir du 19 mars 2014, https://www.admin.ch/opc/fr/federal-gazette/2014/3015.pdf

9 Directives ISO/IEC, Partie 2 — Principes et règles de structure et de rédaction des documents ISO et IEC, 2016-04-30.

10 Pour appréhender l'éventail des normes en matière de protection de la vie privée, voir AFNOR Normalisation, Guide Protection des données personnelles: l'apport des normes volontaires, janvier 2017, http://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf

- ISO 27001 portant sur le système de management de la sécurité de l'information[11] : par exemple le label suisse SQS-OCPD précité, le label « Cloud » de l'association France IT pour les aspects sécurité ou le label *Datenschutzsiegel* de la société allemande d'audit DSZ Datenschutz Zertifizierungs GmbH

- ISO 17024 relative au fonctionnement homogène et fiable des organismes de certification qui mettent en œuvre des dispositifs particuliers de certification de personnes[12] avec l'*APEP-CertifiedPrivacy* en Espagne ou en Italie le *Certificazione del Personale Data Protection* délivré par Bureau Veritas Italie

- ISO 19011 relative à l'audit des systèmes de management[13] avec le label CNIL « Audit de traitements » et les labels allemands *Trust in Privacy* de la société Conformity Trust GmbH et *SCHUFA Datenschutz Siegel* de la SCHUFA Holding AG

- ISO 29190 qui propose une méthodologie qui permet à une organisation d'évaluer ses progrès dans le domaine de la protection de la vie privée[14] avec le label CNIL « Gouvernance Informatique et Libertés »

- ISO 29990 relative aux services de formation[15] avec le label CNIL « Formation »

- ISO 27018 relative aux bonnes pratiques pour la protection des informations personnelles identifiables dans l'informatique en nuage public[16] avec « EuroCloud Star Audit »

---

11 ISO/IEC 27001:2013 : Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences.

12 ISO/IEC 17024 :2012 : Évaluation de la conformité. Exigences générales pour les organismes de certification procédant à la certification de personnes publiée.

13 ISO/IEC 19011:2011 : Lignes directrices pour l'audit des systèmes de management.

14 ISO/IEC 29190:2015 : Méthodologie pour la maturité dans le domaine de la protection de la vie privée.

15 ISO/IEC 29990 :2010 : Services de formation dans le cadre de l'éducation et de la formation non formelles – exigences de base pour prestataires de services, 2010.

16 ISO/IEC 27018:2014 : Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.

Enfin, le référentiel peut se fonder sur des instruments d'***auto-régulation***. Ces instruments, au processus d'élaboration très variable, sont généralement limités aux membres d'un groupe. Dans le cas des données personnelles, il s'agit principalement d'associations professionnelles rassemblant les acteurs du secteur du commerce et de la publicité en ligne.

► On trouve ici le code éthique de la marque de confiance espagnole *Confianza Online*[17], le code de conduite du label *BeCommerce* pour la vente à distance en Belgique[18], et le code déontologique de la FEVAD[19].

Le code déontologique de la FEVAD

Ce code précise que « *les entreprises adhérentes s'engagent à respecter les dispositions légales et réglementaires relatives à l'Informatique, aux Fichiers et aux Libertés, à la vie privée et à la protection des données* » ainsi que « *la déontologie mise en place par les professionnels du marketing direct et digital* »[20]. À cette fin, il rappelle certaines obligations légales et impose à tout adhérent FEVAD le respect du Système Liste Robinson – Stop Publicité.

Ce type d'instrument n'est cependant pas élaboré uniquement par des associations professionnelles, mais aussi par des sociétés.

► La *Market Research Society* (MRS) propose à travers sa marque « éthique » *Fair Data* de certifier dix principes fondamentaux qui viennent compléter la législation britannique sur la protection des données et des normes ISO[21].

17 https://www.confianzaonline.es/documentos/Ethical_Code.pdf

18 https://www.becommerce.be/files/Code_de_conduite_du_Label_de_Qualite_BeCommerce.pdf

19 http://www.fevad.com/wp-content/uploads/2016/09/FEVAD_Codepro_Vsept2015.pdf

20 https://www.fevad.com/le-code-professionnel-de-la-fevad-se-met-de-nouveau-a-jour/

21 http://www.fairdata.org.uk/10-principles/

Une procédure d'évaluation

La procédure d'évaluation permet d'apprécier la concordance entre les critères définis dans le référentiel et les pratiques de l'entité qui souhaite être labellisée. Lorsqu'elle est effectuée par une entité privée, elle donne généralement lieu à la conclusion d'un contrat de service entre le labellisateur et le candidat à la labellisation. La particularité juridique de ce contrat est que sa réalisation demeure incertaine.

De manière générale, l'appréciation d'une politique de protection des données personnelles prend la forme soit d'une auto-évaluation, soit d'un audit.

L'***auto-évaluation***, consiste simplement pour l'entreprise candidate à faire part de ses démarches en matière de protection des données personnelles, par exemple en répondant à des questions : ***l'organisme dit ce qu'il fait***. Le label est attribué si la déclaration correspond aux exigences du référentiel, ce qui n'est pas sans poser question lorsqu'il n'existe pas de vérification (cf. «L'effet potentiellement trompeur», page 126).

- Cette forme « souple » de signe de confiance est très présente dans les labels américains à l'instar du label *TRUSTe Privacy Seal* (désormais délivré par TrustArc) ou de BBBOnline. L'*European Interactive Digital Advertising Alliance* (EDAA) propose également une auto-certification aux entreprises participant au programme d'auto-régulation de l'*Online Behavioural Advertising* (OBA)[22].

- Les accords conclus entre l'Union européenne et les États-Unis, qu'il s'agisse du *Safe Harbor* invalidé par la Cour de l'Union européenne ou du *Privacy Shield*, reposent également sur une auto-évaluation, ce qui ne manque pas de faire l'objet de débats et d'interrogations au sein des États Membres de l'Union européenne[23].

22 Le formulaire est accessible à : https://www.dropbox.com/s/lqkvhl31vcab2si/Self-certification%20form.pdf?dl=0. Sur le *Privacy Shield*, voir Lettre n°5 de la **Chaire Valeurs et Politiques des Informations Personnelles**, décembre 2016 : *Privacy Shield : un bouclier à peine brandi déjà ébréché ?*, https://cvpip.wp.imt.fr/2016/12/05/privacy-shield-un-bouclier-a-peine-brandi-deja-ebreche/

23 Voir https://www.privacyshield.gov/article?id=Self-Certification-Information

De son côté, l'***audit*** vise à obtenir des preuves : ***l'organisme prouve ce qu'il fait*** en fournissant les dites preuves via des documents ou en permettant l'accès à son système d'information[24]. Sa nature diffère donc de celle d'un contrôle.

L'***audit sur pièces*** consiste pour le candidat à fournir des documents attestant la véracité de ses déclarations. À l'instar de la CNIL ou d'EuroPriSe, un auditeur vérifie la concordance en examinant les documents au regard du référentiel. À cette fin, il se réfère au guide d'audit qui décline chaque critère du référentiel et indique comment l'exigence peut être acceptée de façon objective. L'appréciation peut être effectuée de façon stricte. Parfois, des écarts sont tolérés : ils doivent être prévus et spécifiés.

Enfin, un ***audit sur site*** peut être mené par un évaluateur en ce qui concerne la conformité des organismes et des systèmes de management. Cet audit s'ajoute à l'examen des pièces par ce même expert au regard du référentiel. Tel est le cas des labels suisses *GoodPriv@cy* et DPCO délivrés par l'Association Suisse pour Systèmes de Qualité et de Management (SQS).

De manière générale, en matière de protection des données personnelles, la procédure d'évaluation est habituellement menée en interne par le labellisateur, à l'instar de la CNIL[25]. Ce dernier peut cependant recourir à des experts externes, comme EuroPriSe ou le label *BeCommerce* qui a choisi le certificateur Bureau Veritas. L'évaluateur externe peut être un organisme privé dont l'activité est la certification ou un expert. Le plus souvent, il doit être accrédité, ce qui renforce sa crédibilité. Notons que la Fédération des Tiers de Confiance du Numérique (FNTC) accrédite des évaluateurs externes qui ne sont pas choisis par le futur labellisé mais désignés via un système de tirage au sort afin de garantir une certaine indépendance. En Suisse, les organismes suisses ou étrangers qui effectuent des certifications au sens de l'article 11 de la loi sur la protection des données sont accrédités par le Service d'accréditation suisse, qui est associé au Préposé fédéral à la protection des données et à la transparence.

---

24 L'audit est défini par la norme NF ISO19011 comme un « *processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure des critères prédéterminés sont satisfaits* ».

25 Fair Data, Trusted Shops, confianza Online, TÜV Rheinland, DEKRA Certification, TÜV IT, SQS, etc.

Une attestation de conformité

Après avoir réalisé l'évaluation en matière de protection des données, le certificateur conclut à la conformité de l'entité dans l'hypothèse où elle satisfait les exigences du référentiel. Celui qui certifie peut être l'évaluateur comme la CNIL. Si tel n'est pas le cas, la mission du certificateur revient à vérifier les résultats de l'évaluation, à conclure à la conformité des procédures de traitement, du produit, du service analysés et à délivrer l'attestation de conformité.

L'approbation se traduit par une preuve matérielle, l'attestation de conformité, qui peut être délivrée pour une durée très variable (entre un an et cinq ans) soit par l'évaluateur lui-même, soit par le certificateur. Les attestations délivrées par les organismes privés sont en général payantes.

Sur le plan juridique, l'attestation de conformité est souvent une marque de conformité, c'est-à-dire une marque légalement déposée. Il en existe deux types : la marque collective et la marque de certification, huit États membres (l'Allemagne, la Belgique, l'Espagne, la France, le Luxembourg, les Pays-Bas, le Portugal et le Royaume-Uni) ayant mis en place un cadre juridique spécifique dédié à la marque de certification.

Une transparence

Pour instaurer la confiance à l'égard du client, un label implique la transparence et donc sa publicité. Concrètement, l'entreprise labellisée peut se voir attribuer un logo à l'effigie du label, qui peut être personnalisé avec mentions du numéro du label et de sa date d'expiration. Le labellisé peut faire apparaître le logo sur son site web ou ses documents de communication afin de se différencier de ses concurrents. Pour prévenir les fraudes (car on observe des tentatives d'usurpation de logos[26]), le logo peut aussi être numériquement distribué par une source située sur le site du labellisateur : le labellisé insère alors un lien hypertexte sur son site qui renvoie vers site du labellisateur[27]. Le logo peut aussi être hébergé sur un serveur contrôlé par l'organisme qui délivre le label[28].

---

26 Aux États-Unis, TRUSTe a fait condamner pour contrefaçon de marque les sites American-Politics.com et and SurfAssured.-com qui n'avaient pas été labellisés. *Standards in Electronic Transactions v Underwriters Digital Research Inc.*, US DC (Columbia), Civil Action No. 00–02574(CK).

27 Notamment PrivacyMark (online), Danish E-maerket, MRS Fair Data.

28 Par exemple, la marque de confiance Ecommerce Europe est liée à un certificat, tout comme les marques de confiance nationales de ses associations nationales membres. Pour utiliser le certificat, le logo doit être lié à l'adresse : https://ecommercetrustmark.eu/name-of-your-national-association.

Le logo est le signe physique à destination du public et des clients de l'entité labellisée, parce qu'il traduit la conformité de l'entreprise au référentiel, pour lui accorder leur confiance. Encore faut-il que cette marque de confiance soit connue, reconnue et facile à repérer, ce qui suppose en amont la mise en œuvre d'une politique de communication. Dans les faits, celle-ci est quasi-inexistante. Pourtant, la médiatisation est un outil important pour le succès du label. Preuve en est avec le label rouge.

Le logo ne constitue pas le seul indice visible de l'octroi d'un label. Dans certains cas, le public et les clients ont accès aux éléments qui motivent la labellisation comme par exemple le rapport de l'évaluateur et les conclusions de conformité du certificateur. Mais il est rare, si l'on excepte EuroPriSe et EuroCloud Star Audit qui publient les rapports de certification, d'en trouver une quelconque publication. Toutefois, certaines organisations mettent en ligne à disposition du public un registre des entreprises[29] auxquelles elles ont délivré un label, ainsi que les attestations de conformité[30].

Des contrôles, recours et sanctions

L'information du public implique aussi de mettre en place dans l'intérêt de toutes les parties des mécanismes de résolution des conflits dans le cas où un litige surviendrait entre l'entreprise labellisée et la personne dont les données personnelles sont utilisées. Or, il s'avère que la plupart des labels existants taisent leur existence (cf. Chapitre 7).

29 Par exemple, Confianza online, Seriedad online, Good Priv@cy.

30 Par exemple, Danish E-maerket, ePrivacySeal.