HISCOX
ASSURÉMENT UNIQUE

LLC & ASSOCIÉS AVOCATS

PROTECTION DES DONNÉES PERSONNELLES

COMPRENDRE LE RÈGLEMENT EUROPÉEN

1. LES GRANDS PRINCIPES DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (DCP)

QUELQUES DÉFINITIONS DU RÈGLEMENT

Accountability	Principe général de responsabilité, à la charge du Responsable de traitement.
BCR	Binding Corporate Rules, Règles d'entreprises contraignantes.
CEDP	Comité Européen de la Protection des Données, qui remplace le G29.
DPO	Data Protection Officer. Le Règlement prévoit l'obligation de nommer un délégué à la protection des données (Article 37 du Règlement).
DCP	Données à Caractère Personnel.
Privacy by default	Le Responsable de traitement garantit, par défaut, que seules les données qui sont nécessaires à la finalité recherchée sont traitées.
Privacy by design	Le Responsable de traitement garantit, dès la conception du traitement et tout au long de l'exploitation, de l'adéquation du traitement au regard de la finalité recherchée et de la mise en place de mesures telles que la pseudonymisation visant à satisfaire les objectifs de sécurité.
Privacy Shield	Mécanisme par lequel une société de droit US est réputée appliquer un minimum standard de principes de protection de la vie privée.

A. LA CONFIRMATION DES EXIGENCES DE LA DIRECTIVE N°95/46/CE DU 24 OCTOBRE 1995 (ARTICLE 5 DU RÈGLEMENT)

- **Traitement licite, loyal et transparent** des données à caractère personnel
- **Finalités déterminées, explicites et légitimes**
- **Adéquation, pertinence et limitation des traitements**
- **Contraintes d'exactitude et de mise à jour**
- **Limitation de la durée de conservation**
- **Obligation d'assurer la sécurité des données**

B. L'"ACCOUNTABILITY" (ARTICLE 24 DU RÈGLEMENT)

Introduction d'un **principe général de responsabilité, à la charge du Responsable de traitement,** quant à la mise en place de mesures techniques et organisationnelles respectant les principes du Règlement et plus spécifiquement de sécurité et de proportionnalité de la collecte de données à caractère personnel.

Ce principe est d'autant plus essentiel que le Règlement impose au Responsable de traitement l'examen périodique des mesures prises par le sous-traitant.

2. UN SYSTÈME UNIFORMISÉ

A. UNE APPLICATION UNIFORMISÉE DANS L'UE

L'entrée en vigueur d'un Règlement remplaçant la Directive a pour conséquence directe :

- **L'application immédiate des nouvelles règles sur l'ensemble du territoire de l'Union Européenne, aucune transposition nécessaire par une réglementation locale dans chaque Etat n'est nécessaire**
- **La suppression des différences d'interprétation selon les États membres, et aucun délai supplémentaire d'application :**

Le Règlement est pleinement applicable dès le 25 mai 2018 dans tous les États membres.

B. UN GUICHET UNIQUE

Chaque entreprise sera désormais en contact uniquement avec l'autorité de protection des données compétente sur le territoire de l'Etat membre dans lequel est situé son établissement principal.

- **"Etablissement principal" :** lieu du siège central ou établissement au sein duquel sont prises les décisions relatives aux finalités et modalités du traitement
- **En France,** le guichet unique est la Commission nationale Informatique et Libertés (CNIL)

C. UNE COOPÉRATION RENFORCÉE DES AUTORITÉS NATIONALES

En cas de traitement transnational, les décisions seront adoptées conjointement par les différentes autorités, pour assurer des règles et des sanctions harmonisées. Les régulateurs européens chargés de la protection des DCP sont aujourd'hui réunis au sein d'un Comité Européen de la Protection des Données (CEDP), qui remplace le G29.

D. L'ENCADREMENT DES TRANSFERTS DE DONNÉES HORS DE L'UNION EUROPÉENNE

Soumission au Règlement des modalités actuelles de transfert des DCP hors UE, mais également pour tout traitement ou transfert ultérieur : tout transfert hors de l'UE n'est possible que s'il est encadré par des outils garantissant un niveau de protection suffisant et approprié :

Règles d'entreprises contraignantes (Binding Corporate Rules ou "BCR")
Clauses contractuelles types approuvées par la Commission européenne, clauses contractuelles d'une autorité nationale approuvées par la Commission européenne, ou encore adhésion à des codes de conduite ou mécanisme de certification.

Privacy Shield
Mécanisme par lequel une société de droit US est réputée appliquer un minimum standard de principes de protection de la vie privée – *Privacy principles* – par son adhésion, renouvelée annuellement, à une liste dédiée auprès du Ministère du commerce des Etats-Unis. Seul cet agrément autorise l'entreprise à traiter les DCP collectées au sein de l'UE.

3. UN CHAMP D'APPLICATION PLUS LARGE

A. L'ÉLARGISSEMENT DES CHAMPS D'APPLICATION MATÉRIELS ET TERRITORIAUX

Le Règlement couvre tous les domaines du champ d'application du droit de l'UE, et indifféremment des éléments suivants :

- **Le support de collecte des données**
- **La localisation de la personne** dont les données sont collectées
- **Le siège social de l'entreprise – de son sous-traitant –** procédant au traitement.
- **La nationalité de la personne** dont les données sont collectées

Le Règlement s'appliquera alors à une entreprise qui a son siège hors de l'UE mais **dont les activités de collecte sont liées à un sujet de droit soumis au droit de l'Union.**

B. PRÉCISION ET ÉLARGISSEMENT DE LA DÉFINITION DES DCP
(ARTICLE 4 DU RÈGLEMENT)

- **Modernisation de la définition afin de couvrir un champ d'application plus large : nom, données de localisation, identifiant en ligne, éléments propres à l'identité génétique…**
- **Définitions des données génétiques, biométriques et concernant la santé**
- **Introduction de la notion de pseudonymisation** et exclusion du champ du Règlement des données anonymes

C. LE RENFORCEMENT DES DROITS DES INDIVIDUS

DROITS ACTUELS	NOUVEAUX DROITS
• Droit à l'information • Droit d'accès • Droit à la rectification • Droit d'opposition	• **Précision sur les modalités d'expression du consentement de l'utilisateur** • **Portabilité** (L'utilisateur peut récupérer ses données auprès d'un opérateur et les transférer auprès d'un autre) • **Droit à l'effacement** (article 17) • **Recours au profilage encadré** (article 22)

D. LA RESPONSABILITÉ DES SOUS-TRAITANTS ACCRUE
(ARTICLE 28 DU RÈGLEMENT)

- **Extension des obligations des responsables de traitement aux sous-traitants** (notamment tenue d'un registre et désignation d'un DPO)
- **Obligation de conseil auprès du responsable du traitement** en matière de d'études d'impact, failles, sécurité, destruction des données, contribution aux audits
- Le sous-traitant ne peut lui-même sous-traiter tout ou partie du traitement qu'avec **l'accord exprès et préalable du responsable de traitement**

4. L' "ACCOUNTABILITY"

A. LE PRIVACY BY DEFAULT/DESIGN

La mise en œuvre des mesures techniques et organisationnelles nécessaires au respect de la protection des DCP implique **les deux notions suivantes :**

Privacy by design
Le responsable de traitement garantit, dès la conception du traitement et tout au long de l'exploitation, de l'adéquation du traitement au regard de la finalité recherchée et de la mise en place de mesures telles que la pseudonymisation visant à satisfaire les objectifs de sécurité.

Privacy by default
le responsable de traitement garantit, par défaut, que seules les données qui sont nécessaires à la finalité recherchée sont traitées.

Le respect de ces obligations peut être obtenu, notamment, par la constitution des outils suivants :

- **La tenue d'un registre des traitements mis en œuvre**
- **La mise en place d'un processus de notification des failles de sécurité**
- **La certification des traitements**
- **La nomination d'un DPO**
- **Les analyses d'impact et les demandes préalables**
- **La constitution et l'adhésion à de codes de conduite**

B. L'ALLÈGEMENT DES FORMALITÉS ADMINISTRATIVES NATIONALES

Le Règlement ne reprend pas le régime de déclaration et d'autorisation préalables auprès des autorités nationales, **à l'exception des traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.**

Il devient alors impératif de mettre en place des mesures préventives et des analyses d'impact afin d'anticiper tout traitement à risque.

C. LE "DATA PROTECTION OFFICER" (ARTICLE 37 DU RÈGLEMENT)

Le Règlement prévoit l'obligation de nommer un délégué à la protection des données pour les cas suivants :

- **Le secteur public**
- L'activité de l'entreprise consiste en des opérations de traitement qui exigent un **suivi régulier et systématique à grande échelle des personnes concernées**
- L'activité de l'entreprise consistent en un traitement à grande échelle de **catégories particulières de données, comme les données sensibles et les infractions et condamnations pénales**

Le DPO aura une mission d'information, de conseil, de contrôle, de collaboration auprès du responsable de traitement ainsi qu'une mission de coopération avec l'autorité de contrôle. Ces missions dépassent les missions du CIL actuel, procurant au DPO **des fonctions assimilables au management des risques.**

D. L'ANALYSE D'IMPACT (ARTICLE 37 DU RÈGLEMENT)

L'analyse d'impact, réalisée en coordination avec le DPO et amont du traitement, est **obligatoire dès lors que le traitement est susceptible d'engendrer un risque élevé pour les personnes physiques.**

L'analyse a pour objectif d'évaluer **les caractéristiques du traitement, ses risques et les mesures organisationnelles et techniques adoptées** au regard de l'objectif poursuivi.

5. LA NOTIFICATION DES VIOLATIONS DE DONNÉES (ARTICLE 33 DU RÈGLEMENT)

A. LE PRINCIPE DE LA NOTIFICATION

Toute violation de données doit être notifiée à l'autorité de contrôle par tout responsable du traitement, **peu importe son activité.**

Le sous-traitant est soumis à la même obligation envers le responsable du traitement.

En cas de risque élevé pour les droits des individus (discrimination, usurpation d'identité, etc.), la notification individuelle à l'ensemble des personnes concernées sera également obligatoire, à quelques exceptions près (chiffrement des données compromises, conséquences disproportionnées de la notification…).

Pour les entreprises
Le responsable de traitement devra prendre toutes les garanties techniques et juridiques auprès de son sous-traitant afin de satisfaire à cette obligation et vérifier, notamment, ses engagements en matière de sécurité et de confidentialité des DCP.

Pour les particuliers
Tout traitement illicite de DCP pourra faire l'objet d'une action de groupe, ouverte à tout particulier et toute association de défense des consommateurs et devant toute juridiction, tant à l'encontre du responsable de traitement que du sous-traitant.

B. LES MODALITÉS DE LA NOTIFICATION À L'AUTORITÉ DE CONTRÔLE

Dans les meilleurs délais, et de préférence, il faudra prévenir l'autorité de contrôle 72 heures au plus tard après avoir pris connaissance de la compromission de DCP, ou pouvoir justifier du retard de notification en cas de dépassement de ce délai.

La notification devra contenir des éléments sur :

- **La nature de la violation**
- **Les coordonnées du DPO**
- **Les conséquences**
- **Les mesures prises**

Délai de notification
72H
MAXIMUM

La notification devra contenir des éléments sur **les mesures prises.**

6. L'APPLICATION DU RÈGLEMENT ET LES SANCTIONS

A. LES POUVOIRS D'INVESTIGATION DES AUTORITÉS DE CONTRÔLE (ARTICLE 58 DU RÈGLEMENT)

Les autorités de contrôle se voient conférer des **pouvoirs étendus en matière d'investigation :**

B. LE RENFORCEMENT DES SANCTIONS ADMINISTRATIVES

- **Avertissement, mise en demeure.**
- **Limitation du traitement, suspension du flux de données.**
- **Amendes administratives :** 10 à 20 millions d'euros, ou, dans le cas d'une entreprise, 2% jusqu'à 4% du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu).

€

Amendes administratives :

10 à 20M€ ou 2 à 4% du CA mondial

Attention, depuis la Loi pour la République numérique, **la CNIL peut d'ores et déjà prononcer des sanctions jusqu'à 3 millions d'euros.** Par ailleurs, la loi n° 2016-1547 du 18 novembre 2016 (article 60) ouvre la possibilité d'une action de groupe pour faire cesser un traitement illégal de DCP.

CONCLUSION & CONSEILS POUR LA MISE AUX NORMES DE VOTRE ENTREPRISE

A. LES OUTILS

Les moyens de se conformer dès maintenant à ce nouveau Règlement européen, applicable le 25 mai 2018 :

- **Audit**
- **Cartographie des données**
- **Refonte des chartes informatiques**
- **Gestion des sous-traitants**
- **Revue en profondeur des contrats**
- **Désignation d'un (futur) DPO**

B. LES AVANTAGES DE LA MISE EN CONFORMITÉ

- **Réputation fiable**
- **Confiance des utilisateurs**
- **Amoindrissement des risques de sanctions**
- **Assurer son capital données**

C. CONCRÈTEMENT / ET DEMAIN… ?

3 premières étapes pour se mettre en conformité :

1. **Consulter la CNIL pour vérifier ses obligations** en matière de collecte et de protection des données.
2. **Consulter l'ANSSI* pour vérifier ses processus en matière de sécurité des données.**

   *Agence Nationale de la Sécurité des Systèmes d'Information
3. **Identifier les traitements de DCP** et procéder aux analyses d'impact avec l'aide d'un expert.

NOUS VOUS ACCOMPAGNONS

VOTRE AVOCAT

Sa valeur ajoutée :

- **Audit de conformité**
- **Rédaction et mise à jour des contrats de sous-traitance**
- **Rédaction de code de conduite** / chartes informatiques
- **Applications pratiques de l'accountability**
- **Aide à la mise en place des procédures de notification**
- **Réalisation des analyses d'impact, formation des DPO**
- **Représentation dans les procédures administratives et les procédures judiciaires**

Romain Waïss-Moreau
Avocat Associé
LLC et Associés

VOTRE ASSUREUR

Sa valeur ajoutée :

- **Préfinancement d'un plan de réponse** en cas de compromission de DCP
- **Recours à un panel de prestataires spécialistes** en cas de sinistre
- **Couverture des frais de notification, des frais d'expertise / de défense, des dommages & intérêts** et des amendes (assurables)
- **Retour d'expérience sur les cas d'incident,** dans le cadre de l'assurance Hiscox CyberClear

Astrid-Marie Pirson
Directrice
de la Souscription
Hiscox France

DEUX EXPERTS VOUS AIDENT À RÉUSSIR LA MISE AUX NORMES DE VOTRE ENTREPRISE

LLC ET ASSOCIÉS

Le cabinet LLC et Associés a été fondé en 2004 avec l'idée d'accompagner le développement économique des entreprises innovantes.

Il couvre aujourd'hui tous les secteurs du droit des affaires, privées comme publiques, et de la fiscalité.

Les atouts majeurs du cabinet sont ses connaissances dans divers secteurs d'activité, comme les technologies de l'information et de la communication, la propriété intellectuelle, l'énergie, l'immobilier (public et privé) et les affaires publiques.

En France, LLC et Associés est représenté par ses 9 cabinets, comprenant 30 associés et 160 collaborateurs. En parallèle de son développement en France, il s'appuie sur un réseau international de cabinets d'avocats, présents dans 50 pays.

www.llc-avocat.com

HISCOX

Fondé en 1901, Hiscox est un groupe international d'assurances spécialisées coté sur le London Stock Exchange (HSX).

Hiscox est présent depuis 25 ans dans le secteur des métiers de l'informatique (20.000 clients IT en Europe dont 7.500 en France), et depuis plus de cinq ans dans le domaine de la cybercriminalité. En se spécialisant dans des secteurs bien définis et en plaçant l'assuré au cœur de ses préoccupations, Hiscox a mis au point des solutions sur mesure pour garantir les professionnels contre les conséquences potentielles d'une perte ou d'un vol de données.

En France, Hiscox dispose de bureaux à Paris, Lyon et Bordeaux. Hiscox France s'appuie sur ses 110 collaborateurs pour proposer une large gamme d'assurances conçues pour répondre aux besoins des particuliers, des professionnels et des collectivités.

www.hiscox.fr

LLC & ASSOCIÉS AVOCATS

HISCOX
ASSURÉMENT UNIQUE

38 avenue de l'Opéra 75002 Paris
T 0810 50 20 10
F 0810 00 71 02
E hiscox.info@hiscox.fr
www.hiscox.fr