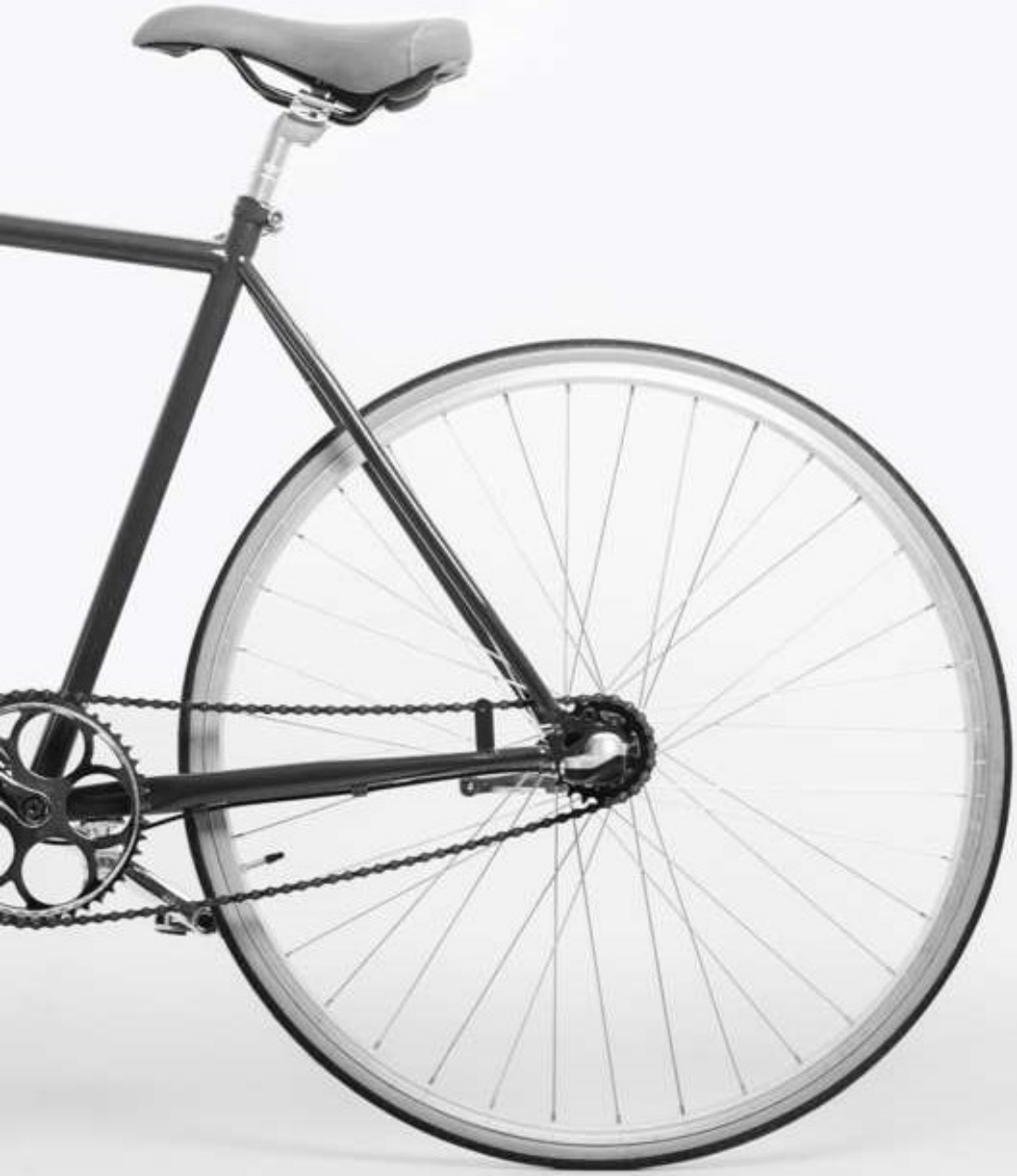
BignonLebray



PROTECTION DES DONNÉES PERSONNELLES

En Chine, en Europe, en France

MARS 2022

INTRODUCTION

CONTEXTE

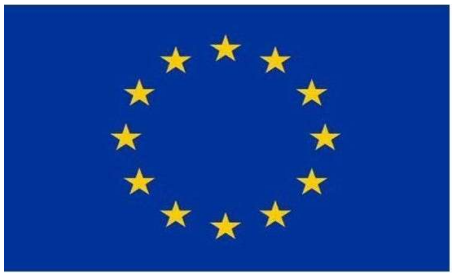
Adoption RGPD — 2016

Entrée en vigueur RGPD — 2018

Adoption PIPL — 20 août 2021

Entrée en vigueur PIPL — 1 nov. 2021

CONTEXTE LÉGISLATIF UNION EUROPÉENNE



Règlement général pour la protection des données RGPD 2016

Objectif : harmoniser à l'échelle européenne le niveau de protection des données personnelles

- Le RGPD est le texte de référence de la protection des données personnelles pour l'ensemble des Etats membres de l'Union européenne
- Il s'applique directement en droit français
- Il définit désormais les principes de protection des données personnelles et indique leurs conditions d'application : licéité des traitements, pertinence des données, information des personnes, durée de conservation et sécurité.

CONTEXTE LÉGISLATIF EN FRANCE

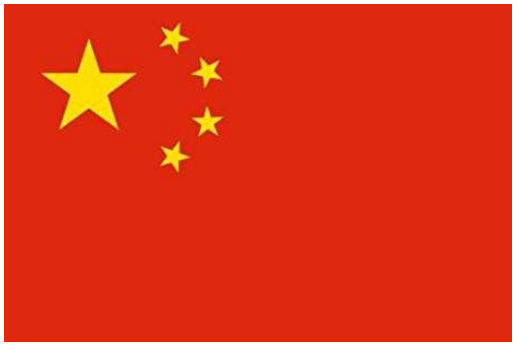
RGPD

- Le RGPD est d'application directe en France depuis 2018

A ce titre la loi Informatique et Libertés a été modifié par la LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles afin de :

- Permettre l'application effective du RGPD et de la directive « police » du 27 avril 2016 portant sur les fichiers en matière pénale, afin de renforcer les droits des citoyens sur leurs données personnelles,
- Mettre en œuvre les marges de manœuvre prévues par le RGPD,

CONTEXTE LÉGISLATIF CHINE

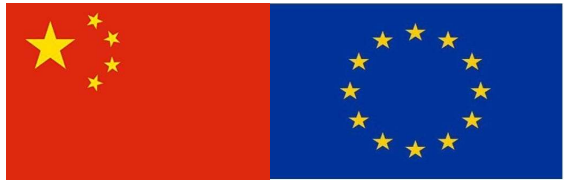


Plusieurs textes lois jusqu'à présent

- Loi sur le e-commerce 2017
- Loi sur la cybersécurité 2017
- Entrée en vigueur du nouveau Code civil chinois le 1er janvier 2021

Entrée en vigueur de la PIPL « *Personal information protection law* » le 1er novembre 2021 qui vise à harmoniser la protection des informations personnelles.

CONTEXTE LÉGISLATIF CHINE



STRUCTURE ET OBJECTIFS DIFFERENTS

RGPD = 11 chapitres, 99 articles et 173 considérants V. PIPL = 8 chapitres, 74 articles et 0 considérant

Protection de l'Etat pour assurer le commerce avec l'exterieur

v.

Protection de l'individu contre l'Etat

Article 11: The State establishes a personal information protection structure, to prevent and punish acts harming personal information rights and interests, strengthen personal information protection propaganda and education, and promote the creation of a good environment for personal information protection, **with joint participation from government, enterprise, relevant social organizations, and the general public**.

Article 12: The State vigorously participates in the formulation of international rules [or norms] for personal information protection, stimulates international exchange and cooperation in the area of personal information protection, **and promotes mutual recognition of personal information protection rules [or norms], standards, etc., with other countries, regions, and international organizations.**

1

LES ÉLÉMENTS ESSENTIELS DE COMPARAISON

DISPOSITIONS GÉNÉRALES

- **Objectifs (art. 1)**
- Etablir les règles de protection des personnes physiques à l'égard du traitement des données et celles relatives à leur libre circulation
- Protéger les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel.
- La libre circulation des données à caractère personnel au sein de l'Union

*General provisions / **Article 1 Subject-matter and objectives 1.***

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

- **Objectifs (art.1)**
- protéger les droits et les intérêts des informations personnelles,
- normaliser les activités de traitement des informations personnelles
- et promouvoir l'utilisation rationnelle des informations personnelles.

Chapter I: General Provisions

Article 1: This Law is formulated, on the basis of the Constitution, in order to protect personal information rights and interests, standardize personal information handling activities, and promote the rational use of personal information.

Article 2: The personal information of natural persons receives legal protection; no organization or individual may infringe upon natural persons' personal information rights and interests.

DISPOSITIONS GÉNÉRALES

- **Application territoriale (art. 3)**
- Critère d'établissement : Union Européenne
- Critère de ciblage : Etablis hors de l'UE mais visent les personnes se trouvant sur le territoire de l'UE pour :
  - leur offrir des biens ou des services
  - suivre leur comportement au sein de l'UE
- ***Article 3 Territorial scope 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. L 119/32 EN Official Journal of the European Union 4.5.2016 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.***

- **Application territoriale (art.3)**
- Critère d'établissement : Territoire Chinois
- Critère de ciblage : activités en dehors de la Chine qui ciblent des ressortissants chinois, soit en leur proposant des produits ou services ou en traitant de données personnelles d'individus situés en chine.

Article 3: This Law applies to the activities of handling the personal information of natural persons within the borders of the People's Republic of China.

Where one of the following circumstances is present in handling activities outside the borders of the People's Republic of China of personal information of natural persons within the borders of the People's Republic of China, this Law applies as well:

- Where the purpose is to provide products or services to natural persons inside the borders;
- Where analyzing or assessing activities of natural persons inside the borders;
-Other circumstances provided in laws or administrative regulations.

PRINCIPES ESSENTIELS

- **Donnée à caractère personnel (art. 4)**
- Toute information se rapportant à une personne physique identifiée ou identifiable (qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale).

Article 4 Definitions For the purposes of this Regulation: (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **Information personnelle (art. 4)**
- Les informations personnelles sont toutes sortes d'informations, enregistrées par des moyens électroniques ou autres, concernant des personnes physiques identifiées ou identifiables, à l'exclusion des informations traitées après anonymisation.

Article 4: Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling.

Personal information handling includes personal information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.

PRINCIPES ESSENTIELS

- **Traitement**
- toute opération effectuée ou non à l'aide de procédés automatisés et appliquées à des à caractère personnel (collecte, enregistrement, organisation, structuration, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission, mise à disposition, rapprochement, limitation, effacement ou destruction),

- ***4 (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;***

- **Traitement**
- Le traitement des informations personnelles comprend la collecte, le stockage, l'utilisation, le traitement, la transmission, la fourniture, la divulgation, la suppression, etc. des informations personnelles.

- ***4, al. 2: Personal information handling includes personal information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.***

PRINCIPES ESSENTIELS

Article 73: *The following terms used in this Law are defined as follows:*

"Personal information handler" refers to organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods.

"Automated decision-making" refers to the activity of using computer programs to automatically analyze or assess personal behaviors, habits, interests, or hobbies, or financial, health, credit, or other status, and make decisions [based thereupon].

"De-identification" refers to the process of personal information undergoing handling to ensure it is impossible to identify specific natural persons without the support of additional information.

"Anonymization" refers to the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore.

PRINCIPES ESSENTIELS

Loi sur la protection des informations personnelles

- *Article 5 Principles relating to processing of personal data 1.*

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); 4.5.2016 EN Official Journal of the European Union L 119/35 (1) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1). (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

PRINCIPES ESSENTIELS

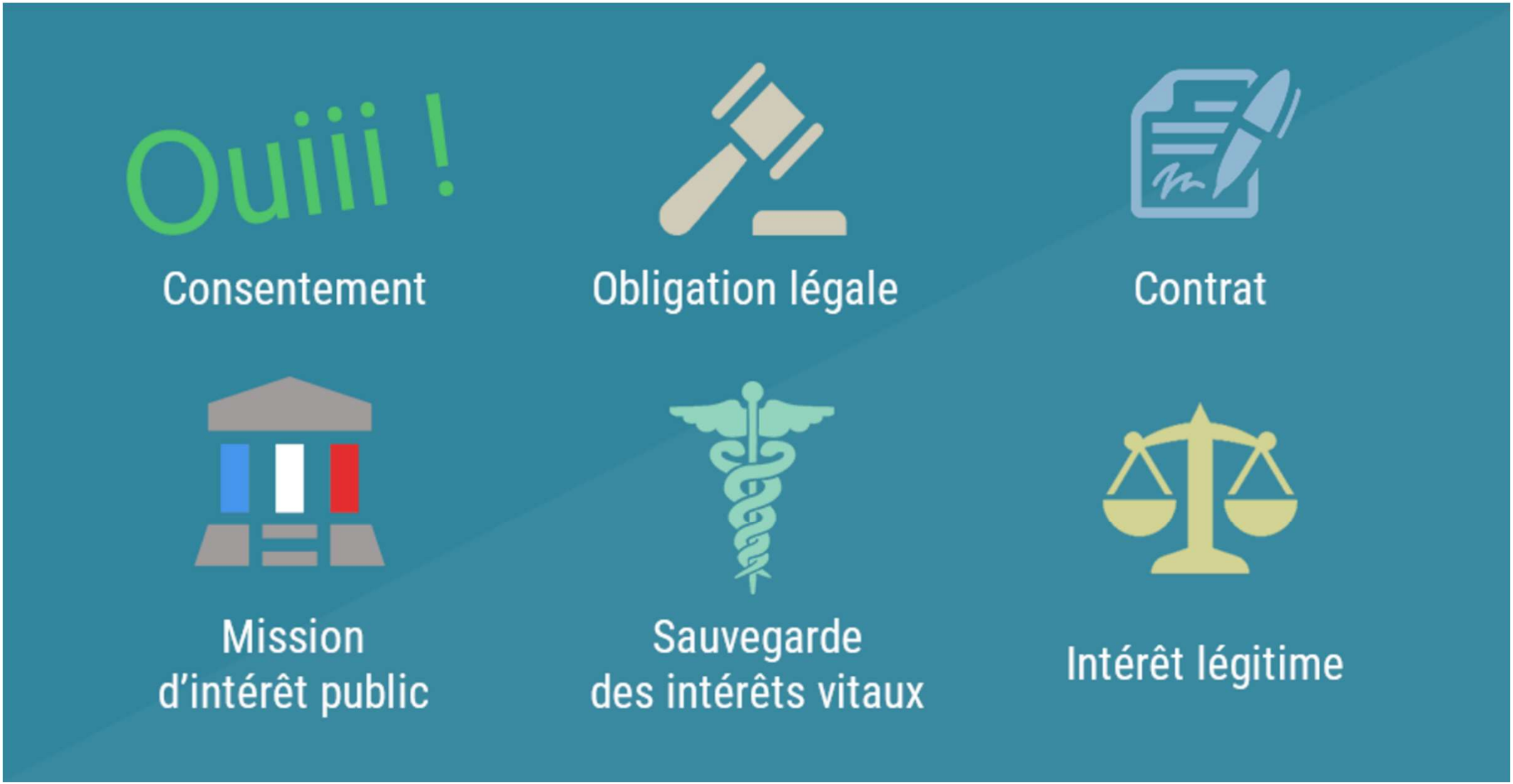
Loi sur la protection des informations personnelles

Article 5: The principles of legality, propriety, necessity, and sincerity shall be observed for personal information handling. It is prohibited to handle personal information in misleading, swindling, coercive, or other such ways. **Article 6:** Personal information handling shall have a clear and reasonable purpose, and shall be directly related to the handling purpose, using a method with the smallest influence on individual rights and interests. The collection of personal information shall be limited to the smallest scope for realizing the handling purpose, and excessive personal information collection is prohibited. **Article 7:** The principles of openness and transparency shall be observed in the handling of personal information, disclosing the rules for handling personal information and clearly indicating the purpose, method, and scope of handling. **Article 8:** The handling of personal information shall ensure the quality of personal information, and avoid adverse effects on individual rights and interests from inaccurate or incomplete personal information. **Article 9:** Personal information handlers shall bear responsibility for their personal information handling activities, and adopt the necessary measures to safeguard the security of the personal information they handle. **Article 10:** No organization or individual may illegally collect, use, process, or transmit other persons' personal information, or illegally sell, buy, provide, or disclose other persons' personal information, or engage in personal information handling activities harming national security or the public interest.

2

LES PRINCIPES DE PROTECTION DES DONNEES

LA BASE LÉGALE DANS LE RGPD



LA BASE LÉGALE DANS LA LOI SUR LA PROTECTION DES INFORMATIONS PERSONNELLES

Article 6 Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official

authority vested in the controller;

(f) is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of

LA BASE LÉGALE DANS LA LOI SUR LA PROTECTION DES INFORMATIONS PERSONNELLES

Article 13: Personal information handlers may only handle personal information where they conform to one of the following circumstances:

- Obtaining individuals' consent;

- Where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts;

- Where necessary to fulfill statutory duties and responsibilities or statutory obligations;

- Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;

- Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;

- When handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of this Law.

- Other circumstances provided in laws and administrative regulations.

In accordance with other relevant provisions of this Law, when handling personal information, individual consent shall be obtained. However, obtaining individual consent is not required under conditions in items 2 through 7 above.

Différence avec le RGPD : absence d'intérêt légitime

LE CONSENTEMENT DE LA PERSONNE

- **Art 13 :** Le consentement n'est pas nécessaire dans les points 2 à 7 de l'article 13.
- **Art 14** : Lorsque le consentement est nécessaire il est donné de façon volontaire, explicite et en connaissance de cause.
- **Art 15 :** Droit de retirer le consentement.

Art. 7 RGPD

Art. 39 de la loi sur la protection des informations personnelles :
Pour les transferts internationaux d'informations personnelles, un consentement distinct doit être obtenu des personnes concernées.

LE CONSENTEMENT DE LA PERSONNE

Article 14: Where personal information is handled based on individual consent, said consent shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Where laws or administrative regulations provide that separate consent or written consent shall be obtained to handle personal information, those provisions are to be followed.

Where a change occurs in the purpose of personal information handling, the handling method, or the categories of handled personal information, the individual's consent shall be obtained again.

Article 15: Where personal information is handled based on individual consent, individuals have the right to rescind their consent. Personal information handlers shall provide a convenient way to withdraw consent.

If an individual rescinds consent, it does not affect the effectiveness of personal information handling activities undertaken on the basis of individual consent before consent was rescinded.

Article 16: Personal information handlers may not refuse to provide products or services on the basis that an individual does not consent to the handling of their personal information or rescinds their consent, except where handling personal information is necessary for the provision of products or services.

LE CONSENTEMENT DE LA PERSONNE

Article 7

Conditions for consent

1. **Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2.**

2. **If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.**

3. **3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.**

LE PRINCIPE DE MINIMISATION

Le principe de la minimisation des données : les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées,

5 (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

Article 19: Except where laws or administrative regulations provide otherwise, personal information retention periods shall be the shortest period necessary to realize the purpose of the personal information handling.

L'INFORMATION DE LA PERSONNE CONCERNÉE

Art. 13 :

Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée

Au moment de la collecte des données le responsable du traitement fournit :

- L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement / les coordonnées du DPO /les finalités et bases juridiques du traitement / les intérêts légitimes éventuels / les destinataires des données / la présence d'un transfert de données hors UE

Au moment de l'obtention des données

- Durée de conservation / droits de la personne concernée / le caractère obligatoire ou non de la collecte / l'existence de décision automatisée

Article 17: Personal information handlers shall, before handling personal information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language:
The name or personal name and contact method of the personal information handler;
The purpose of personal information handling and the handling methods, the categories of handled personal information, and the retention period;
Methods and procedures for individuals to exercise the rights provided in this Law;
Other items that laws or administrative regulations provide shall be notified.
Where a change occurs in the matters provided in the previous paragraph, individuals shall be notified about the change.
Where personal information handlers notify the matters as provided in Paragraph 1 through the method of formulating personal information handling rules, the handling rules shall be made public [disclosed] and convenient to read and store.

Article 18: Personal information handlers handling personal information are permitted **not to notify individuals about the items provided in Paragraph 1 of the previous Article under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary.**
Under emergency circumstances, where it is impossible to notify individuals in a timely manner in order to protect natural persons' lives, health, and the security of their property, personal information handlers shall notify them after the conclusion of the emergency circumstances.

LA PLURALITÉ DE RESPONSABLES DE TRAITEMENTS

Article 26 Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects. 2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject. 3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 20: Where two or more personal information handlers jointly decide on a personal information handling purpose and handling method, they shall agree on the rights and obligations of each. However, said agreement does not influence an individual's rights to demand any one personal information handler perform under this Law's provisions.

Where personal information handlers jointly handling personal information harm personal information rights and interests, resulting in damages, they bear joint liability according to the law.

LA SOUS-TRAITANCE

Art. 4 RGPD : *sous-traitant : personne physique ou morale, autorité publique, service ou autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.*

Art. 28 : Obligations du sous-traitant, par exemple :

- Nécessité d'un contrat écrit avec le responsable du traitement
- Garanties suffisantes pour la mise en œuvre de mesures techniques et organisationnelles appropriées
- Recrutement d'un autre sous-traitant seulement avec autorisation écrite préalable du responsable du traitement
- Même en cas de recrutement de son propre sous-traitant le sous-traitant initial demeure responsable devant le responsable du traitement

LA SOUS-TRAITANCE

Art. 21 : Accord nécessaire entre responsable de traitement et sous traitant sur l'objectif du traitement confié, le délai, la méthode de traitement, les catégories d'informations personnelles, les mesures de protection, les droits et devoirs respectifs.

Les sous traitants doivent traiter les informations personnelles conformément à l'accord ; elles ne peuvent pas traiter les informations personnelles à des fins de traitement ou selon des méthodes de traitement qui vont au-delà de l'accord.

Sans le consentement du responsable du traitement, le sous-traitant ne peut pas sous traiter à d'autres personnes.

Art. 23 : Les destinataires doivent traiter les informations personnelles dans le cadre des objectifs de traitement, des méthodes de traitement, des catégories d'informations personnelles, etc. mentionnés ci-dessus. Lorsque les destinataires modifient la finalité ou les méthodes de traitement initiales, ils doivent à nouveau obtenir le consentement de la personne concernée.

Art. 59 : Les sous-traitants doivent prendre les mesures nécessaires pour préserver la sécurité des informations personnelles qu'elles traitent, et aider les responsables de traitement à remplir les obligations prévues par la loi sur la protection des informations personnelles.

LA SOUS-TRAITANCE

Article 21: Where personal information handlers entrust the handling of personal information, they shall conclude an agreement with the entrusted person on the purpose for entrusted handling, the time limit, the handling method, categories of personal information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information handling activities of the entrusted person.

Entrusted persons shall handle personal information according to the agreement; they may not handle personal information for handling purposes or in handling methods, etc., in excess of the agreement. If the entrusting contract does not take effect, is void, has been cancelled, or has been terminated, the entrusted person shall return the personal information to the personal information handler or delete it, and may not retain it.

Without the consent of the personal information handler, an entrusted person may not further entrust personal information handling to other persons.

Article 23: Where personal information handlers provide other personal information handlers with the personal information they handle, they shall notify individuals about the name or personal name of the recipient, their contact method, the handling purpose, handling method, and personal information categories, and obtain separate consent from the individual. Recipients shall handle personal information within the above mentioned scope of handling purposes, handling methods, personal information categories, etc. Where recipients change the original handling purpose or handling methods, they shall again obtain the individual's consent.

Article 59: Entrusted persons accepting entrusted handling of personal information shall, according to the provisions of this Law and relevant laws and administrative regulations, take necessary measures to safeguard the security of the personal information they handle, and assist personal information handlers in fulfilling the obligations provided in this Law.

LE TRAITEMENT DES DONNÉES SENSIBLES

DÉFINITIONS

Considérant 51 RGPD : Les données à caractère personnel qui sont, par nature, particulièrement sensibles du point de vue des libertés et des droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits.

+ Article 9 RGPD

Art. 28 et suivants de la loi sur la protection des informations personnelles : « *Sensitive personal information means personal information that, once leaked or illegally used, may easily cause* ***harm to the dignity*** *of natural persons* ***grave harm to personal or property security****, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.*

Only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures, may personal information handlers handle sensitive personal information."

LE TRAITEMENT DE DONNÉES SENSIBLES

Art. 9 : Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

Article 29: To handle sensitive personal information, the individual's **separate consent** shall be obtained. Where **laws or administrative regulations provide that written consent** shall be obtained for handling sensitive personal information, those provisions are to be followed.

Article 30: Personal information handlers handling sensitive personal information, in addition to the items set out in Article 17, Paragraph 1, of this Law, shall also **notify individuals of the necessity and influence on the individual's rights and interests of handling the sensitive personal information**, except where this Law provides that it is permitted not to notify the individuals.

Article 31: Where personal information handlers handle the personal information of minors under the age of 14, they shall **obtain the consent of the parent or other guardian of the minor.** Where personal information handlers handle the personal information of minors under the age of 14, they shall formulate specialized personal information handling rules.

LE TRAITEMENT DES DONNÉES SENSIBLES

TRAITEMENT

Art. 9 RGPD : Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

Art. 28 de la loi sur la protection des informations personnelles : Les personnes chargées du traitement des informations personnelles ne peuvent traiter des informations personnelles sensibles que s'il existe un objectif spécifique et un besoin à satisfaire, et dans le cadre de mesures de protection strictes.

3

LES TRANSFERTS DE DONNÉES

L'ENCADREMENT DES TRANSFERTS DE DONNÉES

Les transferts hors Union Européenne (articles 44 et suivants du RGPD)

Les transferts de données depuis le territoire européen vers des pays situés en-dehors de l'UE sont INTERDITS sauf

Si le transfert est fondé sur une décision d'adéquation. Le transfert a lieu vers un pays reconnu par la Commission européenne comme **offrant un niveau de protection des données suffisant** (ex : Brésil, Canada, Argentine, etc.)

Si le transfert repose sur des garanties appropriées :

- **un instrument juridiquement contraignant** et exécutoire entre les autorités ou organismes publics ;
- des **règles d'entreprise contraignantes** (« BCR ») ;
- des **clauses types** adoptées par la Commission ou par une autorité de contrôle et approuvées par la Commission ;
- **un code de conduite** ou un mécanisme de certification, assorti de l'engagement contraignant et exécutoire pris par le RT ou le ST dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne le droit des personnes.

Si le transfert repose sur des garanties appropriées sous réserve de l'autorisation de l'autorité de contrôle :

- clauses contractuelles entre le RT ou le ST et le RT, le ST ou le destinataire des données ;
- dispositions à intégrer dans des arrangements administratifs entre autorités publiques ou organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

L'ENCADREMENT DES TRANSFERTS DE DONNÉES

Les transferts hors de la République populaire de Chine (Chapitre III - articles 38 à 43 de la loi sur la protection des informations personnelles)

Les transferts de données depuis la République populaire de Chine vers des pays situés en-dehors sont possibles à condition de

Réussir une **évaluation de sécurité** organisée par le département d'État de la cybersécurité et de l'informatisation pour les opérateurs d'infrastructures d'information critiques et les responsables (handlers) qui traitent un grand nombre d'informations personnelles au regard des quantités définies par le département de cybersécurité et d'informatisation de l'État (article 38.1)

Se soumettre à une **certification de protection des informations personnelles** menée par un organisme spécialisé conformément aux dispositions du département d'État chargé de la cybersécurité et de l'informatisation (art.38.2)

Conclure un **contrat avec la partie réceptrice étrangère** conformément à un contrat type formulé par le département d'État chargé du cyberespace et de l'informatisation, en convenant des droits et des responsabilités des deux parties (art.38.3)

Respecter les autres conditions prévues par les lois ou les règlements administratifs ou par le département d'État chargé de la cybersécurité et de l'informatisation (art.38.4).

L'ENCADREMENT DES TRANSFERTS DE DONNÉES

Les transferts hors de la République populaire de Chine (Chapitre III - articles 38 à 43 de la loi sur la protection des informations personnelles)

Article 38: Where personal information handlers truly need to provide personal information outside the borders of the People's Republic of China for business or other such requirements, they shall meet one of the following conditions:

(1) Passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of this Law;

(2) Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department;

(3) Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides;

(4) Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.

Where treaties or international agreements that the People's Republic of China has concluded or acceded to contain relevant provisions such as conditions on providing personal data outside the borders of the People's Republic of China, those provisions may be carried out.

Personal information handlers shall adopt necessary measures to ensure that foreign receiving parties' personal information handling activities reach the standard of personal information protection provided in this Law.

L'ENCADREMENT DES TRANSFERTS DE DONNÉES

Les transferts hors de la République populaire de Chine (Chapitre III - articles 38 à 43 de la loi sur la protection des informations personnelles)

Article 39: Where personal information handlers provide personal information outside of the borders of the People's Republic of China, they shall notify the individual about the foreign receiving side's name or personal name, contact method, handling purpose, handling methods, and personal information categories, as well as ways or procedures for individuals to exercise the rights provided in this Law with the foreign receiving side, and other such matters, and obtain individuals' separate consent.

Article 40: Critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the State cybersecurity and informatization department shall store personal information collected and produced within the borders of the People's Republic of China domestically. Where they need to provide it abroad, they shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cybersecurity and informatization department provisions permit that security assessment not be conducted, those provisions are to be followed.

Article 41: Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to handle foreign judicial or law enforcement authorities' requests regarding the provision of personal information stored domestically. Without the approval of the competent authorities of the People's Republic of China, personal information handlers may not provide personal information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies.

Article 42: Where foreign organizations or individuals engage in personal information handling acts violating personal information rights and interests of citizens of the People's Republic of China, or harming the national security or public interest of the People's Republic of China, the State cybersecurity and informatization department may put them on a list limiting or prohibiting personal information provision, issue a warning, and adopt measures such as limiting or prohibiting the provision of personal information to them, etc.

Article 43: Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt reciprocal measures against said country or region on the basis of actual circumstances.

4

LES DROITS DES PERSONNES

DROITS DES PERSONNES

Les droits des personnes dans l'UE (articles 12 et suivants du RGPD)

- Droit à l'information
- Droit d'accès
- Droit d'opposition
- Droit de rectification
- Droit à l'effacement
- Droit à la portabilité
- Limitation du traitement

Spécificité française : directives relatives au sort de ses données à caractère personnel après sa mort (article 48 de la loi Informatique et Libertés)

Les droits des personnes dans la République populaire de Chine (articles 44 et suivants de la loi sur la protection des informations personnelles)

- Droit à l'information (art.44 + art.48)
- Droit d'accès (art. 45)
- Droit d'opposition (art.44)
- Droit de rectification (art.46)
- Droit à l'effacement (art.47)
- Droit à la portabilité (art.45)
- Limitation du traitement (art.47)
- Sort des données après la mort (art.49)

EXERCICE DES DROITS DES PERSONNES

Conditions similaires en cas d'exercice du droit d'accès

Dans l'UE (articles 12 et 15 du RGPD, article 49 de la loi Informatique et Libertés)

Droit de demander au responsable des informations relatives au traitement et une copie de ses données.

Délais de réponse : Dans les meilleurs délais ou au maximum, un mois

Refus motivé : Le responsable du traitement peut refuser de répondre à une demande notamment si :

- Le responsable du traitement ne peut pas identifier la personne concernée
- Les demandes sont manifestement infondées ou excessives notamment en raison de leur caractère répétitif

Le cas échéant, le responsable du traitement doit également informer la personne de la possibilité d'introduire une réclamation auprès de l'autorité de contrôle ou de former un recours juridictionnel.

Dans la République populaire de Chine (articles 45 et 48 de la loi sur la protection des informations personnelles)

Droit de demander au responsable des informations relatives au traitement et une copie de ses données.

Délai de réponse : le responsable du traitement doit répondre « en temps voulu » sans qu'un délai soit précisé

Refus motivé : Le responsable du traitement peut refuser de répondre à une demande et en expliquer la raison.

En cas de rejet de la demande, la personne peut intenter une action en justice auprès d'un tribunal populaire.

EXERCICE DES DROITS DES PERSONNES

Droit à l'effacement / « droit à l'oubli » dans l'UE (article 17 du RGPD) **et dans la République populaire de Chine** (article 47 de la loi sur la protection des informations personnelles)

Cas communs pour lesquels le droit à l'oubli peut être exercé :

1. Les données ne sont plus nécessaires
2. La personne a retiré son consentement
3. Le traitement est illicite

Cas propres à l'UE :

1. Exercice du droit d'opposition par la personne concernée
2. L'effacement correspond au respect d'une obligation légale
3. Offre de services de la société de l'information pour les mineurs

EXERCICE DES DROITS DES PERSONNES

Conditions d'exercice du **droit à la portabilité dans l'UE** (article 20 du RGPD)

Droit pour la personne concernée, de recevoir les données à caractère personnel la concernant dans un format structuré permettant leur réutilisation et d'obtenir du responsable du traitement qu'il transfère directement ses données au tiers de son choix, également responsable du traitement

Deux conditions :

S'applique aux traitements fondés sur :
- le consentement
ou
- un contrat

+

le traitement est effectué à l'aide de procédés automatisés.

Conditions d'exercice du **droit à la portabilité dans la République populaire de Chine** (article 45 de la loi sur la protection des informations personnelles)

Lorsqu'une personne demande que ses informations personnelles soient transférées à un responsable de traitement, et qui répond aux conditions du département national de la cybersécurité et de l'informatisation, ledit responsable doit fournir un moyen de les transférer.

EXERCICE DES DROITS DES PERSONNES

Le sort des données après la mort

Régime juridique encadré par des directives (Article 85 de la loi Informatique et Libertés)

Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.

Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la CNIL.

Les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés.

Régime juridique plus souple (Article 49 de de la loi sur la protection des informations personnelles)

Lorsqu'une personne physique est décédée, ses proches peuvent, au regard de leurs propres intérêts légitimes, exercer les droits du défunt pour consulter, copier, corriger, supprimer, etc. ses informations personnelles, sauf si le défunt en a disposé autrement avant son décès.

EXERCICE DES DROITS DES PERSONNES

Modalités pratiques

Article 50: Personal information handlers shall establish convenient mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason.

Where personal information handlers reject individuals' requests to exercise their rights, individuals may file a lawsuit with a People's Court according to the law.

5

LES OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

Sur la désignation d'un référent à la protection des données

Article 24 Responsibility of the controller
1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 51: Personal information handlers shall, on the basis of the personal information handling purpose, handling methods, personal information categories, as well as the influence on individuals' rights and interests, possibly existing security risks, etc., adopt the following measures to ensure personal information handling conforms to the provisions of laws and administrative regulations, and prevent unauthorized access as well as personal information leaks, distortion, or loss:
-Formulating internal management structures and operating rules;
-Implementing categorized management of personal information;
-Adopting corresponding technical security measures such as encryption, de-identification, etc.;
-Reasonably determining operational limits for personal information handling, and regularly conducting security education and training for employees;
-Formulating and organizing the implementation of personal information security incident response plans;
-Other measures provided in laws or administrative regulations.

OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

Sur la désignation d'un référent à la protection des données

Désignation d'un DPO (Articles 37 à 39 du RGPD)

La désignation du DPO est obligatoire dans trois cas :

1. pour toute autorité publique ou tout organisme public ;
2. si les activités de base de l'organisme consistent en des traitements qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
3. si les activités de base de l'organisme consistent en des traitements à grande échelle de données sensibles, ou de données relatives aux condamnations et infractions spéciales.

Désignation d'un agent de protection des informations personnelles (Article 52 de de la loi sur la protection des informations personnelles)

Les responsables qui traitent des informations personnelles **atteignant des quantités définies par le département de cybersécurité et d'informatisation de l'État** doivent nommer des agents de protection des informations personnelles, chargés de superviser les activités de traitement des informations personnelles ainsi que les mesures de protection adoptées, etc.

OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

Obligation de sécurité similaire entre l'UE (article 32 du RGPD) et la République populaire de Chine (article 51 de la loi sur la protection des informations personnelles)

Le responsable du traitement doit :

- Prévoir des procédures internes, notamment en cas de violation de données
- Mettre en œuvre une gestion des accès et habilitations des données ;
- Adopter des mesures de sécurité techniques telles que le cryptage, la dé-identification des données, etc ;
- Organiser régulièrement des formations sur la sécurité destinées aux employés.

Distinction au regard des audits visés :

Dans le RGPD : l'article 32 vise « *une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

Tandis que dans la loi sur la protection des informations personnelles : l'article 54 prévoit que le responsable doit régulièrement réaliser des audits pour s'assurer de la conformité aux lois et règlements administratifs applicables.

Article 54: Personal information handlers shall regularly engage in audits of their personal information handling and compliance with laws and administrative regulations.

OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

En cas de faille de sécurité, la loi chinoise prévoit:

Article 57: *Where a personal information leak, distortion, or loss occurs or might have occurred, personal information handlers shall immediately adopt remedial measures, and notify the departments fulfilling personal information protection duties and responsibilities and the individuals. The notification shall include the following items:*

The information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred;

The remedial measures taken by the personal information handler and measures individuals can adopt to mitigate harm;

Contact method of the personal information handler.

Where personal information handlers adopt measures that are able to effectively avoid harm created by information leaks, distortion, or loss, personal information handlers are permitted to not notify individuals; however, where departments fulfilling personal information protection protection duties and responsibilities believe harm may have been created, they may require personal information handlers to notify individuals.

Même mécanisme mis en place pour la notification des violations de données auprès des autorités compétentes et des personnes concernées. En revanche, l'article 57 de la loi sur la protection des informations personnelles ne prévoit pas de délai de notification tandis que l'article 33 du RGPD prévoit un délai de 72h.

OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

Sur la nécessité ou non de réaliser une étude d'impact au regard des nombreux critères visés par le RGPD, le CEPD et la CNIL

3 cas prévus par l'article 35 du RGPD dans lesquels une AIPD doit être menée

- L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

- Le traitement à grande échelle de catégories particulières ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

- La surveillance systématique à grande échelle d'une zone accessible au public.

Si le traitement remplit au moins deux des critères posés par le CEPD, l'analyse d'impact est nécessaire

1. Evaluation/Scoring
2. Décision automatique avec effet légal
3. Surveillance systématique
4. Données sensibles
5. Large échelle
6. Croisement de données
7. Personnes vulnérables
8. Usage innovant
9. Blocage d'un droit/contrat

La CNIL a également listé les types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise, par exemple pour les :

- Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médicosociaux pour la prise en charge des personnes
- Traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés

OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

Sur la nécessité ou non de réaliser une étude d'impact : une liste plus restrictive de critères

L'article 55 de la loi sur la protection des informations personnelles vise 5 cas pour lesquels une évaluation préalable de l'impact sur la protection des informations personnelles doit être réalisée :

1. Traitement d'informations personnelles sensibles ;
2. Utilisation d'informations personnelles pour la prise de décision automatisée ;
3. Confier le traitement d'informations personnelles, fournir des informations personnelles à d'autres personnes traitant des informations personnelles, ou divulguer des informations personnelles ;
4. Fournir des informations personnelles à l'étranger ;
5. Autres activités de traitement des informations personnelles ayant une influence majeure sur les individus.

En revanche, les conditions de mise en œuvre sont identiques sur le contenu (article 35 du RGPD et article 56 de la loi sur la protection des informations personnelles) **et la durée de validité est de 3 ans**

Voir à ce sujet : Délibération n° 2018-326 du 11 octobre 2018 portant adoption de lignes directrices sur les AIPD prévues par le RGPD)

OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

Spécificité chinoise : supervision des plateformes Internet (article 58 de la loi sur la protection des informations personnelles)

Article 58: *Personal information handlers providing important Internet platform services, that have a large number of users, and whose business models are complex shall fulfill the following obligations:*

1. Establish and complete personal information protection compliance systems and structures according to State regulations, and establish an independent body composed mainly of outside members to supervise personal information protection circumstances;

2. Abide by the principles of openness, fairness, and justice; formulate platform rules; and clarify the standards for intra-platform product or service providers' handling of personal information and their personal information protection duties;

3. Stop providing services to product or service providers on the platform that seriously violate laws or administrative regulations in handling personal information;

4. Regularly release personal information protection social responsibility reports, and accept society's supervision.

6

LES AUTORITÉS DE CONTRÔLE

AUTORITES DE CONTRÔLE

Dans l'UE (articles 51 et suivants du RGPD), il y a :

Le Comité européen de la protection des données qui est un organe de l'UE qui a notamment pour mission de surveiller et garantir la bonne application du RGPD, de conseiller la Commission sur toute question relative à la protection des données à caractère personnel dans l'Union, de publier des lignes directrices, des recommandations et des bonnes pratiques (articles 68 et suivants du RGPD).

L'autorité de contrôle désignée dans chaque Etat membre chargée de surveiller l'application du RGPD, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union (articles 51 et suivants du RGPD).

- Par exemple en France, il s'agit de la CNIL.

Lorsque le traitement des données à caractère personnel a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant dans l'Union et que ce responsable du traitement ou ce sous-traitant est établi dans plusieurs États membres, ou que le traitement qui a lieu dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant dans l'Union affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres, l'autorité de contrôle dont relève l'établissement principal ou l'établissement unique du responsable du traitement ou du sous-traitant devrait faire office **d'autorité chef de file** (considérant 124 du RGPD). Les autorités de contrôle compétentes et l'autorité chef de file coopèrent ensemble dans le cadre du mécanisme « One Stop Shop » (articles 60 et suivants du RGPD).

AUTORITES DE CONTRÔLE

Dans la République populaire de Chine (articles 60 et suivants de la loi sur la protection des informations personnelles), il y a trois niveaux :

Le **département d'État de la cybersécurité et de l'informatisation** est responsable de la planification et de la coordination globales des activités de protection des informations personnelles ainsi que des activités de supervision et de gestion connexes. Par exemple, il va formuler des règles et des normes concrètes de protection des informations personnelles mais aussi des normes spécialisées destinées aux responsables d'informations personnelles à petite échelle pour le traitement des informations personnelles sensibles, la reconnaissance faciale, l'intelligence artificielle, etc.

Les **départements compétents du « State Council »** sont responsables de la protection, de la supervision et de la gestion des informations personnelles dans le cadre de leurs fonctions et responsabilités respectives.

Les devoirs et responsabilités des **départements concernés des gouvernements populaires de comté et de niveau supérieur** en matière de protection, de supervision et de gestion des informations personnelles sont déterminés conformément aux dispositions pertinentes de l'État. Par exemple,

- Faire de la propagande et de l'éducation sur la protection des renseignements personnels,
- Accepter et traiter les plaintes et les rapports relatifs à la protection des informations personnelles,
- Enquêter et traiter les activités illégales de traitement des informations personnelles.

AUTORITES DE CONTRÔLE

Les pouvoirs d'enquête sont similaires entre les autorités de contrôle (article 58 du RGPD) **et les départements concernés des gouvernements populaires de comté et de niveau supérieur** (article 60 et suivants de la loi sur la protection des informations personnelles)

- Interviewer les parties concernées et enquêter sur les circonstances liées aux activités de traitement des informations personnelles ;
- Consulter et reproduire les contrats, les dossiers et les reçus d'une partie concernée ainsi que d'autres documents pertinents liés aux activités de traitement des informations personnelles ;
- Effectuer des inspections sur place et mener des enquêtes sur les activités de traitement des informations personnelles suspectées d'être illégales ;
- Inspecter les équipements liés aux activités de traitement des informations personnelles.

Focus de la loi sur la protection des informations personnelles sur la découverte d'un incident de sécurité (article 64) :

Lorsque les services chargés de la protection des informations personnelles découvrent que des risques relativement importants existent dans les activités de traitement des informations personnelles ou que des incidents liés à la sécurité des informations personnelles se produisent, ils peuvent s'entretenir avec le responsable, ou lui demander de confier à des institutions spécialisées la réalisation d'audits de conformité de ses activités de traitement des informations personnelles.

MESURES CORRECTRICES

Sur les mesures correctrices pouvant être prononcées avant une sanction

Article 58 du RGPD

Respect des obligations prévues par le règlement, par exemple :

1. Avertir un RT ou un ST d'un risque de violation des dispositions du règlement
2. Rappel à l'ordre du RT ou ST en cas de violation des dispositions du règlement
3. Ordonner la mise en conformité dans un délai déterminé

Respect du droit des personnes concernées, par exemple :

1. Ordonner au RT ou au ST de satisfaire aux demandes de la personne concernée en vue d'exercer ses droits
2. Respect de l'obligation de communication de l'existence d'une violation des données
3. Rectification ou effacement des données ou limitation du traitement et notification au destinataire

Article 66 de la loi sur la protection des informations personnelles

1. Demander la correction du ou des manquements constatés
2. Confisquer les revenus illicites
3. Ordonner la suspension provisoire ou la résiliation de la prestation de services portant sur le système d'information litigieux

SANCTIONS

Article 83 du RGPD

<u>Niveau 1 :</u> Amende maximale de 10 000 000 euros ou 2% du chiffre d'affaires annuel mondial.

- **En particulier le non-respect des obligations du responsable de traitement ou du sous-traitant dans l'organisation du traitement.**

  <u>Ex</u> : absence de tenue d'un registre, le défaut de nomination d'un DPO ou absence de réalisation d'une étude d'impact

<u>Niveau 2 :</u> Amende maximale de 20 000 000 euros ou 4% du chiffre d'affaires annuel mondial.

- **Selon la nature du manquement aux règles de protection des données, en particulier le non-respect des droits des personnes.**

  <u>Ex</u> : le manquement au recueil du consentement de la personne concernée

SANCTIONS

Article 66 de la loi sur la protection des informations personnelles

<u>Niveau 1 :</u> Amende maximale d'1 million de yuans.

Sanctions complémentaires :

- la personne responsable directement en charge et les autres personnels directement responsables doivent être condamnés à une amende comprise entre 10 000 et 100 000 yuans.

<u>Niveau 2 :</u> En cas de manquements graves, 50 millions de yuans, ou 5 % du revenu annuel.

Sanctions complémentaires :

- suspension des activités commerciales connexes ou la cessation d'activité pour rectification,
- faire un rapport au département compétent pour l'annulation des licences administratives correspondantes ou l'annulation des licences commerciales.
- La personne directement responsable et les autres membres du personnel directement responsables sont passibles d'une amende comprise entre 100 000 et 1 million de yuans, et il peut également être décidé de leur interdire d'occuper des postes de directeur, de superviseur, de cadre de haut niveau ou de responsable de la protection des informations personnelles pendant une certaine période.

Les manquements à la loi sur la protection des informations personnelles sont inscrits dans des fichiers de crédit (article 67).

RECOURS

Recours de la personne concernée contre le responsable de traitement (article 82 du RGPD et article 69 de la loi sur la protection des informations personnelles)

Recours par le parquet et les organisations de consommateurs (articles 2 et suivants du Code de procédure pénale et article 70 de la loi sur la protection des informations personnelles)

RECOURS

Article 66: *Where personal information is handled in violation of this Law or personal information is handled without fulfilling personal information protection duties in accordance with the provisions of this Law, the departments fulfilling personal information protection duties and responsibilities are to order correction, confiscate unlawful income, and order the provisional suspension or termination of service provision of the application programs unlawfully handling personal information; where correction is refused, a fine of not more than* ***1 million Yuan is to be additionally imposed****; the directly responsible person in charge and other directly responsible personnel are to be fined between* ***10,000 and 100,000 Yuan.***

Where the circumstances of the unlawful acts mentioned in the preceding Paragraph are grave, the provincial- or higher-level departments fulfilling personal information protection duties and responsibilities are to order correction, ***confiscate unlawful income, and impose a fine of not more than 50 million Yuan, or 5% of annual revenue.*** *They may also order the suspension of related business activities or cessation of business for rectification, and report to the relevant competent department for cancellation of corresponding administrative licenses or cancellation of business licenses. The directly responsible person in charge and other directly responsible personnel are to be fined between* ***100,000 and 1 million Yuan, and it may also be decided to prohibit them from holding positions of director, supervisor, high-level manager, or personal information protection officer for a certain period.***

7

VUE D’ENSEMBLE

VUE D'ENSEMBLE

LES SIMILITUDES

- **Volonté identique**
- **Une structure d'ensemble et un socle textuel similaire**
- **Reprise des acteurs essentiels du RGPD**
- **Mêmes grands droits, notamment pour les personnes concernées**
- **Obligations similaire (analyse d'impact, exigences contractuelles, de sécurité, de notification etc.)**

VUE D'ENSEMBLE

LES DIFFÉRENCES

- **De manière générale, la loi chinoise reste nettement plus vague que le RGPD et nécessitera des lignes directrices pour préciser certains termes équivoques.**
- **Sur les transferts transfrontaliers des données à caractère personnel.**

Dans ce cadre, la PIPL introduit un certain nombre d'exigences semblables au RGPD (l'adoption des mesures nécessaires pour garantir que le destinataire des données assure un niveau de protection comparable)

Cependant, la PIPL va également bien plus loin que le RGPD sur ce point en exigeant une analyse d'impact systématique et la communication d'information précises sur le destinataire des données, elle exige également un consentement distinct. Cela complexifie ainsi les transferts de données.

- **Les dispositions propres aux opérateurs d'infrastructures stratégiques.**

Pour les transferts vers les opérateurs d'infrastructures stratégiques ("Critical information infrastructure operators"), ou à partir d'un certain seuil de données traitées (qui n'a pas encore été défini), l'intégralité des données devra être stockée sur le territoire chinois. Pour de tels acteurs, un éventuel transfert ne sera autorisé qu'après une évaluation de sécurité organisée par le département d'État de la cybersécurité et de l'informatisation.

CONCLUSIONS

Versus

Une protection des données, oui, mais pour des objectifs différents

INTERVENANTES

ELISE DUFOUR

AVOCAT ASSOCIÉ

edufour@bignonlebray.com

Tel : 01 44 17 14 91

MERCI

www.bignonlebray.com

PARIS
75, rue de Tocqueville
75017 Paris