REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (RGPD) : Comment aborder votre mise en conformité ?

Qu'est-ce que le RGPD ?

Le règlement UE 2016/679 du Parlement Européen et du Conseil (RGPD) qui entrera en vigueur à compter du 25 mai 2018 a pour vocation principale de **renforcer les droits des personnes physiques concernées par les données personnelles** traitées par les entreprises dans le cadre de leurs activités, tout en imposant à ces dernières (qu'elles agissent en qualité de responsable de traitement et/ou de sous-traitant), **un niveau de sécurisation et de protection accru desdites données** afin d'assurer une meilleure protection des intérêts des personnes physiques concernées. Ce double objectif résulte du fait que **protection des données personnelles rime notamment avec protection des intérêts de la vie privée et de certains droits fondamentaux.**

Quelle est la portée du RGPD ?

S'inscrivant dans une logique de « responsabilisation » (accountability), le RGPD implique que **chaque entreprise effectue un travail d'auto-évaluation** afin de savoir si les mesures internes existantes qu'elle met en œuvre en matière d'accès aux données, de stockage mais également de gestion tout au long de leur période de traitement permettent d'**être en conformité avec les objectifs poursuivis par le RGPD.**

Cette démarche demande inévitablement de « prendre de la hauteur » par rapport à son organisation interne et de procéder à des arbitrages car, si le RGPD est généralement clair concernant les objectifs poursuivis, les moyens à mettre en œuvre et les mesures à adopter pour les atteindre ne sont quant à eux pas toujours définis dans leur principe ni dans leurs modalités pratiques de mise en œuvre. Quoi qu'il en soit, le principe à retenir est que **chaque entreprise se doit d'adopter un ensemble de mesures jugées suffisamment protectrices** afin qu'elle puisse démontrer le cas échéant être une actrice du traitement de données personnelles fiable et responsable vis-à-vis des personnes physiques concernées par ces dernières.

CSCA – Chambre Syndicale des Courtiers d'Assurances
10 rue Auber - 75009 Paris - Tel : 01 48 74 19 12 - Fax : 01 42 82 91 10
N° Ville de Paris : 20060002 N° Préfecture : 20259
Internet : http://www.csca.fr – E-mail : csca@csca.fr

CSCA

A l'instar de la LCB/FT, Solvabilité II (ou de la DDA demain), le RGPD nécessite pour chaque courtier ou société de courtage de commencer par établir **un « état des lieux » des données qu'il traite et des différents traitements qu'il réalise** dans le cadre de son activité, ce afin de pouvoir bénéficier **d'une vision globale** lui permettant alors d'**identifier les failles et risques en matière de protection des données et d'adopter en conséquence les mesures correctives qui s'imposent.**

Il est très important de souligner que la politique de protection et de gestion des données ainsi que l'ensemble des autres mesures adoptées par une entreprise en vue de se conformer au RGPD doivent être **formalisées par écrit et documentées**, exactement comme les autres process et supports que vous pouvez utiliser dans le cadre de votre activité d'intermédiaire d'assurances. Ces documents formalisant les mesures internes que vous aurez adoptées en matière de protection des données personnelles doivent être **tenus à jour au fur et à mesure des évolutions que vous y apporterez nécessairement** au fil des mois et des années.

L'idée générale à retenir dans le cadre du RGPD, comme dans le cadre de n'importe quelle autre législation requérant **une démarche proactive et responsable des entreprises**, est que vous devez être en mesure de démontrer en cas de contrôle de l'autorité de tutelle (CNIL ou ACPR) ou d'audit de l'assureur (lorsque vous agissez en qualité de sous-traitant de ce dernier), que **les mesures internes adoptées et que les moyens mis en œuvre en vue de poursuivre les objectifs posés par le règlement sont réels et permettent d'assurer un niveau de sécurisation des données suffisamment élevé pour protéger les intérêts des personnes concernées au regard des risques identifiés** (lesquels varient nécessairement d'une entreprise à une autre).

Il n'existe donc pas de liste exhaustive impérative et générale des mesures à adopter et des moyens à mettre en œuvre.

Chaque entreprise, en fonction des données qu'elle traite, des finalités de traitement qu'elle poursuit, de ses réseaux de sous-traitants éventuels, de l'organisation de ses archives papiers ou numériques, mais également (et peut-être surtout) de son environnement informatique, se doit d'adopter des mesures adaptées et personnalisées concourant à l'atteinte des objectifs prévus par le RGPD. Ces dernières doivent être notamment élaborées au regard de l'importance des risques encourus par les personnes concernées lesquels fluctuent notamment en fonction des types de données mais également de l'échelle à laquelle celles-ci sont traitées et enfin des mesures de protection mises en œuvre par l'entreprise.

Les sanctions prévues

Outre cet aspect, il est également à noter que le RGPD prévoit des sanctions bien plus importantes que celles existant actuellement au titre de la Loi du 6 janvier 1978. En effet, si cette dernière plafonnait les sanctions pécuniaires à 150.000 € pour un premier manquement et à 5% du CA HT annuel en cas de récidive (plafonné à 300.000 €), les sanctions prévues par le RGPD sont sans commune mesure :

- 2 % du CA annuel mondial (plafonné à 10 M€) pour un manquement aux principes de « privacy by design » et « privacy by default » ces deux principes recouvrant la notion de protection des données grâce aux outils et mesures adoptés par les entreprise ;
- 4 % du CA annuel mondial (plafonné à 20 M€) pour un manquement aux droits des personnes concernées par les données

A titre de rappel, peuvent venir s'ajouter à ces sanctions spécifiques prévues par le RGPD dans sanctions pénales telles que :

Non-respect des formalités préalables	Articles 226-16 et 226-16-A du Code pénal	300.000 euros d'amende et 5 ans d'emprisonnement
Non-respect de l'article 34 de la loi Informatique et Libertés relatif à l'obligation de sécurité	Articles 226-17 et 226-17-1 du Code pénal	300.000 euros d'amende et 5 ans d'emprisonnement
Détournement de la finalité des données personnelles	Article 226-21 du Code pénal	300.000 euros d'amende et 5 ans d'emprisonnement
Procéder à un transfert de données transfrontières contrevenant aux mesures prises par la Commission des Communautés européennes ou à l'article 70 de la loi Informatique et Libertés	Article 226-22-1 du Code pénal	300.000 euros d'amende et 5 ans d'emprisonnement
Absence d'information des personnes concernées	Article R. 625-10 du Code pénal	1.500 euros d'amende par infraction constatée
Non-respect des droits des personnes	Article R. 625-11 du Code pénal	1.500 euros d'amende par infraction constatée

La CSCA vous accompagne dans une démarche progressive

Afin de **vous accompagner dans la mise en œuvre de cette démarche,** la CSCA vous propose toute une série de documents pédagogiques et opérationnels (telles que des matrices dont vous pourrez vous inspirer en vue d'élaborer vos propres process et politiques de gestion interne).

Comme tous les autres supports opérationnels que la CSCA propose à ses Adhérents, les différents documents que nous mettons à votre disposition en vue de vous accompagner dans votre mise en conformité RGPD **ne sauraient être perçus comme étant des documents « clefs en main » pouvant être utilisés tel quel.** En effet, il est indispensable que chaque courtier Adhérent adopte une démarche globale constructive par rapport à cette nouvelle réglementation évolutive, nécessitant d'adapter à la fois ses mesures opérationnelles, techniques et informatiques protégeant les données personnelles de vos clients et prospects, mais également de modifier (peut-être) certains comportements devenus incompatibles avec les exigences renforcées en matière de protection des données personnelles prévues par le RGPD (telle que la conservation non sécurisée de données ou bien encore l'enregistrement de données sur des disques durs ou clef USB laissés à disposition sur un bureau).

Découvrir le RGPD

Avant tout travail de formalisation de vos process internes liés à la protection des données, lesquels sont la formalisation écrite des mesures internes de protection nécessaire pour lesquelles vous aurez opté en amont, nous ne pouvons que vous conseiller au préalable de vous familiariser avec le RGPD, soit en lisant **le texte intégral du règlement**, soit en prenant connaissance du **Focus RGPD**, lequel vous présente sous une forme synthétique les principaux points de cette nouvelle réglementation.

Structurer votre démarche

Vous pourrez par la suite initier votre démarche de mise en conformité en vous appuyant sur le document socle que nous vous proposons, intitulé « **Tableau de mise en œuvre opérationnelles RGPD** », lequel reprend les points cruciaux du RGPD en soulignant pour chacun d'eux les impacts opérationnels à prévoir, **tout en vous permettant d'accéder aux matrices proposées par la CSCA.**

CSCA – Chambre Syndicale des Courtiers d'Assurances
10 rue Auber - 75009 Paris - Tel : 01 48 74 19 12 - Fax : 01 42 82 91 10
N° Ville de Paris : 20060002 N° Préfecture : 20259
Internet : http://www.csca.fr – E-mail : csca@csca.fr

CSCA

Cartographier votre situation

Dans ce tableau, vous découvrirez notamment un lien vous donnant accès à un logiciel gratuit développé par la CNIL (actuellement en version bêta, une version finalisée sera accessible ultérieurement), lequel vous permettra de vous auto-évaluer par rapport aux mesures internes existantes d'une part mais également de vous fournir, une fois le questionnaire rempli, une cartographie des risques liés au(x) traitement(s) de vos données ainsi qu'un plan des actions à mener afin de renforcer vos mesures internes lorsque cela est nécessaire.

A partir de **ces documents synthétiques générés automatiquement par le logiciel** sur la base de vos déclarations, après avoir suffisamment adapté vos mesures internes permettant d'atteindre un niveau de risque acceptable (lequel doit être apprécié au regard de votre cartographie des risques et de l'analyse d'impact), vous pourrez alors passer à l'étape suivante en procédant à la formalisation de vos process écrits et politique(s) interne(s).

Un accompagnement continu de la CSCA

Le service juridique de la CSCA se tient à votre disposition pour vous accompagner dans votre démarche de mise en conformité RGPD ainsi que dans l'élaboration de votre politique de gestion et de protection des données.

N'hésitez pas à le contacter pour toute question relative à cette nouvelle réglementation certes impactante mais néanmoins très importante d'un point de vue professionnel.

En effet, la conformité RGPD fera partie demain des critères pris en compte par les assureurs en vue d'ouvrir des codes apporteurs et/ou d'accorder (ou de maintenir) des délégations d'une part, mais fera également partie des critères substantiels de valorisation de votre fonds de commerce d'autre part.

CSCA – Chambre Syndicale des Courtiers d'Assurances
10 rue Auber - 75009 Paris - Tel : 01 48 74 19 12 - Fax : 01 42 82 91 10
N° Ville de Paris : 20060002 N° Préfecture : 20259
Internet : http://www.csca.fr – E-mail : csca@csca.fr

CSCA