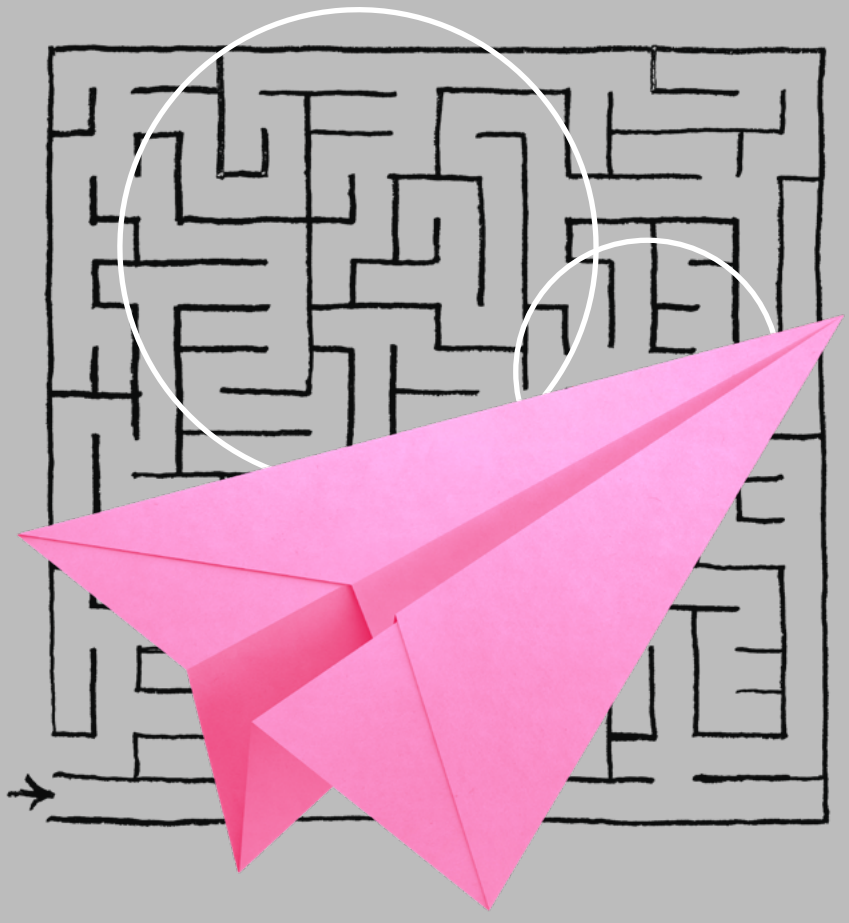
LIVRE BLANC



RGPD

BONNES PRATIQUES
ET NOUVELLES RESPONSABILITÉS

TECH'IN FRANCE

AVIS D'EXPERT

Sylvain Staub

Avocat Associé
DS Avocats

Les éditeurs de logiciels confrontés aux principes de *privacy by design* et de *privacy by default*

Quels sont les principes de protection des données dès la conception et par défaut ?

Le Règlement général sur la protection des données[1] applicable dans l'ensemble des Etats membres de l'Union Européenne depuis le 25 mai 2018, a introduit de nouvelles obligations à l'égard des personnes qui traitent des données à caractère personnel. Au nombre des nouvelles obligations se trouvent **deux principes, particulièrement innovants, qui consiste à assurer la protection des données dès la conception et par défaut**[2].

A travers ces principes de **« protection dès la conception »** (*privacy by design*) et de **« protection par défaut »** (*privacy by default*) il s'agit d'assurer **le respect de la vie privée des personnes concernées et d'éviter la violation de leurs données à caractère personnel, par l'adoption de mesures protectrices en amont et sans action de la part de ces personnes.**

Ajoutons que ces principes doivent s'appliquer aux projets initiés postérieurement au 25 mai 2018 et à ceux qui, bien qu'ils soient antérieurs à cette date, feraient l'objet d'une modification après l'entrée en application du RGPD. Dans ce cadre, l'article 25 du RGPD énonce que le responsable du traitement met en œuvre *« tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées ».* Son objectif demeurant alors la protection des droits de la personne concernée au moyen de mesures techniques appropriées pour garantir que sont traitées « *seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement.* »

A ceci s'ajoute le fait que les éditeurs de logiciels sont incités à « s'assurer que [leurs clients] sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics. »

Quelles sont les obligations de l'éditeur de logiciels vis-à-vis de son client utilisateur ?

Un éditeur de logiciel est en premier lieu **fournisseur d'un bien incorporel,** en l'occurrence une solution logicielle, et à ce titre débiteur d'une « **obligation de délivrance** »[3] conforme aux prévisions contractuelles.

Au-delà de la délivrance conforme, il incombe également à l'éditeur de logiciel de mettre à la disposition de son client – profane en la matière – une compétence professionnelle, qui comprend **une obligation d'information**, voire **une obligation de conseil**[4] qui est la forme la plus avancée de l'obligation d'information. Cette obligation d'information qui pèse sur l'éditeur est à l'origine d'une part importante des litiges informatiques.

L'utilisateur d'un logiciel est tenu de respecter le RGPD, chaque fois qu'il réalise des traitements de données à caractère

LE SAVIEZ VOUS ?

Article 25 du RGPD sur les obligations des éditeurs :

« 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, (…) le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées (…) afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées (…). »

personnel à travers l'utilisation dudit logiciel. Le défaut de prise en compte de la protection des données dès la conception et par défaut placerait d'office l'utilisateur en situation de manquement au regard de la réglementation (il en serait ainsi par exemple d'un logiciel qui prévoirait la saisie de données excédant ce qui est nécessaire à la poursuite des finalités de l'activité exercée).

« C'est pourquoi il semble difficilement envisageable pour l'éditeur de logiciels de faire abstraction de cette exigence qui intéresse l'usage effectif de la chose fournie »

C'est pourquoi il semble difficilement envisageable pour l'éditeur de logiciels de faire abstraction de cette exigence qui intéresse l'usage effectif de la chose fournie, au moins pour ceux des utilisateurs dont les activités de traitement sont soumises au RGPD. Au demeurant lorsqu'il délivre un service complémentaire à l'utilisateur du logiciel – qu'il s'agisse d'une prestation d'hébergement, de maintenance, etc. –, l'éditeur se voit qualifié de sous-traitant au sens du RGPD (cf. article 28); et en cette qualité, il est directement visé par le RGPD.

C'est ainsi qu'en tant que « *sous-traitant* » l'éditeur est tenu notamment de présenter « *des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du [RGPD] et garantisse la protection des droits de la personne concernée* »[5], de prendre « toutes les mesures requises en vertu de l'article 32 » du RGPD[6], etc.

Qu'en est-il de l'émergence d'une cause de responsabilité de l'éditeur au titre des principes de protection des données dès la conception et par défaut ?

La conclusion d'un contrat suppose de la part des cocontractants la conscience des droits et obligations qui en résultent à leur égard. Dit autrement, dans tout processus contractuel chaque partie doit avoir conscience des risques qu'elle endosse, soit à raison de l'inexécution de ses propres obligations, soit en raison de l'inexécution des obligations de son cocontractant.

La Loi Informatique et Libertés dans ses versions antérieures au RGPD n'imposait pas explicitement la mise en œuvre d'une démarche de *privacy by design* et *by default*. La question d'une éventuelle obligation juridique des éditeurs de logiciels n'avait donc pas lieu d'être.

Le fait que le RGPD impose une conformité du traitement dès la conception et par défaut change radicalement la donne : ces nouvelles exigences ont vocation à porter les obligations liées à la protection des données à caractère personnel au niveau de l'éditeur du logiciel. Du reste, l'implication des éditeurs de logiciel à la conformité RGPD était en germe dans certains travaux du G29 antérieurs au texte. Tout particulièrement un avis de 2014 relatif à l'internet des objets relevait **la difficulté pour les utilisateurs de modifier les paramétrages industriels paramétrés par défaut et recommandait aux éditeurs de fournir un niveau adéquat d'informations aux utilisateurs finaux**[7].

LE SAVIEZ VOUS ?

Article 25 considérant n° 78

« (…) Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits (…) il convient d'inciter [les éditeurs de logiciels] à prendre en compte le droit à la protection des données (…) et, compte dûment tenu de l'état des connaissances, à s'assurer que [leurs clients] sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics. »

Le considérant n° 78 précité, qui vise à inciter les éditeurs de logiciels à « *prendre en compte le droit à la protection des données (…) [et] à s'assurer que [leurs clients] sont en mesure de s'acquitter des obligations qui leur incombent* », a donc confirmé cette orientation partagée à la fois par le législateur européen et par les organismes de régulation.

En pratique, cela signifie que l'obligation d'information et de conseil de l'éditeur de logiciel doit désormais intégrer les principes de protection dès la conception et par défaut ?

Ainsi, il est vraisemblable que les contentieux qui seront initiés à l'avenir sur le fondement d'un défaut de conseil de l'éditeur de logiciels et/ou d'un défaut de livraison conforme, seront complétés par l'argument du défaut de prise en compte des principes de protection dès la conception et par défaut (défaut de mise en garde sur le respect de la conformité au RGPD et défaut de conseil dans l'expression subséquente du besoin du client).

Certaines jurisprudences annoncent le risque judiciaire qui pèse désormais sur les éditeurs de logiciels. Il en est ainsi en particulier de la décision qui avait été rendue par la chambre commerciale de la Cour de cassation le 19 février 2008[8] au sujet du passage à l'an 2000, au terme de laquelle : « *(…) tout concepteur d'un progiciel a l'obligation de s'assurer que ce*

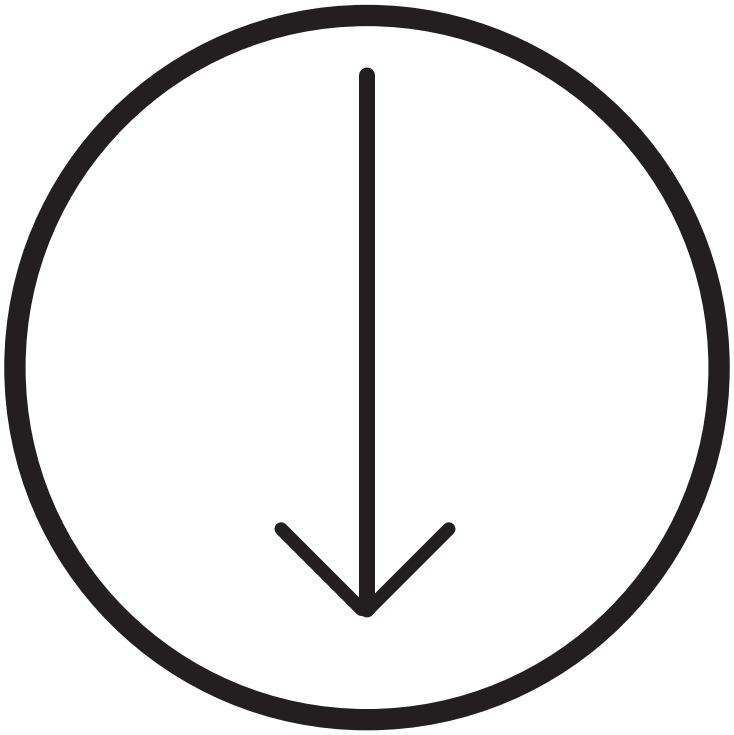
progiciel, au moment de sa cession, réponde tant aux besoins du client qu'aux obligations légales prévues ou prévisibles pour sa durée de vie (…) »

A ce stade on peut entrevoir une limite à cette nouvelle « obligation » des éditeurs de logiciels : l'obligation de conseil au regard des principes de protection dès la conception et par défaut (qui débouche sur l'obligation de fournir un logiciel adapté) ne vaudrait qu'au jour de la conclusion du contrat, l'éditeur ne s'engageant pas (sauf stipulations contractuelles en ce sens) à assurer la maintenance évolutive du logiciel – en l'occurrence la conformité à une réglementation postérieure au contrat – en cours d'exécution du contrat[9]. Autrement dit, seuls les logiciels vendus postérieurement à l'adoption du RGPD devraient être concernés.

Pour finir, on rappellera que le RGPD énonce dans son considérant 78 que les «*principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics* ». Ce qui signifie que les principes de protection dès la conception et par défaut sont et seront de plus en plus des éléments de sélection des logiciels dans le cadre d'appels d'offres publics.
Nul doute que cette exigence se généralisera également dans le secteur privé ; d'ailleurs les opérateurs privés ont déjà tendance à se doter de guides ou de procédures en matière de protection des données dès la conception et par défaut, en vue de sélectionner leurs prestataires et les solutions logicielles qui répondent à leurs impératifs en matière de conformité au RGPD.

Il est possible d'en conclure que la sanction d'un logiciel qui ne tiendrait pas compte des principes de protection dès la conception et par défaut, sera économique (défaut de vente) avant d'être juridique (contentieux).

1. Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données n°2016/679 du 27 avril 2016.
2. Les concepts de privacy by design et by default ont fait leur apparition dans un rapport de 1995 dédié aux « technologies améliorant la confidentialité » préparé par l'Organisation néerlandaise pour la recherche scientifique appliquée, des représentants de l'Autorité de protection des données néerlandaise et la Commissaire à l'Information et la Vie Privée de l'Ontario de l'époque, Madame Ann Cavoukian.
3. CA Versailles, 3ème chambre, 26 octobre 1990 : D. 1991, sommaire p.166 ; Cass 1ère civ. 3 mai 2006, n° 04-20432 : Bull. civ. 2006, I, n° 217 ; Cass. com 11 juillet 2006, n° 04-17.093 ; Cass. com. 19 février 2008, n° 06-17.669 ; Cass. com. 5 octobre 2010, n° 08-11.630 : Jurisdata n° 2010-017800 ; Cass. com 6 décembre 2017, n°16-19615 ; CA Saint Denis 21 février 2018.
4. Cass. com 11 juillet 2006, n° 04-17.093 ; CA Paris, pôle 5 chambre 11, 16 octobre 2015 ; CA d'Aix en Provence 7 juin 2018, n°13/18867.
5. RGPD art. 28 §1.
6. RGPD art. 28 §3 c.
7. Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, adopté le 16 septembre 2014, p.24.
8. Cass. com., 19 février 2008, n° 06-17669.
9. Cf. en ce sens CA Rouen 21 juin 2018, n° 16/05587.



Téléchargez le livre blanc pour le lire en entier

RGPD

BONNES PRATIQUES ET NOUVELLES RESPONSABILITÉS