

## COMMUNICATION <sup>1</sup> 2018/07 DU CONSEIL DE L'INSTITUT DES REVISEURS D'ENTREPRISES

Correspondant sg@ibr-ire.be	Notre référence AC	Votre référence	Date 25/05/2018
--------------------------------	-----------------------	-----------------	--------------------

Chère Consœur,  
Cher Confrère,

**Concerne: RGPD – Application dès le 25 mai 2018 du Règlement (UE) 2016/679 du 27 avril 2016 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, et abrogeant la directive 95/46/CE <sup>2</sup>**

Le Règlement européen 2016/679 du 27 avril 2016 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, et abrogeant la directive 95/46/CE, ci-après le RGPD, est d'application depuis le 25 mai 2018.

Comme toutes les entreprises, les cabinets de révision sont concernés par le RGPD et doivent s'y conformer.

### **Les outils mis à disposition par l'IRE**

L'IRE a mis différents outils à disposition de ses membres sur son site web :  
[https://www.ibr-ire.be/fr/l\\_institut/actualites/actualites\\_ire/Pages/Prets-pour-le-RGPD.aspx](https://www.ibr-ire.be/fr/l_institut/actualites/actualites_ire/Pages/Prets-pour-le-RGPD.aspx)

Vous y trouverez tout d'abord une checklist en 12 étapes établie par le groupe de travail interinstituts « Règlement Général sur la Protection des Données » (IPCF, IEC et IRE). Celle-ci doit vous aider à dresser, pour votre cabinet, un état des lieux de la façon dont les données personnelles sont actuellement traitées et à définir votre plan d'action en conséquence.

---

<sup>1</sup> Par voie de communication, l'Institut développe la doctrine relative aux techniques d'audit et à la bonne application par les réviseurs d'entreprises du cadre légal, réglementaire et normatif qui régit l'exercice de leur profession (art. 31, §7 de la loi du 7 décembre 2016 portant organisation de la profession et de la supervision publique des réviseurs d'entreprises) ; seules les normes et les recommandations sont obligatoires.

<sup>2</sup> <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=NL>

D'autres outils sont disponibles tels qu'un exemple de clause de consentement et de politique de confidentialité mais aussi une checklist informatique et le guide des bonnes pratiques informatiques.

Nous complétons en outre progressivement le site avec des liens vers d'autres sites internet vivement recommandés et des articles de doctrine.

### L'essentiel à savoir

La définition des « données à caractère personnel » est large. Il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable.

Le nom, le prénom, l'image, un numéro national, un identifiant en ligne, une adresse IP, une empreinte digitale constituent des données personnelles.

De même, la notion de « traitement » est définie largement et vise par exemple la collecte, l'enregistrement, la conservation, l'adaptation ou la modification, mais aussi la simple consultation de données.

Le traitement peut être automatisé (fichier numérique), ou pas. Dès lors que les données à caractère personnel sont contenues ou appelées à figurer dans un fichier, le RGPD s'applique (par exemple : les fichiers clients et fournisseurs, l'annuaire interne du cabinet).

Au sein d'un cabinet de révision « type », il faudra donc tout d'abord distinguer les données personnelles internes au cabinet (personnel, collaborateurs, fournisseurs, prestataires de services, etc.) et les données personnelles des clients.

Les principales obligations prévues par le RGPD sont reprises dans la checklist établie par le groupe de travail interinstituts « Règlement Général sur la Protection des Données » :

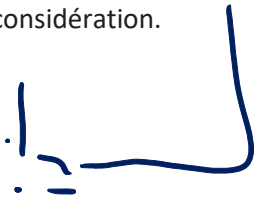
- 1) Répertorier les données personnelles dont vous disposez, leur provenance et les modalités de conservation.
- 2) Identifier le fondement licite sur lequel repose le traitement (en pratique il s'agira le plus souvent du contrat, de la loi, du consentement ou des intérêts légitimes)
- 3) Identifier si vous traitez des données sensibles (par exemple : origine raciale, opinions politiques, données biométriques)
- 4) Vérifier la façon dont le consentement est demandé
- 5) Garantir leurs droits aux personnes concernées
- 6) Sécuriser votre système informatique
- 7) Désigner un délégué à la protection des données (DPO) ou une personne de référence
- 8) Evaluer si vous devez réaliser une analyse d'impact (DPIA)

- 9) Etablir un registre des activités de traitement des données
- 10) Mettre en place une politique de protection de la vie privée.
- 11) Identifier les relations avec les sous-traitants et relire vos contrats
- 12) Etre prêt à réagir en présence d'une violation de données

Il est en outre primordial de documenter chacune de ces étapes étant donné que la Commission vie privée, ou l'Autorité de protection des données, qui lui succèdera se basera sur ces documents, et principalement sur le registre des activités de traitement des données, pour effectuer ses contrôles, qu'ils aient lieu d'initiative ou suite à une éventuelle plainte.

L'IRE veillera à faciliter le plus possible le travail de ses membres à l'aide des différents outils dont question ci-dessus ainsi qu'en s'informant des meilleures pratiques dans le secteur.

Je vous prie d'agréer, Chère Consœur, Cher Confrère, l'expression de ma haute considération.



Thierry DUPONT  
Président