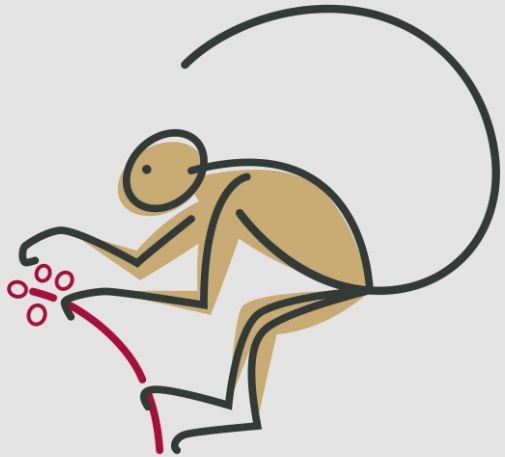
Atelier d'information RGPD

Auvergne-Rhône-Alpes Spectacle Vivant

Journée du 21 mars 2019 - *Valence*

Lionel GOUTALIER
Avocat au Barreau de Lyon
ENTELLE Avocat
27 rue Ferrandière, 69002 Lyon
(06 62 11 49 16 – 04 72 41 00 60)
www.entelle-avocat.fr



La protection des données personnelles en pratique…

Atelier d'information RGPD :

1 – Introduction : cadre législatif et réglementaire

2 – Définitions : données, traitements, responsable de traitement…

3 – Principes clés du RGPD et nouvelles obligations

4 – Fondamentaux des données et traitements

5 – Sanctions, rôle et évolution de la CNIL

6 – Incidences sur la relation client

7 – Comment atteindre la conformité (actions à mener)

1. Introduction :

1.1 Genèse de la Loi de 1978 Informatique et Libertés

Un texte protecteur des droits et libertés individuelles :

- **Article 1er de la LOI n° 78-17 du 6 janvier 1978** (modifié par la LOI n°2016-1321 du 7 octobre 2016 – art. 54)

Al. 1 « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*

Al. 2 « *Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi.* »

(Ord. n° 2018-11235 du 12 déc. 2018 : applicable au 1er juin 2019) :

Al. 2 « Les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant et les obligations incombant aux personnes qui traitent ces données s'exercent dans le cadre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et de la présente loi ».

1. Introduction :

1.2 Un cadre juridique national rénové (4 LIL et 1 décret d'application en attente de compléments)

- **LIL 1. / 1978 : LOI n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**
- **LIL2. / 2004 : LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978**
- + LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique
- **LIL3. / 2018 : LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles** dont l'art. 32 a prévu qu'elle soit suivie dans un délai de 6 mois d'une ordonnance de réécriture de la LIL
- **Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** (modifié par le décret n° 2018-687 du 1er août 2018)
- **LIL4 /2018 : Prise pas ordonnance n° 2018-1125 du 12 décembre 2018 :** réécriture complète de la loi « Informatique et Libertés », afin d'assurer la lisibilité d'un cadre juridique composite (*dixit* la CNIL elle-même), entre en vigueur au plus tard le 1er juin 2019

1. Introduction :

1.3 « *Ce qui est familier n'attire pas l'attention* » (Sun Tzu (-544/-496) : « L'Art de la guerre »)

Petite chronologie des data :

Extraits de « *La vie algorithmique (critique de la raison numérique)* », Éric Sadin, Ed. *L'Echappée*, 2015

- Apparition de l'intelligence artificielle : années 1950 (Alan Turing)
- … … …
- 1977 = l'ordinateur Appel II est mis sur le marché
- 1980 = Philips inaugure le Compact Disc
- 1981 = IBM commercialise son premier PC
- 1982 = Microsoft distribue le système d'exploitation MS-DOS
- 1989 = Définition de la structure du World Wide Web (www)
- 1991 = Protocole http fixe une standardisation universelle de la Toile
- 1994 = Création du site de vente en ligne AMAZON (par Jeff Bezos)
- 1995 = CASIO commercialise le premier appareil photo numérique compact grand public
- 1996 = Nombre estimé d'ordinateurs connectés à Internet dans le monde : 10 millions
- 1997 = Le programme *Deep Blue* d'IMB bat aux échecs le champion du monde Garry Kasparov
- 1998 = Serge Brin et Larry Page fondent GOOGLE sur la base de leur algorithme PageRank
- 1999 = Le Wifi est initié par la société INTERBRAND

1. Introduction :

1.3 Un changement de paradigme : l'ère de la numérisation du monde (le « dataïsme »)

- 2000 = Le nombre de sites consultables est évalué à 10 millions
- 2000 = Bill Clinton ouvre la diffusion des signaux GPS à des applications civiles
- 2003 = Séquençage complet de l'ADN du génome humain
- 2004 = FACEBOOK est mis en ligne (1 milliard d'inscrits 10 ans plus tard)
- 2006 = TWITTER lance sa plateforme de microblogging
- 2007 = Steve Jobs présente l'iPhone qui inaugure l'ère des smartphones et de l'Internet mobile
- 2008 = Le terme Big data entre dans le dictionnaire
- 2009 = 1,5 milliard d'applications ont été téléchargées via le magasin iTunes d'Apple
- 2010 = Les iPad et tablettes numériques tactiles d'Appel sont mis en vente
- 2011 = Le commerce en ligne aurait généré 1000 milliards de dollars de chiffre d'affaires
- 2012 = Les Google Glass entrent en phase de test
- 2014 = 1 milliard de sites Internet sont répertoriés
- 2016/2018 = La société CAMBRIGDE ANALYTICA est impliquée pour avoir influencé le vote de plusieurs centaines de milliers d'américains lors des élections présidentielles de novembre 2016

1. Introduction :

1.4 Une réglementation européenne sur les données des personnes physiques…

Une réglementation européenne unique : le RGPD

Entrée en application en droit interne : 25 mai 2018

- Le règlement (UE) 2016/679 du 27 avril 2016 pour la protection des données personnelles (RGPD) est **entré en application le 25 mai 2018**. Il harmonise depuis cette date les règlementations relatives aux données personnelles au sein des Etats membres de l'Union européenne.

Portée européenne et internationale

- Il a aussi une **portée internationale** puisqu'ils s'applique aux entreprises établies hors de l'Union européenne, dès lors qu'elles proposent des produits ou services aux résidents européens.

Modèle contraignant

Ce règlement vient créer de **nouvelles obligations pour les entreprises** et **renforce les droits des personnes**.

1. Introduction :

1.4 … Une réglementation qui concerne tout le monde

Un champ d'application et un champ territorial très larges :

Tout organisme quelle que soit sa taille (collectivité, administrations, entreprise, y compris comités d'entreprise, associations…), qui traite des données à caractère personnel, quels que soient son pays d'implantation et son activité, est concerné.

- Le RGPD s'applique à **toute organisation, publique ou privée, qui traite des données personnelles** pour son propre compte ou pour le compte d'autrui (sous-traitant), dès lors :

- (hyp. 1) **qu'elle est établie sur le territoire de l'Union européenne ;**
- (hyp. 2) **que son activité cible directement des résidents européens.**

Exemple 1 : une société établie en France, qui exporte l'ensemble de ses produits en dehors de l'Union européenne doit respecter le RGPD.

Exemple 2 : une société établie en dehors de l'Union européenne, proposant un site de e-commerce en français et livrant des produits en France doit respecter le RGPD.

La protection des données personnelles en pratique…

2. Définitions

- *2. 1 – Données à caractère personnel – Quizz données personnelles*
- *2.2 – Données sensibles*
- *2.3 – Traitement de données*
- *2.4 – Fichier*
- *2.5 – Responsable de traitement et sous-traitant*
- *2.6 – Destinataire des données et tiers*

2. Définitions :

2.1 Données à caractère personnel

Données à caractère personnel (art. 4 du RGPG) :

« Toute information se rapportant à une **personne physique identifiée ou identifiable** (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique **qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant**, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Loi de 1978 modifiée (art. 2) : « (…) toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. […] ».

2. Définitions :

2.1 Quizz données personnelles

Parmi ces exemples, lesquels sont des données à caractère personnel ?

- Empreinte digitale OUI / NON
- Les nom, prénom, date de naissance OUI / NON
- Numéro de carte bancaire OUI / NON
- Matricule OUI / NON
- Numéro de Sécurité Sociale OUI / NON
- Photographie OUI / NON
- Enregistrement audio de la voix OUI / NON
- Adresse email OUI / NON
- RIB/IBAN OUI / NON
- Numéro de téléphone OUI / NON
- Numéro de dossier client OUI / NON
- Adresse IP (ex. 225.564.74.12) OUI / NON
- Plaque d'immatriculation OUI / NON

2. Définitions :

2.2 Quizz données sensibles

Parmi ces exemples, lesquels sont des données sensibles ?

- Empreinte digitale, autres données biométriques OUI / NON
- Les nom, prénom, date de naissance OUI / NON
- Numéro de carte bancaire OUI / NON
- Opinions politiques ou appartenance syndicale OUI / NON
- Numéro de Sécurité Sociale OUI / NON
- Convictions religieuses ou philosophiques OUI / NON
- Enregistrement audio de la voix OUI / NON
- Adresse email OUI / NON
- RIB/IBAN OUI / NON
- Origine raciale ou ethnique OUI / NON
- Données de santé OUI / NON
- Données génétiques OUI / NON
- Vies sexuelle ou orientation sexuelle OUI / NON

2. Définitions :

2.2 Données sensibles (principe d'interdiction des traitements de ces données sauf dérogations du texte)

Constituent des catégories particulières de données à caractère personnel (art. 9 du RGPD et art. 8 LOI du 6 janvier 1978 modifiée)

- l'origine raciale ou ethnique,
- les opinions politiques,
- les convictions religieuses ou philosophiques ou l'appartenance syndicale,
- le traitement des données génétiques,
- des données biométriques aux fins d'identifier une personne physique de manière unique,
- des données concernant la santé,
- des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

2. Définitions :

2.3 Traitement de données (toute manipulation de données)

Traitement de données (art. 4 du RGPD)

« **Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données** ou des ensembles de données à caractère personnel, telles que 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** ».

Les traitements sont utilisés par l'organisme pour répondre à différents objectifs (finalités), liés soit au fonctionnement de la structure (ex. gestion RH, gestion financière et comptable), soit à ses missions ou son cœur de métier (ex. gestion clients et prospects, fraude, etc.).

2. Définitions :

2.4 Constitue un fichier

Fichier (art. 4 du RGPD)

« **Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés**, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

Exemple : Un tri de CV ou de cartes de visite selon un ordre logique (alphabétique, thématique, couleur, taille…) constitue un fichier, de même qu'un simple classeur ou un tableur Excel.

Peu importe le support, qu'il soit physique ou dématérialisé.

2. Définitions :

2.5 Responsable de traitement et sous-traitant

Responsable de traitement (art. 4 du RGPD)

« **La personne** physique ou morale, l'autorité publique, le service ou un autre organisme **qui**, seul ou conjointement avec d'autres, **détermine les finalités et les moyens** du traitement ».

C'est celui qui engage sa responsabilité en cas de traitements non conforme de données.

Sous-traitant (art. 4 du RGPD)

« **La personne** physique ou morale, l'autorité publique, le service ou un autre organisme **qui traite des données à caractère personnel pour le compte du responsable du traitement** ».

2. Définitions :

2.6 Destinataire des données et tiers

Destinataire des données (art. 4 du RGPD)

« **La personne** physique ou morale, l'autorité publique, le service ou tout autre organisme **qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers**. […] ».

Le destinataire d'un traitement de données est donc toute personne susceptible de recevoir communication de données à caractère personnel (autre que la personne concernée) : responsable du traitement, sous-traitant, tiers ou personnes qui reçoivent ou sont autorisés (habilitées) à traiter les données…

Tiers (art. 4 du RGPD)

« **Une personne** physique ou morale, une autorité publique, un service ou un **organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes** qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont **autorisées à traiter les données à caractère personnel** ».

2. Définitions :

2.7 Données génétiques, biométriques et de santé

Données génétiques (art. 4 du RGPD)

« Données (…) relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ».

Données biométriques (art. 4 du RGPD)

« Données (…) résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques ».

Données de santé (art. 4 du RGPD)

« Données concernant la santé, (…) relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé [d'une] personne ».

La protection des données personnelles en pratique…

3. Principes clés du RGPD

- *3. 1 – Quasi fin du contrôle a priori de la CNIL*
- *3.2 – Responsabilisation des acteurs ou principe d'accountability :*
  - *registre des traitements*
  - *DPO/ DPD*
- *3.3 – Obligations de sécurité renforcée : Privacy and security by design*
- *3.4 – Notification des failles de sécurité*

3. Principes clés du RGPD :

3.1 Quasi fin du contrôle *a priori* de la CNIL

Fin des formalités préalables remplacées par une obligation générale de conformité :

La Loi de 1978 Informatique et Libertés mettait en place des obligations déclaratives préalables auprès de la CNIL. **Depuis le 25 mai 2018, les formalités auprès de la CNIL ont quasiment toutes disparues.**

La LIL3 maintient toutefois le principe d'une autorisation préalable pour certains traitements mis en œuvre pour le compte de l'Etat et concernant :

- La sûreté de l'Etat, la défense ou la sécurité publique.
- La prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.
- Les traitements de données génétiques ou de données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes…

3. Principes clés du RGPD :

3.2 Responsabilisation des acteurs ou principe d'accountability

Nouvelles obligations du RGPD : Démontrer sa conformité de façon dynamique et continue

Les formalités déclaratives ou de conformité aux normes CNIL (Normes Simplifiées, Autorisations Uniques, etc.) **disparaissent en contrepartie de l'obligation pour les responsables de traitement de mettre en œuvre des mécanismes et des procédures internes, permettant de démontrer le respect des règles relatives à la protection des données** (renversement de l'établissement de la preuve de la conformité).

Principe essentiel : Documenter la preuve de sa conformité !

3. Principes clés du RGPD :

3.2 Responsabilisation des acteurs ou principe d'accountability

Nouvelles obligations du RGPD : Registre des traitements

Registre des activités de traitement : obligatoire pour les organismes comptant au moins 250 employés (art. 30).

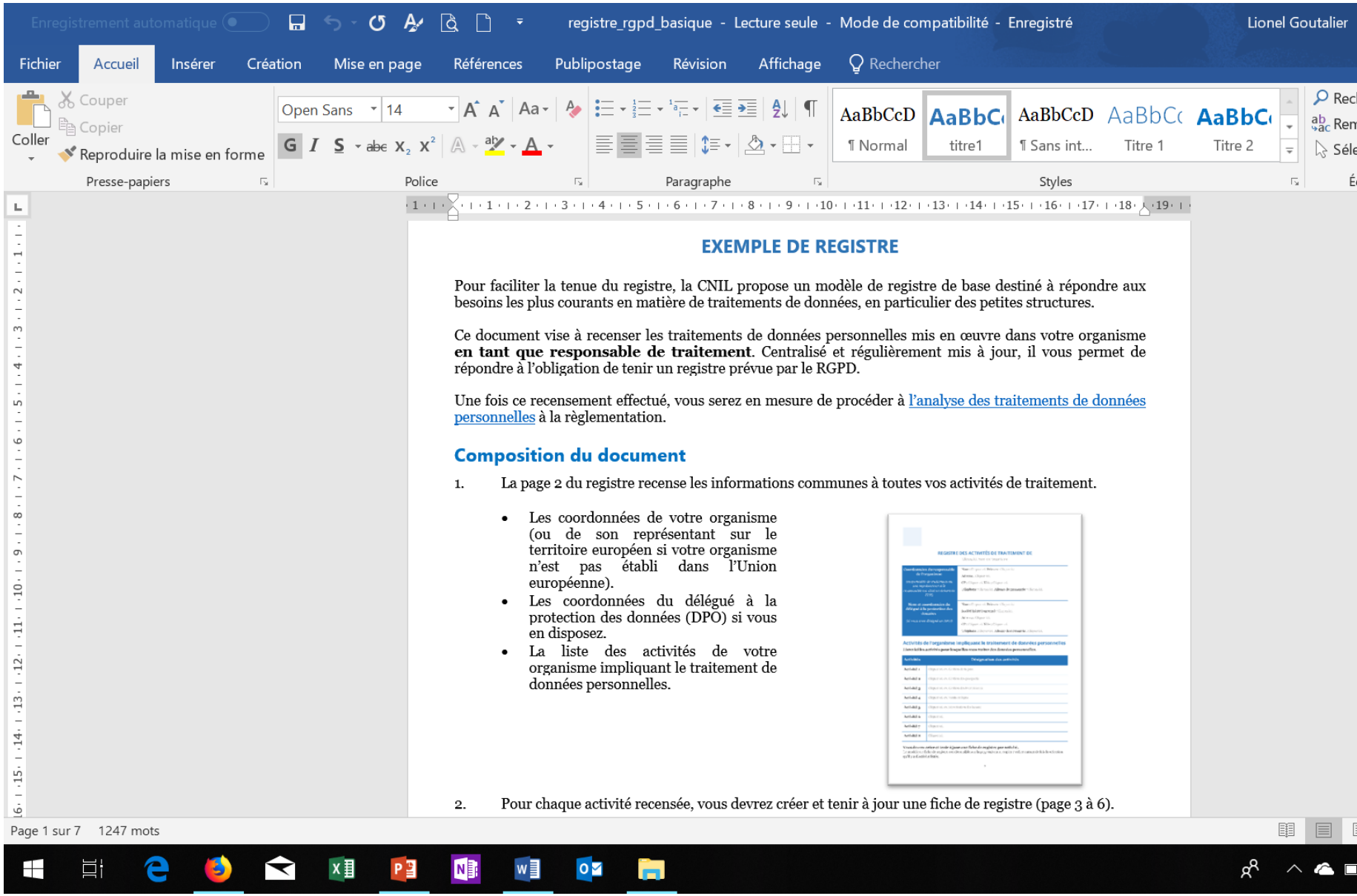
Pas d'obligation au-dessous de ce seuil, sauf :

- **si le traitement comporte un risque pour les droits et libertés des personnes** (ex. : systèmes de géolocalisation, vidéosurveillance, etc.),
- **si le traitement n'est pas occasionnel** (ex. : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.),
- **ou encore, en fonction des catégories de données** (données sensibles, exemple : données de santé, condamnations pénales, infractions, etc.).

Recommandations CNIL :

Exemple de registre simplifié

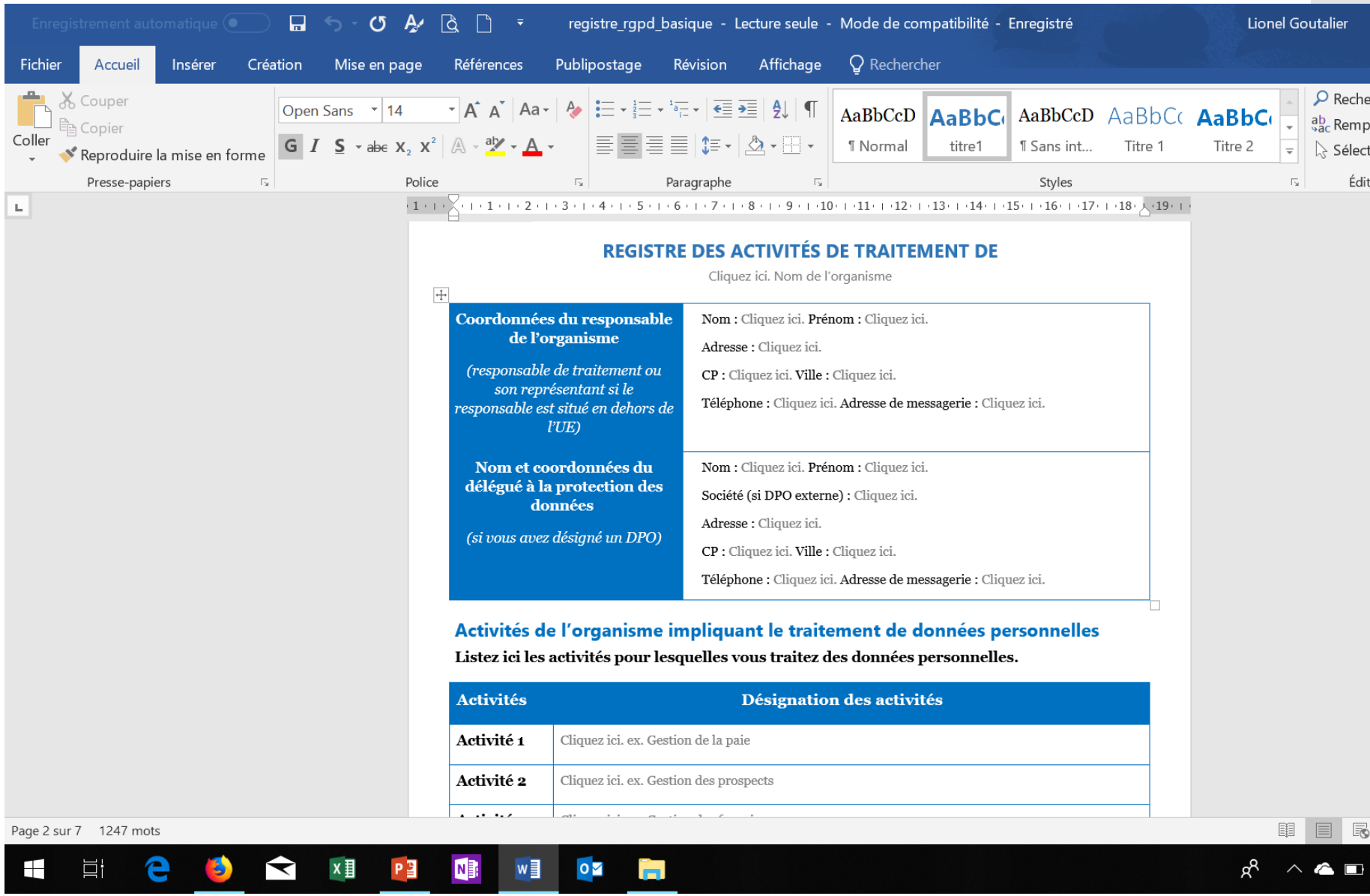
source : www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement



Recommandations CNIL :

Exemple de registre simplifié

source : www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement



registre_rgpd_basique - Lecture seule - Mode de compatibilité - Enregistré — Lionel Goutalier

Fichier | Accueil | Insérer | Création | Mise en page | Références | Publipostage | Révision | Affichage | Rechercher

Coller | Couper | Copier | Reproduire la mise en forme — Presse-papiers

Open Sans 14 — Police

Paragraphe

¶ Normal | titre1 | ¶ Sans int... | Titre 1 | Titre 2 — Styles

REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Cliquez ici. Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	Nom : Cliquez ici. Prénom : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	Nom : Cliquez ici. Prénom : Cliquez ici. Société (si DPO externe) : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.

Activités de l'organisme impliquant le traitement de données personnelles

Listez ici les activités pour lesquelles vous traitez des données personnelles.

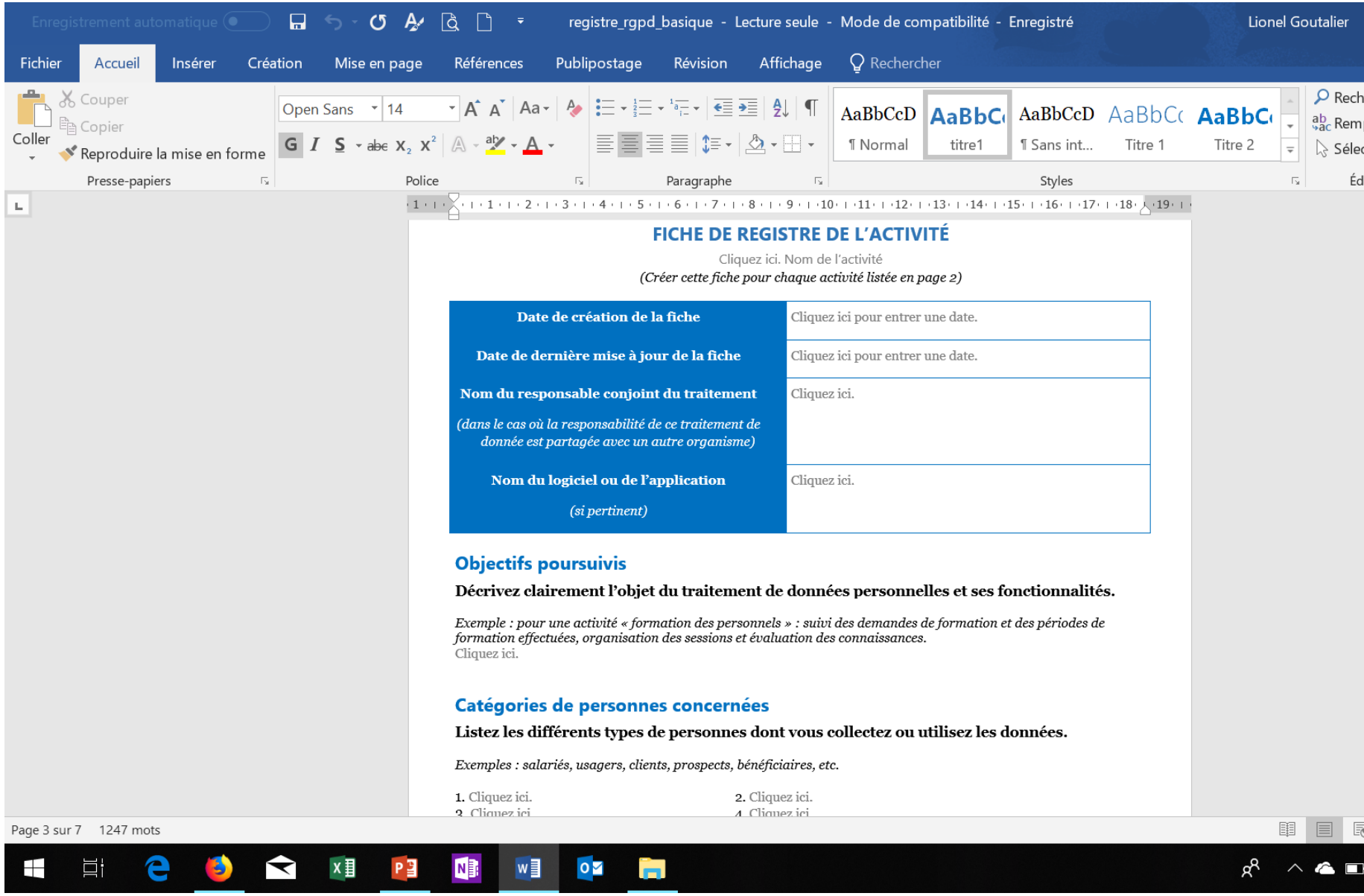
Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects

Page 2 sur 7 1247 mots

Recommandations CNIL :

Exemple de registre simplifié

source : www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement



registre_rgpd_basique - Lecture seule - Mode de compatibilité - Enregistré — Lionel Goutalier

Fichier | Accueil | Insérer | Création | Mise en page | Références | Publipostage | Révision | Affichage | Rechercher

Coller | Couper | Copier | Reproduire la mise en forme — Presse-papiers

Open Sans | 14 — Police

Paragraphe

¶ Normal | titre1 | ¶ Sans int... | Titre 1 | Titre 2 — Styles

FICHE DE REGISTRE DE L'ACTIVITÉ

Cliquez ici. Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.
Cliquez ici.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

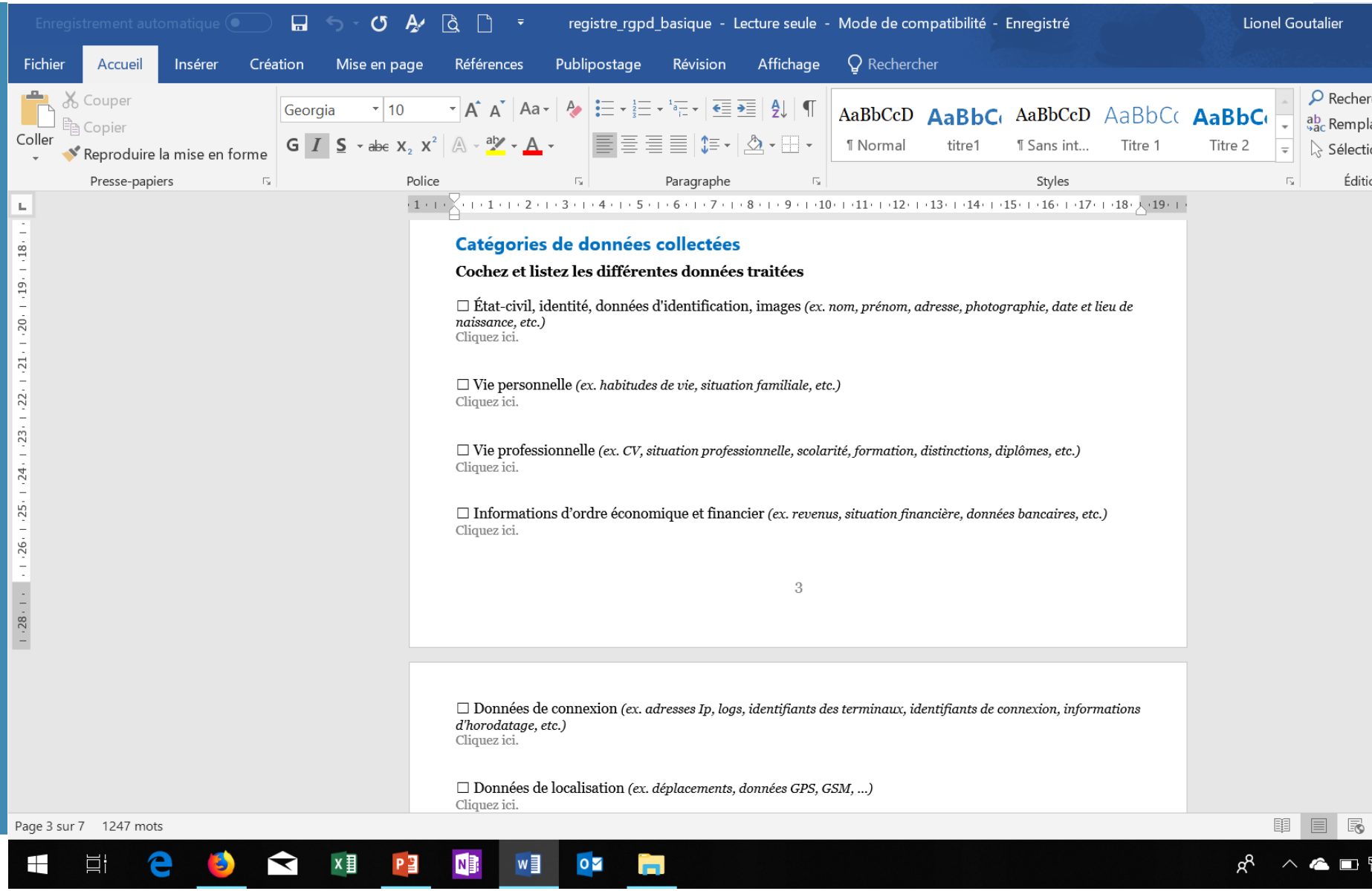
1. Cliquez ici.
2. Cliquez ici.
3. Cliquez ici.
4. Cliquez ici.

Page 3 sur 7 1247 mots

Recommandations CNIL :

Exemple de registre simplifié

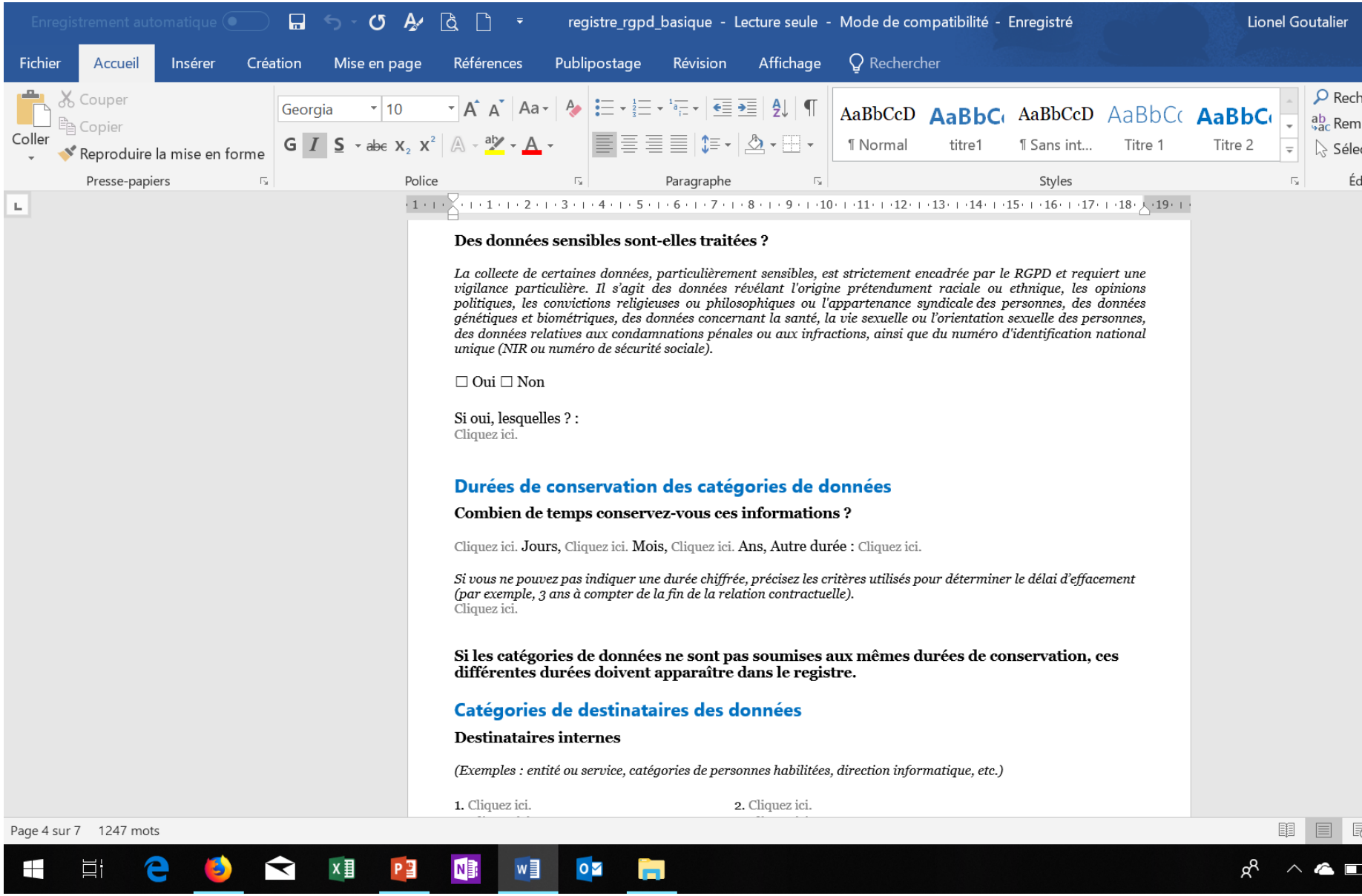
source : www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement



Recommandations CNIL :

Exemple de registre simplifié

source : www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement



3. Principes clés du RGPD :

3.2 Responsabilisation des acteurs ou accountability

Désignation d'un délégué à la protection des données (DPO / DPD)

Dans certains cas, le responsable du traitement et le sous-traitant désignent « *en tout état de cause* » un DPO (art. 37).

La présence d'un DPO est obligatoire dans 3 cas :

1. Dans le cas des autorités publiques ou organismes publics,
2. Si les traitements consistent en des opérations qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées
3. Si les activités consistent en un traitement à grande échelle de catégories particulières de données sensibles et de données à caractère personnel relatives à des condamnations pénales et à des infractions

3. Principes clés du RGPD :

3.2 Responsabilisation des acteurs ou accountability

Le DPO est désigné sur la base de ses **qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions** (art. 37) : **information, conseil, contrôle, coopération avec la CNIL, vérification des analyses d'impact,** etc. (art. 39).

- Soit : **DPO interne :** membre du personnel du responsable du traitement ou du sous-traitant,
- Soit : **DPO externe :** sur la base d'un contrat de service.
- Eventuellement : **DPO mutualisé,** pour les groupes d'entreprises.

Le DPO doit bénéficier d'une certaine indépendance vis-à-vis du responsable de traitement et ne doit pas se trouver en situation de conflit d'intérêts dans l'exercice de sa mission. Par exemple, le maire d'une commune ne peut être DPO (*Rép. min., n° 05775 : JO Sénat, 27 sept. 2018, p. 4914*), pas plus que le dirigeant ou les membres exécutifs d'une entreprise.

3. Principes clés du RGPD :

3.3 Obligations de sécurité renforcée : Privacy and security by design

(AIPD ou *PIA = Privacy Impact Assessment)*

Nouvelles obligations du RGPD : Sécurité des données

Privacy and security by design :

le RGPD impose à tout organisme effectuant des traitements de données de prendre toutes **les garanties et mesures de sécurité techniques et organisationnelles adéquates pour assurer la protection des données**, ceci **dès la conception du traitement**.

Analyse d'impact relative à la protection des données :

Lorsqu'un type de traitement, en particuliers par le **recours à de nouvelles technologies**, et **compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques**, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

3. Principes clés du RGPD :

3.4 Notification des failles de sécurité

Notification des violations et failles de sécurité :

Notification des failles de sécurité (art. 33 et 34 du RGPD) :

En corollaire des obligations de sécurité, le RGPD impose désormais à tout responsable de traitement de procéder à **la notification à l'Autorité de contrôle (CNIL) de toute violation de donnée à caractère personnel dans les meilleurs délais** et si possible, **au plus tard dans les 72 heures** après en avoir pris connaissance.

Et lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

La protection des données personnelles en pratique…

4. Fondamentaux des données et traitements

- *4. 1 – Loyauté et transparence*
- *4.2 – Licéité : les six bases juridiques du traitement*
- *4.3 – Renforcement des droits des personnes*

4. Fondamentaux des données et traitements :

4.1 Loyauté et transparence (art. 5 du RGPD)

Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes soient effacées ou rectifiées sans tarder (exactitude);

e) conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; (…)

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

Recommandations CNIL : https://www.cnil.fr/cnil-direct/question/1308

Le consentement n'est qu'une des modalités de licéité des traitement

4. Fondamentaux des données et traitements :

4.2 Licéité : les six bases juridiques du traitement (art. 6 du RGPD)

Le traitement n'est licite que si, et dans la mesure où, au moins une des 6 conditions suivantes est remplie :

a) Consentement libre, spécifique et éclairé pour une ou plusieurs finalités,

b) Nécessaire à l'exécution d'un contrat ou de mesures précontractuelles,

c) Nécessaire au respect d'une obligation légale à laquelle est soumis le responsable de traitement,

d) Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique,

e) Exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement,

f) Nécessaire aux fins d'intérêts légitimes poursuivis par le responsable de traitement.

4. Fondamentaux des données et traitements :

4.3 Renforcement des droits des personnes

Droits des personnes:

Le RGPD comporte une obligation générale de faciliter l'exercice des droits (fourniture d'une information concise, transparente, compréhensible et aisément accessible – art. 12).

Renforcement des droits existants :

- **Information adaptée aux enfants** (en termes clairs et simples),
- **Information renforcée** (finalités – base juridique – coordonnées du DPO/DPD – durée de conservation, transferts hors UE – art. 13 & 14),
- **Droit d'accès précisé** (art. 15),
- **Droit de rectification maintenu** (art. 16),
- **Droit à l'effacement confirmé** (ou « droit à l'oubli » – art. 17),
- **Droit d'opposition renforcé** (c'est au responsable de traitement de prouver l'existence d'un intérêt légitime supérieur à celui de la personne concernée – art. 21).

4. Fondamentaux des données et traitements :

4.3 Renforcement des droits des personnes

Droits des personnes:

Le RGPD renforce les droits des personnes en intégrant de nouveaux droits spécifiques tels que le droit à la portabilité ou encore le droit à la limitation des traitements.

Droits nouveaux :

- **Droit à la limitation du traitement** (art. 18),
- **Droit à la portabilité des données** (art. 20).

Toutefois, l'ensemble de ces droits, y compris les droits nouveaux ne sont pas absolus.

4. Fondamentaux des données et traitements :

4.3 Renforcement des droits des personnes

Droit à la portabilité : nouveau droit permettant à toute personne :

- **De récupérer** les données la concernant qu'elle a fournies à un responsable de traitement dans un format structuré, couramment utilisé et lisible par machine
- **De les transmettre** à un autre responsable de traitement ou de demander la transmission directement, si possible techniquement

Conditions :

- Le traitement se fonde sur le consentement de la personne ou sur un contrat,
- Le traitement est effectué à l'aide de procédés automatisés ,

Donnée concernées:

- Données fournies sciemment et activement par la personne,
- Données générées par son activité et données observées,

Données exclues : Données anonymes, données déduites ou dérivées.

La protection des données personnelles en pratique…

5. Sanctions, rôle et évolution de la CNIL

- *5. 1 – Des sanctions financières accrues au titre du RGPD*
- *5.2 – Rôle et évolution de la CNIL*
- *5.3 – Contrôles et sanctions de la CNIL*

5. Sanctions, rôle et évolution de la CNIL :

5.1 Des sanctions financières accrues au titre du RGPD

Sanctions financières en fonction de la gravité des violations au RGPD :

Amendes administratives (qui n'excluent pas des sanctions pénales)

1. **Violations des dispositions relatives aux obligations du responsable de traitement ou du sous-traitant :**

Elles peuvent s'élever jusqu'à 10 M€ ou, dans le cas d'une entreprise, jusqu'à 2% du CA annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

2. **Violations des dispositions relatives aux droits des personnes :**

Elles peuvent s'élever jusqu'à 20 M€ ou, dans le cas d'une entreprise, jusqu'à 4% du CA annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

5. Sanctions, rôle et évolution de la CNIL :

5.2 Rôle et évolution de la CNIL

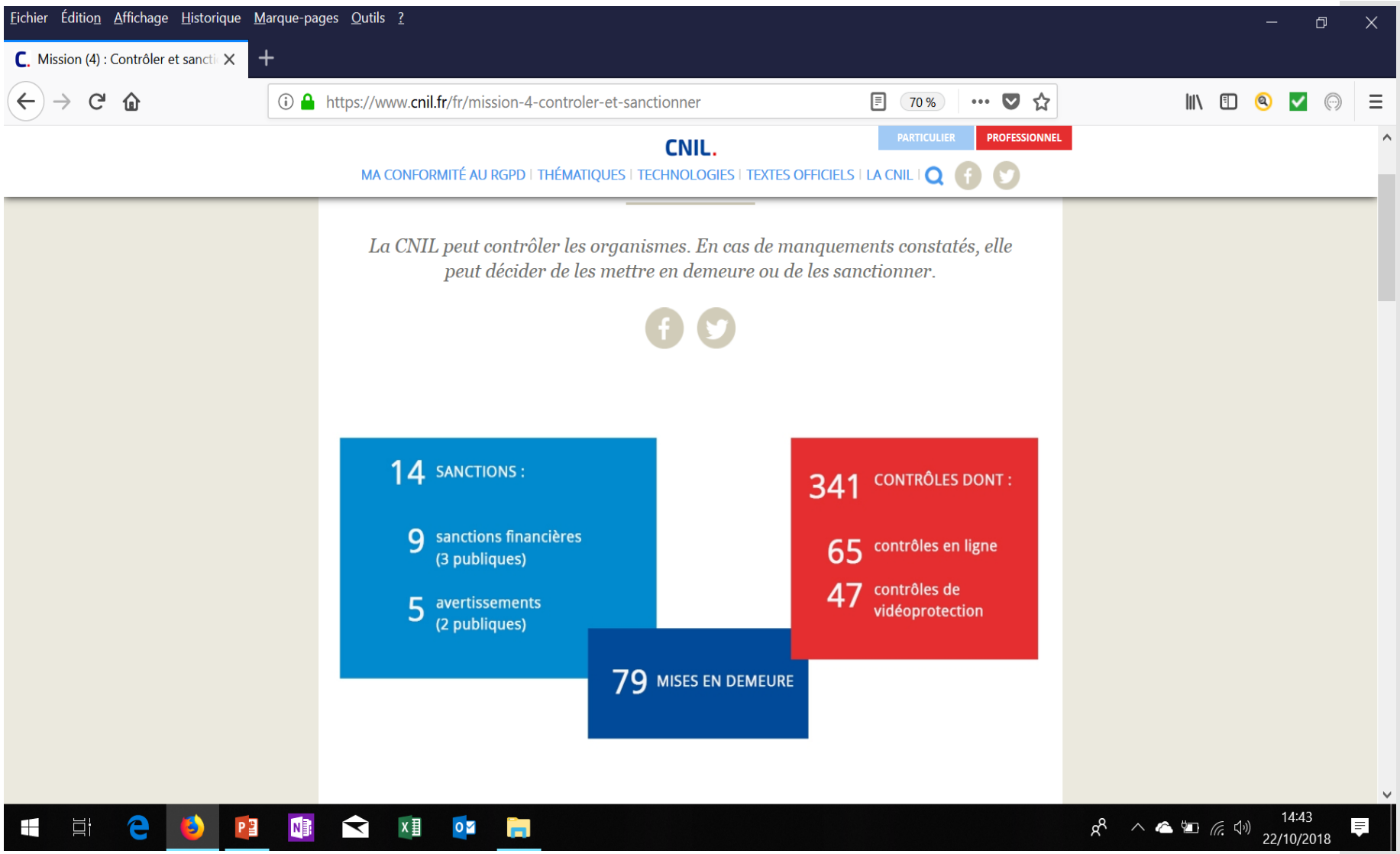
Une autorité indépendante : La CNIL

Renforcement et évolution du rôle de la CNIL

- **Instance de coopération internationale :** représentation de la France au G29 (groupe des CNIL européennes) et autorité de contrôle chef de file en France pour les traitements transfrontaliers
- **Informer, protéger les droits :** toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits en lui adressant une plainte.
- **Autorité de régulation pour la mise en conformité :** conseils, certifications, labels, packs, etc. ; elle est l'interlocuteur des responsables de traitement et des DPO/DPD.
- **Activité d'innovation et de prospective, la CNIL s'intéresse aux signaux faibles et aux sujets émergents**
- **Contrôle et sanctions :** la CNIL peut contrôler les organismes et en cas de manquements constatés, elle peut décider de les mettre en demeure ou de les sanctionner.

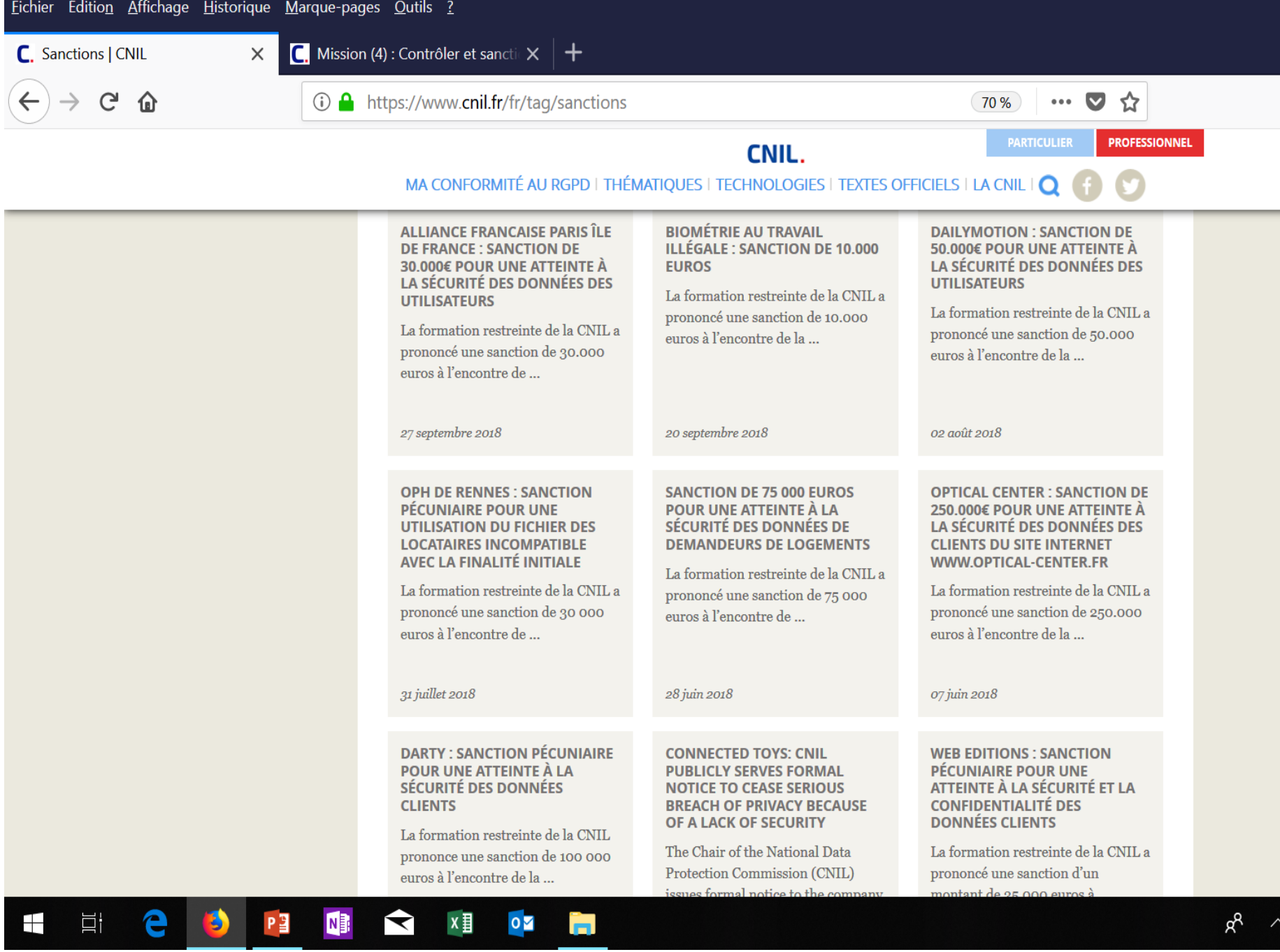
5. Sanctions, rôle et évolution de la CNIL :

5.3 Contrôles et sanctions de la CNIL



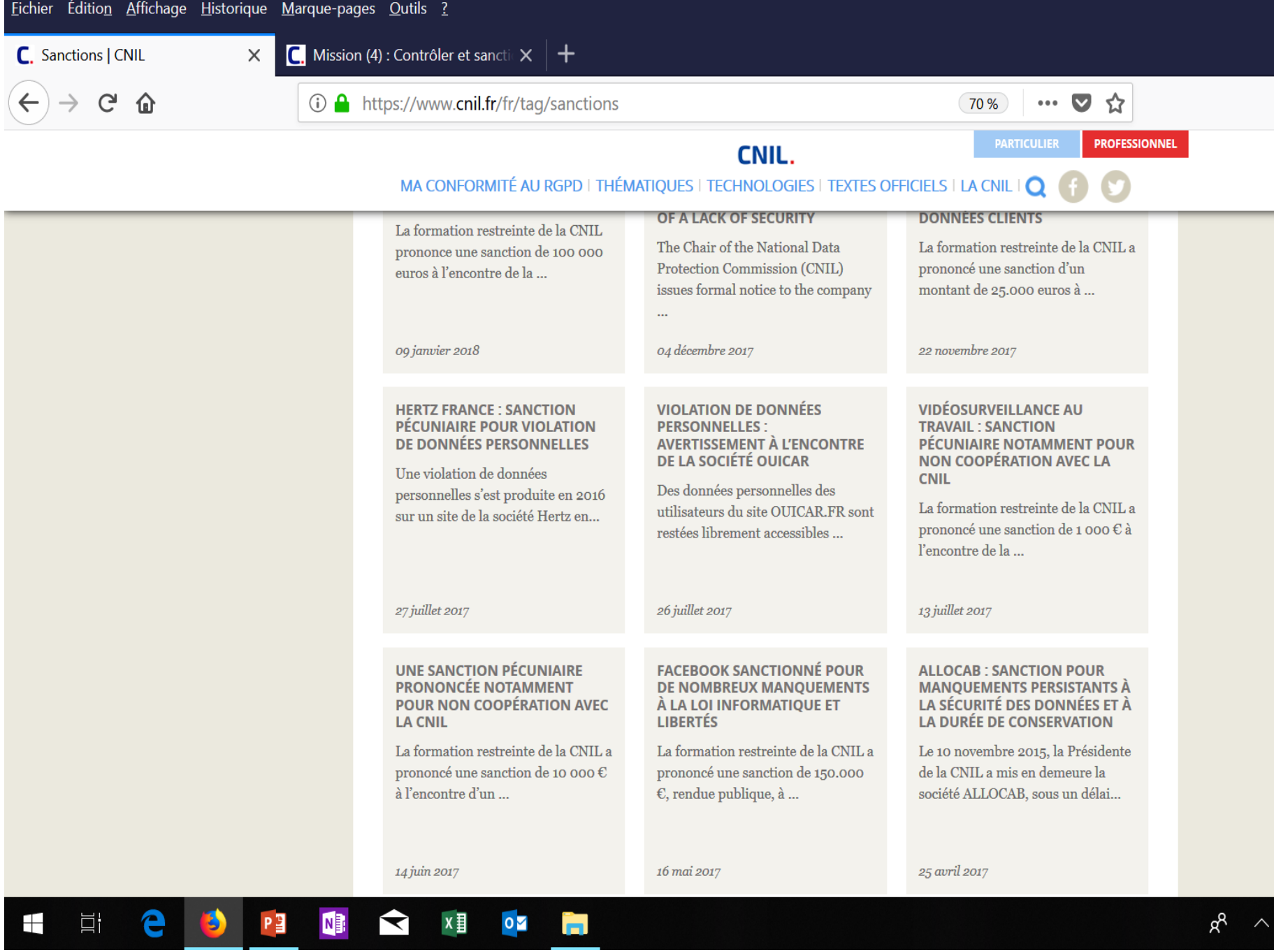
5. Sanctions, rôle et évolution de la CNIL :

5.3 Contrôles et sanctions de la CNIL



5. Sanctions, rôle et évolution de la CNIL :

5.3 Contrôles et sanctions de la CNIL



La protection des données personnelles en pratique…

6. Incidences sur la relation client

- *6. 1 – Information et transparence*
- *6.2 – Consentement (opt-in / opt-out)*
- *6.3 – Droits de personnes*
- *6.4 – Définition d'une politique de confidentialité des données (privacy policy)*

6. Incidences sur la relation client

6.1 Information et transparence

Principaux impacts du RGPD sur la relation client :

Principes : Information et transparence

- Le RGPD fixe une obligation générale de transparence (fourniture d'une **information concise, transparente, compréhensible et aisément accessible** – art. 12, 13 et 14) :

Les finalités des traitements (relation contractuelle, commerciale, profiling… gestion du personnel…) doivent figurer dans les mentions d'informations (CGU/CGV), de même que son fondement juridique, les destinataires, les durées de conservations, les droits des personnes, les points de contact vers qui s'adresser, etc.

L'ensemble de ces informations qui sont à porter à la connaissance du public conduit, en pratique, à mettre en place une **politique de confidentialité ou de protection des données.**

6. Incidences sur la relation client

6.1 Information et transparence

Principaux impacts du RGPD sur la relation client :

Quand informer ?

- **En cas de collecte directe des données :** au moment du recueil des données (formulaire, achat en ligne, souscription d'un contrat, ouverture d'un compte bancaire) ou lorsqu'elles sont recueillies via des dispositifs ou des technologies d'observation (vidéosurveillance, analyse de la navigation sur Internet, géolocalisation et *wifi analytics/tracking* pour la mesure d'audience, etc.) ;

- **En cas de collecte indirecte des données personnelles :** (données récupérées auprès de partenaires commerciaux, de *data brokers*, de sources accessibles au public ou d'autres personnes), dès que possible (notamment lors du 1er contact) et, au plus tard, dans le délai d'1 mois (sauf exceptions),

- **En cas de modification substantielle ou d'événement particulier :** par exemples : nouvelle finalité, nouveaux destinataires, changement dans les modalités d'exercice des droits, violation de données…

6. Incidences sur la relation client

6.1 Information et transparence

Principaux impacts du RGPD sur la relation client :

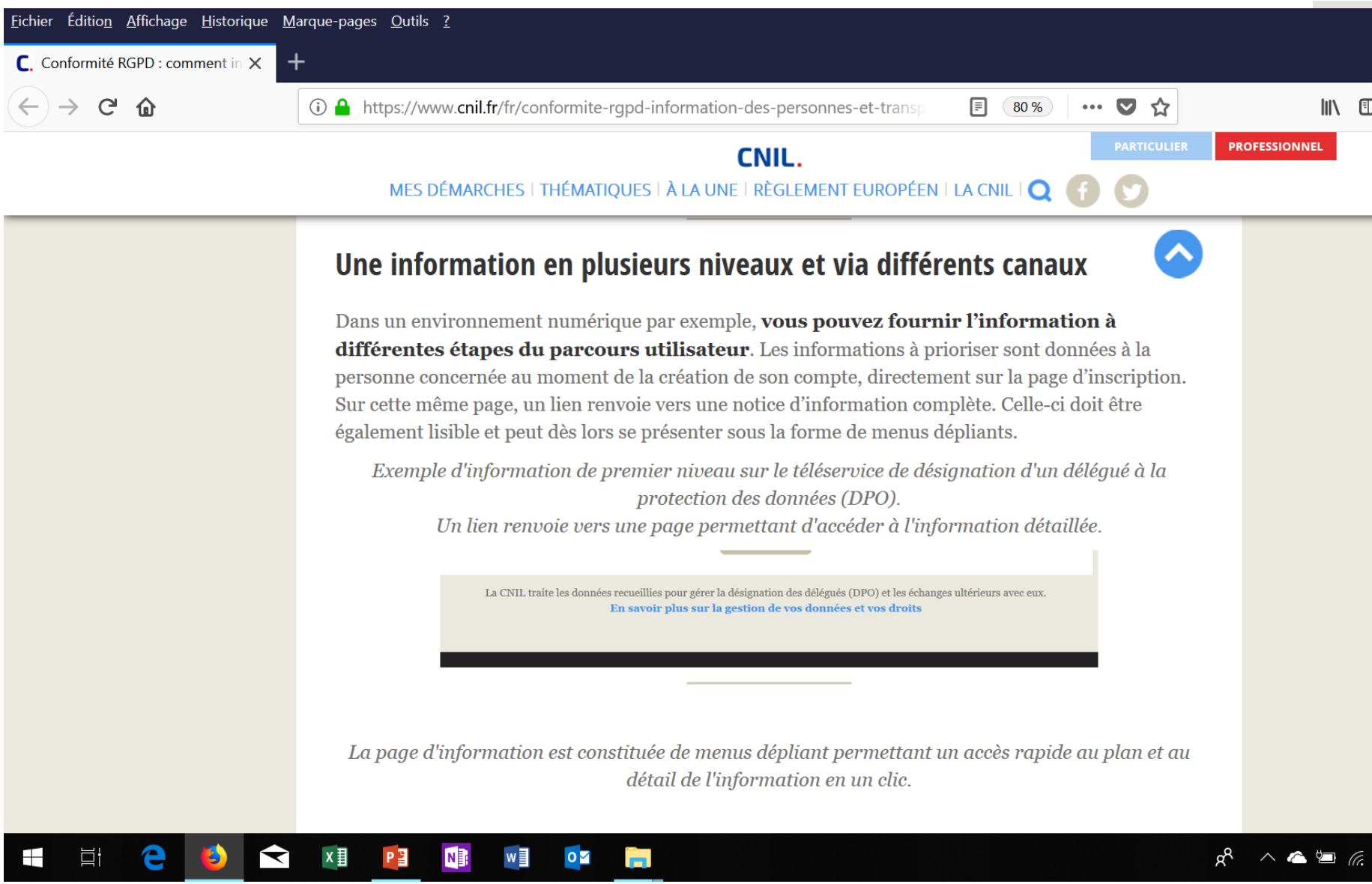
Sous quelle forme ?

- L'information délivrée doit être **concise, transparente, compréhensible et aisément accessible**, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant (art. 12 du RGPD).
- Les informations sont fournies **par écrit ou par d'autres moyens y compris**, lorsque c'est approprié, **par voie électronique**.

Recommandations CNIL : https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparenc

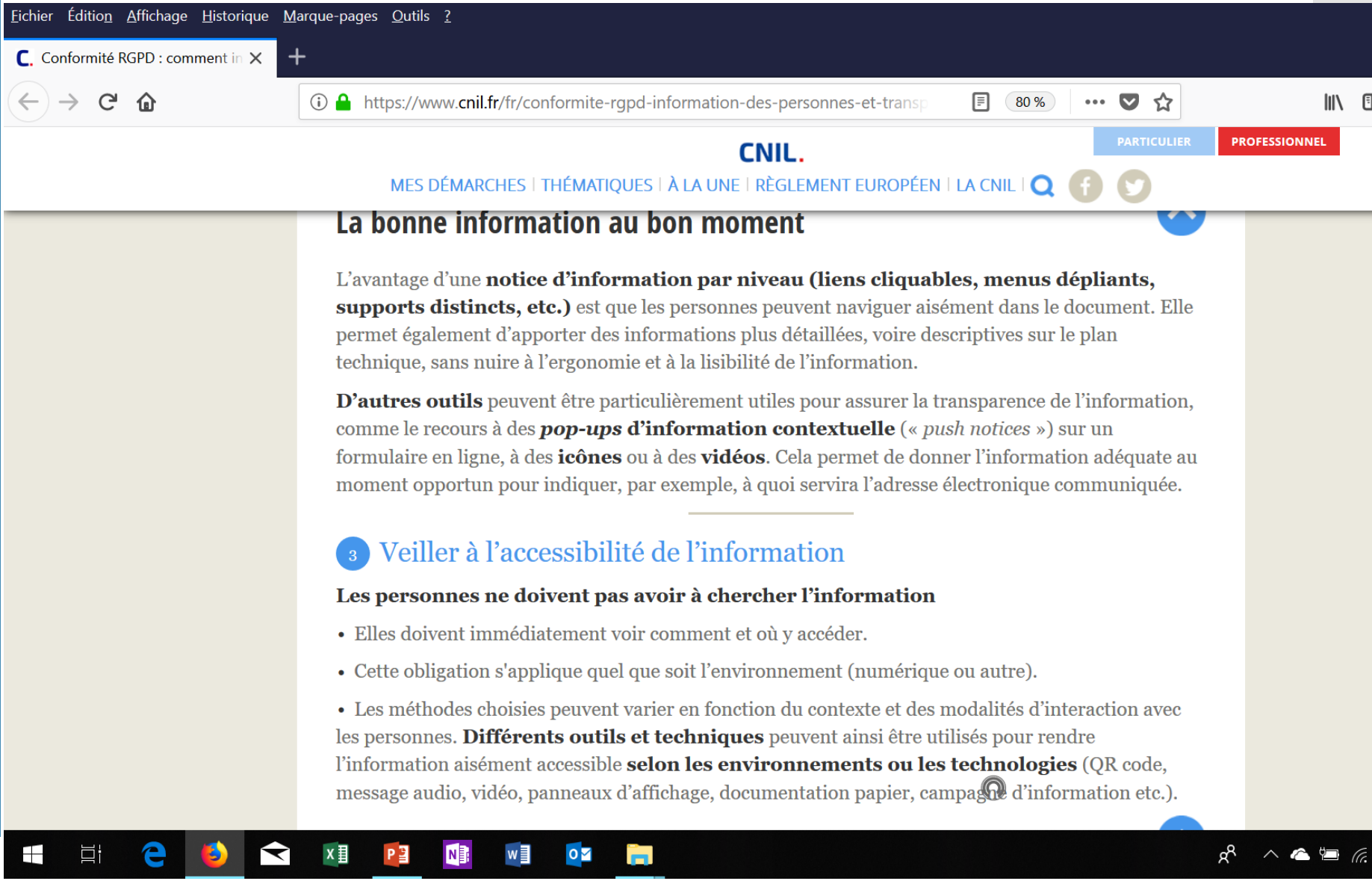
6. Incidences sur la relation client

Recommandations CNIL : https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence



6. Incidences sur la relation client

Recommandations CNIL : https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence



6. Incidences sur la relation client

6.2 Consentement

Principaux impacts du RGPD sur la relation client :

Le consentement

- Le RGPD implique **d'obtenir le consentement préalable, explicite, libre, spécifique, univoque et éclairé** (sur la finalité du traitement) de la part de la personne concernée et de revoir la gestion des opt-in et des opt-out.

Le consentement doit être recueilli au moment de la collecte de données, via les formulaires de recueil de données (abonnement, souscription de service, inscription e-boutique, ouverture de compte…).

Le consentement peut être retiré à tout moment. Lorsque la collecte des données personnelles repose sur ce fondement, l'information de la personne concernée sur sa faculté de retirer son consentement doit être portée à sa connaissance au titre de l'exercice de ses droits.

Exemple, en matière de prospection commerciale : mettre en place un lien de désinscription du type « *Pour vous désinscrire de la newsletter, cliquez ici* ».

6. Incidences sur la relation client

6.2 Consentement

Principaux impacts du RGPD sur la relation client :

Définitions opt-in / opt-out

Selon le mode de prospection (email, téléphone ou sms) utilisé, les personnes sollicitées doivent au préalable avoir donné leur accord (consentement) pour recevoir des messages (opt-in) ou ne pas avoir exprimé leur refus (opt-out).

- **L'opt-in,** c'est obtenir l'accord préalable du destinataire de la publicité : s'il n'a pas dit « oui », c'est « non ». C'est le cas pour envoyer de la publicité « B2C » (du professionnel au consommateur) par email, SMS, MMS, automate d'appels ou fax.

- **L'opt-out,** c'est le contraire, lorsque le destinataire de la publicité ne s'est pas opposé : s'il n'a pas dit « non », c'est « oui ». C'est le cas pour la publicité « B2B » (de professionnel à professionnel) adressée par email et « B2C » adressée par voie postale ou par téléphone.

Sources : https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement - (FICHE 2 : Améliorez et maîtrisez votre relation client)

6. Incidences sur la relation client

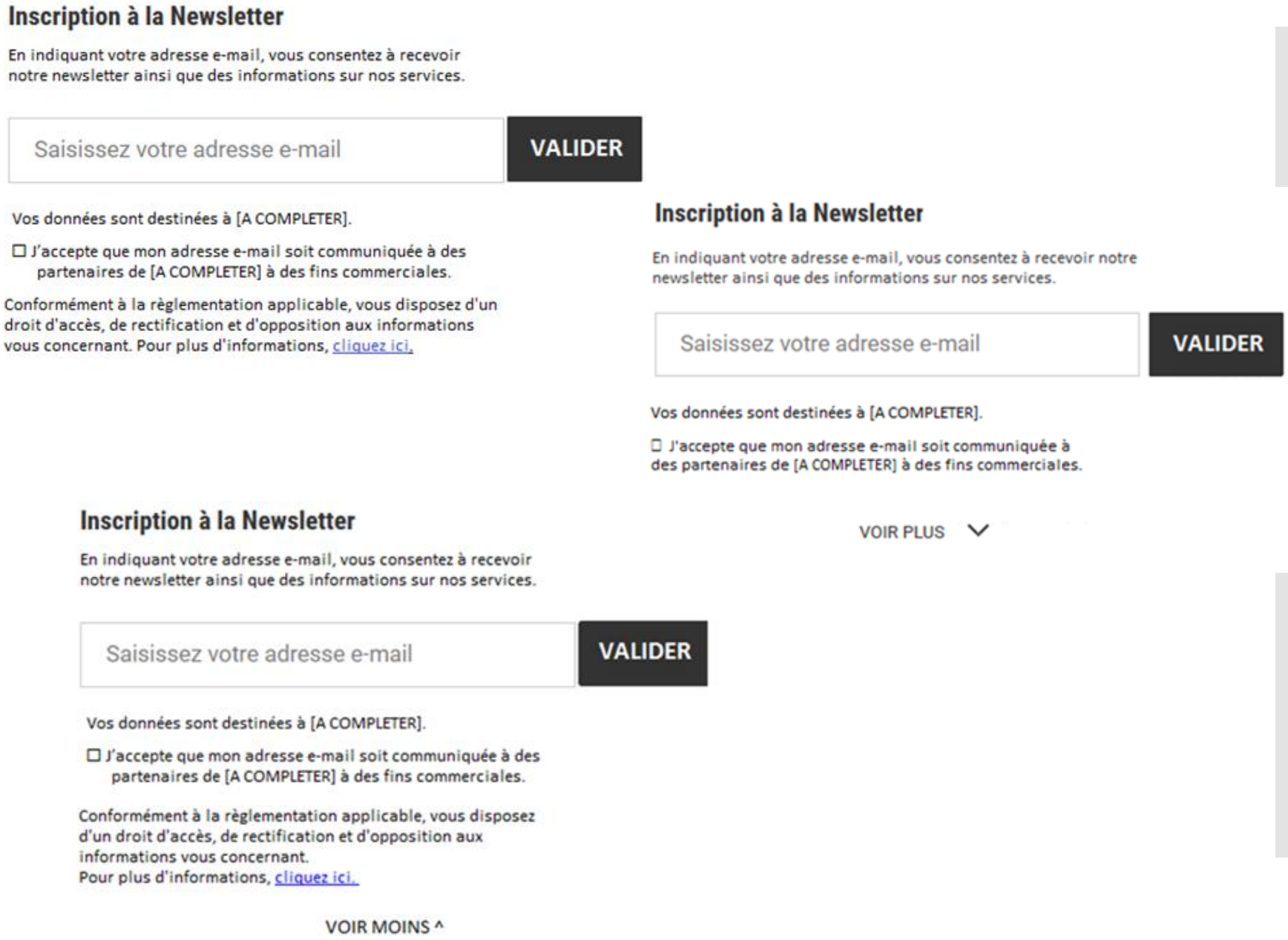
6.2 Consentement

Gestion des opt-in (consentement préalable)

- **L'opt-in** doit être recueilli pour les canaux **email** et **SMS/MMS, automate d'appels ou fax** (les sollicitations par téléphone ou par courrier postal sont soumises à l'opt-out),
- **L'opt-in** doit être recueilli pour chaque canal indépendamment,
- **L'opt-in** doit systématiquement s'exprimer sous forme de cases à cocher par le client (**pas de case pré-cochée**),
- **L'opt-in** doit être exprimé de façon explicite et volontaire et ne se déduit pas de l'acceptation des CGV ou des CGU,
- **L'opt-in** doit être conservé : en cas de litige, il faut pouvoir justifier du consentement de la personne. La conservation papier ou numérique du formulaire d'abonnement signé permet de répondre à cette obligation,
- **L'opt-in** doit être exprimé en autant de fois que de finalités différentes (par exemple, finalité d'entreprise et une transmission à des partenaires).

6. Incidences sur la relation client

6.2 Consentement



6. Incidences sur la relation client

6.2 Consentement

Exemples de formulations :

	Compatibilité RGPD	
❒ Si vous souhaitez recevoir nos offres commerciales, cocher cette case	Oui	Non
❒ Si vous voulez recevoir des offres commerciales de nos partenaires, cocher cette case	Oui	Non
❒ En cochant cette case, vous acceptez de recevoir des offres commerciales de notre part et que vos données soient communiquées à nos partenaires à des fins commerciales	Oui	Non
❒ En acceptant nos CGV, vous acceptez de recevoir des propositions commerciales sur votre adresse e-mail	Oui	Non
❒ Si vous ne souhaitez pas recevoir nos offres commerciales, merci de cocher cette case	Oui	Non
Vous acceptez de recevoir nos offres commerciales : oui ■ non ❒	Oui	Non
Vous acceptez de recevoir des offres commerciales de nos partenaires : oui ■ non ❒	Oui	Non

6. Incidences sur la relation client

6.2 Consentement

Exemples de formulations :

	Compatibilité RGPD	
❒ Si vous souhaitez recevoir nos offres commerciales, cocher cette case	**Oui**	~~Non~~
❒ Si vous voulez recevoir des offres commerciales de nos partenaires, cocher cette case	**Oui**	~~Non~~
❒ En cochant cette case, vous acceptez de recevoir des offres commerciales de notre part et que vos données soient communiquées à nos partenaires à des fins commerciales	~~Oui~~	**Non**
❒ En acceptant nos CGV, vous acceptez de recevoir des propositions commerciales sur votre adresse e-mail	~~Oui~~	**Non**
❒ Si vous ne souhaitez pas recevoir nos offres commerciales, merci de cocher cette case	~~Oui~~	**Non**
Vous acceptez de recevoir nos offres commerciales : oui ■ non ❒	~~Oui~~	**Non**
Vous acceptez de recevoir des offres commerciales de nos partenaires : oui ■ non ❒	~~Oui~~	**Non**

6. Incidences sur la relation client

6.2 Consentement

Gestion des opt-in (précisions)

- Pour les mineurs, il faut recueillir le consentement de leur(s) représentant(s) légaux.

2 exceptions au recueil préalable du consentement lorsque :

1. le message publicitaire est envoyé sur l'adresse électronique professionnelle d'une personne physique (ex : nom.prénom@entreprise.fr) et que l'objet de la sollicitation est en rapport avec sa profession (« B2B ») ;
2. le destinataire est déjà client et le message publicitaire concerne des produits ou services analogues à ceux que le consommateur a déjà acquis auprès du même organisme.

Mais dans ces deux hypothèses, la personne doit être informée, au moment de la collecte :

- que son adresse électronique sera utilisée à des fins de prospection lors de la collecte de ses coordonnées ;
- qu'elle est en mesure de s'opposer à l'utilisation de ses coordonnées de manière simple et gratuite.

6. Incidences sur la relation client

6.2 Consentement

Gestion des opt-out (dispense de consentement)

L'Opt-out correspond à la **dispense d'obtenir le consentement préalable** de la personne concernée pour utiliser des données de contact spécifiques le concernant (un numéro de téléphone ou une adresse postale), **si, au moment de la collecte de ces données, cette dernière :**

- a été informée de leur utilisation à des fins de prospection,
- et a été en mesure de s'opposer simplement et gratuitement au traitement (et qu'elle ne l'a pas fait), par une case à cocher.

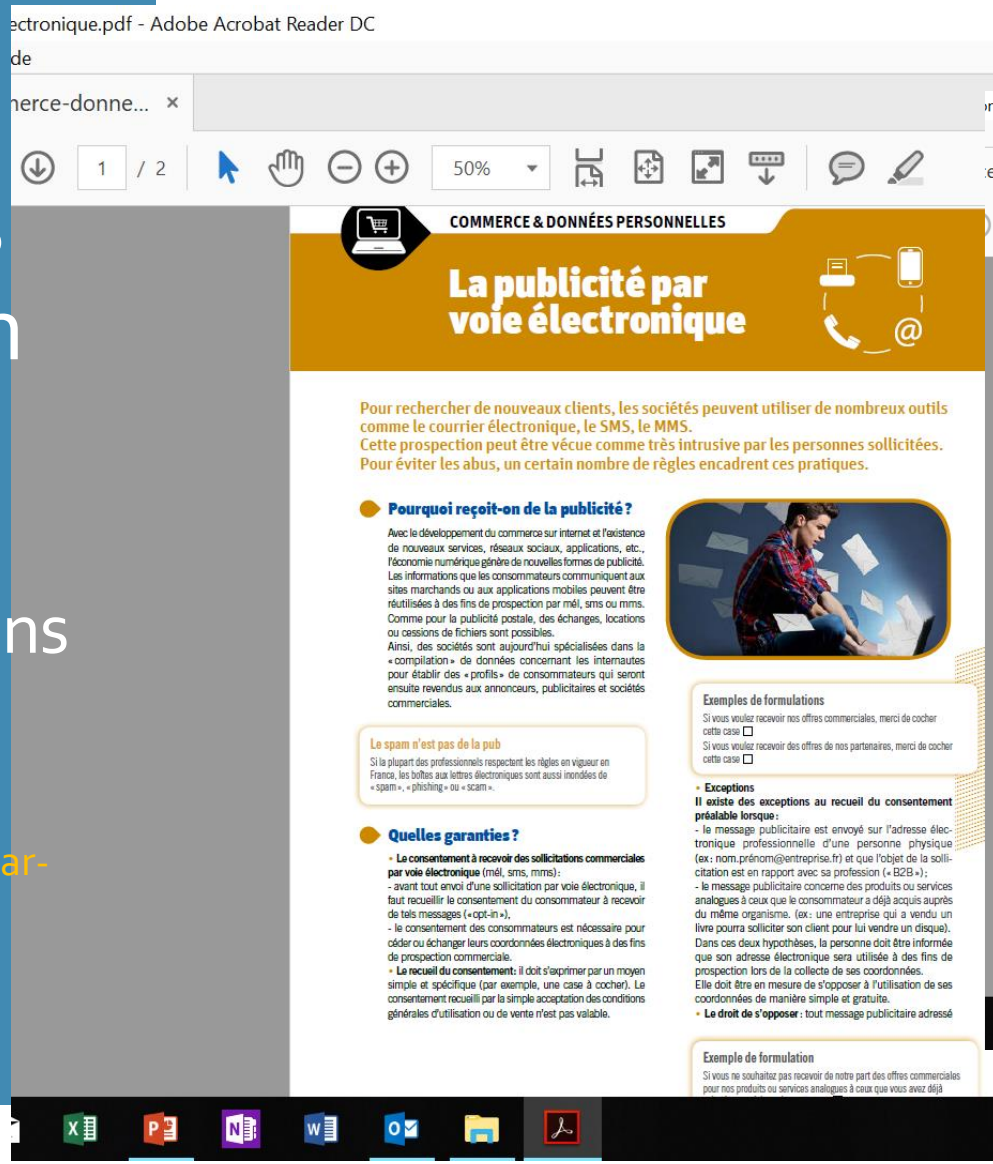
L'opt-out s'applique pour les canaux : adresse postale et téléphone pour le cas des appels téléphoniques.

(Pour les email, SMS/MMS : c'est l'opt-in).

6. Incidences sur la relation client

Recommandations CNIL :

https://www.cnil.fr/fr/la-prospection-commerciale-par-courrier-electronique



6. Incidences sur la relation client

6.3 Droits des personnes

Principaux impacts du RGPD sur la relation client :

Droits des personnes concernées

- Le RGPD **renforce les droits des personnes** : droit d'accès, de modification des données, d'opposition à certains traitements (prospection commerciale, profilage…), droit à la portabilité et à limitation des traitements, etc.

(Voir supra).

- Le délai dans lequel le responsable de traitement doit répondre à l'exercice des droits de personnes concernées est de **1 mois** (3 mois maximum si la réponse est complexe et le nombre de sollicitations important).

6. Incidences sur la relation client

6.3 Droits des personnes

Droit d'accès :

Délais de transmission des informations :

« *Dans les meilleurs délais et en tout état de cause dans un délai* ***d'un mois à compter de la réception de la demande*** ».

- Prolongation possible du délai jusqu'à 2 mois supplémentaires lorsque la complexité et le nombre de demandes le justifient, sous réserve d'informer la personne de cette prolongation et des motifs de report…
- En cas de doutes raisonnables sur l'identité de la personne, le responsable du traitement peut demander des informations supplémentaires en vue de confirmer son identité.

Modalités de transmission :

- Par écrit ou par d'autres moyens, y compris électronique lorsque la demande a été faite par voie électronique (et à moins que la personne concernée ne demande qu'il en soit autrement.

6. Incidences sur la relation client

6.4 Définition d'une politique de confidentialité des données (privacy policy)

Définition d'une politique de confidentialité des données (privacy policy) :

La **« Politique de confidentialité » est un moyen de répondre à l'obligation d'information des personnes**, elle définit notamment les modalités de collecte des données et les différents traitements pouvant être réalisés à partir de leurs données.

Cette politique a pour objet de compléter les mentions d'informations.

Elle doit être systématiquement visée en référence dans les formulaires de collecte de données, les CGV et/ou les CGU.

Un lien vers ce document doit figurer dans tous les documents de communication adressés aux prospects / clients (mailing, email…) quel qu'en soit le support, papier ou numérique.

6. Incidences sur la relation client

6.4 Définition d'une politique de confidentialité des données (privacy policy)

Politique de confidentialité (privacy policy) : (suite)

Cette politique intègre a minima les informations suivantes :

1. Identité et coordonnées de l'organisme (responsable du traitement) ;
2. Finalités (à quoi vont servir les données collectées) ;
3. Caractère obligatoire ou facultatif du recueil des données (ce qui implique une réflexion en amont sur l'utilité de collecter ces données au vu de l'objectif poursuivi : principe de minimisation) et conséquences pour la personne en cas de non-fourniture des données ;
4. Destinataires ou catégories de destinataires des données (qui a besoin d'y accéder ou de les recevoir au vu des finalités définies) ;
5. Durée de conservation des données (ou critères permettant de la déterminer) ;
6. Droits des personnes concernées (opposition, accès, rectification, effacement, nouveaux droits RGPD : limitation, portabilité) ;

6. Incidences sur la relation client

6.4 Définition d'une politique de confidentialité des données (privacy policy)

Politique de confidentialité (privacy policy) : (suite)

+ Informations nouvelles issues du RGPD :

7. Le cas échéant, existence d'un transfert des données vers un pays hors Union européenne ;
8. Coordonnées du délégué à la protection des données (DPO) de l'organisme, s'il a été désigné, ou d'un point de contact sur les questions de protection des données personnelles ;
9. Base juridique du traitement de données (c'est-à-dire ce qui autorise légalement le traitement : il peut s'agir du consentement des personnes concernées, du respect d'une obligation prévue par un texte, de l'exécution d'un contrat, etc.) ;
10. Droit d'introduire une réclamation (plainte) auprès de la CNIL ;

6. Incidences sur la relation client

6.4 Définition d'une politique de confidentialité des données (privacy policy)

Politique de confidentialité (privacy policy) : (suite)

Et, le cas échéant :

11. l'existence d'une prise de décision automatisée ou d'un profilage ;
12. le fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat ;
13. les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (exemple : prévention de la fraude) ;
14. le droit au retrait du consentement à tout moment ;
15. la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne ;
16. (+ Informations supplémentaires à donner en cas de collecte indirecte : catégories de données recueillies ; source des données…)
17. (+ d'information relatives aux cookies, le cas échéant : finalités des cookies ; bandeau de consentement et possibilité de refuser le dépôt de cookies).

La protection des données personnelles en pratique…

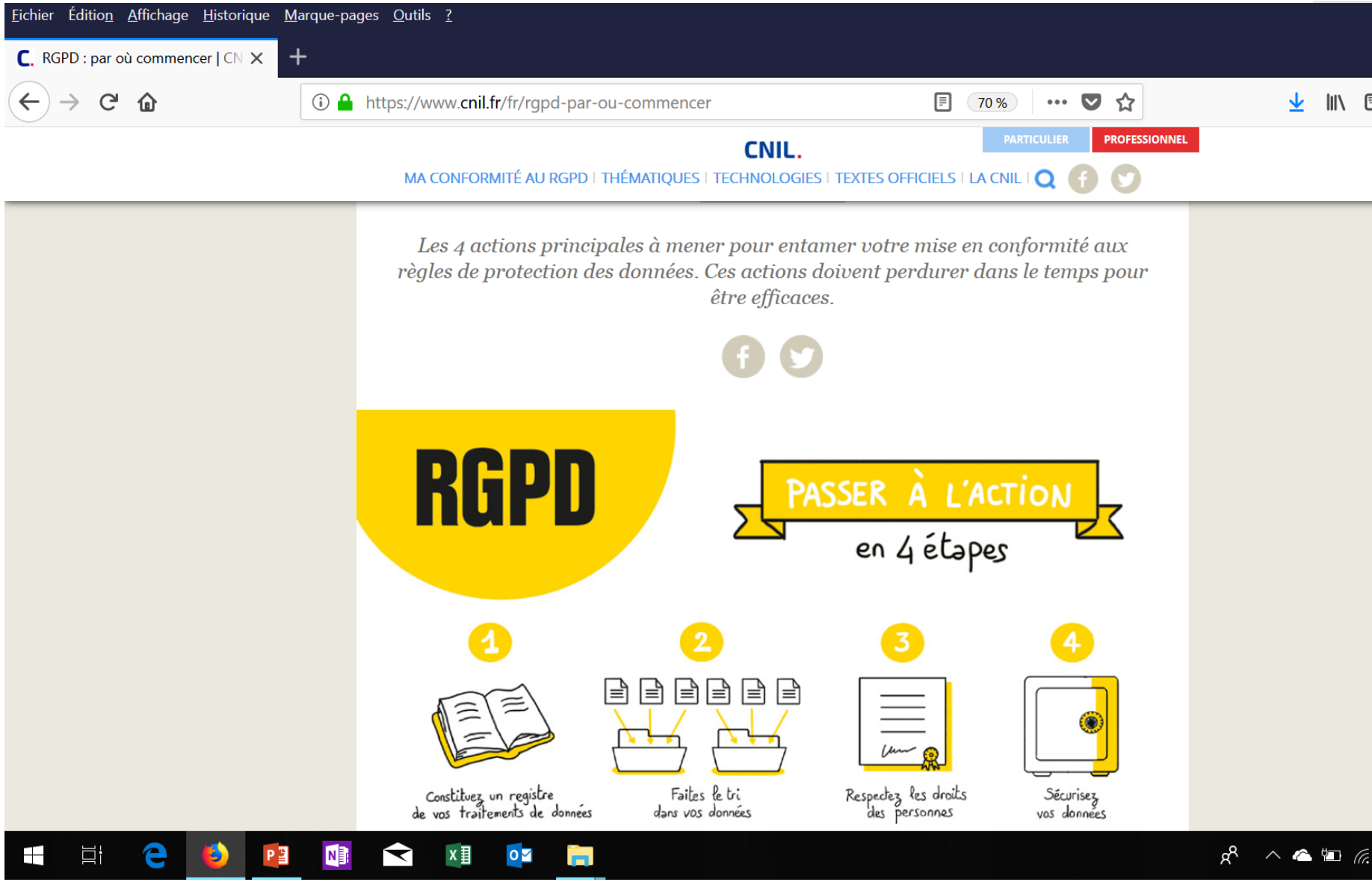
7. Comment atteindre la conformité (actions à mener)

- *7. 1 – Plusieurs méthodes*
- *7.2 – Dix actions à mener*

7. Comment atteindre la conformité

7.1 Plusieurs méthodes :

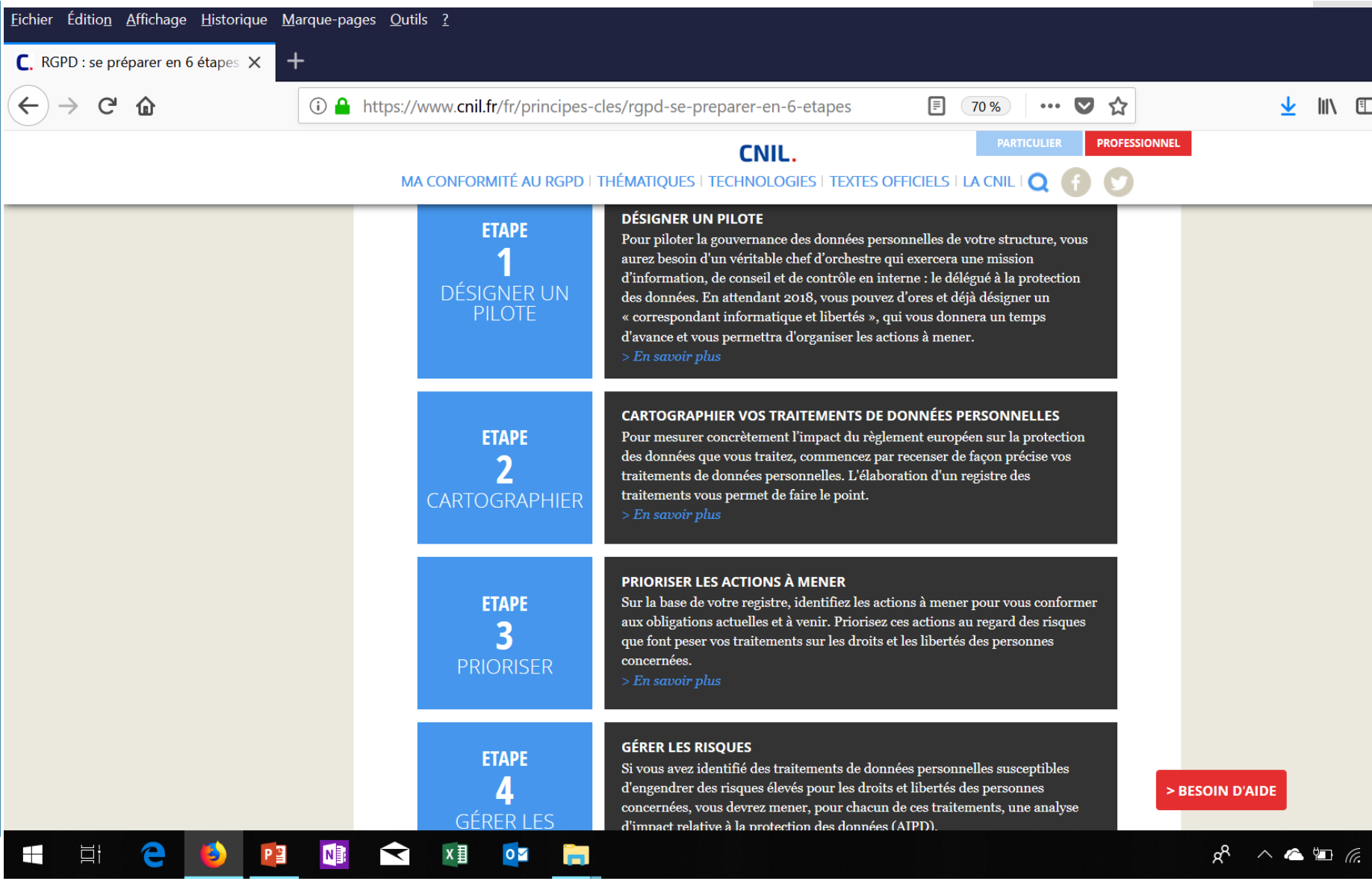
https://www.cnil.fr/fr/rgpd-par-ou-commencer



7. Comment atteindre la conformité

7.1 Plusieurs méthodes

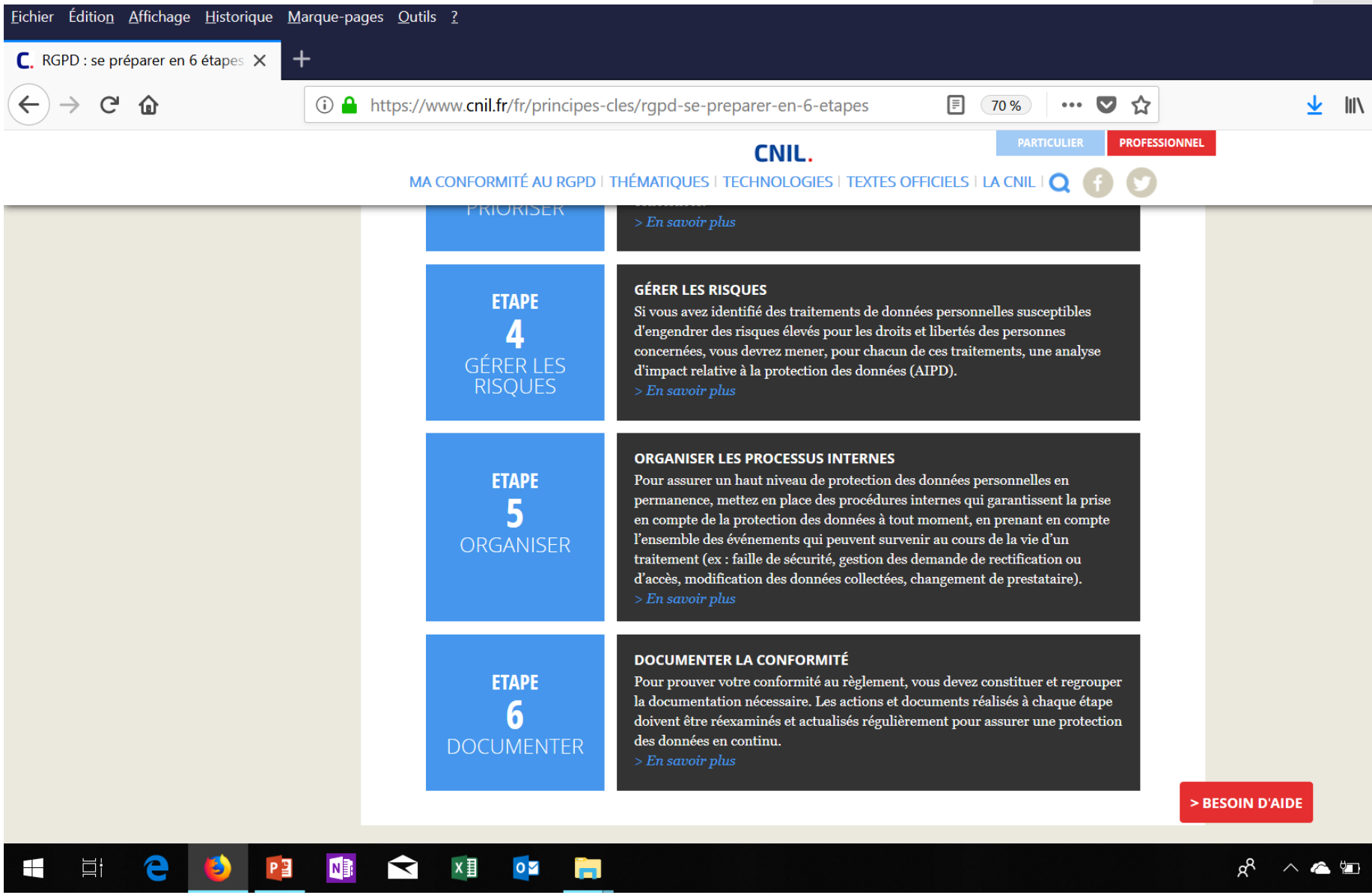
https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes



7. Comment atteindre la conformité

7.1 Plusieurs méthodes (suite)

https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes



7. Comment atteindre la conformité

7.2 Dix actions à mener

I. Cartographier les traitements de données personnelles et faire un audit (flash) de leur conformité au futur RGPD :

1. **Désigner un pilote (DPO/ DPD) ou un chef de projet** pour piloter la gouvernance des données personnelles,
2. **Recenser de façon précise les traitements** de données à caractère personnel (données, informations, durées de conservations, supports, etc.),
3. **Identifier les acteurs** (internes et externes) qui traitent ces données,
4. **Identifier les flux** (origine, transferts)
5. **Etablir un registre de traitements** (art. 30 du RGPD) - pas d'obligation pour les organismes ayant moins de 250 employés, sauf si le traitement comporte un risque pour les droits et libertés, si le traitement n'est pas occasionnel ou encore en fonction des catégories de données).

7. Comment atteindre la conformité

7.2 Dix actions à mener (suite)

II. Prioriser les actions en fonction des risques sur les droits et les libertés des personnes concernées (données sensibles, profilage, transferts de données) :

6. **Identifier la base juridique qui fonde le traitement** (consentement, intérêt légitime, contrat, obligation légale),
7. **S'assurer que seules les données strictement nécessaires** à la poursuite des finalités **sont collectées et traitées** (principe de minimisation,
8. **Vérifier les clauses contractuelles :** vérifier que les sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, s'assurer de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées,
9. **Vérifier les mentions d'information sur la protection des données** afin qu'elles soient conformes aux exigences du RGPD et prévoir les modalités d'exercice des droits des personnes concernées,
10. **Vérifier les mesures de sécurité mises en place**, techniques et organisationnelles.

Merci pour votre attention

Questions – réponses