LE RGPD, UN NOUVEAU PARADIGME POUR LA PROTECTION DES DONNÉES

Didier MARTIN
Délégué à la protection des données

PROTECTION DES DONNÉES, LES PRINCIPES FONDATEURS

LIL Loi 78/17 du 6 jan. 1978 modifiée

- L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

  Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la loi.

UN DISPOSITIF ASSORTI DE DISPOSITIONS ADMINISTRATIVES, CIVILES ET PÉNALES

Au-delà du renforcement du pouvoir de sanction attribué à la CNIL

RGPD et LIL reconnaissent les **actions de groupes** devant les juridictions administratives et civiles en cessation et **réparation** des manquements à la protection des données à caractère personnel.

Les Articles 226-16 à 226-24 du Code Pénal répriment le non-respect des principes s 'appliquant aux traitements de données à caractère personnel. Ces atteintes sont, majoritairement, passibles de

300 000 euros d'amende et 5 ans d'emprisonnement

TROIS DÉFINITIONS ESSENTIELLES ISSUES DU RGPD ART 4

- **Données à caractère personnel**, toute information se rapportant à une personne physique identifiée ou identifiable, [...] directement ou indirectement

- **Traitement**, toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatises et appliquées à des données à caractère personnel

- **Responsable du traitement**, la personne physique ou morale, l'autorité publique qui seule ou conjointement détermine les finalités et les moyens du traitement

LES SIX PRINCIPES DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL ART 5

- Licéité, loyauté, transparence
- Limitation des finalités : *déterminées, explicites et légitimes, sans évolutions incompatibles avec leur définition initiale*
- Minimisation des données : *adéquates, pertinentes et limitées*
- Exactitude des données
- Limitation de la conservation
- Sécurité appropriée : *Intégrité, confidentialité, en mode automatisé ou non*

LE **RESPONSABLE** DU **TRAITEMENT** EST **RESPONSABLE** DU **RESPECT** DE CES **PRINCIPES**

ET **DOIT ÊTRE EN MESURE** DE **DÉMONTRER** LEUR **RESPECT**

LA RESPONSABILITÉ OU « ACCOUNTABILITY », UN PRINCIPE CLÉ

La notion de responsabilité est LA nouveauté essentielle du RGPD, elle substitue,
à un régime de déclaration préalable imposant des obligations de moyens,
un mécanisme d'autocontrôle régulé plus fluide, mais imposant des obligations de résultats

Pour chaque traitement le RT doit :

- ✓ Caractériser sa nature, sa portée, son contexte et ses finalités
- ✓ Évaluer le niveau des risques qui lui sont associés
- ✓ Déterminer les mesures appropriées au respect du RGPD
- ✓ Mettre en œuvre ces mesures et les impératifs légaux
- ✓ Vérifier la conformité opérationnelle du traitement
- ✓ Prendre en compte les éventuelles non-conformités et évolutions

LES SIX FONDEMENTS LÉGAUX - OU LICÉITÉ - D'UN TRAITEMENT ART 6

- Consentement
- Exécution d'un contrat
- Respect d'une obligation légale
- Sauvegarde des intérêts vitaux d'une personne
- Exécution d'une mission d'intérêt public
- Intérêts légitimes du responsable de traitement

⚠ N'est pas un fondement légal s'il existe un déséquilibre manifeste entre la personne et le RT
(RGPD Consid. 43)

⚠ Non applicable aux autorités publiques dans l'exécution de leurs missions
(RGPD Art. 6-1.)

CATÉGORIES DE DONNÉES DONT LE TRAITEMENT EST INTERDIT, SAUF RÈGLES SPÉCIFIQUES ART 9

- Origine raciale ou ethnique
- Opinions politiques, convictions religieuses, philosophiques, appartenance syndicale
- Données génétiques, données biométriques pour l'identification des personnes
- Données concernant la santé
- Données sur l'orientation ou la vie sexuelle

⚠ Le RGPD étend le champ d'application des données de santé
Consid. 35, Art. 4-15.

... ainsi que les données relatives aux condamnations pénales et aux infractions Art 10

DES DROITS FONDAMENTAUX ACCRUS

- Droit d'être informé art 13 & 14 renforcé
- Droit d'accès art 15
- Droit de rectification art 16 & 19 renforcé
- Droit à l'effacement ou « droit à l'oubli » art 17 & 19 créé
- Droit à la limitation du traitement art 18 & 19 créé
- Droit à la portabilité art 20 créé
- Droit d'opposition art 21 & 22 y compris à une décision fondée exclusivement sur un traitement automatisé, telle que le profilage, produisant des effets juridiques ou l'affectant de façon significative renforcé

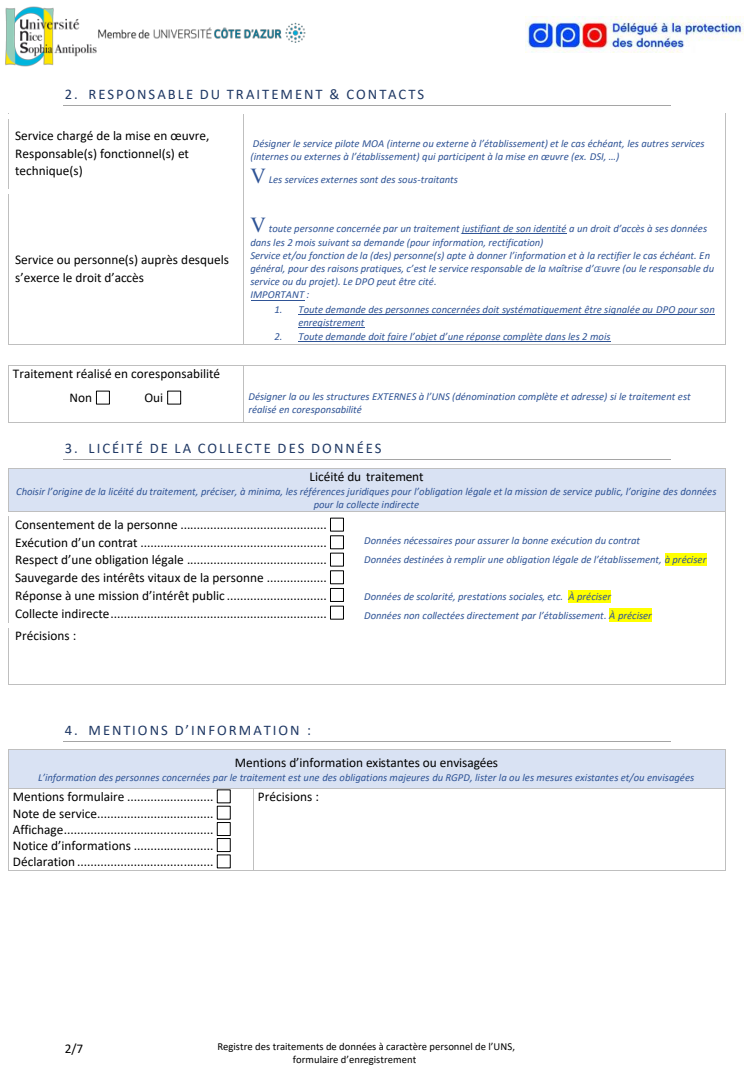
UNE INFORMATION DES PERSONNES RENFORCÉE

- Identité et **coordonnées** du RT et du DPO
- **Finalités** du traitement et base de la **licéité**
- *Droit de **retrait** du **consentement** à tout moment*
- Rappel des **droits des personnes** et de leurs **modalités** d'exercice
- Catégories de **données** et **durées** de conservation
- ***Logique sous-jacente** si le traitement intègre une prise de décision automatisée*
- ***Conséquences** d'un **refus** d'utilisation des données personnelles*
- ***Destinataires** des données et **transferts** vers des pays tiers à l'UE, garanties d'adéquations*
- ***Finalités d'autres traitements** basés sur les données collectées*
- Droit d'introduire une **réclamation** auprès de la CNIL

LE REGISTRE DES TRAITEMENTS, BASE DE LA DOCUMENTATION

Est une **obligation** pour le responsable de traitement il comporte pour tout traitement :

- le nom et **coordonnées** du Responsable du Traitement et du DPO
- les **finalités** du traitement
- les catégories de **personnes concernées**
- les catégories de **données** et de leur **durée** de conservation
- les catégories des **destinataires** des données
- les éventuels **transferts** de données vers un pays tiers - hors UE – présentant des garanties appropriées
- si possible, les délais prévus pour **l'effacement** des différentes catégories de données
- si possible, une description générale des mesures de **sécurité** techniques et organisationnelles



Université Nice Sophia Antipolis — Membre de UNIVERSITÉ CÔTE D'AZUR — Délégué à la protection des données

2. RESPONSABLE DU TRAITEMENT & CONTACTS

Service chargé de la mise en œuvre, Responsable(s) fonctionnel(s) et technique(s)	*Désigner le service pilote MOA (interne ou externe à l'établissement) et le cas échéant, les autres services (internes ou externes à l'établissement) qui participent à la mise en œuvre (ex. DSI, …)* V *Les services externes sont des sous-traitants*
Service ou personne(s) auprès desquels s'exerce le droit d'accès	V *toute personne concernée par un traitement justifiant de son identité a un droit d'accès à ses données dans les 2 mois suivant sa demande (pour information, rectification)* *Service et/ou fonction de la (des) personne(s) apte à donner l'information et à la rectifier le cas échéant. En général, pour des raisons pratiques, c'est le service responsable de la maîtrise d'œuvre (ou le responsable du service ou du projet). Le DPO peut être cité.* *IMPORTANT :* 1. *Toute demande des personnes concernées doit systématiquement être signalée au DPO pour son enregistrement* 2. *Toute demande doit faire l'objet d'une réponse complète dans les 2 mois*

Traitement réalisé en coresponsabilité Non ☐ Oui ☐	*Désigner la ou les structures EXTERNES à l'UNS (dénomination complète et adresse) si le traitement est réalisé en coresponsabilité*

3. LICÉITÉ DE LA COLLECTE DES DONNÉES

Licéité du traitement *Choisir l'origine de la licéité du traitement, préciser, à minima, les références juridiques pour l'obligation légale et la mission de service public, l'origine des données pour la collecte indirecte*	
Consentement de la personne ☐	
Exécution d'un contrat ☐	*Données nécessaires pour assurer la bonne exécution du contrat*
Respect d'une obligation légale ☐	*Données destinées à remplir une obligation légale de l'établissement, à préciser*
Sauvegarde des intérêts vitaux de la personne ☐	
Réponse à une mission d'intérêt public ☐	*Données de scolarité, prestations sociales, etc. À préciser*
Collecte indirecte ☐	*Données non collectées directement par l'établissement. À préciser*
Précisions :	

4. MENTIONS D'INFORMATION :

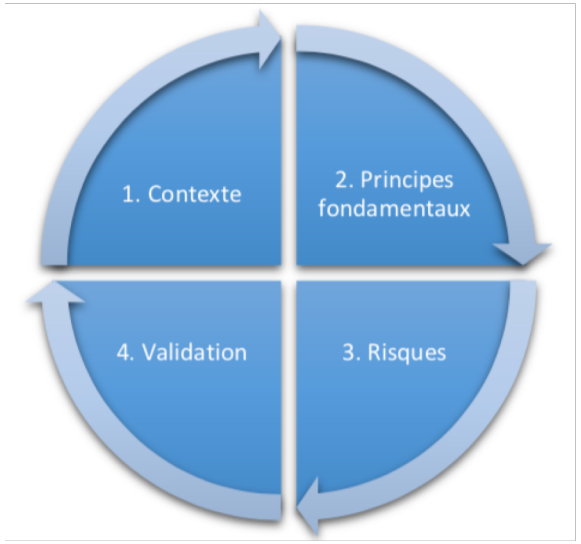
Mentions d'information existantes ou envisagées *L'information des personnes concernées par le traitement est une des obligations majeures du RGPD, lister la ou les mesures existantes et/ou envisagées*	
Mentions formulaire ☐ Note de service ☐ Affichage ☐ Notice d'informations ☐ Déclaration ☐	Précisions :

2/7 Registre des traitements de données à caractère personnel de l'UNS, formulaire d'enregistrement

LES ANALYSES D'IMPACT RELATIVES À LA PROTECTION DES DONNÉES - AIPD -

Outil essentiel de la documentation de conformité des traitements de données personnelles susceptibles d'engendrer des **risques élevés** l'AIPD ou PIA/DPIA – Data Protection Impact Assessment – se compose :

- D'une **description systématique** des **opérations** envisagées et les **finalités** du traitement
- D'une **évaluation** de la **nécessité** et de la **proportionnalité** des **opérations** de traitement au regard des **finalités**
- D'une **évaluation** des **risques** sur les droits et libertés des personnes concernées
- Des **mesures** envisagées pour **faire face aux risques**, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la **protection** des **données** à caractère personnel et à apporter la **preuve** du respect du règlement



Source CNIL, PIA la méthode Ed. fév. 2018

UNE TRANSPARENCE ACCRUE ET DES RESPONSABILITÉS MIEUX RÉPARTIES

Un impératif de transparence face aux atteintes aux données

- Toute violation de données à caractère personnel doit être notifiée par le responsable du traitement à la CNIL 72 heures, au plus tard, après sa découverte.
- Lorsque la violation de données peut engendrer un risque élevé pour les personnes concernées, celles-ci doivent être informées dans les meilleurs délais en termes simples et clairs
- La CNIL peut exiger une communication à destination des personnes concernées ou une diffusion publique de l'information

Des responsabilités mieux réparties

- La coresponsabilité d'un traitement : définition conjointe, par plusieurs entités, des finalités et des moyens
- La sous-traitance d'un traitement de données : le RGPD donne au sous-traitant une responsabilité propre. Il doit respecter et documenter le respect du règlement à son niveau, tenir un registre dédié, présenter des garanties sur les mesures techniques et organisationnelles qu'il met en œuvre.