Toulouse IRIT 4 décembre 2017

- Champ d'application matériel
  - Le RGPD s'applique au traitement de données, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données contenues ou appelées à figurer dans un fichier.
    - Données à caractère personnel
      - Toute information concernant une personne physique identifiée ou identifiable ("personne concernée"); est réputée identifiable une personne qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale"
    - Traitement
      - Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation, l'effacement ou la destruction
    - Fichier
      - Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique
  - Qui est responsable du traitement?
    - La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel
      - Courrier de la CNIL datant de février 2016 : le RT est le DU de l'unité
      - Courrier a été envoyé à l'ensemble des DU CNRS
  - Définition d'un sous-traitant au sens du RGPD
    - La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement
      - Contrat ou "acte juridique" écrit doit lier le RT ou ST
      - ST aide le RT à garantir le respect de ses diverses obligations (droits des personnes, violations de données, analyses d'impact, consultation préalable de la CNIL, etc.)
      - ST a une responsabilité spécifique
- Formalités
  - Si pas de données de santé
    - CIL
    - EIVP peut être nécessaire malgré tout
      - Nécessaire lorsque le traitement présente un risque élevé pour la vie privée
        - Évaluation ou notation : les activités de profilage et de prédiction, portant notamment sur des «aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements»
        - Prise de décisions automatisée avec effet juridique ou effet similaire significatif
        - Surveillance systématique : la collecte de données via des réseaux ou par «la surveillance systématique […] d'une zone accessible au public»
        - Données sensibles ou données à caractère hautement personnel
          - Voir le focus sur les données sensibles
          - On peut ajouter les données financières (paiements frauduleux), données de localisation (remet en cause la liberté de circulation)
        - Données traitées à grande échelle
          - - le nombre de personnes concernées, soit en valeur absolue, soit en proportion de la population considérée
          - - le volume de données et/ou l'éventail des différents éléments de données traitées-
          - - la durée ou la permanence de l'activité de traitement de données;
          - - l'étendue géographique de l'activité de traitement.
        - Données concernant des personnes vulnérables
          - Incapacité de consentir, ou de s'opposer, aisément au traitement de leurs données ou d'exercer leurs droits
          - Personnes pour lesquelles un déséquilibre dans la relation avec le responsable du traitement peut être identifié.
  - Données sensibles : en général à minima santé
- Licité liée à la collecte et au traitement des données à caractère personnel
  - Principe de transparence
    - Obligation d'information des personnes
  - Principe de finalité
    - "Les données sont collectées pour des finalités déterminées, explicites et légitimes (...)"
    - Données "(...) ne sont pas traitées ultérieurement de manière incompatible avec ces finalités"
      - Obligation des formalités complémentaires + Nouvelle information des personnes et droit d'opposition CNIL Délibération n°2009-201 du 16 avril 2009 un système de vidéosurveillance ne peut être utilisé que pour lutter contre le vol et pas pour surveiller les salariés
      - CCas Soc 3 novembre 2011 : un dispositif de géolocalisation ne peut être utilisé qu'à des fins portées à la connaissance du salariés
    - Traitements réalisés à des fins statistiques ou scientifiques ou historiques
      - Compatible sous réserve qu'elle soit réalisée dans le respect des principes et des procédures prévus par la LIL et que les données ne soient pas utilisées pour prendre des décisions à l'égard des personnes concernées.
  - Principe de proportionnalité
    - « les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs. »
    - Habitude de collecter les données dites administratives lors de recherche dans lesquelles il n'y a pas de retour sur les participants
      Intérêt dans la constitution de cohortes d'avoir toutes les informations ?
      => Economie de la donnée
  - Données doivent être exactes et mises à jour
  - Principe d'une durée de conservation limitée
    - « les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. »
    - A l'issue de la période : destruction, anonymisation, archivage dans le cadre de données présentant un intérêt scientifique, historique ou statistique.
      - Archivage
  - Principe de sécurité et de confidentialité
    - « le responsable de traitement est tenu de prendre toutes les précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »
    - Dropbox/Google Drive
      - RSSI : les enjeux localisation/patriot act/PPST
    - Privacy- Security by design
      - Prendre en compte les aspects protection de la vie privée et sécurité dès la conception des outils
        - Le RT adopte des mesures techniques et organisationnelles appropriées – tant au moment de ladétermination des moyens du traitement qu'au moment du traitement lui-même – afin de le rendre conforme au RGPD
        - Le RT adopte des mesures consistant à limiter par défaut le traitement de données à ce qui est strictement nécessaire
  - EIVP
    - Dans le doute on doit en effectuer une