Depuis le 25 mai 2018, le Règlement (UE) 2016/679 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 (règlement général sur la protection des données), est applicable.

De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes sera renforcée. Ils devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Les points à retenir depuis le 25 mai 2018 :

1. Désigner individuellement ou collectivement un **délégué à la protection des données**: même si l’obligation d’un tel délégué peut se discuter en Droit au sein des « petites structures » l’importance du travail à réaliser, et ensuite pour les échanges éventuels avec les autorités de contrôle, l’impose ;
2. Identifier les **actions à mener** en les priorisant au regard des risques que font peser leurs **traitements** sur les droits et les libertés des personnes concernées ;
3. Mettre en place un **registre des traitements** en recensant les traitements de données individuelles au sein de l’entreprise (modèle disponible) ;
4. Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une **analyse d'impact** sur la protection des données (AIPD)) dans certains cas limitativement énumérés mais non exhaustif, cependant le fait que l’analyse d’impact ne soit pas nécessaire dans ces cas énumérés n’exonère en aucun cas  le responsable des traitements de ses autres obligations prévues par le Règlement général à la protection des données. ***(***[cnil.fr](https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf)***)***

|  |
| --- |
| **REMARQUE****TRAITEMENTS À RISQUE**Sont considérés comme à risques les traitements ayant pour objet ou pour effet ([Règl. UE 2016/679 art. 35](https://abonnes-efl-fr.acces-distant.sciencespo.fr/EFL2/convert/id/?id=A5EC3EDAFF6BF788B-EFL" \t "_blank); Délib. Cnil 2018-326 et 2018-327 du 11-10-2018) :* L’évaluation d'aspects personnels ou la notation d'une personne ;
* Une prise de décision automatisée ;
* La surveillance systématique de personnes : télésurveillance, surveillance des réseaux sociaux des salariés, analyse des pages des réseaux sociaux des candidats à un emploi, outils de gestion du temps de présence (badge par exemple), systèmes de géolocalisation ;
* Le traitement de données sensibles (origine raciale ou ethnique ou les opinions philosophiques, politiques ou religieuses, etc.) ;
* Le traitement de données concernant des personnes vulnérables (mineurs, par exemple) ;
* Le traitement à grande échelle de données personnelles ;
* Le croisement d'ensembles de données ;
* Des usages innovants ou l'application de nouvelles technologies ;
* L’exclusion du bénéfice d'un droit, d'un service ou contrat.

Si le traitement de données concerné répond à au moins 2 de ces 9 critères, une analyse d'impact sur la protection des données doit être conduite. La Cnil a mis en place un logiciel facilitant la conduite et la formalisation d'analyses d'impact : [cliquez ici pour y accéder](https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil) ou [fiche explicative et logiciel ici](https://bit.ly/2zD7W0O)***.***Elle a par ailleurs dressé une liste non exhaustive des traitements pour lesquels une analyse d'impact est requise (Délib. Cnil 327 du 11-10-2018 modifiée par Délib. Cnil 11 du 31-1-2019) ainsi qu'une liste de ceux pour lesquels cette analyse n'est pas nécessaire. Figurent notamment parmi ces derniers les traitements mis en œuvre aux seules fins de gestion des contrôles d'accès physique et des horaires pour le calcul du temps de travail, en dehors de tout dispositif biométrique, à l'exclusion des traitements des données qui révèlent des données sensibles ou à caractère hautement personnel, ainsi que ceux destinés à la gestion des CSE (Délib. Cnil 119 du 12-9-2019).Le G29 recommande néanmoins de réaliser une étude d’impact pour tous les nouveaux traitements même si le responsable des traitements n’est pas certains que cela soit nécessaire. ([accéder au PDF](https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf) page 9 dernier paragraphe) |

1. Intégrer au sein de l’entreprise un **schéma d’organisation** assurant un haut niveau de protection des données par la rédaction de **procédures internes**: informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée ; recueil du consentement ; délais de conservation des données ; procédures d’exercice des droits (accès, modification, portabilité, opposition, limitation du traitement, effacement) ; recueil des contrats avec les sous-traitants ; transfert de données personnelles hors UE ; mais également mettre en place un schéma de sécurisation du serveur informatique et des systèmes informatiques utilisés (extranet, accès à distance...) ;
2. Le RGPD ne se focalise pas seulement sur les objectifs de protection des données, il définit aussi les moyens de cette protection et encourage l’adoption de différents outils permettant aux entreprises de communiquer publiquement sur leur conformité. Ainsi, **codes de conduite, certification et règles contraignantes d’entreprise**, font l’objet d’un focus et d’une reconnaissance marqués de la part du RGPD.
3. Actualiser ses connaissances, et ce sur la durée (**formation continue**) : la visite régulière du site de la CNIL est recommandée, s’agissant du régulateur amené à statuer demain sur les violations du RGPD ;
4. Mettre en place une **police cyber-attaque** adaptée aux risques de l’entreprise (recommandation ANACOFI : offres à venir dans la centrale de référencement).

Plus d’informations sur : [accéder au PDF en cliquant ici](https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf)

Intervenants impactés : opérationnels, juridique, informatique, conformité, sécurité mais aussi RH, risque, achat, communication et finance.

La loi n° 2018-493 du 20 juin 2018 supprime l'intégralité des dispositions de la Loi Informatique et Libertés (LIL) qui imposaient une déclaration préalable à la mise en œuvre du traitement (l'article 11 de la loi n° 2018-493 a modifié l'article 22 de la LIL).

|  |
| --- |
| **LIENS UTILES Projet de Loi modifiant la Loi n°78-17 du 6 janvier 1978 modifiée :** [cliquez ici](https://www.legifrance.gouv.fr/affichLoiPreparation.do;jsessionid=51FF97A7D88DA23F08DEDF8A30EAE2A9.tplgfr33s_3?idDocument=JORFDOLE000036195293&type=contenu&id=2&typeLoi=proj&legislature=15)**RGPD en français** : [cliquez ici](http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR)* Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles [cliquez ici](https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte)
* Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles ***cliquez ici***

Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (D. n° 2019-536, 29 mai 2019 : JO, 30 mai) [cliquez ici](https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038528420&categorieLien=id)Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel [cliquez ici](https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037800506&categorieLien=id) |

**6 règles d’or de la protection des données** :

* Un traitement doit avoir une finalité déterminée, explicite et légitime
* Les données doivent être collectées loyalement et de façon licite (information, consentement…)
* Seules les données adéquates, pertinentes et non excessives au regard de la finalité poursuivie doivent être collectées (principe de minimisation)
* Conserver les données le temps nécessaire à l’accomplissement de la finalité poursuivie avec, le cas échéant, une durée d’archivage justifiée par une raison légitime
* Garantir la confidentialité des données en interne et lors des échanges et imposer aux destinataires et sous-traitants de prendre des mesures en ce sens
* Mettre en place les mesures de sécurité organisationnelles, physiques et logiques nécessaires au regard des risques présentés par le traitement et de leurs degrés de probabilité (fiabilité de votre écosystème de cyber sécurité)

|  |
| --- |
| **DEFINITIONS Donnée à caractère personnel :**« *toute information se rapportant à une personne physique identifiée ou identifiable* ». Les données des personnes morales ne rentrent pas dans le champ du RGPD. Mais les données personnelles des dirigeants/salariés de personne morale rentrent dans le champ du RGPD. Les données professionnelles d’une personne (carte de visite) sont considérées, au regard du RGPD, comme des données personnelles.**Responsable du traitement :** il s’agit du chef d’entreprise.**Traitement**: «*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*». |

**Tableau récapitulatif des diverses étapes clés d’une procédure RGPD**

Pour la CNIL, la gouvernance en matière de traitement de données à caractère personnel se comprend comme « l’ensemble des mesures, règles et bonnes pratiques permettant la gestion » de telles données au sein d’une entité.

Afin de respecter les exigences posées par le RGPD, les professionnels sont tenus de mettre en place un ensemble de procédures afin d’assurer une protection optimale des données.

|  |
| --- |
| **PROCEDURE RGPD** |
| **CONSTRUIRE SON ORGANISATION INTERNE DEDIEE** | Le professionnel sera tenu de nommer les acteurs qui auront pour mission de piloter la gouvernance RGPD.Il conviendrait de nommer un responsable de traitement (article 4,7 du RGPD) et un délégué à la protection des données (article 37 du RGPD).-      **Responsable de traitement :** Il s'agit de 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 ainsi la personne à laquelle incombent les missions de fixer les buts du traitement et d'allouer les moyens financiers, humains et matériels nécessaires pour mettre en œuvre ce dernier. -      **Délégué à la protection des données :** Il a pour mission principale de veiller à la conformité des traitements mis en œuvre au sein de la structure qui l'a désigné. Le DPO peut être une personne interne ou externe et doit exercer en toute indépendance, ce qui exclut de nombreuses personnes d’être nommée DPO afin d’éviter tout conflit d’intérêt.***Petite structure :****Dans les petites structures, la désignation d'un DPO en interne relève alors quelquefois du défi dans la mesure où un conflit d'intérêts semble pouvoir atteindre toutes les personnes présentes. Il est alors possible de désigner un DPO en externe qui exercera ses missions sur la base d'un contrat de prestation de services.* |
| **ETABLIR UNE CARTOGRAPHIE / EVALUER LES RISQUES** | Une bonne gouvernance suppose l’identification précise des risques encourus en établissant une cartographie des données prenant la forme d’un registre des activités de traitement. **Registre des activités de traitement**- Le responsable de traitement est tenu d’une obligation de tenir un registre des activités de traitements (art 30 du RGPD).Ce registre ne concerne que les entreprises de plus de **250 salariés,** sauf si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernés, s’il n’est pas occasionnel ou s’il porte sur des catégories de données particulières (cf. articles 9 et 10 du RGPD : données sensibles).Un modèle de cartographie est proposé par la CNIL [sur ce lien](https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles)**Contenu du registre** - Le registre va recenser :-      Les différents traitements de données personnelles,-      Les catégories de données personnelles traitées,-      Les objectifs poursuivis par les opérations de traitements de données,-      Les acteurs interne ou externe qui traitent les données,-      Les flux en indiquant l’origine et la destination des données (UE / Hors UE). |
| **PRIORISER LES ACTIONS A MENER** | Suite à l’identification du traitement des données par le professionnel, il est tenu d’identifier les actions à mener pour se conformer aux obligations prévues par le RGPD notamment :1/ L’obligation du professionnel de **respecter les principes clés du RGPD :**-      **Principe de finalité :** *le responsable et le sous-traitant sont tenus d’utiliser les données dans le seul but pour lequel elles ont été collectées à l'origine.*-      **Principe de minimisation de la collecte *:****le responsable ne peut collecter que les données qui sont nécessaires pour atteindre la finalité escomptée*-      **Principe de conservation des données limitées dans le temps**: pendant toute la durée de la relation d’affaire et 5 ans au-delà pour les CIF, IAS et IOBSP / 10 ans pour les intermédiaires en immobiliers.2/ L’obligation du professionnel de respecter **les droits des personnes :**-      Droit à l’information en cas de collecte directe / indirecte (art 13- 14 du RGPD)-      Droit d’accès et de communication (art 15 du RGPD)-      Droit de rectification et d’effacement (art 16 et 17 du RGPD)-      Droit d’opposition (art 21 du RGPD)-      Droit à la limitation du traitement (art 18 du RGPD)-      Droit à la portabilité des données (art 20 du RGPD)-      Droit à un recours effectif : le droit d’introduire une réclamation en saisissant le CNIL-      Recueil du consentement |
| **GERER LES RISQUES / OPTIMISER ET SECURISER L’USAGE DE LA DONNEE** | Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, **une analyse d'impact relative à la protection des données** (AIPD) :-      **Périmètre de l’AIPD** : art 35 du RGPD-      **Contenu de l’AIPD :** article 35 § 7 du RGPD-      **Modalité de réalisation d’une AIPD :**  les lignes directrices du G29 sur le DPIA et le logiciel en open source développé par la CNIL permettant de procéder à une AIPD ***(***[outil PIA ici](https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil)***)***Le RGPD ne se focalise pas seulement sur les objectifs de protection des données, il définit les moyens de cette protection et encourage l’adoption de différents outils permettant aux entreprises de communiquer publiquement sur leur conformité : ***codes de conduite, certification et règles contraignantes d’entreprise****, font l’objet d’un focus et d’une reconnaissance marqués de la part du RGPD.* |
| **ORGANISER LES PROCESSUS INTERNES** | Tout professionnel est tenu d’intégrer au sein de l’entreprise un schéma d’organisation assurant un haut niveau de protection des données par la rédaction de procédures internes afin de répondre à la nécessité de sécuriser les données à caractère personnel.**Le professionnel doit :**-      Prendre en compte de la protection des données dès la conception-      Sensibiliser et organiser la remontée d’information-      Traiter les réclamations et les demandes des personnes concernées quant à l’exercice de leurs droits-      Anticiper les violations de données en prévoyant la notification à l’autorité de contrôle d’une violation de données à caractère personnel [(formulaire de notification de violation ici)](https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles) et de garantir la communication à la personne concernée d’une violation de données à caractère personnel (art 34 du RGPD).-      Mettre en place une police cyber-attaque adaptée aux risques de l’entreprise (recommandation ANACOFI)-      Garantir l’obligation de sécurité des données (art 32 du RGPD) |
| **DOCUMENTER LA CONFORMITE** | **Le professionnel doit :**-      Actualiser ses connaissances, et ce sur la durée (formation continue) : la visite régulière du site de la CNIL est recommandée, s’agissant du régulateur amené à statuer demain sur les violations du RGPD |

**1. Le délégué à la protection des données (DPO)**

Nommer un délégué à la protection des données dépend du type et de la quantité de données que vous collectez (principale activité, suivi régulier et systématique des personnes à grande échelle…). La CNIL vise entre autres les compagnies d’assurance les banques pour leurs fichiers clients ou encores les sociétés immobilières.

**REMARQUES :**L’ANACOFI recommande de désigner un délégué à la protection des données dans tous les cas.

Les compétences du DPO : Le DPO doit être désigné et déclaré sur le site de la CNIL 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. Le niveau d’expertise doit être apprécié en fonction du type de données collectées (si ce sont des données correspondant à celle cité à l’article 9 et 10 du RGPD), de la quantité des données collecté ainsi des traitements réalisés notamment de l’existence de traitements de données sensibles ou des transferts internationaux de données.

Il convient de s’assurer que le DPO dispose également d’une bonne connaissance du secteur d’activité de l’entreprise concernée. Il est important que le DPO puisse avoir accès aux formations certifiées par la CNIL. (Ces formations sont proposées par certains organisme comme Veritas ou l’AFNOR)

Il convient de prêter une attention particulière aux conflits d’intérêt. Le DPO ne doit pas exercer de missions le conduisant à définir les finalités et les moyens du traitement de données à caractère personnel. (Par exemple un DPO ne doit pas être en même temps responsable de traitement. [www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees](http://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees)***)***

Enfin, le DPO doit disposer d’un budget de fonctionnement.

**2. Traitement des données individuelles**

Champ d’application territorial du RGPD : le RGPD s’applique aux traitements mis en œuvre par les entreprises – responsables de traitement et sous-traitants – établies dans l’UE. Il s’applique également à celles qui ne sont pas établies dans l’UE et qui utilisent des moyens de traitement hors de l’UE, dès lors que le traitement concerne un national ou un résident européen (légal) et porte sur l’offre de biens et services (avec ou sans paiement) ou est lié au suivi d’un comportement ayant lieu dans l’UE.

Un consentement exprès est désormais indispensable : manifestation de volonté « *libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l’objet d’un traitement* ».

Le consentement de la personne n’est pas obligatoire pour recueillir ses données si le traitement de ses données est nécessaire à l’exécution d’un contrat passé avec celle-ci (lettre de mission, mandat, etc.).

En revanche, si on **transfert les données à un agrégateur** : besoin du consentement éclairé, explicite, etc.

Une attention particulière est à porter pour les **clients mineurs**(moins de 16 ans). Plus d’informations sur le site de la CNIL : [www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes](https://www.cnil.fr/fr/conformite-rgpd-comment-recueillir-le-consentement-des-personnes)

Le traitement sera licite s’il repose sur le consentement de la personne concernée. Pour être valide, il doit être rédigé à la 1ère personne « *je reconnais* », «*je consens*», le consentement doit être :

* **Libre :** la personne doit bénéficier d’une véritable liberté de choix (il ne doit notamment pas y avoir de déséquilibre manifeste entre la personne et le responsable de traitement ; un consentement par finalité doit être requis ; enfin, l’exécution d’un contrat ne doit pas être subordonnée à l’obtention du consentement si cela n’est pas nécessaire à une telle exécution).
* **Spécifique :** si le consentement est demandé dans un document regroupant plusieurs questions/informations il convient de distinguer la partie relative à la demande de consentement sous une forme aisément accessible et formulée en des termes clairs.
* **Eclairé :** la personne doit bénéficier des informations nécessaires pour savoir quel est l’objectif du traitement de ses données et ainsi pouvoir décider en connaissance de cause.
* **Résulter d’un acte positif et univoque :** le consentement doit relever d’un comportement actif et sans ambiguïté de la personne (case à cocher par exemple ; en revanche le silence ou tout acte implicite ou passif ne constituent pas un consentement valide).

Le consentement doit pouvoir être retiré à tout moment et la personne doit être informée de cette faculté de retrait. La charge de la preuve de l’obtention du consentement repose sur le responsable de traitement.

Droit à la portabilité (seulement sur les données fournies, pas sur celles issues du traitement) : vous devez donner aux personnes concernées les moyens d’accéder à leurs données et de les transmettre à d’autres entreprises (sauf si obligation légale de les conserver). Par exemple, l’obligation de restituer à un client l’ensemble des pièces fournies par ce même client pour l’obtention d’un prêt, dans un format numérique aisément réutilisable.

Droit à l’oubli : vous devez supprimer leurs données à caractère personnel si les personnes concernées en font la demande sauf si ces données sont nécessaires à l’exercice de votre profession, ou imposées par la loi (ex : 5 ans pour la LCB-FT).

Données sensibles (art.9 du RGPD) : santé, race, orientation sexuelle, religion, opinions politiques => interdiction par principe de réaliser un traitement de ces données sensibles. Exception : la personne concernée a donné son consentement explicite au traitement de ces données pour une ou plusieurs finalités spécifiques, par exemple :

* **Pour les données de santé**, la question se pose dans le cadre de l’assurance emprunteur, il convient d’acter le traitement de ces données dans un contrat. Le seul fait de transférer les données de santé à la compagnie d’assurance constitue un traitement de ces données sensibles dont le consentement exprès est requis. Ces informations ne doivent pas figurer dans le KYC par principe de minimisation des données.
* **Pour les opinions politiques**, il est possible de préciser l’opinion politique d’une Personne Politiquement Exposée (PPE dans le cadre de la LCB-FT) seulement si cette information est de notoriété publique (ex : député). Dans le cas contraire, vous n’avez pas à préciser l’opinion politique de votre client (interdiction de traiter cette donnée).

Données des tiers : En matière d’assurance, l’identification d’une personne par ses noms, prénoms, date de naissance, l’utilisation d’informations qui lui sont associées comme des numéros de contrats, et plus encore les données personnelles de santé ainsi que toute information se rattachant à la personne sont des données à caractère personnel au sens du RGPD. Ces informations ne sont d’ailleurs pas limitées aux assurés, les assureurs recueillant des données à caractère personnel relatives à la famille de l’assuré (par exemple dans un contrat santé) ou à des tiers (bénéficiaires non parents).

Lorsque les données à caractère personnel n’ont pas été collectées auprès de la personne concernée (ex : bénéficiaire nommément désigné dans un contrat d’assurance vie), le responsable du traitement fournit à celle-ci toutes les informations suivantes :

* Identité et coordonnées du responsable de traitement et du DPO,
* Finalités du traitement ainsi que la base juridique du traitement,
* Catégories de données concernées,
* Destinataires des données (ex : compagnie d’assurance vie),
* Si transfert de ces données dans un pays tiers (plus d’informations à [l’article 14 du RGPD](https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3)),
* Durée de conservation des données,
* Intérêts légitimes poursuivis par le responsable du traitement ou par un tiers,
* L’existence du droit d’accès aux données (rectification etc.),
* L’existence du droit de retirer le consentement à tout moment,
* Le droit d’introduire une réclamation auprès d’une autorité de contrôle,
* La source d’où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu’elles sont issues ou non de source accessible au public,
* L’existence d’une prise de décision automatisée, y compris un profilage, et des informations utiles concernant la logique sous-jacente, ainsi que l’importance et les conséquences prévues de ce traitement pour la personne concernée.

Ces informations doivent être fournies dans un délai raisonnable ne dépassant pas 1 mois (après obtention des données).

**EXCEPTION :** lorsque les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel.

Il apparait donc que lorsqu’un courtier en assurance traite les données personnelles de bénéficiaires de contrats (clause nominative), il n’aurait pas à transmettre les informations ci-dessus aux bénéficiaires puisqu’il a un devoir de confidentialité. Néanmoins, le RGPD ne parle que de secret professionnel.

|  |
| --- |
| **L’ANACOFI a interrogé l’ACPR et la CNIL sur ce sujet en avril 2018.**Voici la réponse de la CNIL à notre interrogation :*« Tout d’abord, concernant votre demande de conseil relative à l’interprétation de l’article 14 du GDPR, il me semble en première analyse que le courtier en assurance ne figure pas parmi les personnes légalement tenues au secret professionnel (art 226-13 Code pénal).**En outre, les lignes directrices du G29 sur la transparence prennent comme exemple le médecin, professionnel de santé soumis au secret médical, ce qui semble restreindre la définition de « secret professionnel » aux personnes concernées par un texte légal prévoyant explicitement que la profession est soumise au secret*[accéder au texte](https://www.cnil.fr/sites/default/files/atoms/files/wp260_enpdf_transparency.pdf)*Dès lors, l’exception prévue à l’article 14 relative au secret professionnel ne parait pas applicable au courtier en assurance. De plus, la jurisprudence de la chambre criminelle de la Cour de Cassation considère que le nom du bénéficiaire d’un contrat d’assurance sur la vie ne présente pas un caractère secret (Cass. crim 28 sept 1999).**Ensuite, au regard des dispositions de l’article 14 du GDPR relatif aux informations à fournir lorsque les données à caractère personnel n’ont pas été collectées auprès de la personne concernée, il me semble que l’article 14.3.b trouve application. En effet, le courtier (responsable de traitement) pourra être en mesure de fournir les informations visées au 14.1 et 14.2, si les données doivent être utilisées aux fins de communication avec la personne concernée au plus tard au moment de la première communication avec ladite personne.****Dans le cadre d’une assurance-vie, c’est au moment où le courtier va prendre contact avec le bénéficiaire pour lui verser la somme qui lui revient, qu’il devra l’informer sur les dispositions de l’article 14 du règlement.****Par ailleurs et concernant plus particulièrement les assureurs, en vertu de la Loi Eckert sur les contrats en déshérences, le code de déontologie de la FFA (janvier 2018) indique en page 52 que dans le cas où le bénéficiaire d’un contrat d’assurance-vie est l’ayant droit de l’assuré décédé, l’article 8 de la loi Eckert prévoit que l’assureur obtient sur sa demande auprès du notaire en charge de la succession la communication des informations nécessaires à l’identification du bénéficiaire ayant droit de l’assuré. Dès lors, c’est au moment où l’assureur aura connaissance de l’identité du bénéficiaire qu’il pourra mettre en œuvre ses obligations au titre de l’article 14, en application du 14.3.b. »* |

Procédure en cas de violation des données (article 33 et article 55 du RGPD) : le responsable de traitement devra notifier l’incident à la CNIL si possible dans les 72 heures ; tout en précisant les mesures qu’il sera apte à prendre pour remédier à la violation des données et à ses conséquences dommageables. S’il s’avère que la violation en cause est susceptible de constituer une menace pour les droits et libertés des personnes concernées, il faut les en informer directement. Le DPO (personne de contact) doit informer sur les conséquences envisageables de l’incident, et les mesures de remédiation prises ou à prendre. Si des efforts disproportionnés doivent être déployés pour procéder à cette information, une communication publique notamment est acceptable.

Délai réponse à réclamation (article 12 du RGPD) : Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22 du RGPD, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande. Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement.

Si le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel.

**3) Registre des traitements**

Le registre des traitements doit contenir autant de fiches que de typologies d’activités recensées (activités habituelles seulement).

Les PME doivent tenir, sous forme écrite, un registre des activités de traitement, uniquement dans 3 situations :

* Le traitement n’est pas occasionnel
* Le traitement représente une menace pour les droits et libertés des citoyens
* Le traitement porte sur des données sensibles (santé par exemple) ou des casiers judiciaires.

La documentation de la conformité :

Le registre des activités de traitement représente l'outil de base de la gestion opérationnelle de la conformité et constitue la première obligation de preuve de la conformité.

Le contenu du registre est détaillé à l’article 30 du RGPD. Il doit comporter les informations suivantes :

* **Pour les responsables de traitement :**
* Nom et coordonnées du responsable du traitement, de son représentant et du DPO ;
* Finalités du traitement ;
* Catégories de personnes et de données à caractère personnel ;
* Catégories de destinataires ;
* Transfert vers pays tiers ;
* Délais de conservation ou les moyens de déterminer ce délai de conservation ; et
* Description des mesures de sécurité si possible
* **Pour les sous-traitants :**
	+ Nom et coordonnées du responsable du traitement et du/des sous-traitant, de leur représentant et du DPO ;
	+ Catégories de traitements pour chaque responsable de traitement ;
	+ Les transferts vers des pays tiers ; et
	+ La description générale des mesures de sécurité si possible.

Ce registre ne concerne que les entreprises de plus de 250 salariés (considérant 13 du RGPD), sauf si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernés, s’il n’est pas occasionnel ou s’il porte sur des catégories de données particulières (cf. articles 9 et 10 du RGPD : données sensibles).

L’ANACOFI recommande de tenir un registre des activités de traitement simplifié dans tous les cas dont vous trouverez un modèle publié et mise à jour régulièrement par la CNIL (ci-dessous :

**4) Analyse d’impact sur la vie privée (Privacy Impact Assessment – PIA)**

Quand réaliser une analyse d'impact ? Au titre de l'article 35 du RGPD, les responsables de traitement ont l'obligation d'effectuer une analyse d'impact dans certains cas limitativement énumérés et principalement lorsque le traitement ou le produit qui sera déployé est « *susceptible d’engendrer un risque élevé pour les droits et libertés des personnes physiques concernées*» (ex : mineurs, santé, PPE).

Cependant dans la pratique il serait préférable de réaliser une étude d’impact pour tous les nouveaux traitements de données.

Comment réaliser une analyse d’impact ? Le RGPD n’impose pas de méthodologie particulière pour la conduite de l’analyse d’impact mais prévoit néanmoins ce que le rapport d'analyse devra contenir à minima :

* Une description systématique des opérations de traitement et de ses finalités ;
* Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
* Une évaluation des risques pour les droits et les libertés des personnes concernées ;
* Les mesures envisagées pour faire face à ces risques.

Il s’agit d’anticiper les impacts d’un nouveau produit ou service sur la vie privée des clients. Un PIA, mené par le responsable de traitement, avec le concours du DPO et des sous-traitants, doit être réalisé avant la mise en œuvre du traitement susceptible d’exposer les personnes à un risque élevé au regard de leurs droits et libertés. Cette analyse d’impact permet de mieux mettre en œuvre les principes de *privacy by design* et *privacy by default* introduits par le RGPD. Le PIA favorise une logique de conception respectueuse de la vie privée (*Privacy by Design*), il est ainsi un moyen pour les entreprises de montrer que leurs solutions sont respectueuses de la vie privée et assure un niveau de protection conforme aux obligations du droit de l’Union. Par ailleurs, le PIA devrait permettre à l’entreprise de s’affranchir de la plupart des déclarations ou autorisations CNIL liées aux traitements de données personnelles, et d’avoir une cartographie des différents traitements et des risques.

Pour la réalisation d’un PIA, voir les documents CNIL suivants :

* « PIA, la méthode » : ce document indique la marche à suivre pour faire une étude d’impact sur la vie privée. Il fournit différents modèles et un guide de mesures conseillées, en précisant le domaine d’application, les responsables de l’étude, les différentes catégories de risques à prendre en compte par rapport à la notion de vie privée, et les processus de validation du PIA.
* « PIA, l’outillage : modèles et bases de connaissances » : ce document propose quant à lui une échelle et des règles pour estimer la gravité d’une violation, avec 4 niveaux de risques.
* Guide en 6 étapes pour se préparer au règlement européen : la 4ème étape intitulée « Gérer les risques » décrit la démarche de PIA en cas de traitements de données personnelles susceptibles d’engendrer des risques pour les droits des personnes.

Détection et notification de toute intrusion dans les bases de données personnelles. Chaque entreprise doit donc procéder à l’évaluation des risques d’atteinte aux libertés qui découlent de ses propres traitements de données personnelles. La CNIL diffuse un intéressant outil d’évaluation des risques des données personnelles (auto-analyse), le PIA : [outil PIA ici](https://www.cnil.fr/fr/PIA-privacy-impact-assessment)

**5) Schéma d’organisation – procédures internes**

La procédure interne comprend les coordonnées du DPO, le registre des traitements, les actions à mener au regard de la cartographie des données, les modalités d’information des droits, les modalités d’exercice des droits (accès, rectification, portabilité, etc.), les protocoles internes (droit d’accès des postes de travail, déclaration à la CNIL en cas de violation des données, etc.), les contrats passés avec les sous-traitants et le cas échéant, le PIA (les risques avec les actions à mener en priorité).

**Typologie de risques :**

Il convient de répertorier les risques liés aux composants de votre système d’information (SI) (*voir annexe intitulée «****Check-list du RGPD - Mesures techniques à mettre en place pour être conforme au******RGPD****» sur notre site internet ou sur demande au service juridique de l’ANACOFI*).

Trois typologies de risques ont été identifiées :

* La sécurité du SI : il faut prendre conscience de la criticité du SI en sa qualité de « berceau des données », comme le formule l’ANSSI dans son Guide d’Hygiène Informatique : Renforcer la sécurité de son système d’information en 42 mesures.

Cette typologie de risque soulève des problématiques comme l’intrusion du SI par un malware, l’usurpation d’un compte utilisateur ou encore le défaut d’application des mises à jour de sécurité.

* La protection des données personnelles : elle consiste à définir la marche à suivre en cas, par exemple, de défaut de cartographie actualisée des données personnelles et des traitements, de divulgation malveillante de données personnelles, ou encore à décrire les dispositifs de chiffrement et d’anonymisation/pseudonymisation. ***(***[Article sur l'anonymisation ici](http://www.cnil.fr/fr/lanonymisation-des-donnees-un-traitement-cle-pour-lopen-data)***)***
* Les droits de la personne : comment garantir le droit à la portabilité, le droit à l’oubli ou tout ce qui a trait à la transparence des traitements, au profilage, à la rétention des données, au consentement, etc. Cette catégorie très large a été découpée par grandes familles de risques, et fait l’objet d’un développement détaillé, proposé ci-après par le Cabinet De Gaulle, Fleurance & Associés : la non disponibilité ; le défaut d’intégrité ; la perte de confidentialité ; l’absence de traçabilité ; les usages illicites ; la répudiabilité.

**Mesures applicables et recommandations :**

Les mesures (techniques, organisationnelles, juridiques) potentiellement applicables aux 3 typologies de risques identifiées précédemment sont détaillées en annexes. Par exemple, voici une série de mesures proposées pour gérer le risque « Transfert non sécurisé de données personnelles ».

Composants du SI exposés à ce risque : Cloud, Applications, Base de Données, Datawarehouse, Big Data, GED-Archivage, Fichiers Partagés, Messagerie, Données en sortie.

**Mesures potentiellement applicables pour se protéger de ce risque :**

* Intégrer les contraintes dès la phase de design (privacy-by-design)
* Politique sur les droits et devoirs en matière de sortie des données
* Chiffrement et anonymisation
* Encadrement contractuel avec le partenaire (NDA, clause de confidentialité, clause de suppression des données…)
* Contrôle des accès (utilisation d’un double firewall)
* Gestion centralisée des logs (SIEM, Security Information Event Management)
* EDRM, Enterprise Digital Right Management (Protection bureautique avec chiffrement, watermarking…)
* Limitation des accès internet
* Interdiction de clés USB (dans certains pays), sauf certains types de clé USB définit par l’entreprise ou avec un digicode.
* Blocage de sites de transferts (type Wetransfer, Dropbox…)
* Détection de téléchargements/transferts de fichiers importants
* Intégration de données « pièges »
* Audit Sensibilisation/Formation utilisateurs et IT
* Filtrage IP des applications multi-tiers

**6) Code de conduite sectoriel**

Les principaux outils de confiance vis-à-vis des tiers et la présomption de conformité :

Instruments encore méconnus de la pratique, les codes de conduite, certifications, et marques ou encore règles contraignantes d'entreprise, pourraient se révéler être des outils précieux pour guider les organisations dans leurs efforts de conformité, en leur fournissant un cadre de conformité plus adapté et personnalisé que les règles génériques du RGPD.

C'est donc un **code de conduite "sectoriel"** que vise l’article 40 du RGPD, sans pour autant définir ce terme, ce qui ouvre la voie à une approche de la conformité non pas limitée à une entreprise ou un groupe d'entreprises mais à l'ensemble des entreprises relevant du secteur concerné.

Les conditions de validité et d'approbation d'un code de conduite sectoriel au sens du RGPD :

Concernant la rédaction d'un code de conduite sectoriel, le RGPD fournit les indications suivantes sur son contenu qui devra aborder les thèmes suivants :

« *a) le traitement loyal et transparent ;*

1. *b) les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques ;*
2. *c) la collecte des données à caractère personnel ;*
3. *d) la pseudonymisation des données à caractère personnel ;*
4. *e) les informations communiquées au public et aux personnes concernées ;*
5. *f) l'exercice des droits des personnes concernées ;*
6. *g) les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant ;*
7. *h) les mesures et les procédures visées aux articles 24 et 25 [concernant la responsabilité du responsable du traitement, la protection dès la conception et la protection par défaut] et les mesures visant à assurer la sécurité du traitement visées à l'article 32 [obligations relatives à la sécurité du traitement] ;*
8. *i) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées ;*
9. *j) le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales ; ou*
10. *k) les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement, sans préjudice des droits des personnes concernées au titre des articles 77 et 79 [réclamations auprès d’une autorité de contrôle et recours juridictionnels].* »

En outre, le code de conduite doit prévoir un mécanisme permettant le contrôle de l’application de ce code par un organisme de contrôle agréé par l’autorité de contrôle.

**REMARQUES**

L’ANACOFI va mettre en place, seule ou dans le cadre d’ANCIA, un code de conduite sectoriel, si possible en 2019.

**7) Sanction**

**Des pouvoirs de sanction renforcés :**

Articles 50, 51, 52, 226-16 à 226-24 du Code pénal : peines d’emprisonnement (5 ans) + amendes (300k€) si manquement à la loi Informatique et Libertés + sanctions CNIL (3M€ + retrait d’autorisation + dénonciation aux autorités).

Sanctions prévues par le RGPD (responsables de traitement + sous-traitants + coresponsables de traitement) :

* 10M€ ou 2% du CA annuel mondial : mineurs, données sensibles, sous-traitance, registre des traitements, coopération, sécurité, notification des failles de sécurité, analyse d’impact, DPO.
* 20M€ ou 4% du CA annuel mondial : principes de base d’un traitement et consentement, droit des personnes, transferts des données hors UE, interdiction d’accès aux locaux, dispositions spécifiques des Etats membres, non-respect d’une injonction d’un Etat membre.

|  |
| --- |
| **LIENS UTILES**CNIL – protection particulière des données de santé (données sensibles) [cliquez ici](http://www.cnil.fr/fr/sante)CNIL – Outil PIA : nouvelle version beta du logiciel [lien outil PIA ici](https://www.cnil.fr/fr/outil-pia-nouvelle-version-beta-du-logiciel)RGPD : comment la CNIL vous accompagne dans cette période transitoire ? [Cliquez ici](https://www.cnil.fr/fr/rgpd-comment-la-cnil-vous-accompagne-dans-cette-periode-transitoire)CNIL – Un nouveau guide de la sécurité des données personnelles [cliquez ici](https://www.cnil.fr/fr/un-nouveau-guide-de-la-securite-des-donnees-personnelles)CNIL – Les outils de conformité [cliquez ici](https://www.cnil.fr/fr/les-outils-de-la-conformite)Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du Personnel [cliquez ici](https://www.cnil.fr/sites/default/files/atoms/files/referentiel_grh_novembre_2019_0.pdf) |

Concernant les données personnelles de vos salariés :

* Un mot de passe sur un PC n’est pas suffisant pour la sécurité de ces données Cependant il faut suivre certaines règles données par la CNIL pour avoir un système de mot de passe fort ***(***[Retrouvez les conseils de la CNIL ici](https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe)***)*** ;
* Ne conserver pas les questionnaires santé remplis de vos salariés pour leur mutuelle ;
* Le numéro de sécurité sociale (données sensibles) ne pourra être demandé qu’après le recrutement.