Réflexion du GTSI concernant le projet de lignes directrices sur les notions de responsable du traitement et de sous-traitant (07/2020) adopté le 02 septembre 2020 - Version 1.0 pour consultation publique

I) Présentation du Groupe de Travail Sécurité Informatique (GTSI) 2

II) Remerciements 2

III) Réflexion 2

- Paragraphes (§§) 18 et 20 2
- Paragraphe (§) 34 2
- Paragraphes (§§) 37, 38, 39 et 82 3
- Paragraphe (§) 63 3
- Paragraphe (§) 70 et exemple associé 3
- Paragraphe (§) 75 4
- Paragraphe (§) 88 4
- Paragraphe (§) 107 4
- Paragraphe (§) 111 5
- Divers 1: Certifications des prestataires de services 5
- Divers 2: Lignes directrices plus spécialisées par secteur 5

I) Présentation du Groupe de Travail Sécurité Informatique (GTSI)

Le GTSI (Groupe de Travail sur la Sécurité de l'Information) regroupe plus de cinquante professionnels de la sécurité de l'information et de la protection des données œuvrant dans les autorités publiques de la Région Wallonne, de la Fédération Wallonie-Bruxelles et de la Communauté germanophone en Belgique. La vocation de ce groupe est de partager les connaissances, les pratiques et d'émettre des conseils en termes de protection des données et sécurité.

II) Remerciements

Le GTSI remercie le Comité européen pour la protection des données pour l'initiative prise en vue de fournir de nouvelles lignes directrices relatives aux concepts de Responsable de Traitement afin d'aider les acteurs concernés à agir en conformité au RGPD.

Ces nouvelles lignes directrices apportent des précisions, compléments et exemples qui sont éclairants pour les professionnels de la sécurité de l'information et de la protection des données.

III) Réflexion

La réflexion du GTSI adressée au Comité européen de la protection des données sur les présentes lignes directrices est le fruit d'une collaboration entre les différents acteurs de ce groupe.

Le GTSI émet des commentaires, suggestions, propositions en renvoyant directement aux paragraphes correspondants des lignes directrices pour plus de clarté et de compréhension.

- ### Paragraphes (§§) 18 et 20

  Selon le paragraphe 20, la qualification du responsable de traitement doit résulter d'une analyse factuelle. Il convient de ne pas tenir compte de la qualification donnée de façon formelle.
  Cependant, la lecture du paragraphe 18 induit une confusion car il est question que la responsabilité incombe dans tous les cas au responsable de traitement. Or cela va à l'encontre de l'analyse formelle.

  Est-ce l'entité légale « *legal entity* » (analyse formelle) ou l'entité fonctionnelle (analyse factuelle) qui doit être désignée Responsable de Traitement ?

- ### Paragraphe (§) 34

  Il ressort de la lecture du paragraphe 34 que le Responsable de Traitement détermine à la fois les finalités « **ET** » les moyens. Il est rappelé que le Sous-Traitant ne peut définir les finalités car cela appartient uniquement au Responsable de traitement.

  Ainsi, dans le cas où le Responsable de Traitement est la partie qui détermine à la fois la finalité et les moyens, et que le Sous-traitant ne peut pas définir les finalités, comment qualifier la partie qui détermine uniquement la finalité d'un traitement sans décider des moyens ? Comment qualifier la partie qui détermine tous moyens ? Les parties doivent-elles automatiquement être considérées comme des Responsables de Traitements conjoints ?

La détermination d'un seul moyen essentiel suffit-elle à désigner la partie comme responsable conjoint ?
Ne risque-t-on pas une confusion entre responsable de traitement et responsable conjoint?
Faut-il encore opérer une distinction subtile entre moyens essentiels et/ou non essentiels?
Ne convient-il pas de modifier la formulation afin de couvrir toutes les situations rencontrées?

Le GTSI souhaiterait une clarification de la définition donnée.

- Paragraphes (§§) 37, 38, 39 et 82

Le GTSI apprécierait des critères plus précis pour définir ce qu'est un « moyen essentiel » et un « moyen non-essentiel », ce qui aiderait aussi à déterminer la qualification de responsable ou de sous-traitant.

Il est suggéré d'ajouter un exemple de recours à une solution cloud de type SaaS (exemple très fréquemment rencontré : utilisation de Microsoft Office 365) ainsi que des exemples de configurations impliquant les GAFAM comme l'utilisation des solutions telles que *Google Analytics*,...et expliquer les relations de sous-traitance et de responsabilité conjointe, voire de responsabilité distincte, dans des cas aussi complexes.

- Paragraphe (§) 63

Le GTSI propose que des exemples de cas de responsabilité conjointe dans des situations complexes soient donnés. Par exemple, l'utilisation de solutions de type *Google Analytics*, et solutions SaaS, …

- Paragraphe (§) 70 et exemple associé

Le GTSI suggère :

  - De préciser quelles sont les responsabilités qui incombent au Responsable de Traitement initial à qui un Responsable de Traitement ultérieur demande de lui communiquer des données. Par exemple :
    - que faire s'il s'agit de deux responsables de traitement distincts ?
    - doit-il procéder à une vérification de la licéité du traitement ultérieur des destinataires ?
    - quelle est la responsabilité du Responsable de Traitement initial dans le transfert de données vers le Responsable de Traitement ultérieur ?

  - D'insister sur la responsabilité du Responsable de Traitement ultérieur pour le transfert :
    - Détermination des moyens de ce transfert ;
    - Transparence ;
    - Formalisation éventuelle dans des protocoles d'accord ou tout autre instrument juridique négocié entre les parties

- Paragraphe (§) 75

  Le concept d' «entité séparée » suscite encore de nombreuses interprétations. Pour y remédier, le GTSI suggère que des critères supplémentaires soient ajoutés afin d'aider à mieux qualifier ces entités et connaître les implications de cette qualification (notamment du point de vue des obligations, des responsabilités...)

- Paragraphe (§) 88

  Le GTSI suggère d'apporter un éclaircissement sur les conséquences liées au fait que, dans cette situation particulière, les autorités publiques ne sont pas considérées comme des « destinataires ». Cela signifie-t-il par exemple que :
  - Le Responsable de Traitement du traitement initial est dispensé d'informer les personnes concernées de l'existence d'éventuelles communications de données de ce type ? N'est-ce pas contraire au principe de transparence ? Est-ce une disposition prévue pour éviter les omissions éventuelles car il est très difficile de savoir qui est susceptible d'opérer de telles enquêtes ?
  - Le Transfert vers une telle autorité publique dans le cadre d'une enquête, n'est pas considéré comme faisant partie du traitement ? Ce type de transfert serait donc exempté dans les analyses d'impact ?

- Paragraphe (§) 107

  Le GTSI propose qu'une guidance soit fournie afin d'aider les plus petites structures à parvenir à se conformer au RGPD lorsque les conditions sont imposées unilatéralement par des acteurs dominants (ex : GAFAM).

  Si le GTSI comprend très bien la position théorique que le Responsable de Traitement ne peut pas invoquer un déséquilibre de force face à certains Sous-Traitant. Il n'en est pas moins vrai que certaines entreprises sont dominantes sur le marché et instaurent des standards que les organisations publiques ou privées n'ont pas d'autre choix dans les faits que de suivre sans émettre d'objections sous peine de « mourir » ou de ne pas être au niveau de service attendu (à titre d'exemple, le cas d'un service public gratuit d'un niveau au moins équivalent à celui d'un service privé).
  Par exemple, le système d'exploitation Windows de Microsoft occupe une place prédominante dans le monde professionnel et il est impossible ou presque aujourd'hui de faire fonctionner les dernières versions de Windows sans transfert de données vers Microsoft.
  Les acteurs du terrain qui souhaitent se conformer au RGPD et aux enseignements des arrêts de la Cour de Justice de l'Union Européenne sont rattrapés par l'actualité dont l'arrêt de la Cour du 16 juillet 2020 pour ne pas le citer, se trouvent démunis quant aux alternatives conformes RGPD qui n'émaneraient pas de grandes entreprises imposant leurs propres standards.

  C'est la raison pour laquelle le GTSI prône l'instauration de certifications des prestataires de services (voir ci-dessous).

- Paragraphe (§) 111

  Le GTSI suggère qu'un ou des modèles de contrat de sous-traitance soi(en)t proposé(s) au niveau européen en vue d'aboutir à une harmonisation entre Etats membres.

- Divers 1: Certifications des prestataires de services

  A l'instar des services « qualifiés » du règlement eIDAS[1], la mise en œuvre de normes européennes certifiant la conformité de certaines fournitures de services de type « cloud computing » (SaaS, PaaS,IaaS) permettrait à la fois de garantir une meilleure protection des données et des personnes concernées, ainsi que des économies d'échelles importantes tant chez les responsables de traitements que chez les sous-traitants.

  En effet, les certifications pourraient apporter des garanties qui dispenseraient les Responsables de Traitement et les Sous-Traitant de devoir se contrôler et se justifier mutuellement. Par exemple :
  - certification de la conformité quant aux transferts des données ;
  - certification de la conformité des clauses contractuelles imposées par les fournisseurs de solutions cloud, et plus particulièrement les entreprises dominantes et puissantes telles que les GAFAM ;
  - certification de la conformité des usages des données pour les seules finalités déterminées par le client ;
  - certification d'un niveau de sécurisation requis minimal pour le traitement de données particulières (sensibles) ;
  - …

- Divers 2: Lignes directrices plus spécialisées par secteur

  Le GTSI suggère que les présentes lignes directrices sur les concepts de responsable de traitement et sous-traitant soient complétées par d'autres plus spécifiques dépendantes des secteurs, notamment pour le secteur public, le secteur de la santé,... avec des exemples prégnants.

FIN

[1] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE