Règlement général de protection des données personnelles (RGPD) : Démarche et outils qualité pour la mise en conformité de l'entreprise

MANCET Claire
Stage professionnel de fin d'études
www.utc.fr/master-qualité, puis « travaux »
« Qualité-management », réf 443, juillet 2018

1- Contexte

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (DCP) et à la libre circulation de ces données (RGPD)

Entrée en application: 25/05/2018

Points majeurs du RGPD

- Mis en place pour tous les traitements de données automatisés ou non et appelés à figurer dans un fichier
- Responsabilisation des acteurs traitant des données à caractère personnel sur les citoyens européens (entreprises de l'UE ou hors UE)
- Renforcement de la protection de la vie privée et maîtrise des citoyens sur leurs données personnelles
- Disparition des formalités administratives sauf exception, démonstration de conformité par le responsable de traitement

2-Données personnelles

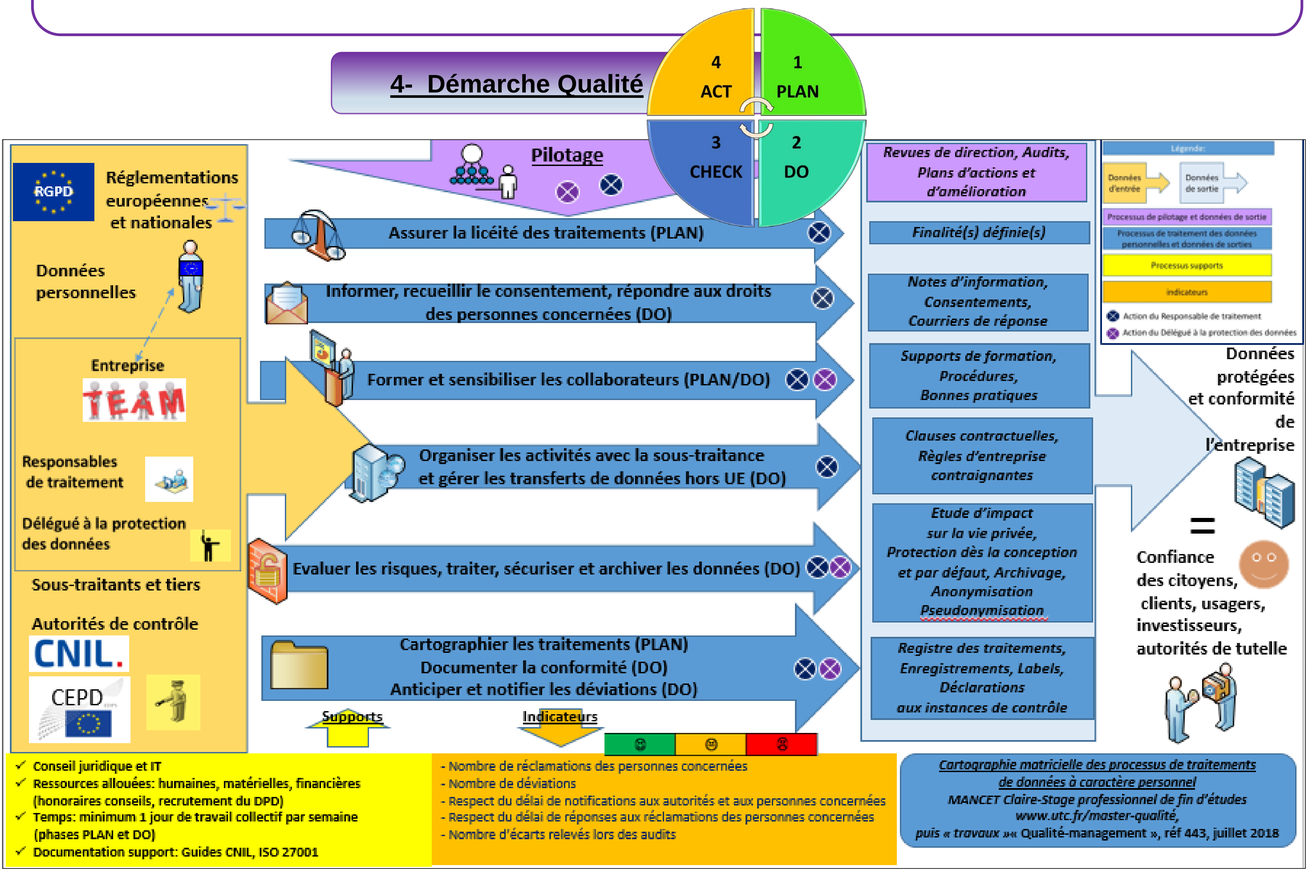
- Données d'identification directe ou indirecte
- DCP courantes (Identité, coordonnées …)
- DCP sensibles (santé, génétiques, biométriques, infractions, condamnations, origine raciale, opinion politique religieuse…)

3- Enjeux et objectifs de l'entreprise

Mettre en place une démarche qualité et une organisation efficiente pour :

- La confiance des citoyens, des clients, des investisseurs et des partenaires
- Un gain de compétitivité et la pérennité de l'entreprise
- Un développement numérique facilité
- Faire face aux enjeux financiers & juridiques(sanctions jusqu'à 20 millions € ou 4% du CA mondial)

4- Démarche Qualité



- ✓ Conseil juridique et IT
- ✓ Ressources allouées: humaines, matérielles, financières (honoraires conseils, recrutement du DPD)
- ✓ Temps: minimum 1 jour de travail collectif par semaine (phases PLAN et DO)
- ✓ Documentation support: Guides CNIL, ISO 27001

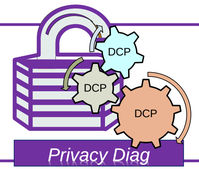
- Nombre de réclamations des personnes concernées
- Nombre de déviations
- Respect du délai de notifications aux autorités et aux personnes concernées
- Respect du délai de réponses aux réclamations des personnes concernées
- Nombre d'écarts relevés lors des audits

Cartographie matricielle des processus de traitements de données à caractère personnel
MANCET Claire-Stage professionnel de fin d'études
www.utc.fr/master-qualité,
puis « travaux »« Qualité-management », réf 443, juillet 2018

5- Bilan:

Outil d'autodiagnostic PRIVACY DIAG

- Outil excel basé sur la cartographie des processus, facile d'utilisation, adaptable à toute entreprise
- 83 critères à évaluer seulement au lieu de 137 paragraphes « Considérants » et 99 articles du RGPD
- Solution visuelle: présentation synthétique des résultats et des plans d'actions

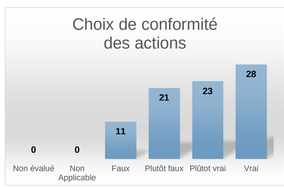


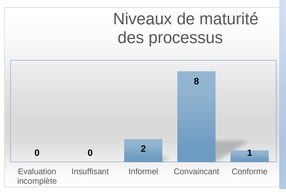
1- Grille d'évaluation des exigences

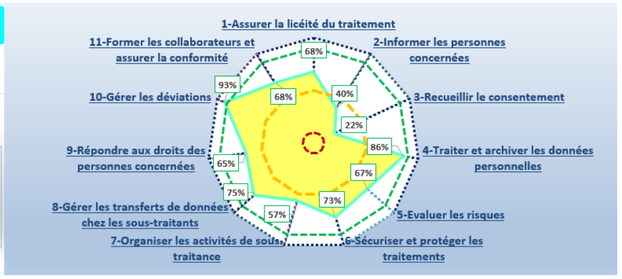
Titres des Articles/Considérant/ Ligne Directrice du G29	Processus et actions associées	Indications	Evaluation	Taux %	Libellé de l'évaluation
Article 6.1 Considérant 40	**1-Assurer la licéité du traitement initial et du traitement ultérieur**	Le traitement est licite s'il fait l'objet d'un consentement ou s'il correspond à un intérêt légitime ou à une obligation légale	**Convaincant**	**53%**	**Niveau 3 : Les activités doivent être tracées et améliorées.**
6.1 a)	Les personnes concernées ont donné leur consentement au traitement de leur DCP pour une ou plusieurs finalités données **OU**		**Non Applicable**	NA	Non Applicable.
6.1 b)	Les personnes concernées sont parties d'un contrat pour lequel le traitement des données est nécessaire.		**FAUX**	0%	L'action n'est pas réalisée selon l'avis du responsable de traitement.
6.1 c) Considérants 41 & 45	Le traitement répond à une obligation légale ou réglementaire.	Ex: pharmacovigilance, transparence des liens	**Choix de conformité**		L'action n'a pas encore été évaluée.
6.1 d) Considérant 46	Le traitement est nécessaire à la sauvegarde des intérêts vitaux des personnes concernées ou d'une autre personne.	Ex: traitement nécessaire à des urgences sanitaires ou humanitaires	**Plutôt faux**	30%	L'action est réalisée quelques fois ou de manière aléatoire.
6.1 e) Considérant 45	Le traitement est nécessaire à une mission d'intérêt public ou relevant de l'exercice de l'autorité publique;		**Plûtot vrai**	70%	L'action est réalisée et formalisée.
6.1 f) Considérants 47, 48, 49, 50	Le traitement est effectué à des fins légitimes	Ex: traitement à des fins de marketing direct ou de prévention des fraudes, transmission de DCP au sein d'un groupe d'entreprise	**VRAI**	100%	L'action est réalisée, formalisée, tracée et améliorée.
6.4	En cas de nouvelle finalité de traitement: la finalité initiale pour laquelle les données ont été collectées initialement permet cette		**FAUX**	0%	L'action n'est pas réalisée selon l'avis du responsable de traitement.

2- Résultats pour chaque processus de traitement

Résultats







3- Plan d'actions

COMMENTAIRES sur les RÉSULTATS obtenus			
Commentaires (collectifs si possible) :			
Plan d'actions de progrès envisagées :			
Action	**Pilote (qui)**	**Échéance**	**Résultats après actions**

Outils disponibles pour la démarche:

- Guides, modèle de registre de la CNIL
- analyse d'impact interne ou logiciel PIA (Privacy Impact Assessment) de la CNIL
- Cartographie des traitements et outil d'autodiagnostic PRIVACY DIAG

6-Références bibliographiques

1-**Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel**
2-NF EN ISO 9000 - Systèmes de management de la qualité - Principes essentiels et vocabulaire ». Afnor Editions, www.afnor.org, 15-oct-2015.
3-La Sécurité des données personnelles-CNIL
4-RGPD: se préparer en 6 étapes-CNIL
5- Analyse d'impact relative à la protection des données-CNIL
6-Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises-CNIL

Résultats

- Synthèse des exigences d'un référentiel complexe dans une cartographie des processus et un outil d'autodiagnostic adaptable et évolutif,
- Cartographie des traitements et initiation de la dynamique de gouvernance des données dans une PME,
- Gain de temps pour réaliser les diagnostics.

Retour d'expérience

- Prioriser les actions sur les traitements de données sensibles,
- Trouver des leviers à la résistance au changement et prendre en compte la charge de travail des collaborateurs dans une petite structure.