ITEANU
Société d'Avocats | Law Office

Contrats de services et données
la question du plafond de responsabilité

Par Olivier ITEANU
ITEANU AVOCATS
Paris, le 8 Juin 2023

Constat

- Les clients prennent les prestataires pour leur assurance « perte de données »
  - Ils ne veulent pas de plafond
- Les prestataires doivent :
  - gérer leur risque
  - composer avec des sous-traitants qui, eux, limitent leurs responsabilités

Quelle est la pratique classique des prestataires

- Préqualification des dommages dits « indirects », exclus de l'indemnisation au titre de la responsabilité contractuelle
  - La « perte de données » est souvent assimilée à un dommage indirect. Logique du prestataire :
    - Le prestataire fournit un service « standard », il veut donc gérer un niveau de responsabilité « standard » qui ne varie pas selon que les données que le client choisit d'utiliser en relation avec son service soient « banales », ou soient des secrets de fabrique, des informations confidentiel défense, etc.
    - Report sur le client d'obligations de sécurité : le client s'engage contractuellement à effectuer la sauvegarde de ses données
    - Les obligations liées aux données à caractère personnel en application du RGPD changent toutefois la problématique

Les contraintes du RGPD liées à la sécurité

- Contenu de l'obligation de sécurité (article 32 RGPD) :
  - *« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:*
    - *a) la pseudonymisation et le chiffrement des données à caractère personnel;*
    - *b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;*
    - *c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;*
    - *d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. »*
- Sanction et dommages pouvant résulter du non respect de l'obligation de sécurité résultant du RGPD :
  - Article 83 du RGPD : amendes administratives infligées par l'autorité de contrôle pouvant s'élever jusqu'à 10 000 000 € ou, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu
  - Articles 226-17 du Code Pénal : peines maximales de 5 ans d'emprisonnement et de 300 000 € d'amende
  - Dommages causés aux personnes concernées (article 82 du RGPD), sachant que des actions collectives sont rendues possibles (article 80 du RGPD)

Une gestion technique, financière et opérationnelle du risque RGPD

- Le RGPD introduit une responsabilité partagée du RT et du ST sur l'obligation de sécurité.
  - De façon remarquable, un des critères de détermination des mesures appropriées est le coût de mise en œuvre
  - Le jeu contractuel va consister, pour le prestataire (ST) :
    - à proposer à son client (RT), un niveau de sécurité standard, pour le prix standard du service (ou différents niveaux au choix, pour des prix différents)
    - en lui renvoyant la responsabilité de choisir un niveau plus élevé (en payant le prix correspondant), ou de se manifester s'il estime le niveau insuffisant en demandant des mesures additionnelles (sous réserve de faisabilité et d'accord du prestataire)
    - *la gestion du risque commence en amont de la clause de responsabilité, par les choix techniques, financiers et opérationnels qui sont faits par le client sur propositions du prestataire*

Une gestion juridique du risque selon le type de données

- L'intérêt du prestataire est de faire tomber le régime de responsabilité contractuel lié à une atteinte à la sécurité des données dans sa clause générale d'exclusion ou de limitation de responsabilité
- L'intérêt du client est de distinguer les cas
  - Omniprésence des données à caractère personnel : en matière de contrat de service portant sur des données, il est difficile de concevoir un contrat ne comprenant le traitement de données à caractère personnel. Toutefois, même si l'objet du contrat n'est pas de traiter des données à caractère personnel, ce service va au moins traiter des données personnelles pour l'authentification au service et pour la maintenance :
    - exemple : service PaaS de fourniture de puissance de calcul, utilisé pour traiter des relevés de mesures, ou pour entraîner un réseau de neurones et créer un modèle en intelligence artificielle.
      - son objet principal n'est pas un traitement de données à caractère personnel
      - cependant, incidemment :
        - le prestataire traite les identifiants et mots de passe des personnes autorisées à utiliser le service
        - Le prestataire traite les noms et coordonnées de contact des personnes qui le sollicitent pour une assistance
- Certains incidents de sécurité vont ainsi impacter des données à caractère personnel, et le cas échéant le respect du DPA ou accord de protection des données visé en annexe du contrat de service et d'autres non
- On peut donc, aménager dans la clause limitative de responsabilité, les conséquences d'une atteinte à la sécurité des données selon le type de données concernées :
  - pour les incidents n'impactant pas des données à caractère personnel, plafond de responsabilité standard (prix du service)
  - pour les incidents impactant des données à caractère personnel, dans l'intérêt du client, plafond de responsabilité plus élevé négocié, voire déplafonnement

Une gestion juridique du risque selon le type de responsabilité

- Dès lors que le prestataire accepte de distinguer son niveau de responsabilité contractuelle selon le cas, en distinguant les incidents impactant des données à caractère personnel des autres, la question se pose du type de dommage couvert par la clause :
  - S'agit-il de tout dommage résultant d'un manquement à l'accord de protection des données (DPA) ?
    - Intérêt du client
      - Dans ce cas, le client pourra tenter de réintégrer dans le champ des dommages indemnisables des dommages éventuellement habituellement exclus, par exemple, son atteinte à l'image résultant de l'incident, ses frais internes et désorganisation de son entreprise, les frais de reconstitution des données, etc.
  - S'agit-il seulement du cas où l'une des parties est condamnée à une amende administrative infligée par l'autorité de contrôle, pour une situation qui résulte d'une faute contractuelle dont le client peut établir qu'elle est imputable au prestataire ?
    - intérêt du prestataire
      - Dans ce cas, les parties peuvent convenir, d'ailleurs que le plafond est déterminé selon les règles prévues à l'article 83 du RGPD (10 000 000 € ou, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu)

Merci !

Questions / Réponses

ITEANU
Société d'Avocats | Law Office

www.iteanu.com
blog.iteanu.com
@iteanu

ITEANU
Société d'Avocats | Law Office

Contrats de services et données
la question du régime de responsabilité « in solidum » *de l'article 82 du RGPD*

Par Olivier ITEANU
ITEANU AVOCATS
Paris, le 8 Juin 2023

De quoi parle-t-on ?

- Article 82 § 4 et § 5 du RGPD :
  - *« 2. Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par le présent règlement qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.*
  - *3. Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre du paragraphe 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.*
  - ***4. Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.***
  - *5. Lorsqu'un responsable du traitement ou un sous-traitant a, conformément au paragraphe 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2. »*

Cas concernés et possibilités de traitement contractuel

- Ce cas de responsabilité « *in solidum* » correspondant à une hypothèse particulière où :
  - le RT et ST sont tous deux responsable d'un dommage causé à une personne concernée (tiers au contrat)
  - Ce dommage résulte d'un manquement commis à la fois par le RT et le ST au RGPD
  - Alors la personne concernée peut obtenir l'indemnisation pour l'intégralité de son dommage à l'une ou l'autre, à charge pour celui qui indemnise de se retourner contre l'autre pour la part du dommage qu'il n'a pas causé
- Peut-on valablement exclure ou limiter contractuellement cette responsabilité ?
  - Pas de jurisprudence sur ce point toutefois, certainement pas vis-à-vis de la personne concernée
  - Vis-à-vis de son co-contractant probablement pas, les termes de cette action récursoire étant très clairs au RGPD
    - Il s'agit d'un recours contre son co-contractant prévu par la loi, dans le contexte d'une action en responsabilité extra-contractuelle initiée par la personne concernée, ou un organisme mandaté pour la représentation collective de personnes concernées
- À notre sens, on ne peut que mitiger le risque en identifiant clairement la répartition des responsabilités d'un commun accord :
  - qui est responsable de sécuriser quoi, à quel moment et comment ?

Merci !

Questions / Réponses

ITEANU
Société d'Avocats | Law Office

www.iteanu.com
blog.iteanu.com
@iteanu