CGO
Expertise & Audit

INFOS LETTRE

Votre partenaire au quotidien

Mai 2018
N° 5

CRCC
COMPAGNIE RÉGIONALE DES COMMISSAIRES AUX COMPTES ORLÉANS

Damien BOUTRY
Expert-Comptable - Commissaire aux Comptes

ORDRE DES EXPERTS-COMPTABLES
Région Pays de Loire

Pour toute information ou documentation complémentaire, contactez-nous au :
Tél. : 02 47 39 52 52 • **Fax :** 02 47 39 59 96
E-mail : accueil@cgo37.fr • **Site :** www.cgo37.fr

SOMMAIRE

SOCIAL
RGPD : Quels impacts pour les entreprises à partir du 25 mai 2018 ? 4-13

FISCAL
Redevance audiovisuelle : Minoration étendue aux chambres d'hôtes 14

AGENDA JUIN 2018 ET INDICES 15-16

RGPD

Quels impacts pour les entreprises à partir du 25 mai 2018?

Le règlement général relatif à la protection des données 2016/679 du 27 avril 2016 (RGPD), qui entre en vigueur le 25 mai 2018, substitue au régime de formalités préalables prévu par la loi informatique et libertés, un système fondé sur la responsabilité des acteurs qui devront démontrer la conformité de leurs traitements à ce règlement à tout moment.

La particularité du règlement est d'être directement **applicable à partir du 25 mai 2018** dans l'ensemble de l'Union européenne sans nécessiter, contrairement à une directive, de transposition dans les différents Etats membres. Les traitements déjà mis en œuvre à cette date doivent être mis en conformité avec ses dispositions.

La Commission nationale informatique et libertés (Cnil), sur son site et dans plusieurs guides pratiques, analyse l'impact de l'entrée en vigueur de ce texte notamment pour les entreprises.

A noter : Le RGPD s'applique à un grand nombre de domaines et ne prévoit pas de règles particulières en matière de droit du travail laissant aux Etat-membres le soin de définir, sur ce point, les adaptations qu'ils jugent nécessaires.

1° Ce qui change par rapport à la situation antérieure

Alors que l'ancienne directive 95/46/CE du 24 octobre 1995 reposait en grande partie sur la notion de formalités préalables (déclaration, autorisations), le règlement européen y substitue une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement de la Cnil.

Les responsables de traitements doivent mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, dès la conception du produit ou du service et de façon continue, c'est-à-dire être en mesure de démontrer la conformité de leurs traitements tout moment.

La conséquence de cette responsabilisation des acteurs est la suppression des obligations déclaratives préalables.

Le CE ou le CSE doit être informé sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci.

Cette suppression des obligations déclaratives est susceptible de poser des difficultés en cas de litige. L'absence de déclaration obligatoire à la Cnil permettait à un salarié

sanctionné ou licencié de se prévaloir de l'irrecevabilité de la preuve des faits qui lui étaient reprochés tirée d'un dispositif de contrôle non déclaré.

2. Qui est concerné ?

Tout organisme, quels que soient sa taille, son pays d'implantation et son activité, peut être concerné. En effet, le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

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

Le RGPD concerne aussi les **sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes, notamment les entreprises. Les sous-traitants sont soumis à des obligations particulières : protection des données personnelles et de la vie privée dès la conception de leur service ou de leur produit, conseil auprès de leurs clients, tenue d'un registre des activités de traitement effectuées pour le compte de leurs clients. Le contrat de sous-traitance doit prévoir une clause spécifique sur la protection des données personnelles. Des exemples de clauses sont disponibles sur le site internet de la Cnil.

3. De quoi parle-t-on ?

On entend par donnée personnelle toute information permettant d'identifier directement (nom, prénom, par exemple) ou indirectement (numéro client, numéro de téléphone, numéro d'immatriculation pour la gestion d'un parking, donnée biométrique, etc.) une personne. Une personne peut ainsi être identifiée à partir d'une seule donnée (ex : numéro de sécurité sociale) ou à partir du croisement d'un ensemble de données (personne vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

A noter : Les adresses IP et Mac constituent des données personnelles.
La collecte de certaines données doit donner lieu à une vigilance particulière, notamment celles ayant trait aux ayants-droit des salariés dans la mesure où elles peuvent renseigner sur leur orientation sexuelle.
La notion de fichier recouvre 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 (ex : dossiers classés par ordre alphabétique ou chronologique).

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, rapprochement).

A noter : Un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles.
Par ailleurs, un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent également être protégés.

Un traitement de données personnelles doit avoir un objectif, une finalité. Il n'est pas possible de collecter ou traiter des données personnelles simplement au cas où cela pourrait s'avérer utile un jour.

Le responsable du traitement est 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 et sur lequel reposent les obligations prévues par le règlement.

La personne concernée par un traitement est celle à laquelle se rapportent les données objet du traitement.

Le destinataire d'un traitement est toute 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, ce dernier s'entendant de toute personne 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.

4. Comment se mettre en conformité avec le RGPD ?

Le règlement repose sur les principes suivants. Les données à caractère personnel doivent être :

- traitées de manière **licite, loyale et transparente** au regard de la personne concernée ;
- collectées pour des **finalités déterminées**, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ;
- **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;
- **exactes** et **tenues à jour** ;
- **conservées** sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- 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 (intégrité et confidentialité).

Concrètement, les différentes actions à mener pour se conformer à ces principes sont les suivantes :
- désigner un pilote ;
- recenser les fichiers ;
- repérer les traitements à risque ;
- respecter le droit des personnes ;
- sécuriser les données ;
- s'assurer, en cas de sous-traitance que le prestataire respecte le RGPD.

5. Désigner un pilote

La désignation d'un **délégué à la protection des données** (DPO) n'est obligatoire que pour les organisme publics et les entreprises dont l'activité de base amène à réaliser un **suivi régulier et systématique** des personnes à **grande échelle**, ou à traiter à grande échelle des données dites sensibles ou relatives à des condamnations pénales et infractions.

Toutefois, même si l'entreprise n'est pas formellement dans l'obligation de désigner un tel délégué, la Cnil recommande de désigner une personne disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen.

Chef d'orchestre de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :
- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'entreprise sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Le délégué peut être désigné en interne parmi les salariés de l'entreprise ou en externe. Il peut aussi être mutualisé entre plusieurs organismes ou au sein d'associations ou fédérations professionnelles.

A noter : La notion de traitement à grande échelle n'est pas définie par le RGPD. La Cnil donne sur ce point les exemples suivants : les traitements gérant les données des voyageurs utilisant les transports en commun ou ceux relatifs aux données de leurs clients administrés par les banques, les compagnies d'assurance, les opérateurs téléphoniques ou fournisseurs d'accès internet sont des traitements de données à grande échelle.

6. Recenser les traitements

L'obligation de tenir un **registre** des traitements de données personnelles ne concerne que les entreprises d'**au moins 250 salariés,** mais la Cnil en préconise la réalisation de manière plus large.

L'objectif est d'identifier les activités principales de l'entreprise qui nécessitent la collecte et le traitement de données (exemples en ce qui concerne la gestion des ressources humaines : le recrutement, la gestion de la paie, la formation, les déclarations sociales obligatoires, la gestion des badges et des accès, etc.).

Il s'agit de répertorier pour chaque activité recensée :
- le **responsable** du traitement ;
- l'**objectif** poursuivi ;
- les **catégories de données** utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
- qui a **accès aux données** (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- la **durée de conservation** de ces données (durée pendant laquelle les données sont utiles d'un point de vue opérationnel et durée de conservation en archive).

Le registre est placé sous la responsabilité du dirigeant de l'entreprise. La Cnil en propose un modèle sur son site Internet.

Selon la Cnil, il n'est pas nécessaire de répertorier dans ce registre les traitements purement occasionnels (exemple : fichier constitué pour une opération événementielle ponctuelle comme l'inauguration d'une boutique).

7. Repérer les traitements à risques

Le responsable des traitements devant désormais prouver à tout moment que les traitements qu'il gère sont conformes à la réglementation, le RGPD amène à s'interroger sur la pertinence des données collectées.

Pour chaque traitement, il conviendra de vérifier :
- quelles ont été les circonstances de collecte des données : y-a-t-il eu consentement des personnes concernées ? Dans la négative la collecte répond-elle à des obligations particulières (collecte nécessaire au contrat, respect d'une obligation légale, par exemple le traitement de données relatives aux salariés pour les communiquer à la sécurité sociale ou l'administration fiscale…) ? ;
- quelle a été l'information délivrée aux personnes faisant l'objet de la collecte et du traitement : celles-ci ont-elles été informées de la finalité du traitement et de leurs droits ? ;
- la nature des données collectées au regard de la finalité du traitement : seules les données strictement nécessaires au traitement peuvent être collectées et traitées ;

- que seules les personnes habilitées ont accès aux données dont elles ont besoin et que les données ne sont pas conservées au-delà de ce qui est nécessaire.

Certains traitements réclament une **vigilance particulière**. Il s'agit des traitements **ayant pour objet ou pour effet** :

- 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. Sont concernées les données révélant l'origine prétendument raciale ou ethnique, portant sur les opinions politiques, philosophiques ou religieuses, relatives à l'appartenance syndicale, concernant la santé ou l'orientation sexuelle, les données génétiques ou biométriques, les données d'infraction ou de condamnation pénale ;
- Le traitement de données concernant des personnes vulnérables (exemple : mineurs) ;
- Des usages innovants ou l'application de nouvelles technologies (exemple : objet connecté) ;
- 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 (PIA : Privacy Impact Assesment) doit être conduite. La Cnil a mis en place un logiciel facilitant la conduite et la formalisation d'analyses d'impact : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

A noter : L'article 8 du projet de loi relatif à la protection des données personnelles adopté par le Parlement le 14 mai 2018 interdit le traitement des données sensibles visées au 4° ci-dessus. Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne seront cependant pas soumis à cette interdiction notamment les traitements conformes à des règlements types établis par la Cnil mis en œuvre par les employeurs et portant sur des données biométriques strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux stagiaires ou aux prestataires.

Dans un souci de simplicité et d'accompagnement, la Cnil n'exigera pas la réalisation immédiate d'une analyse d'impact pour les traitements existants qui ont régulièrement fait l'objet d'une formalité préalable auprès de la Cnil avant le 25 mai 2018 (récépissé, déclaration de conformité à certaines normes, autorisation, avis de la Cnil), ou qui ont été consignés au registre d'un correspondant informatique et libertés. Les entreprises concernées disposent d'un délai de **3 ans** à compter du 25 mai 2018 pour effectuer cette étude d'impact. Cette tolérance ne s'applique pas aux traitements, antérieurs au 25 mai 2018 et régulièrement mis en œuvre, mais qui ont fait l'objet d'une **modification substantielle** depuis l'accomplissement de leur formalité préalable.

Le responsable du traitement (ou son sous-traitant) doit **consulter la Cnil** préalablement à la mise en œuvre du traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

En cas de **transfert de données hors de l'Union européenne**, il conviendra de vérifier si le pays vers lequel les données sont transférées dispose d'une législation de protection des données et si elle est reconnue adéquate par la Commission européenne. Une carte du monde présentant les législations de protection des données est disponible sur le site de la Cnil. Sinon, l'entreprise devra encadrer juridiquement ses transferts pour assurer la protection des données à l'étranger.

8. Informer les salariés

Quel que soit le support de collecte utilisé (formulaire, questionnaire, etc.) celui-ci doit comporter les informations suivantes :

- l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;
- les catégories de données à caractère personnel concernées ;
- le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel (service interne à l'entreprise, prestataire...) ;
- la durée de conservation des données ;
- les modalités selon lesquelles les intéressés peuvent exercer leurs droits (via leur espace personnel sur le site internet de l'entreprise, par un message sur une adresse email dédiée, par un courrier postal à un service identifié…) ;
- en cas de transfert de données hors de l'Union européenne, l'indication du pays concerné, l'existence ou l'absence d'une décision d'adéquation rendue par la Commission européenne ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

Ces informations doivent être données :

- dès la **collecte des données** dans le cas où celle-ci sont **recueillies directement auprès du salarié** (lors de l'embauche, par exemple) ;
- au **maximum un mois** après cette collecte si les données sont recueillies de façon indirecte, auprès d'une **autre source**.

Elles n'ont pas à être fournies si le salarié en dispose déjà.

A noter : S'agissant plus particulièrement des relations de l'entreprise avec ses salariés, la Cnil préconise d'informer ces derniers à chaque fois qu'il leur est demandé des informations (exemples : mises à jour de données administratives, demande de formation, formulaire d'entretien d'évaluation etc.) ou lors de la mise en place d'un dispositif de surveillance, selon des modalités à déterminer selon l'organisation de

l'entreprise (note de service, avenant au contrat de travail, information sur l'Intranet, courrier joint au bulletin de paie etc.).

9. Garantir les droits des salariés sur leurs données

Les salariés ont des droits sur leurs données, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement (droit à l'oubli), droit à la portabilité et à la limitation du traitement.

Les moyens d'exercer effectivement leurs droits doivent être mis à leur disposition : formulaire de contact sur un site web, numéro de téléphone ou adresse de messagerie.

Le droit à l'oubli est le droit pour une personne d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant. Les motifs justifiant l'exercice de ce droit sont limitativement énumérés par l'article 17 du RGPD. De façon générale, le RGPD impose de procéder à la suppression des données dès lors qu'elles ne sont plus utiles au regard des finalités pour lesquelles elles ont été collectées. Il est recommandé au-delà de la fixation de délais de suppression des données selon les fichiers, de prévoir des mécanismes de suppression automatique ou des alertes sur les outils utilisés pour la conservation des fichiers. En ce qui concerne plus particulièrement le recrutement, les informations sur les candidats non retenus doivent être supprimées sauf s'ils acceptent de rester dans le « vivier » de l'entreprise (durée de conservation limitée à 2 ans).

Le droit à limitation d'un traitement s'entend de la faculté pour une personne de demander à ce que le responsable du traitement ne puisse se servir de certaines données collectées.

Le droit à la portabilité constitue une nouveauté. Il s'agit du droit pour une personne d'obtenir, voire de réutiliser, les données la concernant pour ses besoins personnels.

Trois conditions doivent être réunies :
- les données personnelles ont été fournies par la personne elle-même ;
- les données sont traitées de manière automatisée, sur la base du consentement de l'intéressée ou pour l'exécution d'un contrat ;
- la portabilité ne doit pas porter atteinte aux droits et libertés de tiers.

10. Sécuriser les données

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données traitées et des risques qui pèsent sur les personnes en cas d'incident.

Différentes actions doivent être mises en place : mises à jour des antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement des données dans certaines situations.

L'entreprise victime d'une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou il a été constaté un accès non autorisé à des données) doit le signaler à la Cnil dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées. Cette notification s'effectue en ligne sur le site internet de la Cnil.

Il faut aussi notifier à la ou les personnes concernées que leurs données ont été potentiellement mises en danger.

A noter : S'il n'est pas possible d'identifier précisément les personnes susceptibles d'être impactées par les failles de sécurité, il faut notifier au public ce qui peut s'avérer très grave en termes d'image.

11. Des sanctions graduées, encadrées et renforcées

Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du règlement : avertissement, mise en demeure, injonction de cesser le traitement, suspension des flux de données etc.

Les **amendes administratives** peuvent s'élever, selon la catégorie de l'infraction, à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, à 2 % jusqu'à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Ce dernier montant doit être rapporté au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée par l'ensemble des autorités de régulation concernées, donc potentiellement pour le territoire de toute l'Union européenne.

Dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de protection sera infligée à l'entreprise.

12. Comment la Cnil contrôlera-t-elle le respect du RGPD à partir du 25 mai 2018 ?

D'une manière générale, les pouvoirs de contrôle de la Cnil restent inchangés. Elle continuera à procéder à des vérifications dans les locaux des organismes, en ligne, sur audition et sur pièces. Les modalités de déclenchement des contrôles restent également les mêmes : la décision de réaliser un contrôle s'effectuera sur la base du programme annuel des contrôles, des plaintes reçues par la Cnil, des informations figurant dans les médias, ou pour faire suite à un précédent contrôle.

La principale nouveauté réside dans le fait que les contrôles effectués sur des acteurs internationaux s'effectueront dans un contexte de coopération très poussée qui conduira à une décision harmonisée à portée européenne.

Les principes fondamentaux de la protection des données restent pour l'essentiel inchangés (loyauté du traitement, pertinence des données, durée de conservation, sécurité des données, etc.). Ils continueront donc à faire l'objet de vérifications rigoureuses par la Cnil.

En revanche, pour ce qui est des nouvelles obligations ou des nouveaux droits résultant du RGPD (droit à la portabilité, analyses d'impact, etc.), les contrôles opérés auront essentiellement pour but, dans un premier temps, d'accompagner les entreprises vers une bonne compréhension et la mise en œuvre opérationnelle des textes. En présence d'organismes de bonne foi, engagés dans une démarche de conformité et faisant preuve de coopération avec la Cnil, ces contrôles n'auront normalement pas vocation à déboucher, dans les premiers mois, sur des procédures de sanction sur ces points.

Editions Francis Lefebvre

Redevance audiovisuelle

Minoration de la redevance audiovisuelle des hôtels de tourisme saisonniers étendue aux chambres d'hôtes

Le ministre de l'action et des comptes publics admet que les exploitants de chambres d'hôtes bénéficient, comme les exploitants d'hôtels de tourisme, de la minoration de **25 %** de la contribution à l'audiovisuel public (ex-redevance audiovisuelle), sous réserve qu'ils soient en mesure de justifier d'une période d'activité n'excédant pas la même période de 9 mois.

En effet, les hôtels de tourisme dont la période d'activité annuelle n'excède pas 9 mois bénéficient d'une minoration de 25 % sur la contribution à l'audiovisuel public. Ils peuvent justifier du bénéfice de cette minoration par tout moyen, en particulier par la fourniture de l'arrêté préfectoral portant les mentions de saisonnalité, de la déclaration de CFE ou d'un extrait du registre du commerce et des sociétés précisant l'activité saisonnière.

Rép. Vigier n° 6364, JO 15 mai 2018, AN quest. p. 4066

Juin 2018

FISCAL

Entreprises soumises à la TVA :

☑ déclaration DES (déclaration européenne de services) et déclaration DEB (déclaration d'échange de biens) pour les opérations intracommunautaires réalisées en mai 2018

Toute personne ayant payé des dividendes en mai 2018 :

☑ déclaration (2777-D) en mode EDI au service des impôts des entreprises ou à la DGE (dividendes et/ou intérêts des comptes d'associés, à l'exclusion d'autres revenus)

Impôt Société :

☑ pour les entreprises assujetties clôturant au 28/02/2018
- solde de liquidation

☑ pour les entreprises soumises à l'IS
- acompte

Entreprises redevables de la Cotisation Foncière des Entreprises - IFER :

☑ télépaiement de l'acompte de CFE 2018 égal à 50 % des cotisations 2017

Entreprises redevables de la Cotisation sur la Valeur Ajoutée des Entreprises :

☑ télépaiement du premier acompte de CVAE 2018

Entreprises redevables de la TASCOM :

☑ déclaration et paiement

Redevables de l'Impôt sur la Fortune Immobilière dont la valeur nette du patrimoine immobilier excède 1 300 000 € :

☑ déclaration (dématérialisée ou papier)

Délai variable :

- déclaration de TVA du mois de mai 2018

SOCIAL

Toutes les entreprises ayant des salariés (DSN)

Indices du coût de la construction (ICC)

Période	2011	2012	2013	2014	2015	2016	2017
1er trimestre	1554	1617	1646	1648	1632	1615	1650
2ème trimestre	1593	1666	1637	1621	1614	1622	1664
3ème trimestre	1624	1648	1612	1627	1608	1643	1670
4ème trimestre	1638	1639	1615	1625	1629	1645	**1667**

INSEE, 21 mars 2018

Indices de référence des baux

	Indices de référence			
	2ème trimestre 2017	3ème trimestre 2017	4ème trimestre 2017	1er trimestre 2018
Baux d'habitation (IRL)	126,19	126,46	126,82	**127,22**
Baux commerciaux (ILC)	110,00	110,78	**111,33**	
Baux professionnels (ILAT)	109,89	110,36	**110,88**	

INSEE, 21 mars 2018 et 12 avril 2018