

**25 mai 2018**  
**RGPD**

**DS**  
AVOCATS

**Savoir,  
Faire**

[www.dsavocats.com](http://www.dsavocats.com)



## CONTACT

**Catherine Verneret**, Associée et Responsable du  
Département Droit de la Propriété Intellectuelle,  
Technologies Numériques et Data

[rgpd@dsavocats.com](mailto:rgpd@dsavocats.com) +33.1.53.67.67.93

**4** Continents

**24** Bureaux / Offices

**300** Professionnels  
du Droit / Lawyers

**Etes-vous prêts pour le 25 mai 2018 ?  
Il est encore temps de réagir...**

Le Règlement Général sur la Protection des Données («RGPD») sera applicable dans tous les Etats membres de l'UE à partir du 25 mai 2018. Il vient se substituer à la Directive de 1995 et modifie largement la Loi Informatique et Libertés du 6 janvier 1978 qui constituait jusqu'à présent le référentiel légal français.

## Qui est concerné ?

Dès qu'une entreprise ou une administration est **basée ou mène des activités localisées sur le territoire de l'UE**, dès qu'un prestataire propose des biens ou services à des **personnes se trouvant sur le territoire de l'UE** ou qu'il se contente « d'observer » le comportement de ces personnes, il est soumis au RGPD et ce, **quand bien même il n'est pas lui-même établi sur le territoire de l'UE** (il doit y désigner un représentant).

**Toutes les entreprises, tous secteurs confondus, sont concernées**, dès lors qu'elles manipulent des données personnelles (ex : l'entreprise qui déploie un système de gestion de paie, le groupe qui échange des données clients ou salariés avec ses filiales, le prestataire qui développe un outil CRM, l'assurance qui délocalise la gestion de ses services IT, etc.).

## Qu'est ce qui change ? Simplification des démarches administratives

### Fin des formalités préalables

Sauf exception, il ne sera plus nécessaire d'effectuer des déclarations ou demandes d'autorisation préalables à la mise en place de traitements de données personnelles. Désormais, les entreprises doivent être en mesure de justifier, en permanence, la protection des données personnelles en leur sein (**principe d'accountability**).

### « Guichet unique »

Les sociétés seront en contact uniquement avec l'autorité de protection des données de leur « établissement principal », désignée comme autorité « chef de file » et n'auront ainsi qu'un seul interlocuteur pour l'Union européenne.

## Responsabilisation des acteurs

**Le responsable de traitement** doit mettre en place des mesures techniques et organisationnelles appropriées et notamment :

- la mise en place et la tenue à jour d'un registre des activités de traitement ;
- **la notification des failles de sécurité** ;
- la protection des données dès la conception des services et architectures de données (**privacy by design**) et par défaut (principe de « minimisation » des données) ;
- analyse d'impact préalable à la mise en œuvre des traitements à risque (« Privacy Impact Assessment » ou « PIA ») ;
- la désignation d'un délégué à la protection des données.

Le **sous-traitant** a des obligations spécifiques :

- conseil auprès du responsable de traitement (PIA, failles, sécurité, destruction des données, contribution aux audits) ;
- garantie de la sécurité et la confidentialité des données ;
- la mise en place et tenue à jour d'un registre des activités de traitement.

Le RGPD prévoit l'élaboration de codes de conduite et la mise en place de certificats, labels et marques pour aider à démontrer la conformité aux règles de protection des données.

## Renforcement du droit des personnes

### Création de nouveaux droits

En complément des droits classiques déjà reconnus aux personnes par la Loi informatique et Libertés de 1978, les personnes physiques sont titulaires de nouveaux droits : droit à l'**oubli** et à l'**effacement**, droit à la **portabilité** des données, droit à la limitation des traitements, droit à la **réparation** des dommages matériel ou moral, introduction d'actions collectives, etc.

### Consentement

**Le consentement des personnes physiques doit résulter d'actes positifs, univoques et aisément révocables. Le responsable de traitement doit pouvoir fournir la preuve de la matérialisation du consentement de la personne**, ce qui nécessite l'implication de tous les services de l'entreprise concernée (pas seulement du DPO).



## Sécurité des données et notification des violations

La protection des données personnelles adresse aussi la **sécurité informatique**. Le responsable de traitement et tout sous-traitant doivent garantir une sécurité et une confidentialité appropriées (pseudonymisation, chiffrement, capacité de restauration rapide des données, etc.). Les outils de l'entreprise et ceux qu'elle acquiert auprès de tiers doivent répondre aux nouvelles exigences.

Si une violation des données personnelles est constatée, celle-ci doit être notifiée dans les meilleurs délais :

- Pour le responsable de traitement : à l'autorité de contrôle compétente et dans certains cas, à la personne concernée ;
- Pour le sous-traitant : au responsable de traitement.

## Flux transfrontaliers de données hors UE

Ils sont toujours possibles mais les modalités de leur encadrement vont évoluer au regard de nouvelles exigences. De nouveaux outils sont prévus en complément de ceux existants.

## Le Délégué à la Protection des Données (Data Protection Officer), le chef d'orchestre de la conformité

Sa désignation est obligatoire si :

- le traitement est effectué par une autorité publique ou un organisme public ;
- les activités de base du responsable ou sous-traitant :
  - exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
  - consistent en un traitement à grande échelle de données dites « sensibles ».

Il remplacera le CIL. Revêtu de l'autorité nécessaire et tenu au secret professionnel, il sera l'interface entre l'entreprise et l'autorité de contrôle.

## Des sanctions graduées et renforcées

Les sanctions qui étaient jusqu'à présent plafonnées à un montant de 150 000 euros peuvent désormais s'élever à **10 ou 20 millions d'euros ou de 2 à 4% du chiffre d'affaire annuel mondial** (le montant le plus élevé étant retenu.)

## Comment DS Avocats peut vous aider ?

Quel que soit votre secteur d'activités (privé ou public), quel que soit le type de données personnelles que vous traitez (données clients, données de santé, données bancaires, données des salariés, etc.) et quel que soit le lieu d'implantation de vos filiales à l'étranger (UE ou hors UE), DS AVOCATS est l'un des seuls cabinets d'avocats français à pouvoir offrir à ses clients une **expertise juridique transversale et multi-juridictionnelle** grâce aux différents bureaux et desks de DS dans le monde.

Déjà partenaire de ses clients et de leurs Correspondants Informatique et Libertés (CIL) depuis de nombreuses années, nous sommes en mesure de **vous accompagner dans vos projets de mise en conformité** en mettant à votre service une **équipe d'avocats dédiée, réactive, pragmatique**, et disposant d'un savoir-faire transversal dans une économie toujours plus digitalisée.

## Notre offre est flexible et nous l'adapterons en fonction de vos besoins, de vos objectifs et de votre budget.

Notre intervention, à vos côtés, peut être plus ou moins étendue, selon votre situation actuelle : (i) mise en conformité complète, (audit de l'existant, analyse des écarts, feuille de route, actions de mise en conformité), (ii) accompagnement de votre DPO interne dans votre mise en conformité (ex : formalisation du référentiel sécurité, réalisation d'une PIA/étude d'impact, etc.), (iii) accompagnement sur un projet en particulier (ex : mise en œuvre de nouveaux outils, transferts de données hors de l'UE, etc.), (iv) accompagnement dans le cadre de vos relations avec les autorités de contrôle (CNIL, etc.), (v) séances de sensibilisation/ de formation au RGPD à destination de vos équipes, et/ou (vi) assistance dans le cadre de précontentieux ou contentieux (assistance en cas de contrôle de la CNIL, suite à une mise en demeure d'un client, etc.) etc.

**Paris**

+33.1.53.67.50.00  
courrier@dsavocats.com

**Bordeaux**

+33.5.57.99.74.65  
bordeaux@dsavocats.com

**Lille**

+33.3.59.81.14.00  
lille@dsavocats.com

**Lyon**

+33.4.78.98.03.33  
lyon@dsavocats.com

**Reunion**

+33.2.62.50.99.10  
reunion@dsavocats.com

**Barcelona**

+34.93.518.01.11  
info@ds-ovslaw.com

**Madrid**

+34.91.533.53.08  
info@ds-ovslaw.com

**Brussels**

+32 2286 80 33  
bruxelles@dsavocats.com

**Milan**

+39.02.29.06.04.61  
milan@dsavocats.com

**Stuttgart**

+49.711.16.26.000  
info@ds-graner.com

**Quebec**

+1.418.780.4321  
info@dsavocats.ca

**Montreal**

+1.514.360.4321  
info@dsavocats.ca

**Toronto**

+1.647.477.7317  
info@dsavocats.ca

**Vancouver**

+1.604.669.8858  
info@dsavocats.ca

**Ottawa**

+1.613.319.9997  
info@dsavocats.ca

**Buenos Aires**

+54 11 48 08 91 73  
info@dsbuenosaires.com.ar

**Lima**

lima@dsabogados.pe

**Santiago**

+562.32.45.45.00  
info@dsabogados.cl

**Beijing**

+86.10.65.88.59.93  
beijing@dsavocats.com

**Guangzhou**

+86.20.81.21.86.69  
guangzhou@dsavocats.com

**Shanghai**

+86.21.63.90.60.15  
shanghai@dsavocats.com

**Ho Chi Minh City**

+84.8.39.10.09.17  
dshochiminh@dsavocats.com

**Singapore**

+65.62.26.29.69  
singapore@dsavocats.com

**DS Consulting Afrique - Dakar**

+221.77.255.68.18  
dakar@dsconsultingafrique.com

**Partenariat**

**DS Squaris Union Européenne**

+32 2286 80 38  
secretariat@squaris.com