4 Le périmètre du RGPD

Fiche pratique

Nathalie METALLINOS,
avocat à la Cour, Idea AARPI

Romain PERRAY,
avocat à la Cour, McDermott Will & Emery AARPI

1. Quand est-ce que le RGPD s'applique ? Quelles données sont concernées ? Quels traitements ? Quels organismes ?

Champ d'application territorial du RGPD : Le critère essentiel pour déterminer le champ d'application géographique du Règlement général sur la protection des données est celui du **lieu d'établissement du responsable** de traitement. Toutefois, **des critères additionnels** ont été retenus pour permettre l'élargissement de son champ d'application territorial à des acteurs non établis dans l'Union européenne (UE) mais traitant des données relatives aux personnes se trouvant dans l'UE.

Responsables de traitement ou sous-traitants établis dans l'Union européenne, ou

non établis dans l'UE, mais offrant des biens ou services dans l'Union ou suivant le comportement des personnes au sein de l'Union.

Champ d'application matériel : le RGPD s'applique aux traitements de données à caractère personnel, que ceux-ci soient automatisés ou non, qu'ils soient mis en œuvre par des **entreprises, des associations ou des organismes publics, quelle que soit leur taille** ou **leur forme**. Les traitements de **particuliers** peuvent être concernés s'ils ne sont pas mis en œuvre à des fins exclusivement personnelles (i.e. usage strictement domestique), comme par exemple la gestion d'un blog sur Internet qui permettrait à des tiers de poster des commentaires.

Exemples : systèmes de paye, géolocalisation, gestion des clients, objets connectés...

Mais aussi : fichiers manuels (fichier du personnel, dossier contentieux...)

Données concernées : toute information se rapportant à une personne physique vivante, identifiée ou identifiable par un nom, un numéro, un identifiant technique ou tout autre procédé permettant de lui attribuer des données (comprend les données pseudonymes*)

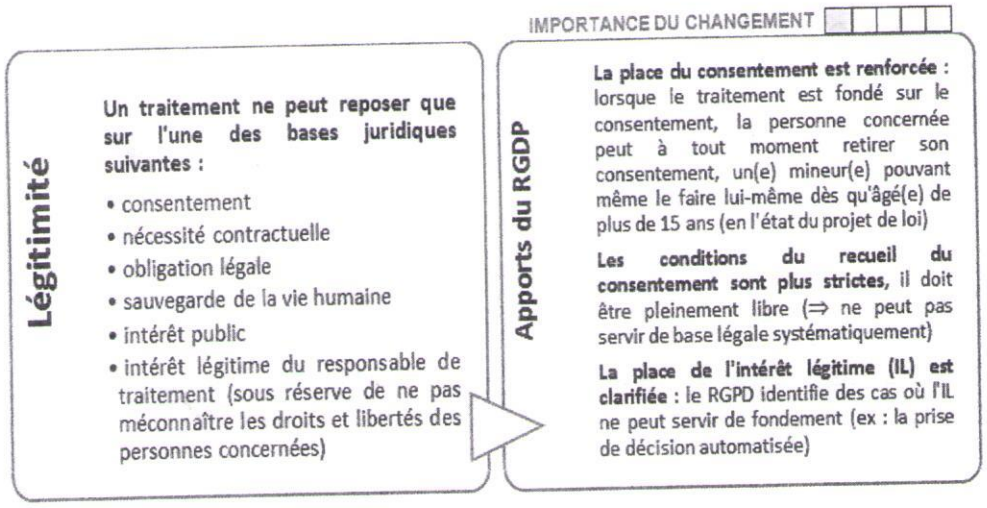
concerne aussi bien la vie privée, que la vie professionnelle, les relations sociales, les habitudes de vie et de consommation, les opinions

s'applique aux données déduites, appréciations, évaluations

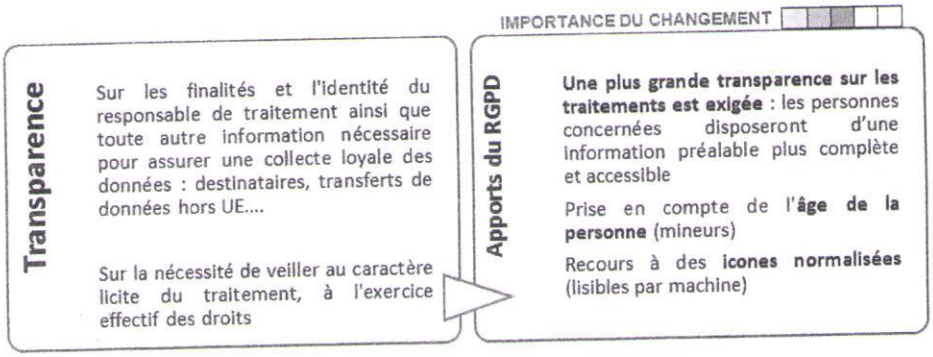
Pseudonymisation : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

2. Les principes et règles à respecter pour les responsables de traitements

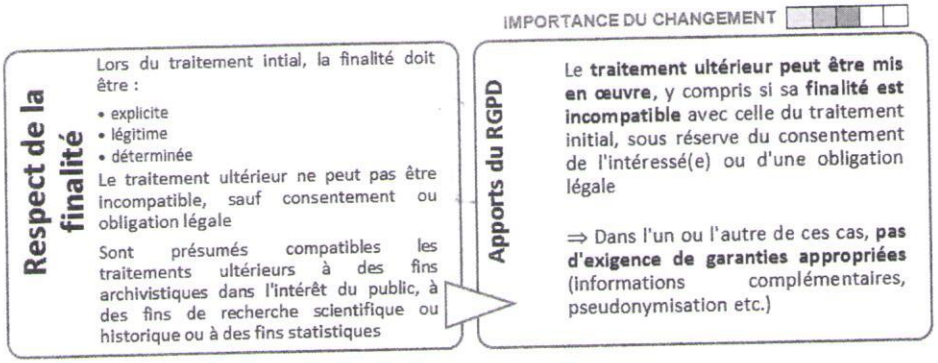
A. - Vérifier l'existence d'une base légale permettant la collecte de données à caractère personnel



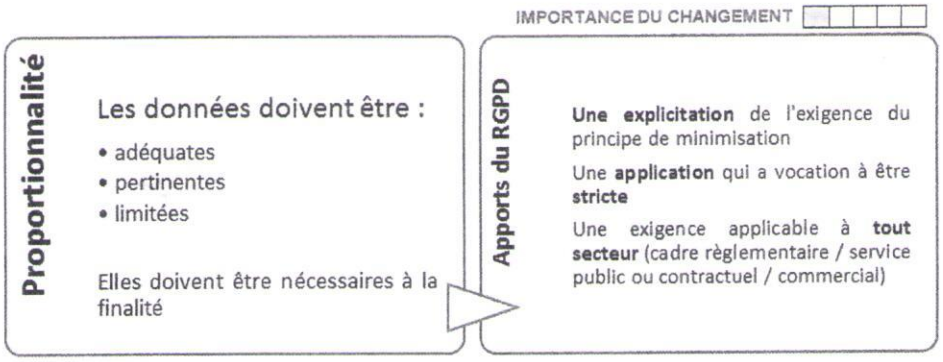
B. - Assurer une collecte loyale et licite (transparence)



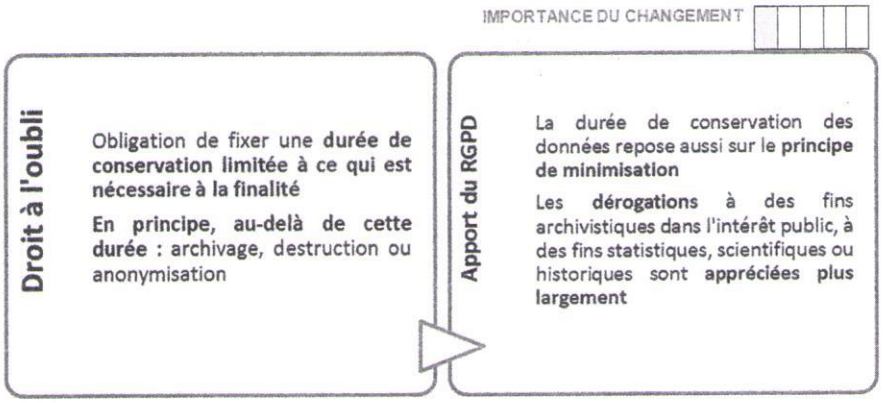
C. - Ne traiter les données que pour une finalité déterminée, explicite et légitime, et ne pas traiter ultérieurement les données d'une manière incompatible



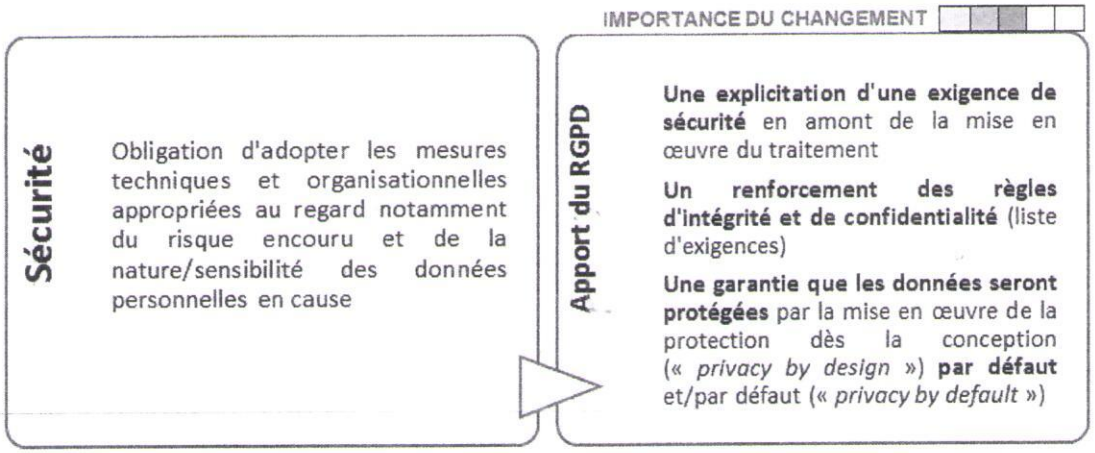
D. - Limiter la collecte aux données pertinentes, adéquates et strictement nécessaires au regard de la finalité du traitement



E. - Limiter la conservation des données à ce qui est nécessaire au regard de la finalité du traitement



F. - Garantir une sécurité appropriée des données à caractère personnel par des mesures physiques, logiques et organisationnelles



G. - Garantir les droits des personnes

IMPORTANCE DU CHANGEMENT

Reconduction des droits existants

Droits d'accès, de rectification et de suppression, d'opposition pour motif légitime

Droit à la tranquilité (*i.e.* opposition à l'utilisation des données à des fins de sollicitations commerciales)

Droit à ne pas faire l'objet d'une prise de décision automatisée et de contester la logique qui sous-tend le traitement

Nouveaux droits pour assurer le plein contrôle des individus sur leurs données

Le droit à l'oubli est revisité : il comporte désormais des déclinaisons nouvelles (droit à l'effacement, droit au déréférencement, droit au retrait du consentement, droit à la limitation du traitement)

(Nouveau) droit d'opposion au profilage à des fins de prospection commerciale

(Nouveau) droit à la portabilité

Le droit pour les personnes concernées d'être informées en cas de piratage ou de perte des données (notification des violations de données)

H. - Documenter la conformité afin d'être en mesure de démontrer le respect du RGPD

IMPORTANCE DU CHANGEMENT

Accountability

L'allègement des formalités et la mise à disposition d'outils de conformité (Registre, Délégué à la protection des données, études d'impact sur la vie privée, codes de conduite/certifications...) qui pourront être modulés en fonction du risque sur les droits et libertés des personnes

Apports du RGPD

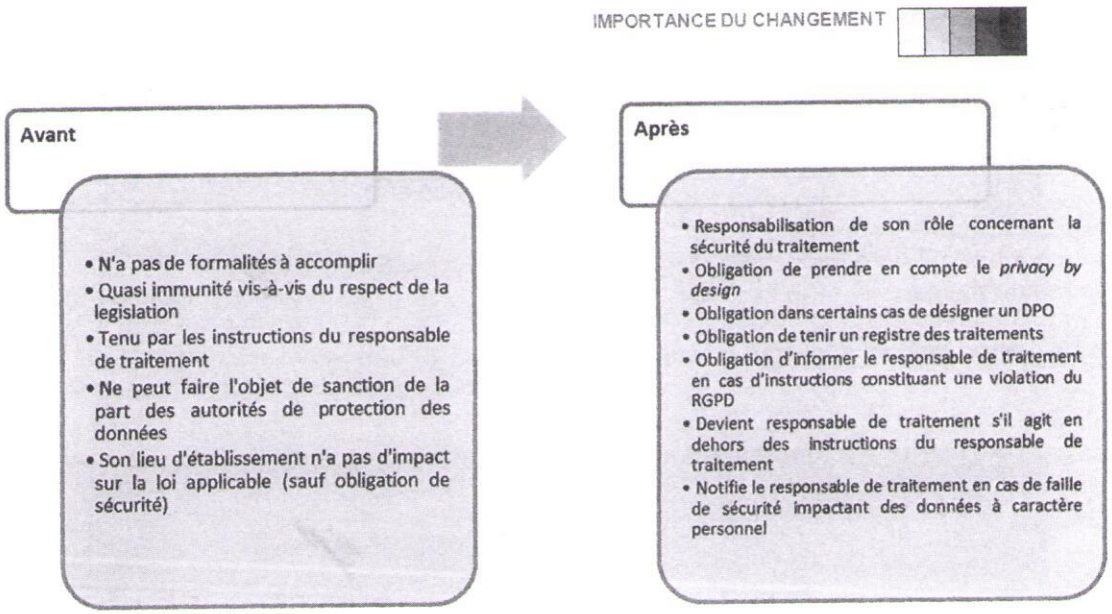
Une exigence d'amélioration de la connaissance par les **auteurs des traitements** qu'ils mettent en œuvre

Une mise en œuvre plus stricte des règles et principes (l'obligation de documenter l'ensemble des traitements et de pouvoir rendre compte de leur conformité) y compris en cas de flux transfrontaliers

Des sanctions plus importantes (jusqu'à 20 millions € ou 4 % du chiffre d'affaires consolidé)

Pour les entreprises multinationales, la possibilité d'un interlocuteur unique (guichet unique) pour toutes les autorités de protection des données européennes

3. Les changements induits pour les prestataires



4. Les changements pour les autorités de protection (la CNIL en France) :

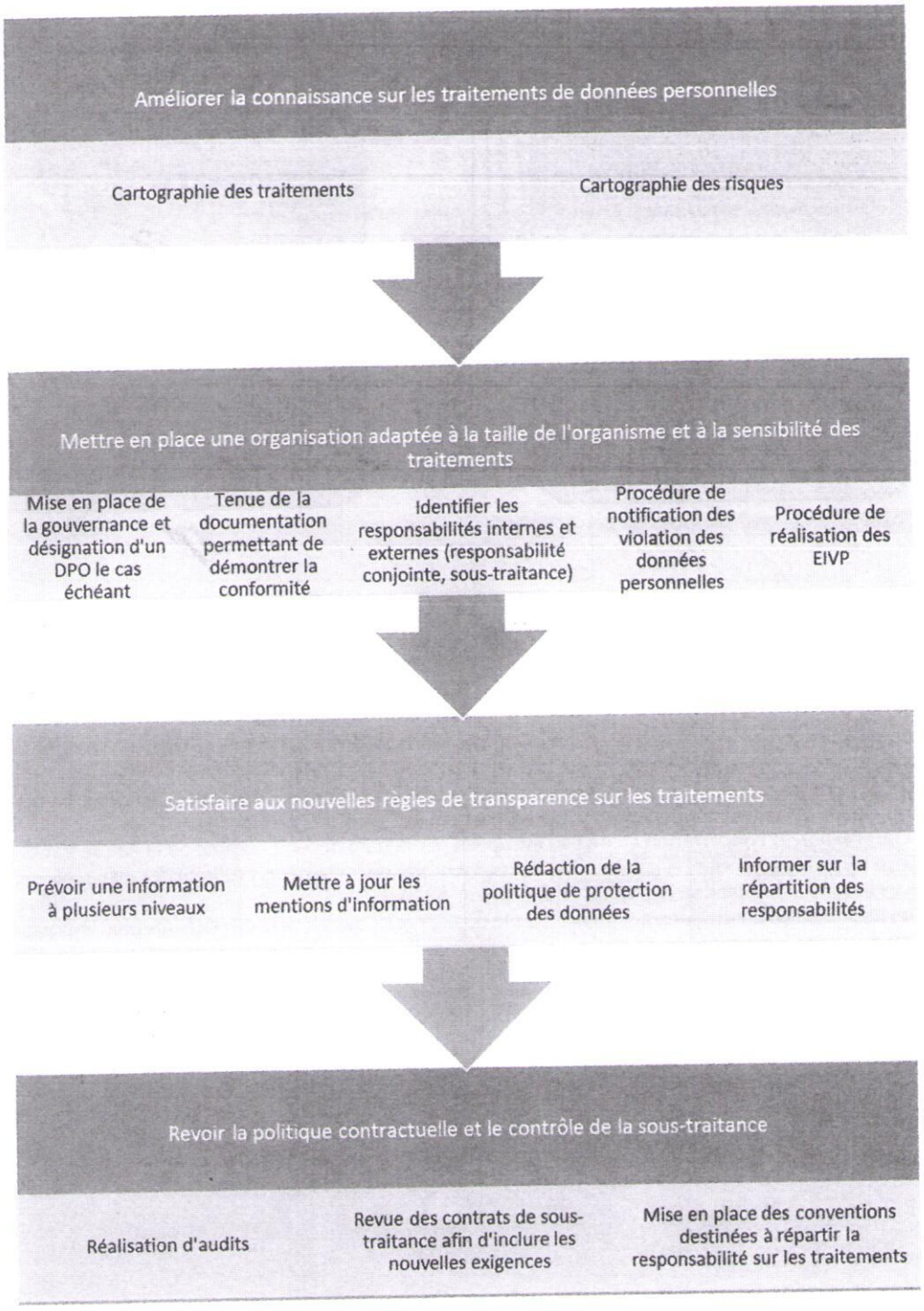
• **Une affirmation de leurs compétences (extraterritorialité)** dès lors qu'il existe un établissement sur le territoire de l'Union ou que leurs citoyens sont affectés par le traitement

• **Le renforcement de leurs pouvoirs**, notamment répressifs avec la possibilité de prononcer des sanctions administratives pouvant aller jusqu'à 4 % du chiffre d'affaires mondial de l'entreprise concernée

• **Des règles de coopération et concertation au niveau européen** permettant de tenir compte de la nature transfrontière des traitements de données à caractère personnel et d'éviter que les responsables de traitements profitent des disparités entre les droits des États membres pour choisir l'interprétation la plus favorable à leurs intérêts

• **La création d'un nouvel organe européen** qui prend la suite du G29 mais qui est doté de pouvoirs plus importants dont celui de rendre des avis contraignants : le Comité Européen de la Protection des Données (CEPD) en charge d'arbitrer les différends entre les autorités et également d'élaborer la doctrine « européenne ».

5. La nouvelle feuille de route pour assurer la conformité au RGPD



Mots-Clés : RGPD - Périmètre