RGPD

Passez à l'action !

Amphithéâtre de la CCISM

Vendredi 7 mars 2019

De 14h à 18h30

esci

CCISM
POLYNÉSIE FRANÇAISE

DGEN
DIRECTION GENERALE DE L'ECONOMIE NUMERIQUE

OPEN
Organisation des Professionnels de l'Économie Numérique

CLUSIR
TAHITI

TAHITI NUI FORTRESS

DT
DIGITAL TAHITI

SPILOG
Partner Consulting Services

ACTECIL
RGPD SOLUTIONS

IAORA systems
SERVICES ET INGÉNIERIE INFORMATIQUES

Le RGPD

En quoi sommes nous concernés ?

SIPF
SERVICE DE L'INFORMATIQUE
DE LA POLYNESIE FRANCAISE

Quelques éléments de contexte

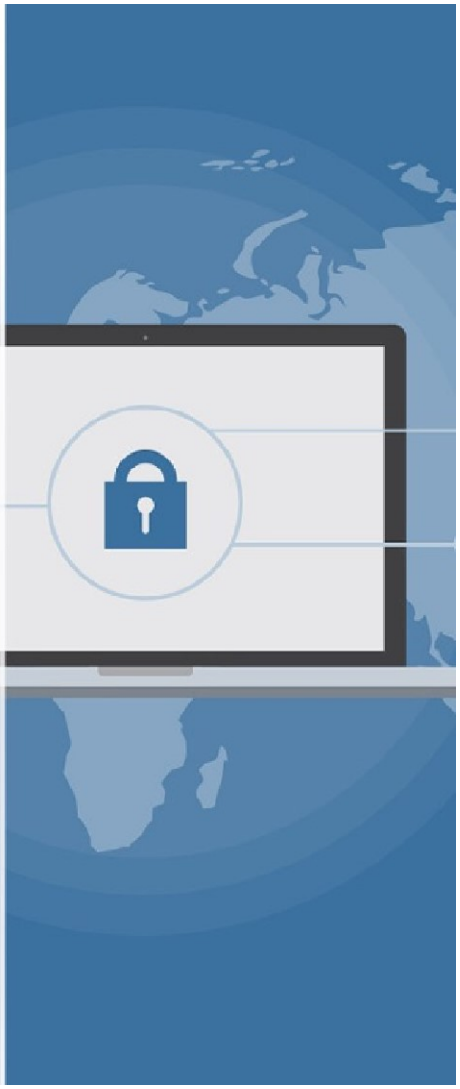
Le RGPD renforce la protection des données personnelles (loi « Informatique et libertés » de 1978 et directive européenne de 1995) et offre une nouvelle approche : instauration du principe de responsabilité.

Protéger les individus face à une évolution numérique qui présente des risques pour leur vie privée :

- l'omniprésence d'internet, des réseaux sociaux, du e-commerce,
- la collecte quasi systématique de données, leur « marchandisation », le transfert international des données,
- la traçabilité et le profilage des individus,
- la facilité de faire des recherches sur les individus, sur internet.

C'est quoi être protégé(e) :

- savoir ce qui est collecté sur soi, pourquoi et pour combien de temps,
- avoir accès à ses données, en demander la rectification, la suppression, se faire oublier,
- Etre sûr que ceux qui traitent des données personnelles sont responsabilisés et ont pris les mesures nécessaires.



Quelle règlementation en Polynésie française ?

- ✓ La protection des individus en matière informatique a été instaurée par la loi n°78-17 du 6 janvier 1978 relative aux fichiers, à l'informatique et aux libertés, applicable en Polynésie française depuis 1980 et modifiée plusieurs fois.

- ✓ En 2018, le droit a évolué de manière importante. Le règlement UE 2016/ 679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) est en effet entré en application le 25 mai 2018 dans l'Union européenne.

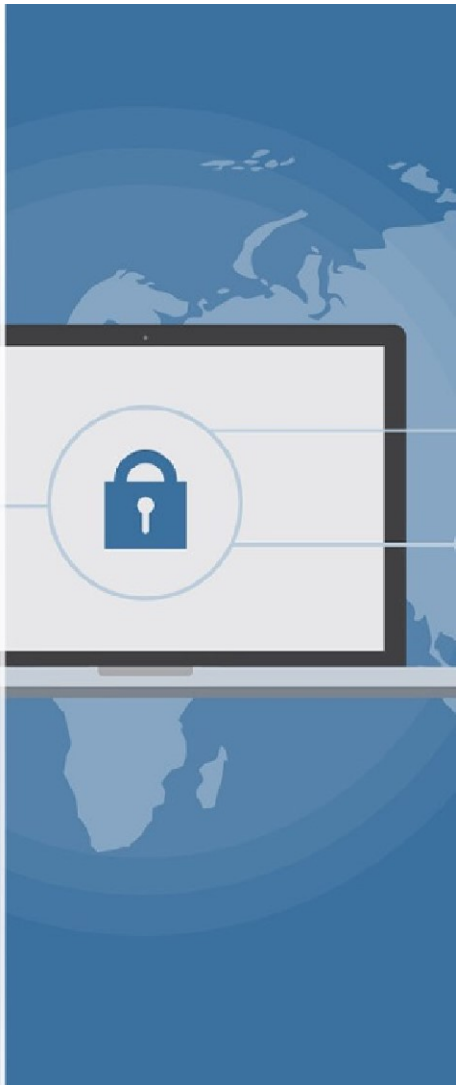
  Pour tenir compte du RGPD, la loi de 1978 a été modifiée, par une loi du 20 juin 2018.

  Mais ni le RGPD ni la loi du 20 juin 2018 ne nous étaient applicables en raison de notre statut particulier (PTOM- spécialité législative).

- ✓ ***Enfin, par une ordonnance n°2018-1125 du 12 décembre 2018, la loi de 1978 a été totalement réécrite.***

  En Polynésie française, la nouvelle réglementation nous est applicable, puisque l'ordonnance en prévoit l'extension dans notre collectivité. L'ordonnance a été publiée au JOPF du 21 décembre 2018.

C'est la loi du 6 janvier 1978, dans la version issue de l'ordonnance, qui nous est désormais applicable. Elle entrera en vigueur en même temps que le décret pris pour son application (modification du décret n° 2005-1309 du 20 octobre 2005) et au plus tard le 1er juin 2019.



« Art. 27 bis.— Les dispositions du présent décret sont étendues aux territoires d'outre-mer, sous réserve des modalités d'adaptation énoncées à l'annexe jointe ».

Art. 2.— Le ministre de l'intérieur et le secrétaire d'Etat auprès du ministre de l'intérieur (Départements et territoires d'outre-mer) sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 23 janvier 1980.

Raymond BARRE.

Par le Premier ministre :
Le ministre de l'intérieur,
Christian BONNET.

Le secrétaire d'Etat auprès du ministre de l'intérieur (Départements et territoires d'outre-mer),
Paul DIJOUD.

ARRETE n° 3343 AA du 28 janvier 1980 *promulguant des actes du pouvoir central.*

Le haut-commissaire de la République en Polynésie française, chef du territoire,
Officier de la Légion d'Honneur,

Vu la loi n° 77-772 du 12 juillet 1977 relative à l'organisation de la Polynésie française, notamment son article 64 ;

Vu l'article 237 du décret du 21 novembre 1933 portant réorganisation judiciaire et fixant les règles de procédure en Océanie ;

Le conseil de gouvernement informé en séance du 19 décembre 1979,

Arrête :

Article 1er.— Sont promulgués dans le territoire pour y être exécutés selon leur forme et teneur :

- la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (et rectificatif) ;
J.O.R.F. n° 6 du 7 janvier 1978, page 227 et J.O.R.F. n° 21 du 25 janvier 1978, page 491.

- le décret n° 78-774 du 17 juillet 1978 pris pour l'application des chapitres Ier à IV et VII de la loi n° 78-17 du 6 janvier 1978 relatives à l'informatique, aux fichiers et aux libertés ;
J.O.R.F. n° 171 du 23 juillet 1978, page 2006.

- le décret n° 78-1223 du 28 décembre 1978 modifiant l'article 26 du décret n° 78-774 du 17 juillet 1978 pris pour l'application des chapitres Ier et VII de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
J.O.R.F. n° 303 du 29 décembre 1978, page 4323.

Art. 2.— Le présent arrêté sera enregistré, communiqué et publié selon la procédure d'urgence partout où besoin sera.

Papeete, le 28 janvier 1980.

Le haut-commissaire,
par délégation :
Le secrétaire général,
Michel KUHNMUNCH.

LOI n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés.*

L'Assemblée nationale et le Sénat ont adopté,

Le Président de la République promulgue la loi dont la teneur suit :

CHAPITRE Ier

Principes et définitions.

Article 1er.— **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.

Art. 2.— Aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Art. 3.— Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés.

Art. 4.— Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale.

Art. 5.— Est dénommé traitement automatisé d'informations nominatives au sens de la présente loi tout ensemble d'opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives.

CHAPITRE II

La commission nationale de l'informatique et des libertés.

Art. 6.— Une commission nationale de l'informatique et des libertés est instituée. Elle est chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations, en se concertant avec elles et en contrôlant les applications de l'informatique aux traitements des informations nominatives. La commission dispose à cet effet d'un pouvoir réglementaire, dans les cas prévus par la présente loi.

Art. 7.— Les crédits nécessaires à la commission nationale pour l'accomplissement de sa mission sont inscrits au budget du ministère de la justice. Les dispositions de la loi du 10 août 1922 relative au contrôle financier ne sont pas applicables à leur gestion. Les comptes de la commission sont présentés au contrôle de la Cour des comptes.

Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés

Dispositions rendues applicables à la Polynésie française

par :

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JOPF n° 9 du 15/03/1980 page 275 (Mention d'applicabilité en Polynésie française, Art. 47– 1ère extension)

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 relative à l'informatique, aux fichiers et aux libertés, JOPF n° 35 du 26 août 2004, page 2802 (Mention d'applicabilité en Polynésie française, Art. 13 – 2ème extension)

Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers (article 13) ; JOPF n° 6 du 09/02/2006, page 497 (Mention d'applicabilité en Polynésie française, Art. 28)

Loi n° 2007-1787 du 20 décembre 2007 relative à la simplification du droit, non publiée au JOPF [1] (changement terminologique relatif à la CNIL, applicable de plein droit)

Loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allégement des procédures, JOPF n° 23 du 04/06/2009 page 2324 (modification des articles 11, 13 et 15 relatifs à la CNIL applicables de plein droit)

Loi organique n° 2010-704 du 28 juin 2010 relative au Conseil économique, social et environnemental, non publiée au JOPF (modification de l'article 13 relatif à la composition de la CNIL applicable de plein droit)

Loi n° 2011-334 du 28 mars 2011 relative au défenseur des droits, publiée au JOPF n°14 du 07/04/2011, p1589 (modification des articles 11, 13, 16, 17, 44 à 51 relatifs à la CNIL applicables de plein droit)

Loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit, non publiée au JOPF (modification de l'article 13 relatif à la composition de la CNIL applicable de plein droit)

Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, non publiée au JOPF (Mention d'applicabilité en Polynésie française, Article 60)

Loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, publiée au JOPF n° 50 du 22/10/2013 à la page 10004 (Mention d'applicabilité en Polynésie française, Article 35)

Loi n° 2014-344 du 17 mars 2014 relative à la consommation, publiée au JOPF n° 24 du 25/03/2014 à la page 3947 (modification des articles 11 et 44 applicables de plein droit)

[1] La LOI n° 2008-696 du 15 juillet 2008 relative aux archives modifie l'article 36 de la loi n° 78-17, mais n'a pas été étendue à la Polynésie française. Elle n'est donc pas prise en compte dans la consolidation.

Secrétariat général du gouvernement de la Polynésie française

ACTES PUBLIES A TITRE D'INFORMATION

ACTES DU POUVOIR CENTRAL

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.

Le Président de la République,

Sur le rapport du Premier ministre et de la garde des sceaux, ministre de la justice,

Vu la Constitution, notamment son article 38 ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ;

Vu le code du cinéma et de l'image animée ;

Vu le code de commerce ;

Vu le code de la consommation ;

Vu le code de la défense ;

Vu le code des douanes ;

Vu le code de l'éducation ;

Vu le code de l'entrée et du séjour des étrangers et du droit d'asile ;

Vu le code de l'environnement ;

Vu le code de justice administrative ;

Vu le code des juridictions financières ;

Vu le code monétaire et financier ;

Vu le code du patrimoine ;

Vu le code pénal ;

Vu le code des postes et des communications électroniques ;

Vu le code des procédures civiles d'exécution ;

Vu le code de procédure pénale ;

Vu le code de la propriété intellectuelle ;

Vu le code de la recherche ;

Vu le code de la route ;

Vu le code rural et de la pêche maritime ;

Vu le code de la santé publique ;

Vu le code de la sécurité intérieure ;

Vu le code de la sécurité sociale ;

Vu le code des transports ;

Vu le code du travail ;

Vu le livre des procédures fiscales ;

Vu la loi n° 70-9 du 2 janvier 1970 réglementant les conditions d'exercice des activités relatives à certaines opérations portant sur les immeubles et les fonds de commerce ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée ;

Vu la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;

Source LEXPOL

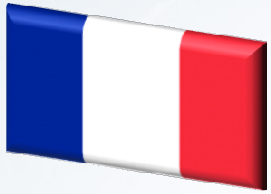
Quel périmètre ?

Le RGPD s'applique :

1. à tous ceux qui ont un établissement sur le territoire européen :
critère de la localisation de l'établissement
2. également à tous ceux qui
- offrent des biens et services (même gratuits) à une personne qui se trouve sur le territoire de l'union
- ou suivent son comportement (profilage, géolocalisation, navigation...) :
critère de la localisation de la personne concernée

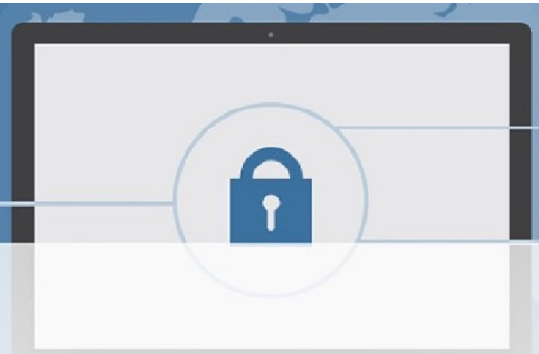
La loi française s'applique :

- à ceux qui ont un établissement sur le territoire français,
- dès lors que la personne concernée réside en France.



Dès son application en Polynésie française, la loi va s'appliquer dans les mêmes conditions à toute entité disposant d'un établissement en Polynésie française et aux personnes qui y résident.

Quelles entités concernées ?

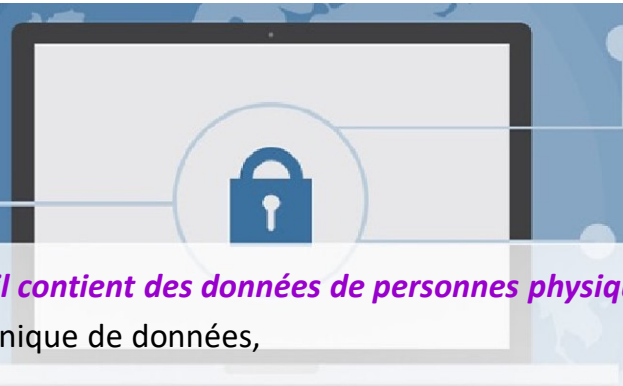


Est concernée toute personne physique ou morale qui déploie des traitements de données à caractère personnel
sauf les traitements mis en œuvre par une personne physique pour l'exercice d'activités strictement personnelles ou domestiques.

Sont donc notamment soumises à la loi :
- **les entreprises,**
- **les personnes physiques dans leurs activités professionnelles,**
- **les associations,**
- **les organismes publics.**

mais aussi les particuliers dans leurs activités qui ne sont pas exclusivement personnelles (par exemple la gestion d'un blog recueillant des commentaires)

Qu'est-ce un traitement ?



Le traitement est tout outil que vous utilisez, dès lors qu'il contient des données de personnes physiques.

- vos applications métier ou logiciels, votre gestion électronique de données,
- votre site internet,
- vos dossiers numériques, fichiers word, pdf, classeurs excell …
- votre vidéo-surveillance, vos contrôles d'accès (badges),
- les documents et dossiers papiers contenant les données de vos clients, personnels, fournisseurs.

Dans quelles conditions peut il être mis en œuvre ?

Un traitement ne peut être mis en œuvre que s'il se fonde sur : le consentement de la personne concernée, ou l'exécution d'un contrat, ou le respect d'une obligation légale ou règlementaire, ou l'exécution d'une mission d'intérêt public (…).

Il doit remplir certaines conditions :

- répondre à une finalité déterminée : à quoi sert il ?
- ne contenir que les données nécessaires, celle dont on a vraiment besoin,
- contenir des données exactes, tenues à jour,
- être sécurisé,
- ne pas conserver les données plus longtemps que nécessaire…

Qu'est ce qu'une donnée personnelle?

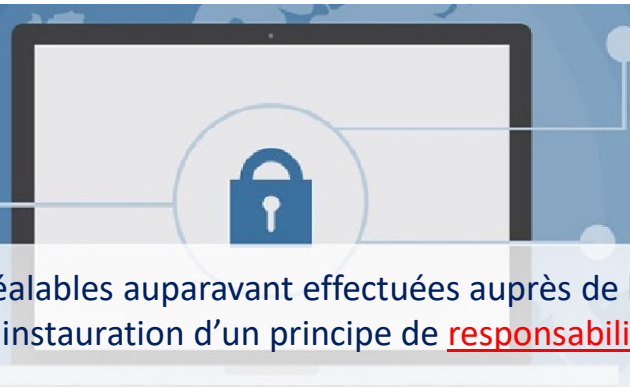
Une donnée personnelle est toute information, quelque en soit la forme (écrite, numérique, photographique, sonore…), qui permet, seule ou par combinaison avec d'autres informations, d'identifier quelqu'un.

Les données courantes	✓**État-civil, identité, données d'identification** ✓**Vie personnelle (habitudes de vie, situation familiale…)** ✓**Vie professionnelle (CV, scolarité, formation professionnelle, carrière, distinctions, notations ou évaluations…)** ✓**Informations d'ordre économique et financier (revenus, situation financière, situation fiscale…)** ✓**Données de connexion (adresses IP, journaux d'événements…)** ✓**Données de localisation (déplacements, données GPS, GSM…)** ✓**Données bancaires**
Les données sensibles	➢origine raciale ou ethnique, ➢opinions politiques, convictions religieuses ou philosophiques, ➢appartenance syndicale, ➢données génétiques, biométriques, ➢données de santé, ➢données concernant la vie sexuelle et l'orientation sexuelle.
Les données particulières Source CNIL	✓Le numéro d'immatriculation au répertoire national d'identification des personnes physiques (NIR) ✓les infractions, condamnations, mesures de sureté

En Polynésie française, il est plus facile d'identifier une personne à partir d'informations éparses, car la population y est peu nombreuse et beaucoup de personnes se connaissent ou entretiennent des liens amicaux, familiaux ou professionnels.

Des initiales, un prénom, une information sur le lieu de vie, une information sur l'activité professionnelle peuvent suffire à identifier quelqu'un de manière quasi certaine. C'est ce que l'on appelle le risque de ré identification.

Quelles contraintes ?



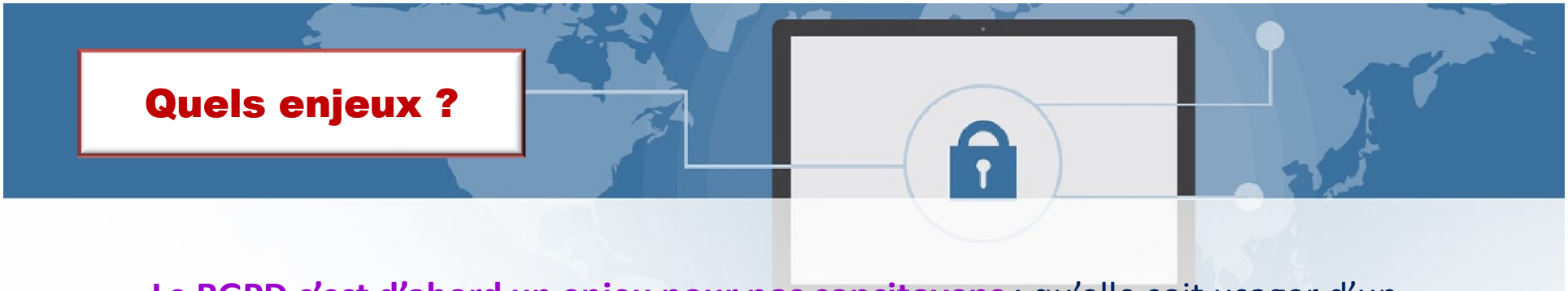
Suppression de la quasi totalité des formalités préalables auparavant effectuées auprès de la CNIL (allègement des formalités) Mais en contrepartie instauration d'un principe de responsabilité accrue des responsables de traitement.

Ils doivent prendre toutes les mesures techniques et organisationnelles et notamment :

- tenir un registre de traitements,
- nommer un délégué à la protection des données,
- évaluer les traitements, éventuellement faire réaliser des analyses d'impact pour les traitements présentant des risques, les mettre en conformité,
- introduire la protection des données dès la conception et par défaut,
- organiser l'information et les droits des personnes concernés,
- former les personnels ….

C'est ce changement d'approche qui constitue l'apport majeur du RGPD.

Quels enjeux ?



Le RGPD c'est d'abord un enjeu pour nos concitoyens : qu'elle soit usager d'un service public ou cliente d'une entreprise privée, toute personne a le droit au respect de sa vie privée et de ses données.

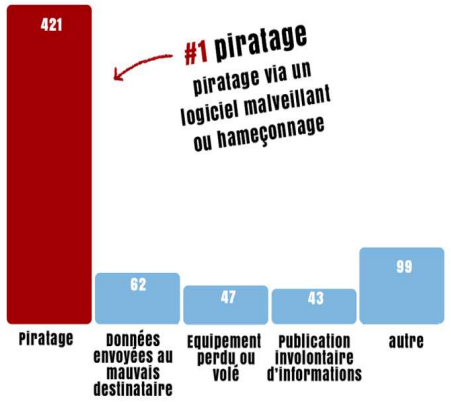
Un enjeu pour l'entreprise, mais aussi pour le service public : sa crédibilité (la confiance que l'on peut lui accorder) et sa réputation

Premier bilan de la CNIL

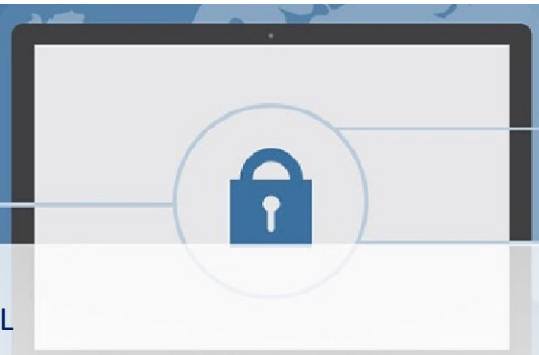
La CNIL a reçu 742 notifications de violations (entre le 25 mai et le 1er octobre) qui concerneraient les données de 33 727 384 personnes situées en France ou ailleurs.

Ces violations concernent :
- des atteintes à la confidentialité des données ;
- des atteintes à la disponibilité ;
- des atteintes à l'intégrité.

Deux grandes tendances se dessinent :
- Les piratages et vols intentionnels imputables à un tiers malveillant ;
- Les erreurs involontaires imputables à un personnel.



Quelles sanctions ?



Des sanctions administratives prononcées par la CNIL

Plusieurs degrés de sanctions selon l'infraction : rappel à l'ordre, injonction de mise en conformité, limitation du traitement, suspension d'un transfert de données hors UE, sanction pécuniaire de 10 millions d'euros ou 2% du chiffre d'affaire ou de 20 millions d'euros ou 4% du chiffre d'affaires (pour les infractions aux principes de base des traitements et aux droits de personnes)

La CNIL peut être saisie par les usagers ou agir de sa propre initiative.

Pour se prononcer elle prend en compte la nature de la violation, sa gravité, sa durée, le nombre de personnes concernées, les données en cause, si la violation est délibérée ou due à une négligence, les mesures prises pour atténuer le dommage, la bonne foi et la réactivité du responsable de traitement dans la gestion de la violation.

Des sanctions pénales. Elles font l'objet des articles 226-16 et suivants du code pénal.
Notamment, le fait de détourner des données de leur finalité, ainsi que le fait de divulguer à un tiers des informations qui pourrait porter atteinte à la considération d'une personne ou à l'intimité de sa vie privée sont punis de 5 ans d'emprisonnement et de 300 000 euros d'amende. La divulgation de données est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende si elle commise par négligence ou imprudence.
Le juge est saisi par la personne concernée.

Quelques exemples

Avertissement *prononcé contre OUI CAR en 2016 : Etaient accessibles à partir d'une adresse URL les données des utilisateurs du site : nom, prénom, adresse, numéro de téléphone, date de naissance, numéro de permis de conduire et données de localisation du véhicule proposé à la location.*

Cet accès et incident avait duré près de trois ans et était lié à un défaut élémentaire de sécurité. La violation a concerné 52 505 personnes.

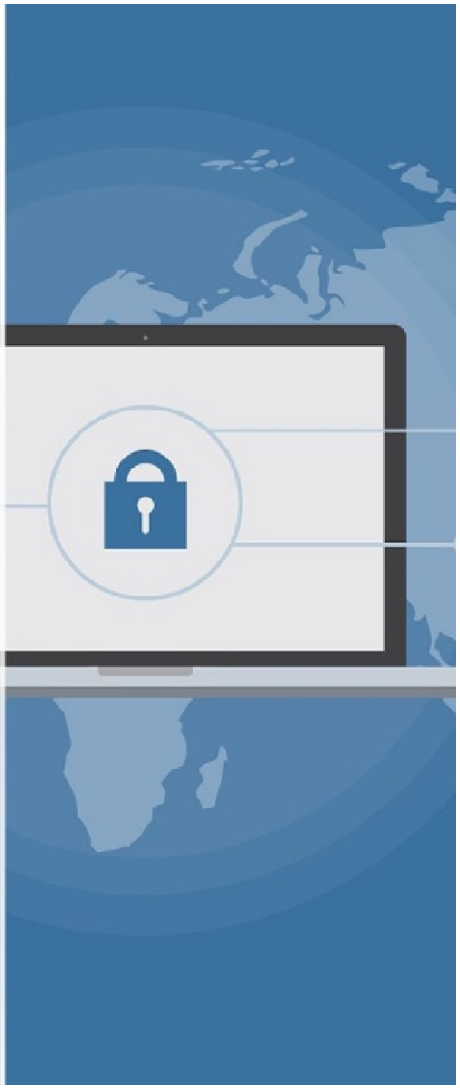
Amende de 40 000 euros *prononcée contre HERTZ France en 2017 : On lui a reproché d'avoir laissé un accès libre, à partir d'une adresse URL, aux données personnelles renseignées par 35 357 personnes inscrites sur le site (identité, coordonnées, numéro de permis de conduire).*

La faille était due à la suppression involontaire d'une ligne de code au moment du remplacement de l'un des serveurs assurant l'interface avec le prestataire en charge des paiements.

Amende de 250 000 euros *contre BOUYGUES en décembre 2018 pour un manquement à la sécurité des données personnelles de plus de deux millions d'utilisateurs de son site. La vulnérabilité trouvait son origine dans la fusion des systèmes informatiques des marques Bouygues Telecom et B&You. À l'occasion de tests effectués à la suite de la fusion de ces bases de données, le code informatique rendant nécessaire l'authentification au site web www.bouyguestelecom.fr avait été désactivé. En raison d'une erreur humaine commise par une personne agissant pour le compte de la société, ce code n'a pas été réactivé à l'issue des tests.*

Amende de 400 000 euros *contre UBER après que des individus aient dérobé les données personnelles de 57 millions d'utilisateurs (dont 1,4 millions situés sur le territoire français) en accédant à des identifiants stockés en clair sur la plateforme collaborative de développement « Github ». Ils ont ensuite utilisé ces identifiants pour accéder à distance à un serveur sur lequel sont stockées les données. Ils y ont téléchargé les informations relatives aux utilisateurs.*

Amende de 50 millions d'euros prononcée le 21 janvier 2019 par la CNIL, dans le cadre du règlement européen sur la protection des données, à l'encontre de la société GOOGLE LLC en application du RGPD pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité.



Des outils mis en ligne par la CNIL