DESMARAIS
AVOCATS

Contrôle des prestataires

Erreurs à ne pas commettre

34, rue Pétrelle • 75009 PARIS
contact@desmarais-avocats.fr • www.desmarais-avocats.fr

L’organisation doit s’assurer que les processus externalisés sont définis et contrôlés

Pourquoi externaliser?

- Bonnes raisons:
  - Réaliser des économies d'échelle en recourant à un spécialiste
  - Partager un risque avec un spécialiste
  - …

- Mauvaises raisons:
  - Se déresponsabiliser en transférant un risque
  - Réaliser des économies en recourant à de la main d'œuvre moins onéreuse
  - …

L’encadrement des sous-traitants, la pratique et le droit

- Est une problématique classique, tant pour les professionnels de la sécurité de l’information, que pour les professionnels du droit

- Est quelque chose qui n’intéresse pas les organisations
  - Sur les 4 dernières années, la CNIL a retenu le défaut d’information dans 28,95% de ses décisions, là où seulement 2,63 % concernaient expressément un défaut de contrôle du sous-traitant

- Devrait rapidement devenir un sujet d’intérêt pour les organisations
  - Forte évolution de la gravité des sanctions CNIL: Orange → Hertz
  - Des textes plus stricts sur le sujet: Directive Solvabilité 2 & RGPD

TOP 5
DES ERREURS À NE PAS COMMETTRE

#1 – Contractualiser avec un sous-traitant sans avoir évalué le risque que représentait cette relation

Diagnostic

- ISO27001 (A.7.1)
- Loi *Informatique et Libertés* (Art. 34)
- RGPD (Art. 28§1)

Risque

- Administratif
- Pénal (CNIL)
- Civil
- Réputationnel

Niveau de risque


Élevé


Moyen


Faible

#2 – Laisser le service Achats conclure/modifier seul les contrats

Diagnostic	Risque	Niveau de risque
• ISO27001 (A.15.1.1) • RGPD (Art. 28§1) • Solvabilité 2 (41§3)	• Administratif (CNIL / ACPR) • Pénal (CNIL) • Civil • Réputationnel	

#3 – Reposer exclusivement sur ses CGA, sans prise en considération des CGV des sous-traitants

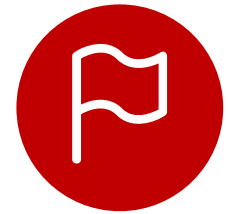
Diagnostic

- ISO27001 (A.7.1)
- Loi *Informatique et libertés* (Art. 35)
- RGPD (Art. 28§1)

Risque

- Administratif (CNIL)
- Pénal (CNIL)
- Civil
- Réputationnel

Niveau de risque




Élevé


Moyen


Faible

#4 – Ne pas insérer des clauses d'audit, de confidentialité et de non-exploitation ou les avoir mal construites

Diagnostic

- ISO27001 (A.15.2.1)
- Loi *Informatique et libertés* (Art. 35)
- RGPD (Art. 28§3)
- Solvabilité 2 (Art. 38)

Risque

- Administratif (CNIL / ACPR)
- Pénal (CNIL)
- Civil
- Réputationnel

Niveau de risque

Absence

Mal rédigée

Élevé

Moyen

Faible

#5 – Imposer des mesures de sécurité ou des clauses en sachant qu'elles seront inapplicables

Diagnostic	Risque	Niveau de risque
• ISO27001 (A.15.1.2) • RGPD (Art. 28§1) • Solvabilité 2 (Art. 49)	• Administratif (CNIL / ACPR) • Pénal (CNIL) • Civil • Réputationnel	

Tendance à l'alignement des normes et du droit

- Normes ISO apparaissent dans les textes
  - La certification *Hébergeur de données de santé* avec notamment l'ISO27001 et l'ISO27018 (le projet de référentiel soumis à concertation vise expressément les normes)

- En parallèle, renvoi à des référentiels propriétaires
  - Recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance prend expressément PCI-DSS en tant qu'exemple

- Pourquoi?
  - Volonté du législateur de coller aux technologies = obsolescence programmée de la loi
  - Les normes sont-elles plus détachées du contexte technologique?
  - Le résultat de l'espérance mathématique liée au non respect de la norme est-il plus dissuasif que la loi?

Mesures à prendre pour assurer l'efficacité de ce contrôle

Mesures organisationnelles

- Systématiser l'analyse de risques *ante* signature:
  - action sur les erreurs #1 et #3

- Permettre la saisine du service juridique par les métiers, et vice-versa:
  - action sur l'erreur #2

- En clair, avant d'externaliser, il faut mettre en place un mécanisme de *Contract Management*:
  - action sur l'erreur #5

Systématiser l'analyse de risques *ante* signature

- L'ISO27001 conduit à imposer l'analyse de risques lier à l'externalisation d'une activité
- La directive *Solvabilité 2* donne corps à cette obligation pour la banque et l'assurance en imposant:
  - De qualifier l'activité transférée: est-elle importante ou critique?
  - De vérifier que la méthodologie et les moyens du sous-traitant ne présentent ou pas un risque grave ou n'accroissent pas indûment un risque
- Le RGPD n'est plus souple qu'en apparence:
  - Vérifier l'existence de garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées impose:
    - D'obtenir et étudier la PSSI, les documents contractuels, etc. du sous-traitant antérieurement à la signature
    - De pouvoir documenter les sous-traitants du sous-traitant

Permettre la saisine du service juridique par les métiers… et vice-versa

- Les métiers agissent souvent sans le service juridique, ce qui aboutit à :
  - Un risque:
    - Sur le plan juridique
    - En termes de sécurité de l'information
  - Une importante variabilité des contrats ➔ la revue de contrats perd de son utilité
  - Une complexification du pilotage des sous-traitants
- Les métiers devraient avoir la possibilité d'échanger rapidement avec le service juridique
- La saisine du service juridique n'a d'intérêt que si ledit service est sensibilisé aux besoins

Mettre en place le *Contract Management*

- Un contrat n'est pas un acte juridique
  - C'est la formalisation juridique des relations mises en place entre deux ou plusieurs personnes

- Le *Contract Management* est « *l'activité qui consiste à*
  - *développer et contrôler le cycle de vie d'un contrat complexe, de la phase d'initialisation jusqu'à son terme,*
  - *par la coordination systématique et méthodique des ressources et des processus utiles à la maîtrise des risques et à l'optimisation financière* » (***G. Leveau, Pratique du Contract Management, Lextenso***)

Mesures d'ordre contractuel

- Trois mesures prioritaires:
  - De l'*intuitu personae* dans les clauses d'encadrement (audit, confidentialité et non-exploitation):
    - action sur l'erreur #4
  - Insérer une clause de garantie:
    - Action sur l'erreur #5
  - Une revue de contrat ouverte à la *sécurité de l'information*:
    - action sur l'erreur #5

La clause d'audit

- Périodicité:
  - Combien de contrôles possibles sur un an?
  - Augmentation de la fréquence avec la sensibilité de l'activité externalisée
- Préavis:
  - Faut-il prévenir l'entreprise?
  - Nécessité fonction du degré de confidentialité / sécurité encadrant l'activité
- Confidentialité:
  - Faut-il un accord de confidentialité pour l'auditeur ou recourir à un tiers de confiance?
  - Nécessité fonction du degré de confidentialité / sécurité encadrant l'activité
- Conséquences de la détection de manquement:
  - En cas de manquement, correction, sanction ou résiliation?
  - Gradation en fonction de la nature du manquement et de la sensibilité de l'activité

La clause de confidentialité et de non-exploitation

- Champ de la confidentialité:
  - Toutes les informations transmises ou seulement celles estampillées « *Confidentiel* »?
  - Fonction de la nature de l'information, puis le cas échéant des besoins de l'organisation et enfin des besoins d'interaction du sous-traitant avec des tiers
- Mesures à prendre:
  - Donner des lignes directrices ou imposer des mesures précises?
  - Fonction de la nature de l'information, puis le cas échéant de leur sensibilité
  - Laisser la définition des mesures à la discrétion du sous-traitant n'est pas une option
- Durée de la confidentialité:
  - Combien de temps les informations sont-elles confidentielles?
  - Fonction de la nature de l'information, puis le cas échéant des besoins de l'organisation
- Non-exploitation:
  - Clause à systématiser pour assurer la sécurité de l'information, quelle qu'en soit la nature

La clause de « garantie »

- Aujourd'hui, les mesures de sécurité contractuellement imposées sont souvent acceptées « *en la forme* », sans aucune adhésion sur le fond
  - Et ce par chacune des parties

- La clause de garantie vient garantir le créancier de l'obligation contre tout manquement à cette obligation
  - La bilatéraliser permettrait de garantir le respect de ses obligations par le sous-traitant… mais également par le mandant
  - Il est en effet un peu facile de reprocher un manquement manifeste à un sous-traitant alors que la clause d'audit n'a jamais été mise en œuvre

La revue de contrats

- Tendance à réserver les revues aux aspects financiers et économiques
- Tout peut évoluer et tout doit pouvoir être adapté
    - Mesures de sécurité, cadre juridique, prestations confiées, etc.
    - Indispensable de pouvoir faire évoluer des mesures de sécurité de façon souple
- La revue de contrats devrait réunir:
    - Les métiers
    - Les juristes
    - Les financiers
    - Et *last but not least*, le RSSI et le CIL
- La revue de contrat est d'autant plus *performante* si elle trouve place dans un processus de *Contract Management*

Susciter l’adhésion des sous-traitants aux mesures de contrôle

Mettre l'accent sur l'origine légale des contraintes…

- Aujourd'hui, les clauses relatives à la sécurité, à la confidentialité et aux audits sont:
  - Soit vécues comme des contraintes
  - Soit totalement ignorées par des prestataires faisant primer leurs CGV

- La réappropriation des rênes de la relation contractuelle est facilitée par le fait qu'elle est désormais expressément inscrite et détaillée dans les textes de loi:
  - Le mandant n'a pas de marge de manœuvre, c'est la loi qui lui impose l'adjonction de ces clauses
  - Ne pas les faire figurer pourrait remettre en cause l'existence même de la relation d'affaires

… et sur la volonté de responsabiliser les sous-traitants

- L'externalisation n'écarte pas la responsabilité du mandant
  - Le « transfert » de risque est un mythe
  - La directive Solvabilité 2 et le RGPD le rappellent expressément

- L'absence de transfert du risque ne doit pas conduire à une indifférence des sous-traitants au cadre juridique et aux obligations contractuelles:
  - La responsabilisation des sous-traitants est la réaction à ce phénomène
  - Un sous-traitant qui était auparavant une sorte de « *complice* » du manquement (susceptible d'un recours *récursoire*) est désormais le « *co-auteur* » de ce manquement (action directe contre lui)

Conclusion

- L'externalisation est parfois un mécanisme aboutissant à brader la sécurité de l'information
- Initialement peu vigilants sur ce point, les pouvoirs publics commencent à sanctionner le défaut d'encadrement d'un sous-traitant
- Les mesures permettant un meilleur encadrement de la sécurité de l'information sont souvent très proches des prescriptions de l'ISO27001
- L'implémentation de ces mesures supposent une refonte du processus contractuel dans l'organisation

DESMARAIS

AVOCATS

34, rue Pétrelle • 75009 PARIS
contact@desmarais-avocats.fr • www.desmarais-avocats.fr