NOTE TECHNIQUE

L'application du RGPD aux professions économiques - différentes catégories de données et principes de base

La présente contribution vise à illustrer à l'aide d'exemples concrets, l'impact du RGPD pour les titulaires des professions économiques.

Les professions économiques recouvrent les professions de comptables et fiscalistes (membres IPCF), experts-comptables et conseils fiscaux (membres IEC) et réviseurs d'entreprises (membres IRE).

Ces professions traitent et gèrent régulièrement un certain nombre de données à caractère personnel au sens du RGPD : p.ex. les données de leurs clients, de leurs fournisseurs, les données des clients de leurs clients mais aussi les données de leurs collaborateurs, de leurs employés, de leurs clients potentiels, de leurs relations d'affaires, ...

La plupart du temps, ces données seront traitées à l'aide de programmes comptables, applications fiscales, outils d'audit et systèmes de gestion des documents et d'archivage utilisés dans le cabinet.

En tant que responsable du traitement, le cabinet identifiera tout d'abord les différentes catégories de données qu'il traite.

Les différentes catégories de données

Le RGPD s'applique aux données à caractère personnel faisant l'objet d'un traitement, automatisé ou non.

Données à caractère personnel :

La définition des données à caractère personnel est large.

Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable

> *Par exemple : le nom, le prénom, l'image (photos ou vidéos permettant de l'identifier directement), un numéro national, un identifiant en ligne, une adresse IP, une empreinte digitale*

Les informations relatives à des personnes morales ne sont donc pas visées.

Traitement des données

Le traitement est également défini de façon large et vise la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction de ces données.

Si le traitement n'est pas automatisé, le RGPD s'applique également pour autant que les données à caractère personnel soient contenues ou appelées à figurer dans un fichier.

> *Par exemple: les fichiers clients, les fichiers fournisseurs, l'annuaire interne du cabinet*

Les informations « papier », pour autant qu'elles soient structurées selon des critères déterminés (p.ex. un classement alphabétique), tombent donc également sous le champ d'application du RGPD (le cas échéant : les dossiers papiers, classeurs, archives physiques).

Catégories particulières de données à caractère personnel :

Certaines catégories de données à caractère personnel font l'objet d'une protection renforcée :

- les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, des données génétiques, biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle.

Le traitement de ces données est en principe interdit mais des exceptions sont prévues et se fondent notamment sur le consentement explicite, les intérêts vitaux, la défense en justice, l'intérêt public, la médecine du travail.

> *Les cabinets en charge de la comptabilité ou de l'audit des comptes d'une compagnie d'assurances, d'une organisation syndicale ou d'un parti politique seront particulièrement attentifs et veilleront à documenter le fondement sur lequel repose le traitement des données en question.*
>
> *Le procès-verbal d'une réunion d'une délégation syndicale ou d'un conseil d'entreprise sera donc jugé plus sensible que le procès-verbal d'un conseil d'administration.*
>
> *De même, la liste d'une patientèle est plus sensible qu'une liste de clients de vente de détail.*

- les données à caractère personnel relatives aux condamnations pénales et aux infractions

Le traitement de ces données ne peut être effectué que sous le contrôle de l'autorité publique.

Ceci constitue un point d'attention pour les comptables et les commissaires des cabinets d'avocats spécialisés en droit pénal.

- les données à caractère personnel des enfants

Lorsque le traitement des données repose sur le consentement et que l'enfant dont les données sont traitées est âgé de moins de 16 ans, le consentement est donné par le titulaire de la responsabilité parentale. Toutefois, cette obligation ne s'applique que s'il s'agit de services de la société de l'information (réseaux sociaux, p. ex.). En principe, ce cas ne se présente pas pour les professions du chiffre.

Le droit des obligations belge (p. ex. les règles relatives à la validité, à la formation ou aux effets d'un contrat à l'égard d'un enfant) restent toutefois applicables.

Vous devez donc pouvoir prouver que vous avez fourni des efforts raisonnables afin de vérifier le consentement du parent ou du tuteur, par exemple dans le cas suivant :

Une déclaration d'enfant mineur handicapé afin de bénéficier d'une réduction d'impôts.

Principes de Base

Accountability

La responsabilisation des entreprises est au cœur de la nouvelle règlementation RGPD.

L'obligation de déclarer les traitements des données à caractère personnel à la Commission de la protection de la vie privée est supprimée. Il revient désormais aux entreprises de veiller elles-mêmes, de façon proactive, à la conformité de leur organisation avec le RGPD.

En pratique, cela signifie que les entreprises doivent être en mesure d'expliquer et de démontrer ce qu'elles ont entrepris afin de se conformer au RGPD.

La **documentation** des entreprises, le cas échéant via leurs contractants IT, est donc essentielle et constituera le point de départ du dialogue avec l'autorité de contrôle.
La rédaction d'un **registre des données** constitue une obligation en ce sens.

Autres exemples de documentation à rédiger :

- description des procédures mises en place afin de limiter les risques de perte des données

- description des procédures mises en place en cas de perte/vol de données

- le cas échéant, rédaction d'une analyse d'impact

- le cas échéant, désignation d'un data protection officer, ci-après « DPO » ou une fonction similaire

-Licéité du traitement

La licéité du traitement se fonde, alternativement, sur :

Le consentement
Lequel doit être donné par un acte positif clair.
Il doit être aussi simple de retirer que de donner son consentement.

P.ex. : une déclaration écrite, le cas échéant par voie électronique, le fait de sélectionner une case sur un site internet.

Les cases pré-cochées sont exclues.

Une obligation légale
Par exemple dans le cadre des obligations AML : identification des clients, mandataires, bénéficiaires effectifs (Know your customer) et conservation de la carte d'identité.
Il n'est donc pas nécessaire de demander le consentement du client pour traiter des données personnelles le concernant lorsque ce traitement est imposé par la loi.

Un contrat ou des mesures précontractuelles
Dans un cabinet comptable ou d'audit, la licéité du traitement se fonde la plupart du temps sur base de l'exécution d'un contrat.
Il est donc inutile de demander systématiquement le consentement du client.
En revanche, il est capital d'établir une lettre de mission et/ou des conditions générales qui traitent cet aspect.

Une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement
Par exemple, le traitement des données à caractère personnel par le Collège de supervision des réviseurs d'entreprises.

Des intérêts légitimes
Le considérant 47 à 49 du RGPD citent à titre d'exemple le traitement des données des clients ou de clients potentiels à des fins de prospection.
La prévention de la fraude est également citée.
Les responsables du traitement qui font partie d'un groupe d'entreprises peuvent également avoir un intérêt légitime à transmettre des données à caractère personnel au sein du groupe à des fins administratives internes.
La sécurité du réseau des informations peut aussi constituer un intérêt légitime.

Ces intérêts légitimes devront toutefois être mis en balance par rapport à l'atteinte éventuelle aux droits et libertés de la personne concernée (pondération des intérêts en présence). La nature des données traitées et les attentes raisonnables des personnes concernées seront prises en considération.

-Principe de loyauté et de transparence

Les droits de la personne concernée occupent une place prépondérante dans la nouvelle règlementation.

Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

Le droit d'accès de la personne concernée implique que celle-ci a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées. Lorsqu'elles le sont, la personne concernée doit avoir accès auxdites données à caractère personnel ainsi que les informations portant notamment sur :

- les finalités du traitement,

- les catégories de données à caractère personnel concernées,

-les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées,

- la durée de conservation des données à caractère personnel envisagée (…).

Le responsable du traitement dispose d'un délai d'un mois pour répondre à la demande d'information de la personne concernée (éventuellement prolongé de deux mois). Tout refus de faire droit à la demande doit être motivé.

Mentionnons également le droit pour la personne concernée de demander au responsable du traitement la rectification ou l'effacement (droit à l'oubli) de données à caractère personnel.

Le cabinet évaluera donc les procédures existantes afin de vérifier notamment si les systèmes permettent à la personne concernée d'exercer ses droits.

La déclaration de confidentialité du cabinet sera également évaluée et le cas échéant modifiée de sorte qu'elle contienne les informations exigées par le RGPD telles que le fondement licite du traitement des données et les délais pendant lesquels les informations seront conservées.

Le cabinet s'assurera également que les données conservées sont exactes et tenues à jour. Toutes les mesures doivent être prises pour que les données inexactes soient effacées ou rectifiées sans tarder.

A PROPOS DU PROFILAGE

Le RGPD définit le profilage par toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

En vertu des dispositions AML chaque cabinet est tenu d'établir un profil de risque de chaque client. La communication par le cabinet d'informations à ce sujet au client reste bien sûr interdite.

-Principe de pertinence et de minimisation

Le traitement des données à caractère personnel doit toujours être limité à ce qui est strictement nécessaire.

Les données ne peuvent être conservées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Dans le cadre d'une mission, un cabinet rassemble diverses données à caractère personnel. Seules les données nécessaires à l'exercice de la mission seront enregistrées. Le cabinet doit en outre avoir une procédure permettant de s'assurer que les données enregistrées ne seront pas conservées au-delà de la période utile.

Il appartient aux cabinets d'identifier les données personnelles non conservées en vertu d'une obligation légale, lesquelles doivent impérativement être détruites à l'expiration du délai de conservation.

Isoler les données conservées à ce titre des autres données conservées en vertu de la loi et dont le délai de conservation peut être plus long, n'est pas aisé. Ceci implique une gestion adéquate des archives en ce compris les archives électroniques.

Dans certains cas, il peut être justifié de conserver les données à caractère personnel au-delà de ce qui est nécessaire en vertu d'une législation particulière, par exemple afin de pouvoir, le cas échéant, se défendre efficacement en justice.