RGPD : contrainte ou opportunité ?

Annabel QUIN
Maître de conférences en droit privé et sciences criminelles
Université Bretagne Sud

Notions

- Responsable de traitement (RT) = celui qui détermine les finalités et les moyens du traitement
  - Liberté et responsabilité (et incertitude)
  - Obligation d'accountability (preuve)
- Traitement = toute opération (automatisée ou pas) sur des données ou des ensembles de données (collecte, enregistrement, structuration, conservation, extraction, consultation, communication, interconnexion, effacement, destruction, etc.)
- Données à caractère personnel (DCP)

Les données identifiantes « classiques »

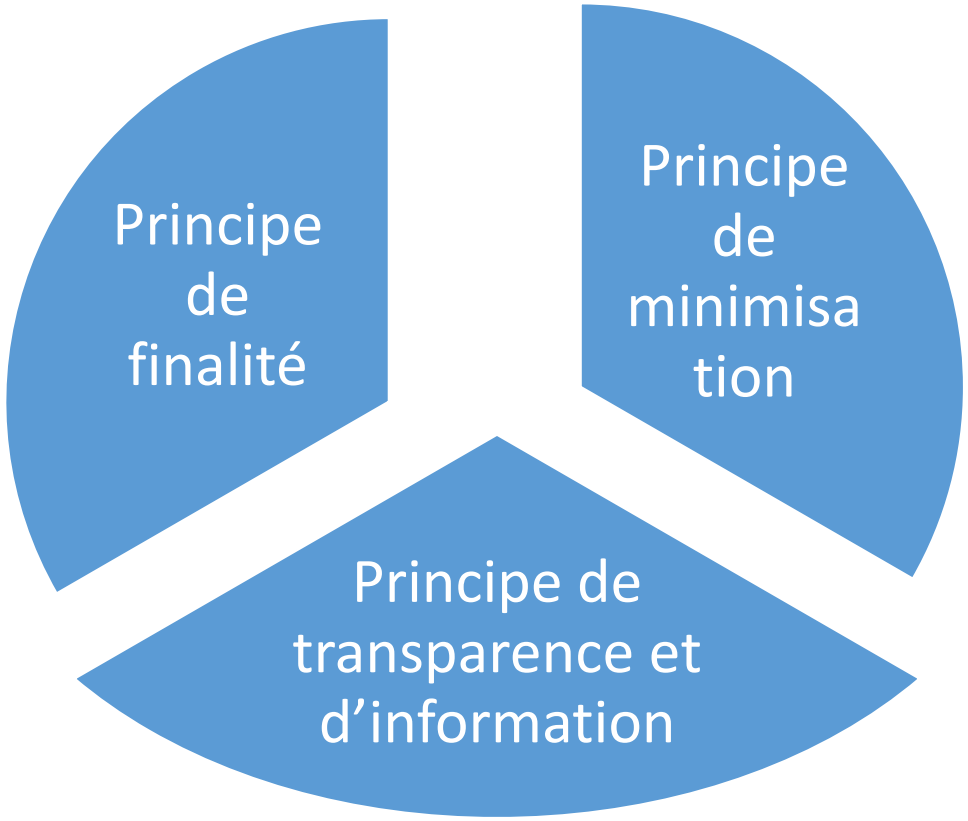
- Données permettant d'identifier une personne physique, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un n° d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » (art. 4)

Les données sensibles

- Les différentes catégories
  - Traitement de DCP *qui révèle* l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale,
  - Traitement des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique
  - Traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique (nouveauté du RGPD)
- Traitement en principe interdit, sauf 9 exceptions (cf diapo suivante)
- Appréciations plus rigoureuses des obligations d'information, de l'intérêt légitime, du consentement éclairé et libre, etc.

Qqs cas d'autorisation de traitement des données sensibles

- Consentement explicite pour des finalités déterminées
- Traitement portant sur des DCP qui sont manifestement rendues publiques par la personne concernée
- Traitements nécessaires pour des motifs d'intérêt public (santé publique, médecine du travail, etc.)
- Traitement nécessaire à des fins archivistiques, à des fins de recherche scientifique ou historique ou à des fins statistiques, sur la base du droit de l'UE ou d'un Etat membre et à condition que ce soit « proportionné à l'objectif poursuivi », que soit respecté « l'essence du droit à la protection des données » et que soient prévues « des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée »


Principe de finalité
Principe de minimisation
Principe de transparence et d'information

PRINCIPE DE FINALITE : finalités déterminées, explicites et légitimes

- Finalités = les raisons pour lesquelles les données sont collectées et/ou traitées
- Enonciation des finalités dans un langage clair
- Détermination suffisamment précises, à apprécier en fonction de la complexité du traitement
- Pour les traitements massifs et intrusifs : explications sur la portée du traitement au regard de la protection de la vie privée des personnes (données collectées, partenaires collecteurs, données inférées des données collectées, etc)

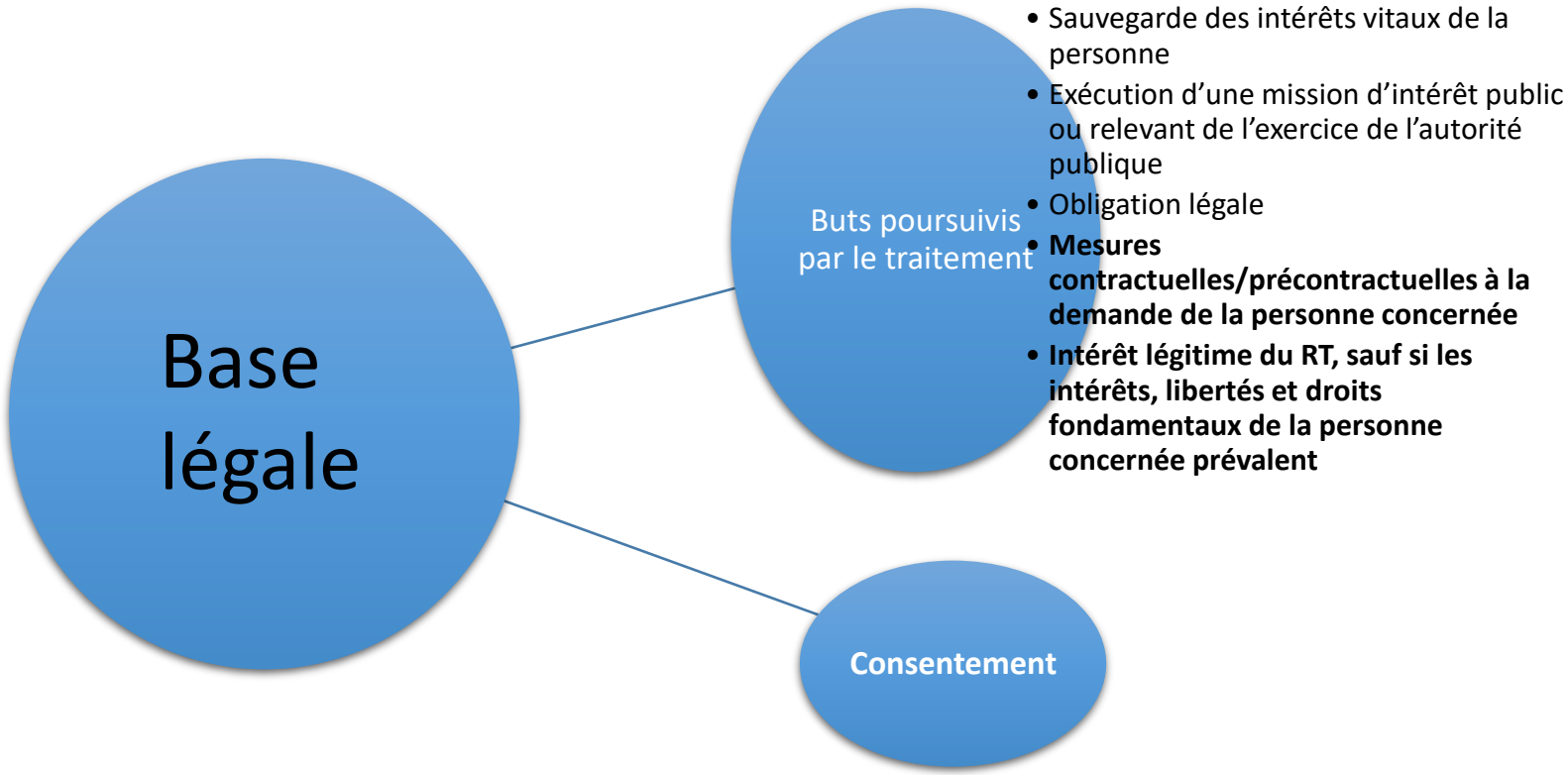
Norme simplifiée 48 sur les Fichiers clients-prospects et vente en ligne (modifiée par la délib. du 21 juillet 2016)

- Pas de caractère obligatoire depuis l'entrée en vigueur du RGPD (Déclaration de la CNIL du 5/11/2019). Simple outil d'orientation des actions de mise en conformité (en attendant l'édiction de référentiels par la CNIL.
- Enumération des finalités possibles :
  - Effectuer des opérations relatives à la gestion des clients
  - Effectuer des opérations relatives à la prospection
  - Elaborer des statistiques commerciales
  - Céder, louer, échanger ses fichiers de clients et ses fichiers de prospects
  - Actualiser ses fichiers de prospection par l'organisme en charge de la gestion de la liste d'opposition au démarchage téléphonique
  - Organiser des jeux concours, loteries, ou toute opération promotionnelle
  - Gérer les demandes de droit d'accès, de rectification et d'opposition
  - Gérer les impayés et le contentieux
  - Gérer les avis des personnes sur des produits, services ou contenus
- Exclusion du champ de la norme des traitements susceptibles d'exclure des personnes au bénéfice d'un droit, d'une prestation ou d'un contrat

  CF – RGPD – profilage décisionnel

Des finalités légitimes : les « bases légales »

- Choix de la base légale lors de la collecte



Rqs sur les « bases légales » en fonction des buts poursuivis (1)

- Indiquer précisément la base légale
- Base légale des mesures contractuelles souscrites envers la personne concernée/mesures précontractuelles prises à la demande de la personne concernée
- Base légale de l'intérêt légitime du RT ou d'un tiers

  à mettre en balance avec les « intérêts, libertés et droits fondamentaux des personnes concernées »

  et en tenant compte des garanties protégeant les droits et intérêts des personnes concernées

  Ex: déc. Google de janvier 2019

Rqs sur les bases légales en fonction des buts poursuivis (2): l'extension à de nouvelles finalités compatibles avec les finalités initiales

- Test de compatibilité en fonction :
  - Du lien entre les finalités initiales et les nouvelles finalités
  - De la nature des données collectées
  - Des conséquences du nouveau traitement pour les personnes concernées («évaluation du risque)

  Prise en compte des mesures techniques ou organisationnelles protégeant les droits des personnes concernées (chiffrement, anonymisation, etc.)
- Pas de test de compatibilité en cas de base légale fondée sur le consentement : nécessiter de recueillir à nouveau le consentement

Base légale fondée sur le consentement (pour les DCP classiques et les données sensibles)

- Consentement précédé d'une information (V. plus loin)
- Consentement recueilli préalablement
- Consentement univoque (formel ou résultant d'un comportement)
- Consentement libre
  - Tenir compte du fait que l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de ses DCP (art.7 §4 du RGPD)
    - Possibilité d'une alternative payante ?
    - Données biométriques : prévoir une autre alternative (ex : données de la voix ou mot de passe)
- Consentement spécifique
- Consentement révocable
- Consentement des mineurs de moins de 15 ans

PRINCIPE DE MINIMISATION (OU DE PROPORTIONNALITE) : données adéquates, pertinentes et limitées

- Appréciation par rapport à ce qui est indispensable pour atteindre les finalités
- Minimisation des DCP
- Limitation de la durée de conservation (à compter de la fin de la relation ou bien de la collecte ou du dernier contact du prospect)
- Minimisation des accès aux DCP
- Déc. CNIL du 28 mai 2019 : sanction de 400 000 euros contre SERGIC pour failles de sécurité + absence de durées de conservation

Astuce pratique n° 1 – Les archivages progressifs (sans retour en arrière possible)

Suppression ou Anonymisation dès qu'on peut se passer de données identifiantes pour atteindre les finalités poursuivies = sortie du RGPD
Ex.: suppression des enregistrements de voix après la création des gabarits

Astuce pratique n° 2 – La répartition des risques avec des partenaires : la pseudonymisation

- Séparation du fichier identifiant et du fichier pseudonymisé dans deux entités distinctes (ou deux services « étanches »)
- Remise du fichier identifiant à un tiers de confiance avec obligation de confidentialité
- Remise des clés de chiffrement/déchiffrement à un tiers de confiance avec obligation de confidentialité
- Partage des données pseudonymisées avec des entités qui n’ont pas accès aux identifiants = données non personnelles

Astuce pratique n° 3 – Partage des risques avec la personne concernée : la « délégation de la maîtrise » de certaines DCP

- Interdiction de conserver le cryptogramme visuel de la carte bancaire après la transaction (même si consentement donné à la conservation du n° et de la date d'expiration de la carte bancaire pour des paiements ultérieurs)
- Interdiction de conserver l'entière maîtrise du gabarit créé à partir de la voix : soit remise du gabarit à la personne concernée (sur un badge ou sur son mobile), soit détention par elle de la clé de déchiffrement
- Avantages : limitation des risques en cas de cyber attaque + respect de la souveraineté des personnes concernées

PRINCIPE DE TRANSPARENCE ET D'INFORMATION

- Information concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples (art.12)
- Accroissement des exigences pour les informations à destination des mineurs
- Examen de l'architecture de l'information (ex : décision Google de Janvier 2019):
  - Le nombre d'actions à accomplir pour obtenir l'information (liens hypertextes)
  - Le choix des intitulés des rubriques
  - Le caractère intuitif du parcours à suivre pour obtenir les informations
  - Présentations graphiques (nombre de données collectées, partenaires collecteurs, etc.)

MERCI POUR VOTRE ATTENTION

Annabel QUIN

annabel.quin@univ-ubs.fr