



Travaux communs sur RGPD

Interclubs Utilisateurs

13 mars 2018

64 rue du Ranelagh

75016 Paris

www.usf.fr

Patrick GEAI – Président USF

Présentation de l'USF



Historique :

- Création en 1989
- Association Indépendante régie par la Loi 1901
- Indépendance financière qui donne une totale liberté d'action et de jugement à l'Association

Les chiffres clés 2017 de l'USF



Événements

Printemps USF

120
participants



Convention USF



Convention USF 2018
10 & 11 octobre à Lyon
La donnée au cœur des
nouveaux usages

- ❑ **La nouvelle réglementation sur les données personnelles entrera en vigueur le 25/05/2018**
- ❑ **Des sanctions importantes pourront être appliquées en cas de non-conformité des entreprises (jusqu'à 4% du CA monde)**
- ❑ **Contrairement à la réglementation précédente, les fournisseurs sont parties prenantes : tenus de respecter la réglementation pour le compte de leurs clients**

Article 40 du RGPD :

→ Les états membres, **les autorités de contrôle**, le comité et la commission **encouragent l'élaboration de codes de conduites** destinés à contribuer à la bonne application du présent règlement...

→ **Les associations** et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants **peuvent élaborer des codes de conduite**, les modifier ou les proroger, aux fins de préciser les modalités d'application du présent règlement ...

→ **Les associations** et autres organismes qui ont l'intention d'élaborer un code de conduite ou de modifier ou de proroger, **soumettent le projet de code à l'autorité de contrôle. L'autorité de contrôle rend un avis** sur la question de savoir si le projet de code respecte le règlement **et approuve ce projet de code** si elle estime qu'il offre des garanties appropriées suffisantes ...

- ❑ **Elaborer un Code de Conduite définissant les engagements fournisseurs et portant sur la mise en œuvre du RGPD dans le contexte d'utilisation de progiciels infogérés ou dans le cloud**

- ❑ **Ce code de conduite doit être :**
 - Évolutif en définissant dans une première version le cadre général mais pourra ensuite mieux préciser les engagements attendus
 - Rédigé de façon à ce que les clients puissent en faire une pièce contractuelle

- ❑ **Soumettre ce Code de Conduite pour approbation aux instances concernées (françaises et/ou européennes)**

- ☐ **AUFO**
- ☐ **Groupe Francophone des Utilisateurs JD Edwards**
- ☐ **Club des Utilisateurs PeopleSoft**
- ☐ **DynsClub**
- ☐ **USF**
- ☐ **Cabinet Feral Schuhl / Sainte Marie**

- ☐ **Trois types de fournisseurs différents**
 - Editeur de progiciel
 - Intégrateurs (notamment pour la partie privacy by design)
 - Les fournisseurs de solutions SaaS

- ☐ **Contenu**
 - ☐ Identifier les engagements à demander aux fournisseurs pour que les clients puissent se conformer au RGPD
 - ☐ Définir des indicateurs et points de contrôle pour vérifier la mise en œuvre

- ☐ **Nous avons écarté**
 - Les infogérants
 - Les fournisseurs IaaS

Quelle méthodologie utiliser ?

RGPD et impacts fournisseurs



99 articles

173 considérants

CHAPITRE I Dispositions générales	
Article premier Objet et objectifs	
Article 2 Champ d'application matériel	
Article 3 Champ d'application territorial	
Article 4 Définitions	
CHAPITRE II Principes	
Article 5 Principes relatifs au traitement des données à caractère personnel	
Article 6 Licéité du traitement	
Article 7 Conditions applicables au consentement	
Article 8 Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information	
Article 9 Traitement portant sur des catégories particulières de données à caractère personnel	
Article 10 Traitement des données à caractère personnel relatives aux condamnations et infractions	
Article 11 Traitement ne nécessitant pas d'identification	
Droits de la personne concernée	
Article 12 Transparence des informations et des communications et modalités d'exercice des droits de la personne concernée	
Article 13 Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée	
Article 14 Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée	
Article 15 Droit d'accès de la personne concernée	
Article 16 Droit de rectification	
Article 17 Droit à l'effacement (« droit à l'oubli »)	
Article 18 Droit à la limitation du traitement	
Article 19 Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement	
Article 20 Droit à la portabilité des données	
Article 21 Droit d'opposition	
Article 22 Décision individuelle automatisée, y compris le profilage	
Article 23 Limitations	
CHAPITRE IV Responsable du traitement et sous-traitant	
Article 24 Responsabilité du responsable du traitement	
Article 25 Protection des données dès la conception et protection des données par défaut	
Article 26 Responsables conjoints du traitement	
Article 27 Représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union	
Article 28 Sous-traitant	
Article 29 Traitement effectué sous l'autorité du responsable du traitement ou du sous-traitant	
Article 30 Registre des activités de traitement	
Article 31 Coopération avec l'autorité de contrôle	
Article 32 Sécurité du traitement	
Article 33 Notification à l'autorité de contrôle d'une violation de données à caractère personnel	
Article 34 Communication à la personne concernée d'une violation de données à caractère personnel	
Article 35 Analyse d'impact relative à la protection des données	
Article 36 Consultation préalable	
Article 37 Désignation du délégué à la protection des données	
Article 38 Fonction du délégué à la protection des données	
Article 39 Missions du délégué à la protection des données	
Article 40 Codes de conduite	
Article 41 Suivi des codes de conduite approuvés	
Article 42 Certification	
Article 43 Organismes de certification	
CHAPITRE V Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales	
Article 44 Principe général applicable aux transferts	
Article 45 Transferts fondés sur une décision d'adéquation	

Article 46 Transferts moyennant des garanties appropriées	
Article 47 Règles d'entreprise contraignantes	
Article 48 Transferts ou divulgations non autorisés par le droit de l'Union	
Article 49 Dérogations pour des situations particulières	
Article 50 Coopération internationale dans le domaine de la protection des données à caractère personnel	
CHAPITRE VI Autorités de contrôle indépendantes	
Article 51 Autorité de contrôle	
Article 52 Indépendance	
Article 53 Conditions générales applicables aux membres de l'autorité de contrôle	
Article 54 Règles relatives à l'établissement de l'autorité de contrôle	
Article 55 Compétence	
Article 56 Compétence de l'autorité de contrôle chef de file	
Article 57 Pouvoirs d'enquête	
Article 58 Pouvoirs d'avis	
Article 59 Règles applicables aux autorités de contrôle	
CHAPITRE VII Coopération et assistance mutuelle - Article 60 à 66	
Article 60 Coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées	
Article 61 Assistance mutuelle	
Article 62 Opérations conjointes des autorités de contrôle	
Article 63 Mécanisme de contrôle de la cohérence	
Article 64 Avis du comité	
Article 65 Règlement des litiges par le comité	
Article 66 Procédure d'urgence	
Article 67 Échange d'informations	
Article 68 Comité européen de la protection des données	
Article 69 Indépendance	
Article 70 Missions du comité	
Article 71 Rapports	
Article 72 Pouvoirs d'enquête	
Article 73 Pouvoirs d'avis	
Article 74 Mission d'assistance technique	
Article 75 Secrétariat	
Article 76 Confidentialité	
CHAPITRE VIII Voies de recours, responsabilité et sanctions - Article 77 à 78	
Article 77 Droit d'introduire une réclamation auprès d'une autorité de contrôle	
Article 78 Droit à un recours juridictionnel effectif contre une autorité de contrôle	
Article 79 Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant	
Article 80 Représentation des personnes concernées	
Article 81 Suspension d'une action	
Article 82 Droit à réparation et responsabilité	
Article 83 Conditions générales pour imposer des amendes administratives	
Article 84 Sanctions	
CHAPITRE IX Dispositions relatives à des situations particulières de traitement - Article 85 à 88	
Article 85 Traitement et liberté d'expression et d'information	
Article 86 Traitement et accès du public aux documents officiels	
Article 87 Traitement du numéro d'identification national	
Article 88 Traitement de données dans le cadre des relations de travail	
Article 89 Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques	
Article 90 Obligations de secrets	
Article 91 Règles existantes des églises et associations religieuses en matière de protection des données	
CHAPITRE X Actes délégués et actes d'exécution - Article 92 à 93	
CHAPITRE XI Dispositions finales - Article 94 à 99	

❑ Parmi les 99 articles du RGPD, focaliser sur les 12 éléments clés dans la mise en œuvre du RGPD

1. L'extra territorialité du RGPD
2. Les bases légales de traitement et consentement
3. Le délégué à la protection des données personnelles (DPO)
4. Autorité chef de file et CEPD
5. L'accountability et la gouvernance des données
6. L'analyse d'impact relative à la vie privée (DPIA)
7. Sécurité et notification des violations de sécurité
8. Les certifications et codes de conduite
9. Le régime et les nouvelles obligations des sous-traitants
10. Information des personnes et transparence
11. Droits des personnes
12. Sanctions

- ☐ Reprendre chacun des 12 éléments clés
- ☐ Identifier si les fournisseurs sont concernés par l'élément
- ☐ Si oui, décrire :
 - Exigences RGPD (exemple : extra territorialité)
 - Le niveau des attentes du client vis-à-vis du fournisseur
 - Décrire les engagements/actions attendus du fournisseur
 - Les modalités de contrôle, indicateurs à mettre en place

Code de conduite pour les fournisseurs

Thèmes du RGPD	Exigences RGPD	Attentes clients	Engagements/actions Fournisseurs	Modalités de contrôle, indicateurs
Extra Territorialité du RGPD	Traitements effectués par des responsables de traitement (RT) établis sur le territoire de l'UE	Conformité pour les sous traitants	Même si traitement a lieu hors UE, que les sous traitants soient établis sur le territoire UE	Contrôle pour chacun des traitements concernés

Exemple

- ❑ **11 des 12 thèmes ont été étudiés en plénière**

- ❑ **Reste à faire :**
 - ❑ Alimenter le dernier thème
 - ❑ Mettre en forme et rédiger du livrable
 - ❑ Effectuer la relecture

- ❑ **Objectif : Publication d'un livrable pour le 1^{er} semestre 2018**