

Personal data : your compliance

European Regulation on Personal Data
Law for a Digital Republic
Law for the modernisation of justice in the XXIth century



18 PRACTICAL SHEETS



The date of the coming into force of the General Data Protection Regulation on May 25th, 2018 has become real for all stakeholders (administrations, key accounts, start-ups, etc.).

This regulation will apply in the 28 Member States of the European Union as well as to any personal data processing activity which aims at offering goods and services to European residents or at targeting them.

Regardless of the substantial amount of sanctions in the event of a breach, personal data is at the heart of the economy with its new exponential uses (artificial intelligence, data mining, etc.).

The GDPR, far from being a hinderance, aims at allowing each stakeholder to implement its compliance by defining its own measures or procedures namely through data mapping, flows between the different providers as well as by secured contracts (accountability of the stakeholders).

This conformity must be a “win-win” situation for the users (“all of us”) with this need for confidence, increased transparency, as well as for the professionals by reinforcing their credibility. Let us not forget that in this digital economy, personal data are immaterial assets having a definite economic value.

Conformity and governance tools are already available for stakeholders to enable them to have their own risk management such as the registry, the DPIA or preparing for the designation of a DPO (DPO, the keystone to compliance).

Furthermore, in France, the “protection of personal data” culture has been implemented since 1978. Some stakeholders have appointed a Freedoms and Computer Correspondent (FCC, in French “Correspondant Informatique et Libertés, CIL”) since 2005. Thus, it is possible to build

on pre-existing material. The Bill amending Act n°78-17 of the 6th of January 1978 on Information technology, Data files and Civil liberties which incorporates certain aspects of the GDPR is in line with this continuity.

As attorneys, we are confronted on a daily basis with the management of strategic issues. We help stakeholders with their legal compliance and digital transformation.

We hope you enjoy the reading and that this article will be useful for your projects.

Mathias Avocats remains at your disposal,

Garance Mathias

Avocat à la Cour

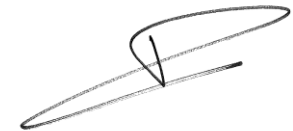


Table of contents

- **Sheet n°1:** Background
- **Sheet n°2:** The key concepts of personal data protection
- **Sheet n°3:** The stakeholders of personal data protection
- **Sheet n°4:** The reaffirmation of the principles of personal data protection
- **Sheet n°5:** The territorial application of the GDPR
- **Sheet n°6:** Accountability
- **Sheet n°7:** DPIA
- **Sheet n°8:** Crisis management reinforced
- **Sheet n°9:** The DPO's key role in compliance
- **Sheet n°10:** The data processor's obligations reinforced
- **Sheet n°11:** Joint controllers
- **Sheet n°12:** Strengthening data subjects' rights and enshrining new rights
- **Sheet n°13:** Transfers of personal data
- **Sheet n°14:** Supervisory authorities – With the removal of prior formalities, what is their role ?
- **Sheet n°15:** The deterrent effect of sanctions
- **Sheet n°16:** The changes brought by the Law for a Digital Republic
- **Sheet n°17:** The changes brought by the Law for the modernisation of justice in the XXIst century
- **Sheet n°18:** The contributions of the Bill on personal data



Sheet n°1: Background

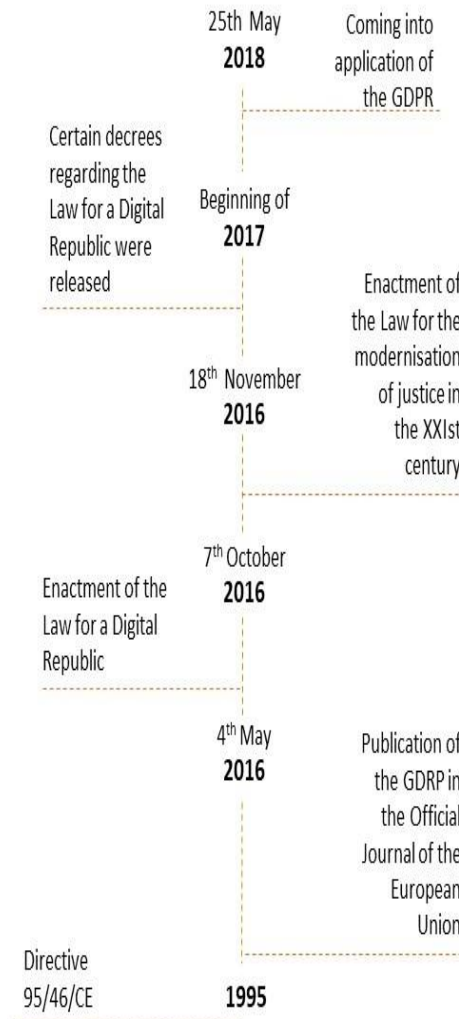
2016 was the year of personal data protection. After four years of debating, the European Commission, the European Parliament and the European Council finally came to an agreement December 15th, 2016.

The GDPR was published in the Official Journal of the European Union on **May 4th 2016** after having been formally approved by the institutions. The singularity lies in the fact that the GDPR will only be applicable two years from the date of its coming into force May 25th 2018.

During the year, numerous organisations undertook a compliance process to incorporate the new requirements under the General Data Protection Regulation. This movement will continue throughout the first quarter of 2018 until the Regulation comes into force on May 25th 2018.

The Member States' national institutions and supervisory authorities also took advantage of this transitional period.

Let us recall that the GDPR stems from Directive 95/46/EC of the October 24th, 1995¹. Each Member State then transposed the Directive into its national law. The Directive will be repealed when the GDPR comes into application on May 25th 2018.



In particular, the GDPR intends at harmonizing European legislations seeing as it will be directly applicable in each Member State without any transposition being necessary.

Nevertheless, the GDPR refers to the national law of member States in certain areas. Furthermore, some countries, such as Germany, have already passed a law incorporating the GDPR's requirements. In France, a Bill amending Act n°78-17 should be examined by parliamentarians within the following months.

Supervisory authorities have also been very active, whether collectively or individually. Indeed, the Article 29 Working Party (WP29) has adopted and published guidelines on certain notions (supervisory authorities, Data Protection Officer, data portability, data protection impact assessment...). Additionally, certain supervisory authorities have provide tools for the stakeholders. For example, the Belgian supervisory authority published template for records of processing activities. The French supervisory authority (*Commission nationale de l'informatique et des libertés*) created a tool which helps carry out data protection impact assessments².

It must be underlined that another European Regulation is expected during the 1st semester of 2018, namely the e-Privacy Regulation on electronic communications. In particular, it will have an impact on metadata processing and the use of cookies.

¹ Directive 95/46/CE of the European Parliament and of the Council of the 24th of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

² <https://www.cnil.fr/professionnel>

Simultaneously, the “Sowden Case”, regarding the surveillance of European citizens by the American authorities illustrated the complexity of achieving an efficient protection.



The Court of Justice of the European Union's jurisprudence also fueled the debates on the reinforcement of personal data protection.

In April 2014, it declared Directive 2006/24/CE on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks invalid³. In May 2014, the court affirmed the right to be forgotten for all individuals⁴.

The Court of Justice also expanded the notion of establishment as defined by Article 4 of Directive 95/46/EC⁵. Under this article, a Member State is allowed to apply its national law to the processing of personal data by a controller which is not established in the Member State's territory. The Court also reminded that an administration must inform the data subject of the transfer of his or her data to another administration. The administration must also inform the data subject of the implemented data processing⁶.

Furthermore, the Court of Justice struck down the European Commission's adequacy decision allowing the transfer of personal data to the United-States within the provision of the Safe Harbor⁷.

On February 2nd 2016, the Commission announced that it had reached a new consensus with the American authorities on the baselines of a new agreement called Privacy Shield. According to the European Commission this agreement should allow the transfer of personal data to the United-States while respecting the fundamental rights of the European citizens⁸. On the 12th of July, European officials and the American administration validated the new rules.

Several laws have been passed in France namely Law n°2016-1321 for a Digital Republic which anticipates, in certain respects, the coming into force of the GDPR. Another important law is the Law for the modernisation of justice in the XXIst century which establishes a class action for personal data.

Certain provisions of the Law are applicable as of today such as the increased cap for penalties imposed by the Cnil. However, other provisions will be implemented later on after clarifications have been given. The latter are planned for beginning of 2017.

³. CJEU, gde ch., 8 avril 2014, aff. C-293/12, Digital Rights Ireland.

⁴. CJEU, gde ch., 13 mai 2014, aff. C-131/12, Google Spain SL, Google Inc.

⁵. CJEU, 3e ch., 1er oct. 2015, aff. C-230/14, Weltimmo.

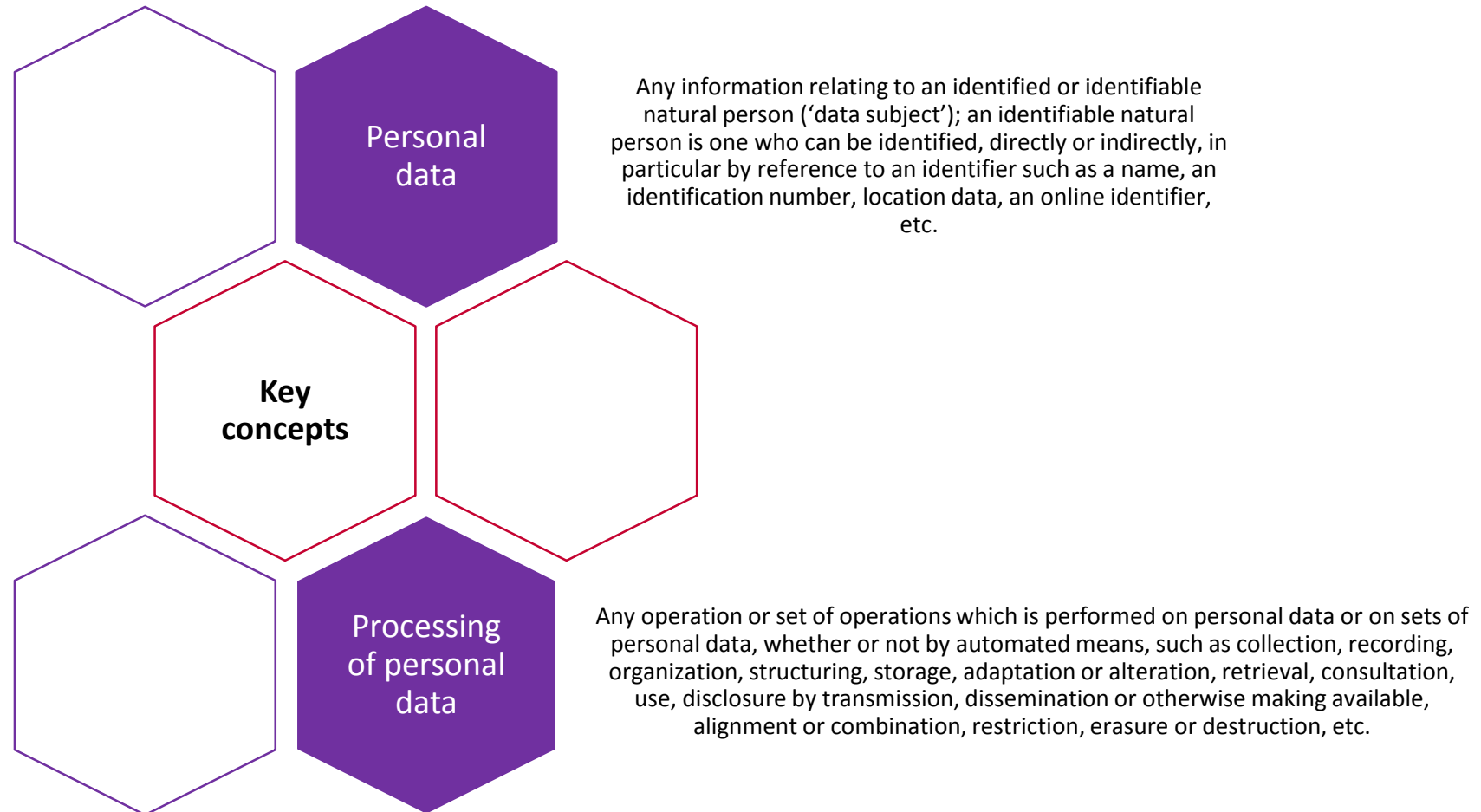
⁶. CJEU, 3e ch., 1er oct. 2015, aff. C-201/14, Bara.

⁷. CJEU, gde ch., 6 oct. 2015, aff. C- 362/14, Schrems.

⁸. « Privacy Shield » : un bouclier pas si protecteur ?, Mathias avocats, <http://www.avocats-mathias.com/donnees-personnelles/privacy-shield-donnees-personnelles>

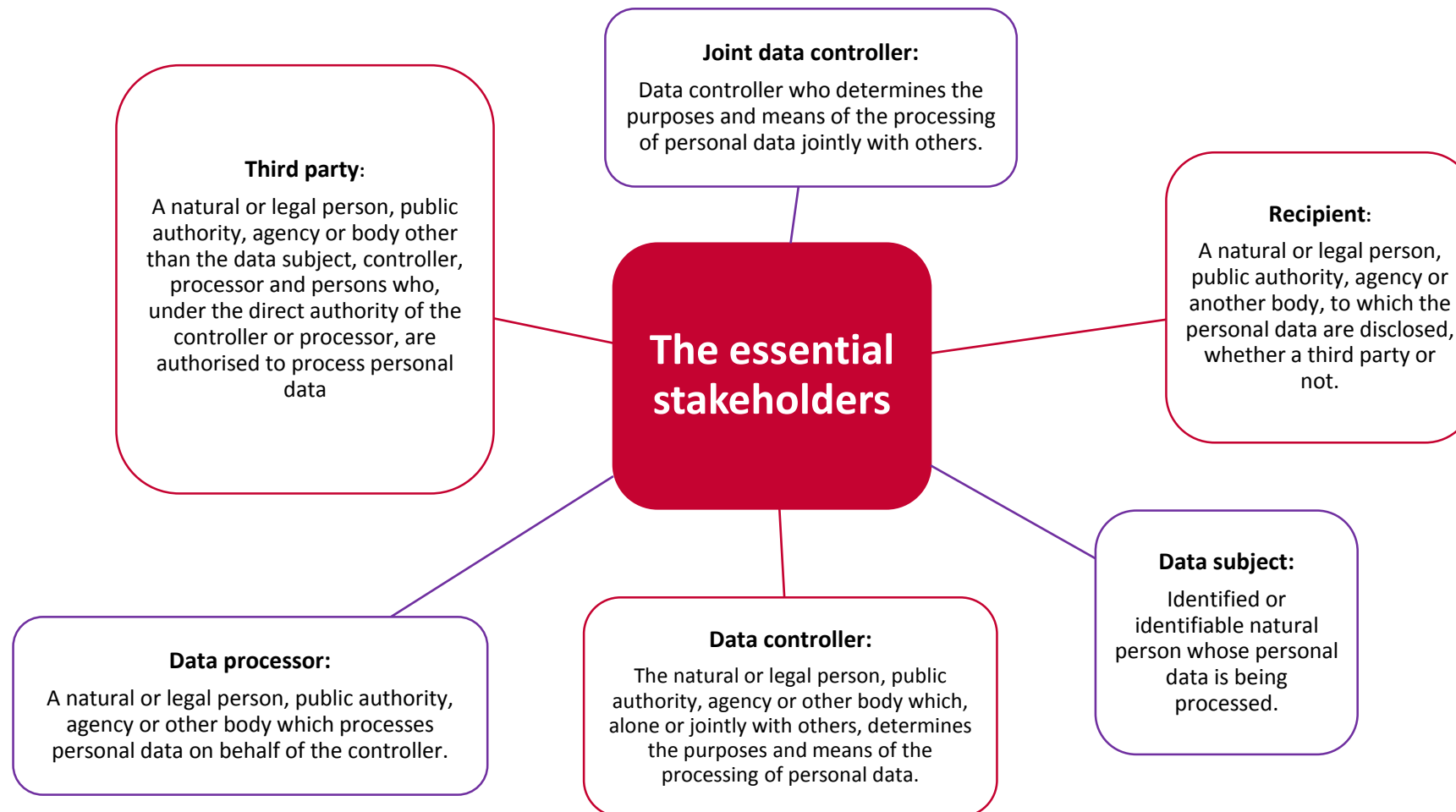
Sheet n°2: The key concepts of personal data protection

Let us recall the definitions of the key concepts of personal data protection, enriched by the contributions of the GDPR, before proceeding to the analysis of the said Regulation⁹.

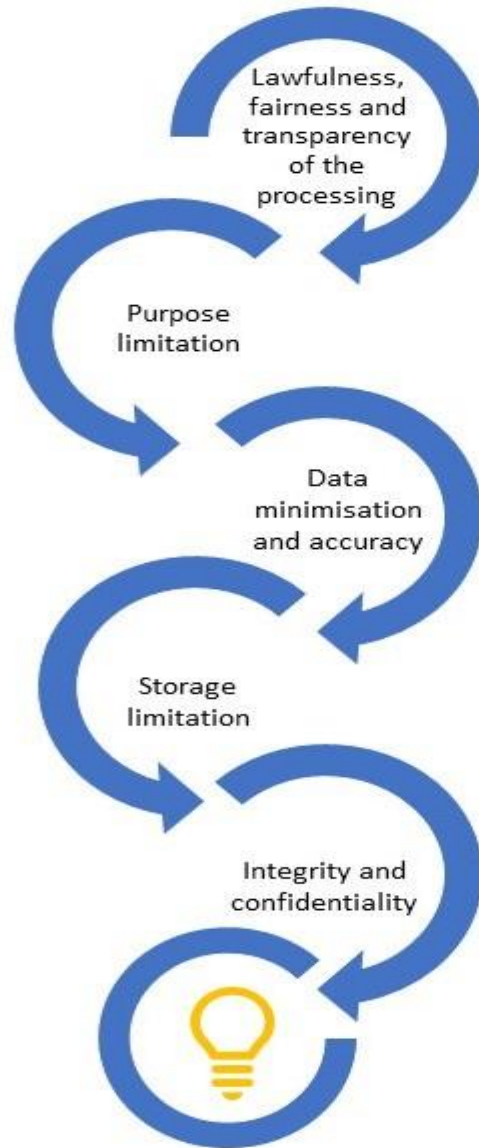


⁹ Article 4 "Definitions" of the GDPR.

Sheet n°3: The stakeholders of personal data protection



Sheet n° 4: The reaffirmation of the principles of personal data protection



The corner stone of data protection: the key principles

Article 5 of the GDPR holds the following principles : lawfulness, fairness and transparency of the personal data processing, purpose limitation of the processing, data minimization, accuracy of the data, storage limitation of the data and the integrity and confidentiality of the personal data.

If the principles have new names, they are not unknown to data controllers.

The lawfulness of the processing of personal data refers to its legal ground whereas the fairness of the processing applies to the conditions under which the personal data is collected (it must be understood in conjunction with the principle of transparency and the information to be provided to the data subjects).

Similarly to the current situation, and even after the coming into application of the GDPR, data controllers will only be able to collect and process personal data for specified, explicit and legitimate purposes.

Therefore, they must define the aim pursued prior to any processing so the purposes for which the personal data is being processed can be easily understood by data subjects. This step is of particular importance in so much as the purposes will further limit the potential reuse of the personal data.

What is the minimisation of personal data? The principle refers to the proportionality between the personal data processed and the purpose of the processing. The personal data processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The quality of the personal data is also a principle of data protection. They must be accurate and where necessary kept up to date. Thus, inaccurate personal data must be erased or rectified without delay.

This principle is of particular importance in relation to exclusion files.

Limited storage of the personal data is a significant issue for data controllers. Indeed, the time for which the data will be stored must be indicated in the information statement given to the data subjects. Henceforth the latter will be able to check if the entity, acting as a data controller, respects the limitation it determined.

Finally, the security of personal data remains a cornerstone of the protection of personal data. In practice, a reading grid taking up each of these principles can be drawn to determine whether they have been taken into account in the implementation of personal data processing activities.

Informed consent: a specified and reinforced principle

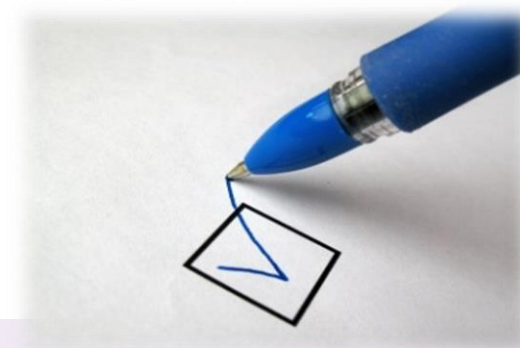
Article 6 of the GDPR lays down the conditions for the lawfulness of data processing. As data controller, the entity may lawfully process personal data only to the extent that at least one of the following requirements is met:

- the data subject has given consent to the processing of his or her data;
- performance of a contract;
- compliance with a legal obligation;
- the protection of vital interests of the data subject;
- performance of a task carried out in the public interest;
- legitimate interests pursued by the data controller (financial or commercial interest, compliance with an organization's object, safety of people and property...).

Under Article 4 of the GDPR, **consent** is defined as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. This definition completes the one in Directive 95/46/CE in so far as the Directive clearly states that consent must result from an unequivocal act. The burden of proof for consent lays on data controllers. They must use **traceability solutions**. As a practical manner, and concerning cookies, let us recall that a checkbox or further navigation on the website is sufficient to characterise a positive act of consent.

The specific status of minors

The GDPR provides a specific legal regime according to the applicable national legislation for the processing of personal data for services offered to minors whom are under 16 years old or under 13 years old (ex: social media). Indeed, the consent of the person having parental authority is required. Therefore, the data controller will have to ensure that the consent is validly obtained and that the person consenting is of age or has parental authority. Dual traceability procedures must thus be provided for.



Sheet n° 5: The territorial application of the GDPR

Directive

Versus

Regulation

Territorial Application

 Article 4 of Directive 95/46/CE	 Article 3 of the GDPR
Economic operators not established in the European Union	Economic operators not established in the European Union
Automated or non-automated means of data processing located on EU territory	Offering goods or services to persons within the EU or observing their behaviour
Appointment of a representative	Appointment of a representative

The European institutions called for the broad applicability of the protection of European citizens' personal data.

As such, Article 3 of the GDPR provides for a wide territorial scope of the Regulation. The GDPR applies to the processing of personal data of data subjects who are in the Union, by a controller, whether or not the he or she is established in the Union, where the processing activities are related to the offering of good or services to data subjects in the Union or the monitoring of their behavior as far as their behavior takes place within the Union.

More particularly, an entity established in the United-States which markets its products directly to residents of the European Union, without being physically present in the Union, will be subject to the requirements of the GDPR.

It should be noted that pursuant Article 4 of Directive 95/46/CE on the applicable national law, a Member State shall apply the national provisions it adopted to a controller not established on Community territory if he or she “for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State”. This provision was broadly construed in order to subject a majority of data controllers to a Member State’s Protection Law. Moreover, the notion of equipment could be characterized by the use of data-collection software tools, data collection forms, computer servers or the use of cookies.

Although the broad understanding of the territorial application of the GDPR is not fundamentally new, it is more precisely defined. This has important consequences for entities established outside the European Union. They will namely have to designate a representative within the Union. The representative is a physical or moral person established in the Union and designated by the data processor to represent him or her.

Sheet n°6: Accountability

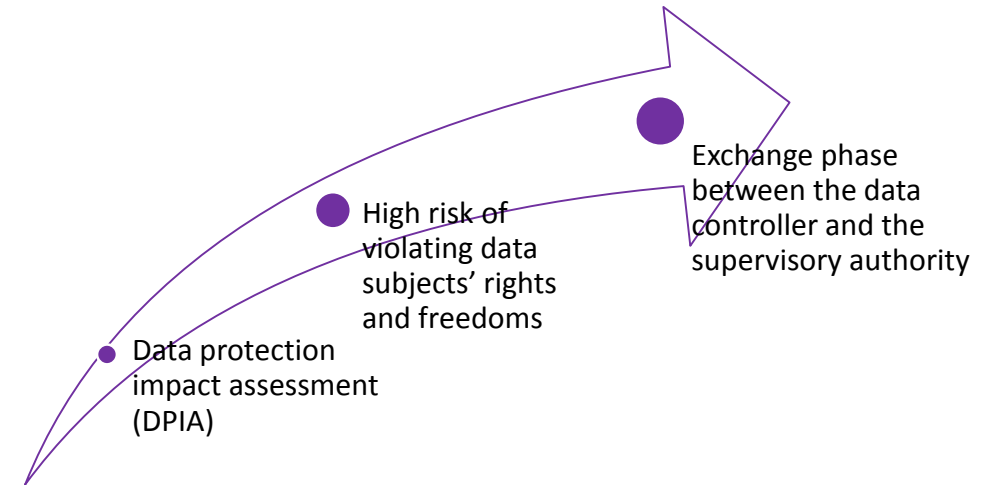
The GDPR changes the current declaration system to one of accountability. The entity acting as data processor must be able to prove that it complies with its obligations regarding the protection of personal data and must demonstrate its compliance to the competent authority.

Article 24 of the GDPR

- “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.”

The data controller will no longer be subject to prior formalities for data processing. They are currently defined in the Act of January 6th 1978 as amended.

However, Article 36 of the GDPR provides for prior consultations with the supervisory authority as illustrated in the figure below.



The Article further provides that in specific areas, Member State law may require data controllers to consult with and obtain prior authorisations from the supervisory authority in relation to data processing. This namely includes processing operations carried out by a controller in the context of a public service mission or within the framework of social protection and public health.

In practice, the principle of accountability will imply that the data controller adopt all technical and organisational measures to ensure compliance with the GDPR.

Appropriate measures

The measures will be appropriate according to several elements such as the nature of processing, the context of the processing or the scope and the purposes of the processing.

The risk of violating data subjects' rights and freedoms must be identified including the possibility of the violation occurring and its severity. The measures will not be the same for all entities. **Impact studies and risk analyses should be favored.**

The policies on data protection adopted by an entities will be unique to each entity.

Diversified measures

The technical and organisational measures put in place by the data controller are diverse. In general, these measures are all the steps taken by the entity to comply with its obligations under the GDPR (principles of privacy by design and by default, safeguarding the rights of individuals, DPIAs where applicable, security and confidentiality of personal data, notifying breaches, maintaining the registry, etc.).



The notions of privacy by design and privacy by default will namely be an integral part of a DPIA¹⁰. They ensure that personal data protection is a default rule and will be considered from the moment of conception.

The protection of personal data will have to be integrated from the moment of conception of the systems and technologies put in place. The GDPR specifies that this principle must be applied at the stage of determining the means of treatment as well as at their implementation.



This requirement is closely related to the principle of personal data minimisation. The latter holds that personal data be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”¹¹.

The principle is well known to data controllers. Indeed, Directive 95/46/CE and the French Data Protection Act also state that only the data strictly necessary to achieve the defined purpose must be collected. Thus, a precise analysis of the data processing must be done to identify its characteristics and ascertain that those characteristics comply with the applicable data protection rules (limited storage time of the data, adequacy of the data, etc.).

It should be underlined that the GDPR expressly states that personal data should not be made accessible “to an indefinite number of natural persons without the individual’s intervention”. The data subject should be given some leeway regarding the processing of his or her data. From this standpoint, the individual regains **control** over his or her personal data seeing as he or she can change the parameters.

¹⁰. Article 25 of the GDPR.

¹¹. Article 5, 1, c) of the GDPR.

Accountability

Proving the measures taken by the data controller to protect personal data is the most important aspect.

...

The protection of personal data comes in many forms. Here are few examples.

In practice ?

Example n°1

Internal procedure for handling complaints and requests to exercise rights.

Example n°2

Processing outsourcing policy.

Example n°3

Binding Corporate Rules defining a group's data protection policy.

Example n°4

Labels issued by the Cnil.

Example n°5

Geolocation of people disabled by default and no data sharing by default.

Example n°6

Pseudonymisation techniques.

Record of processing activities, a pertinent measure and a general obligation

The **generalisation** of maintaining a record of processing activities also furthers accountability. Until now, the only record of processing activities was kept by the Data Protection Correspondent (CIL, *Correspondant Informatique et Libertés*) designated by the data controller. The GDPR stresses the importance of the record by stating that “each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility”¹².

Under the GDPR, the Data Protection Officer (DPO) has no obligation to keep the record of processing activities. In practice however a question arises as to the possibility of no longer keeping the record for a CIL who has become DPO. In such a situation, wouldn't the constant updating of the record require the DPO to keep the record?

Regardless of this question, it must be underlined that companies of less than 250 employees are not under the obligation to keep a record. However, the exception will not apply if the processing carried out is “likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes sensitive personal data or personal data relating to criminal convictions and offences”.

The GDPR lists a certain number of elements which were already mentioned in the CIL's record. Other requirements are new. Hence, the record must specify:

- the purposes of the processing;



- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- a description of the categories of data subjects and of the categories of personal data;
- where applicable, the transfers of personal data to a third country or an international organisation, including the identification of that third

country or international organisation and the documentation of suitable safeguards (BCR, standard contractual clauses, etc.);

- a general description of the technical and organisational security measures taken;
- the envisaged time limits for erasure of the different categories of data.

How to tackle these requirements ?

You can already prepare your entity to the coming into application of the GDPR by identifying and reviewing the various internal policies regarding personal data protection. The data processing carried out can also be audited with the help of technical and legal experts. There are only a few months left to determine an action plan by comparing the existing data processing activities with the requirements of the GDPR.

¹² Article 30 of the GDPR.

Moreover, the Cnil published an infographic detailing the practical steps to be taken and the key principles¹³. Other supervisory authorities have also taken steps to help data controllers. For example, the Swiss Federal Data Protection and Information Commissioner provides a questionnaire which enables the data controller to anticipate the risks early on in the development of his or her project¹⁴.

¹³. <https://www.cnil.fr/fr/lignes-directrices-du-g29-sur-les-dpia>

¹⁴. <https://www.apps.edoeb.admin.ch/dsfa/fr/index.html>



Fiche n° 7 : DPIA

One of the novelties of the GDPR is the obligation to carry out, prior to the processing, an assessment impact of the envisaged processing operations on the protection of personal data (Data Protection Impact Assessment, DPIA)¹⁵.

A DPIA is a multi-purpose instrument in so far as it is used to identify the risks to the rights and freedoms of data subjects (origin, nature, gravity of the risk...), to envisage appropriate personal data protection measures and to demonstrate the processing's conformity to the GDPR (the DPIA leads to the drafting of documentation). As such, the DPIA contributes to the accountability approach adopted by the GDPR.

The Cnil published an infography to help professionals identify the situations in which a DPIA is required and to guide them when carrying out the assessment¹⁶. Furthermore, the Cnil also published a tool to help carry out DPIAs¹⁷.

Is the carrying out of a DPIA mandatory?

A DPIA is not mandatory for all processing activities. However, depending on the internal policy established, some entities may opt for a systematic DPIA.

A DPIA must be carried out where a type of processing «is likely to result in a high risk to the rights and freedoms of natural persons»¹⁸. This will namely be the case for processing data concerning health on a large scale.

A single assessment may address a single processing operation or a set of similar processing operations that present similar high risks. The risk will be evaluated according to the nature, scope, context and purposes of the processing.

Moreover, Article 35§3 of the GDPR determines three non-exhaustive cases in which a DPIA is also required. The WP29 published guidelines on the DPIA to clarify the cases described in the GDPR¹⁹.

❖ «A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person».

This case covers any evaluation, including profiling, or rating of a natural person which significantly affect him or her (ex: loan denied on the grounds of the result of a screening against a credit reference).

A processing activity will be considered as systematic if it meets one or more of the following criteria: it occurs according to a pre-arranged, organised or methodical system, taking place as part of a general plan for data collection and/or carried out as part of a strategy. It should be underlined that this definition is derived from WP29's guidelines on DPOs²⁰.

¹⁵. Recital 84 et Article 35 of the GDPR.

¹⁶. <https://www.cnil.fr/fr/lignes-directrices-du-g29-sur-les-dpia>

¹⁷. <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>



¹⁸. Article 35§1 of the GDPR.

¹⁹. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, G29, 4 oct. 2017.

²⁰. Guidelines on Data Protection Officers (DPOs), WP29, 5 April 2017.

MANDATORY DPIA



Processing operation is on the list established by the supervisory authority.

Systematic and extensive evaluation of personal aspects relating to the natural person, including profiling, on which decisions are namely made.



Systematic monitoring of a publicly accessible area on a large scale.

Large scale processing of special categories of data (data concerning health, biometric data...) or of personal data relating to criminal convictions and offences.



Mathias
Avocats

- ❖ «Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences».

Due to the lack of a definition given by the GDPR, WP29 identified several non-exhaustive factors to be taken into account to determine whether a processing is on a large scale: the volume of the data being processed, the geographical extent of the processing activity, number of data subjects concerned and the duration of the data processing activity.

Furthermore, this case also concerns the processing of special categories of personal data as defined by Article 9 of the GDPR (data concerning health, political opinions, biometric data, genetic data...) and as defined by Article 10 of the Regulation (personal data relating to criminal convictions, offences or related security measures).

- ❖ «A systematic monitoring of a publicly accessible area on a large scale».

In this respect, WP29 was able to specify that the processing activity carried out makes it possible to observe, monitor or control data subjects, including communication networks. It should be noted that this case covers situations in which the data subjects would be unable to escape the processing (for example, surveillance in a public area).

When must the DPIA be carried out?

The DPIA must be carried out prior to the implementation of the processing activity. This allows for corrective measures to be taken if necessary. The DPIA should be carried out as soon as possible, even if all the processing activities are not yet clearly defined.

Moreover, if the data processing activity, covered by the DPIA, changes, the DPIA must also be adapted. Thus, the assessment will have to be amended when the conditions under which the processing activity is implemented change (changes in the nature of the personal data collected, the period during which the data are kept, etc.) and this change poses a risk to the rights and freedoms of data subjects. This enables the data controller to ensure that the safeguard measures defined are always in line with the risks presented by the processing operation.

Who intervenes in the carrying out of a DPIA?

Under Article 35 of the GDPR, the data controller must carry out the DPIA²¹. In practice, business teams will have a preponderant role seeing as they know the characteristics of the envisaged processing activity. Therefore, they will namely be able to describe the context in which the processing will be carried out as well as its purposes and the categories of data processed, to assess the number of data subjects or to identify the storage periods to be applied...

The business team will probably have to rely on the technical or legal expertise of other employees in order to gather all the information needed for the DPIA.

The DPO's involvement may vary from one entity to another depending on several factors such as the level of consideration given to the GDPR and the challenges it raises for the entity or the awareness of the business teams. The DPO may also act as a guide for the business teams. If this is the case, the DPIA will be a means to raise their awareness.

Thus, the DPO will ensure that a quality DPIA is carried out, requesting amendment or additions where appropriate. However, if the protection of personal data is integrated by the business teams, the DPO will not be as involved. In any event WP29 recommends documenting the DPO's opinion regarding the DPIA²².

DPIA: who intervenes ?

BUSINESS TEAMS

- Describes the processing activities (context, purposes, type of data processed, source of the data, data location...).
- Identifies and evaluates the risks.

SUPERVISORY AUTHORITY

- Publishes a list of processing operations which are subject to a DPIA and those which are not.
- Guides data controllers during the process of prior consultation.

DPO

- Checks whether a DPIA has been properly carried out.
- Checks the quality of the DPIA.
- Makes recommendations, requests for amendments or additions to the DPIA.
- Accompanies the data processor or controller through the DPIA process according to his or her awareness to data protection issues.

In addition, the data processor must assist the controller and provide him or her with the information available to the processor²³.

The data controller may seek the views of data subjects or their representatives on the intended processing (Article 35§9 du GDPR). WP29 recommends documenting the decision to consult or to abstain from consulting the latter.

Finally, the data controller is free to consult any person susceptible of assisting him or her (lawyers, IT or security experts, deontologists depending on his or her sector of activity...).

²¹. Recital 84 et Article 3 §§1 et 2 of the GDPR.

²². Article 39§1 c) of the GDPR.

²³. Article 28§3 f) of the GDPR.

What information must a DPIA contain?

The DPIA must contain at least²⁴ :

- ❖ a systematic description of the envisaged processing operations and the purposes of the processing;
- ❖ an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- ❖ an assessment of the risks to the rights and freedoms of data subjects;
- ❖ the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

In order to be able to demonstrate that the protection of personal data has been taken into account, each step of the DPIA must be documented. In this context, whether the data controller or processor complies with approved code(s) of conduct will be taken into account in assessing the impact of the processing operations performed. Certification mechanisms and data protection labels will also be considered. Furthermore, Binding Corporate Rules (BCR) can also be taken into account. On November 27th 2017, the European Union Agency for Network and Information Security (ENISA) published [guidelines](#) concerning certification mechanisms as defined by the GDPR.

WP29 stresses the fact that publishing a DPIA will instil confidence in the data subjects concerned. However, the GDPR does not provide for mandatory publication of the DPIA. Considering the content of a DPIA, a majority of data controllers could opt for the confidentiality of the assessment.

What is the supervisory authority's role in the carrying out of a DPIA?

Prior to the carrying out of a DPIA, the supervisory authority can establish a list of processing activities for which a DPIA shall be required and/or a list of processing activities for which an assessment shall not be required²⁵.

The supervisory authority can also intervene after the carrying out of a DPIA but prior to the implementation of the processing activity when the DPIA indicates that the processing would result in a high risk to the rights and freedoms of the data subjects²⁶ (ex: being fired, financial difficulties). Thus, in some instances, the Cnil must intervene.

In this context, the data controller shall provide several elements namely the DPIA as well as the measures and guarantees provided to protect the rights and freedoms of data subjects. The supervisory authority is thus involved in drawing up the technical and organisational measures of the controller.

If the processing envisaged by the controller is likely to constitute a breach of the GDPR, the supervisory authority will issue a written opinion and may exercise its powers (investigation, corrective measures, etc.).

²⁴. Article 35§7 of the GDPR.

²⁵. Article 35§§ 4 et 5 of the GDPR.

²⁶. Article 36 of the GDPR.



Particular case: a DPIA carried out when a European or national regulation is being adopted

Article 35§10 of the GDPR provides for a particular case in which the data processor is under no obligation to carry out a DPIA.

However, the following conditions must be met:

- ❖ the implemented processing activity is **necessary to comply with a legal obligation or for the performance of a task carried out in the public interest**;
- ❖ **the Union law or the law of the Member State regulates** the processing;
- ❖ **a DPIA has already been carried out** in the context of the adoption of that legal basis.

However, it should be stressed that the GDPR leaves a margin of discretion to Member States, which may provide that even in the case described above, a DPIA may be required.

Processing activities for which the GDPR does not require a DPIA

Processing is not likely to result in a high risk to the rights and freedoms of natural persons.

Processing activity on the list established by the supervisory authority.

Processing is necessary for complying with a legal obligation or for the performance of a task carried out in the public interest and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis.

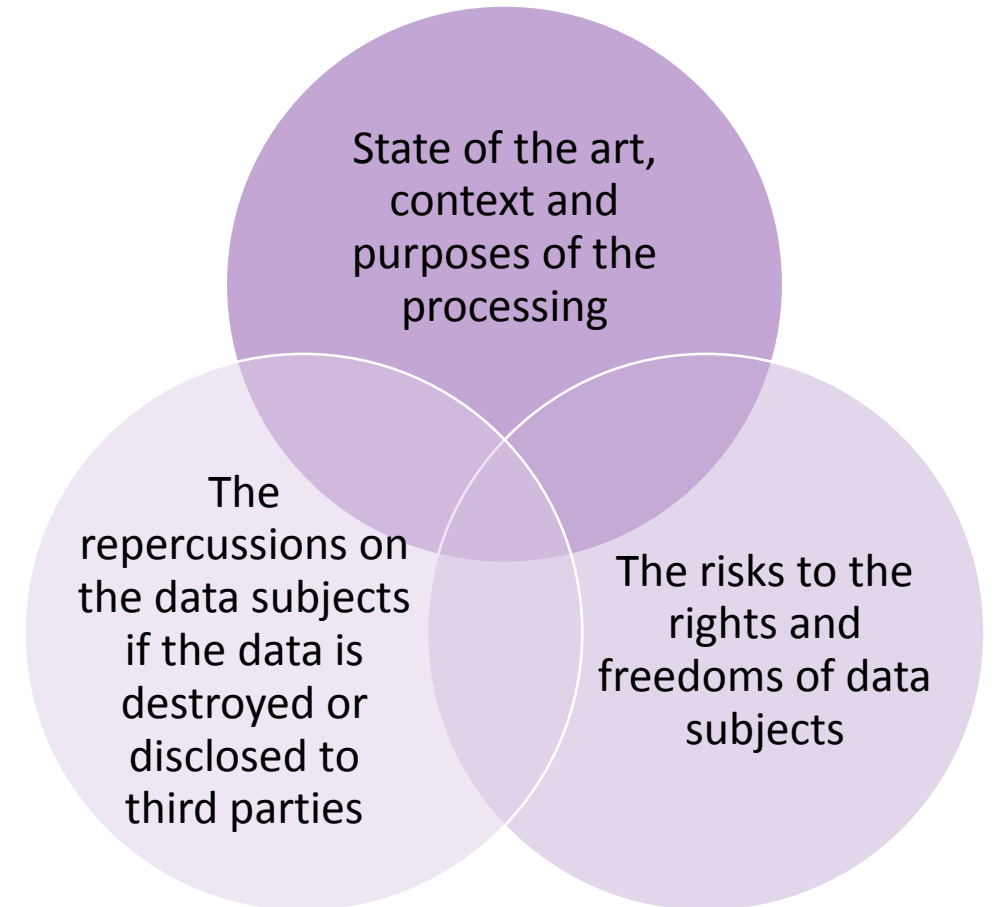
Sheet n°8: Crisis management reinforced

What factors should be taken into account?

Security of personal data has always been a technical and legal issue of personal data protection. A **technical** issue in the sense that the measures taken must be adapted to the nature of the data and to the risks presented by the processing. It is also a **legal** issue considering, on the one hand, that security impacts the different contracts with contractors and, on the other hand, that violations to data protection can be criminally sanctioned and the Cnil can issue an administrative penalty.

Reinforcement of the security of personal data – prior to the processing activities

Under the GDPR, both the data controller and data processor will have to ensure the security of personal data. Indeed, Article 32 compels them to take into account different security factors such as those presented here.



Mathias
Avocats

It should be noted that security measures must namely aim to ensure the **confidentiality, integrity and accessibility** of the data processing system and access to the data. These measures can only be determined after having identified the risks. Therefore, risk assessment tools used today remain valuable under the GDPR.

Furthermore, the GDPR introduced the new concept of “ongoing resilience of processing systems and services”. According to the glossary of the French Network and Information Security, resilience in IT is “an information system’s capacity to resist to a hardware failure or cyberattack and to return to its initial state after the incident”, Therefore, backup solutions and redundancy systems will have to be strengthened.

In accordance with the principle of responsibility, all these measures should be described in a security policy by the controller to show compliance with his or her obligation to ensure the security of personal data. In addition, the need to adapt security measures will require an assessment of the effectiveness of the measures taken to adjust them where necessary.



Security of personal data

What to do ?

Access tracking

Locating the data

Raise the employees’/actors’ awareness

Pseudonymisation

Transaction encryption

Managing access rights / Authorisations

Identification/authentication

Security policy

Audit

The general notification of security breaches – during the processing activities

Data controllers must imperatively be proactive when it comes to notifying breaches of personal data to the Cnil.

The GDPR imposes a general obligation of notifying such breaches. Nowadays, it lies only with providers of electronic communication services (for example, Internet service providers, fixed and mobile operators)²⁷. A personal data breach means a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”²⁸.

The personal data breach must be notified to the Cnil no later than 72h after having discovered the breach. The notification can – could – be made from the Cnil’s website by means of an online form²⁹.

The GDPR provides for the cooperation with providers where the data processing is being outsourced. Indeed, Article 33³⁰ provides that in the case of a personal data breach, the processor shall notify the controller without undue delay after becoming aware of the breach. In this respect, the data controller must inquire under what time limit his or her processors will be able to notify him or her of any data breach.

This cooperation is all the more necessary considering the fact that, in some instances, the data breach shall be notified to the data subject (if the breach creates a high risk of impacting the rights and freedoms of that person). However, the GDPR does not specify whether providing this information will be left to the discretion of the data controller. Once the Cnil has been notified, and has assessed the measures put in place to mitigate the data breach, it will most likely inform the data controller of whether or not he or she must notify the data subject(s). The data controller must establish a notification process so as to be able to quickly respond.



²⁷. Sources: Ordinance of August 24th, 2011 transposing Article 2 of Directive 2009/136/EC of November 25th, 2009, Article 34bis of the French Data Protection Act.

²⁸. Article 4 of the GDPR.

²⁹. <https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles>

³⁰. Article 33§2 of the GDPR.

Sheet n°9: The DPO's key role in compliance

The European institutions have placed the DPO at the centre of the entities' compliance approach³¹. What are his or her obligations? And liability? By what means can his or her independence be guaranteed? Who must cooperate with the DPO? What existing tools are available to the DPO?

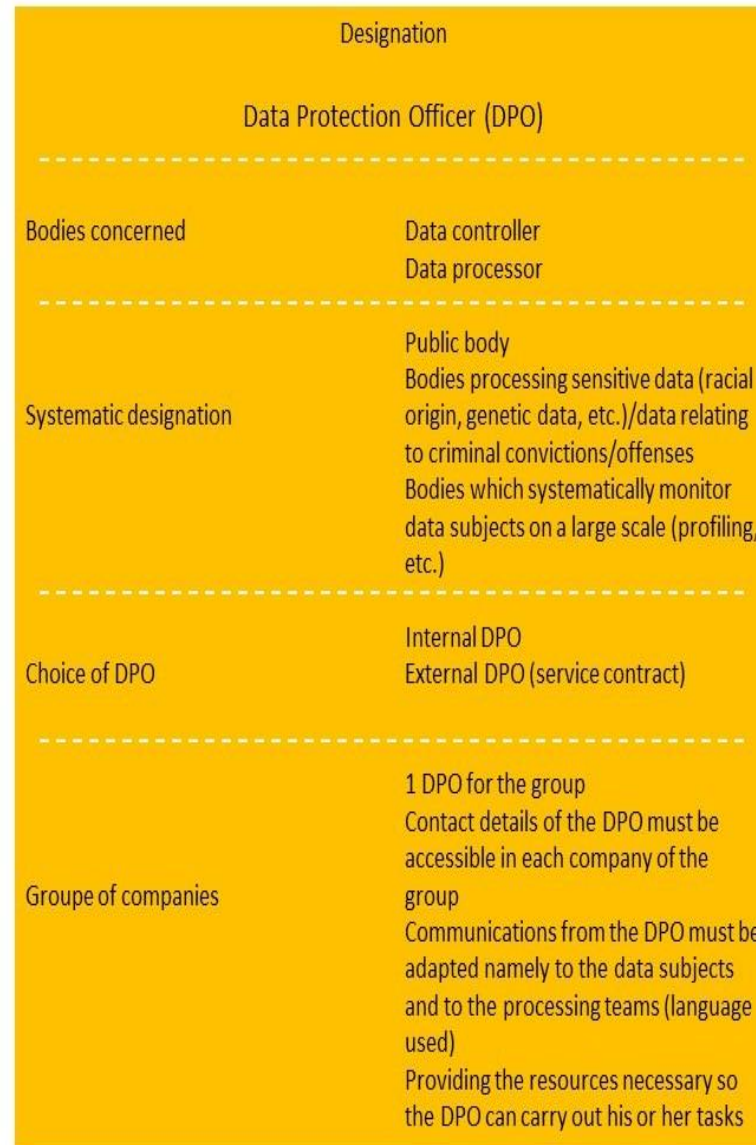
For this reason, the DPO will not only be designated by data controllers but also by data processors under the conditions set down by the GDPR.

Furthermore, the European institutions have established a new profession within data protection considering the skill requirements for the DPO and the tasks entrusted to him or her .

This new profession raises numerous questions. Last December, in an attempt to answer some of the latter, WP29 published guidelines regarding the DPO. They were revised on the April 5th, 2017³².

A quasi-systematic designation of a DPO?

During the discussions on the GDPR, the European institutions were able to express their disagreement on the mandatory nature of the designation of the DPO.



The European Commission and the European Parliament considered that a DPO must be designated in specific cases.

On the contrary, the Council of the European Union left each Member State determine the mandatory or optional nature of the DPO's designation.

In the end, a compromise was found. **The designation of a DPO will be mandatory for three categories of entities.**

Apart from those specific cases, Article 35 of the GDPR provides that the designation will be voluntary unless the Member State's national law requires the designation of a DPO.

It should also be underlined that **the designation procedure is more flexible than the current one**. This is namely illustrated by the fact that staff representative bodies do not have to be informed of the designation.

Moreover, a written undertaking of the DPO is no longer required and the different types of designation (extended, general or partial) have been repealed. Additionally, the one month delay from the date on which the Cnil was notified for the designation to take effect no longer applies.

³¹. Garance Mathias, Amandine Kashani-Poor et Aline Alfer, *Le Délégué à la protection des données (DPO)*, Les essentiels de la banque et de la finance, Revue Banque, 2017.

³². Guidelines on Data Protection Officers (DPO), WP29, 5th April. 2017.

How to determine whether your entity will be required to designate a DPO?

In addition to public bodies and public organisations, two other categories of entities must systematically designate a DPO.

As a reminder, they are data controllers or processors whose:

- “core activities (...) consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale”;
- “core activities (...) consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10”.

That being said, what is a core activity? What is regular and systematic monitoring?

What is data processing on a large scale?

These notions are not defined by the GDPR despite the fact that they determine whether the designation of a DPO is mandatory.

Under Recital 97 of the GDPR, the **core activities** of a controller in the private sector relate “to its primary activities and do not relate to the processing of personal data as ancillary activities”.

WP29’s guidelines on the subject indicate that the notion of core activity should not be excluded when the entity’s activity intrinsically consists of data processing.

As such, WP29 considers for example that a supervisory company responsible for monitoring a shopping mall or other places open to the public must designate a DPO. In this example, the company’s monitoring activity implies data processing.

Regarding **large scale processing operations**, Recital 91 of the GDPR on DPIAs provides clarification.

On the one hand, Recital 91 defines the notion by giving its opposite: “the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer” .

Thus, the personal data processing activities of a doctor or lawyer, acting in his or her individual capacity, are not considered as large scale processing operations and do not require the designation of a DPO.

On the other hand, the Recital also states that large scale processing operations are those “which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk”.

In this context, WP29 recommends taking into account several factors namely the number of data subjects, the volume of data processed, the duration of the processing operations or the geographical extent of the processing operations.

For example, the operation of processing the personal data of users of a transport service would be considered as a large scale processing operation.

It must be kept in mind that WP29 does not exclude publishing thresholds for the DPO's designation.

Finally, regarding the **regular and systematic monitoring** of data subjects, Recital 24 of the GDPR refers to the notion of “monitoring” in the definition of territorial scope³³. The monitoring of data subjects who are in the Union is a criterion for the application of the above-mentioned Regulation (Article 3§2 of the GDPR).

It must be underlined that monitoring can be carried out on the Internet and outside network. Subsequently, WP29 adopted an extensive interpretation of the notion of regular and systematic monitoring of data subjects so as to include any and all forms of monitoring and profiling, including behaviour advertising.



For example, tracking a user's geographical position through the use of mobile applications, loyalty programs or the monitoring and recording of so-called welfare and fitness data from connected objects would be considered as a regular and systematic monitoring of persons.

A strong position for the DPO

The DPO will “directly report to the highest management level of the controller or the processor”. As such, he or she must have access to the entity's decision-making bodies (ex: executive committee, general secretariat, general management, etc.). An illustration of the DPO's strong position is his or her ability to **have access to the personal data and to its processing data activities**. He or she will therefore be able to assess in practical terms the conditions under which processing operations are carried out.

In any case, the DPO's position must enable him or her to be informed and consulted on all areas pertaining to the entity's compliance with the GDPR.

The DPO, whether a staff member or third party to the entity, must be consulted sufficiently early to give him or her the time to make recommendations. The latter must be taken into account. **If there is a disagreement, WP29 advises documenting the reasons for which the DPO's recommendations were not followed.**

Furthermore, given the DPO's position, he or she will have to be consulted in the event of a data breach or any other security incident, which is not unrelated to the DPO profile.

³³. “In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.” (GDPR, Recital.24).

WP29 generally encourages entities to establish guidelines listing the situations in which a DPO must be designated. These guidelines can be used to demonstrate the entity's compliance.

The GDPR takes into account the fact that not all entities will be able to provide a full time DPO position. In such situations, the DPO may perform other tasks within the entity as long as there is no conflict of interest. It should be noted that WP29 has identified the existence of a **conflict of interest** between the function of DPO and managerial functions (head of the marketing department, head of human resources, etc.). In any case, the entity needs to ensure that the DPO will have enough time to fulfil his missions.

The DPO will not benefit from a protected employee status. However, the GDPR expressly provides that the DPO cannot be dismissed or penalised, in any way, for performing his or her tasks. WP29 confirmed this interpretation in its guidelines last adopted and revised on the 5th of April 2017³⁴.

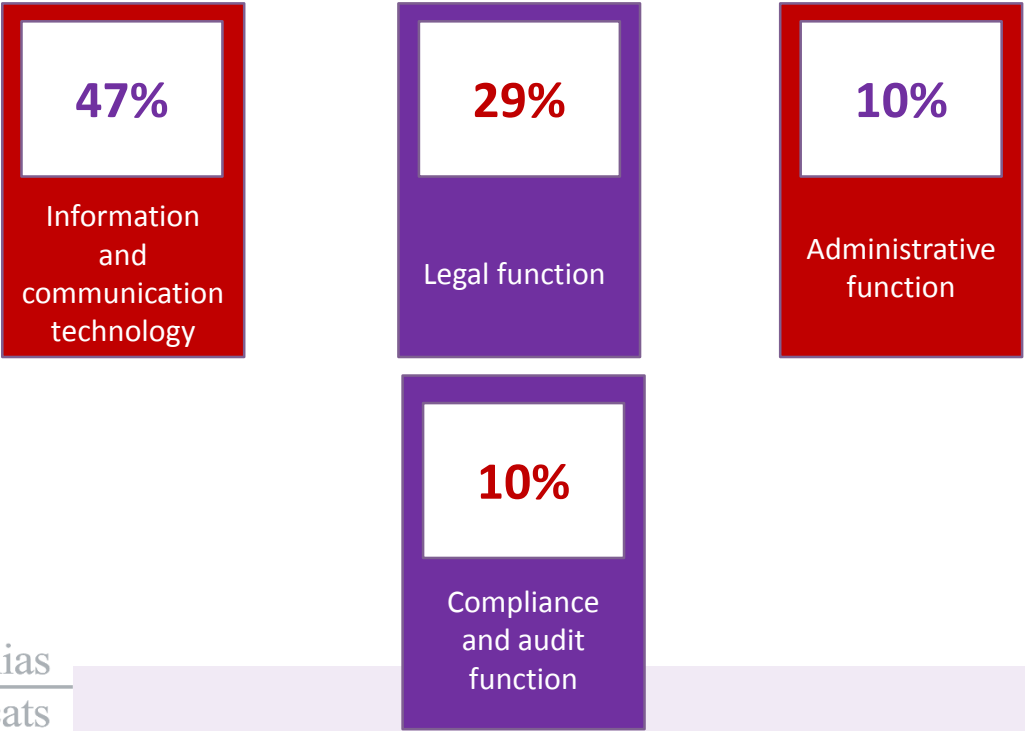
However, the GDPR does not provide a framework for the end of the DPO's mission. Must internal rules be relied on? Will the term of the mission, renewable or not, be specified by each entity in its internal personal data protection policy?

Recognised skills and diversified tasks

European GDPR (Article 37§5)

“The data protection officer shall be designated on the basis of **professional qualities** and, in particular, expert knowledge of data Protection Law and practices and the ability to fulfil the tasks referred to in Article 39”.

Within these entities, what path did the CIL take? In 2015, the Cnil conducted a survey and here are the results³⁵.



³⁴. https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf

³⁵. <https://www.cnil.fr/fr/cil-un-metier-davenir>

The **DPO's profile** is more precisely defined in the GDPR than in any other previous regulations. Future DPOs must have expert knowledge of Data Protection Law or be accompanied by their legal department and/or a lawyer. WP29 insists on the DPO's availability, his or her priority being to bring the company into compliance with the GDPR.

The DPO's main task within the entity will be to inform and advise the controller or the processor. For this reason, the DPO must be fully involved in any question regarding data protection.

The DPO must also inform and advise the employees who carry out data-processing activities. Thus, he or she has an **enhanced role in communication and raising awareness** compared to the current function of CIL.

The DPO must have expert knowledge of the GDPR as well as sector-specific laws impacting data protection. Indeed the GDPR provides that certain areas are left to be determined by each Member State's national law.

Legal skills will also be required when assessing the entity's compliance to the GDPR, internal policies as well as any other applicable national or European laws. The GDPR provides a non-exhaustive list of factors requiring particular attention from the DPO namely the allocation of responsibilities (ex: joint-responsibility, working with a processor). Moreover, specific rules pertaining to data protection should be incorporated to staff training and awareness raising events.

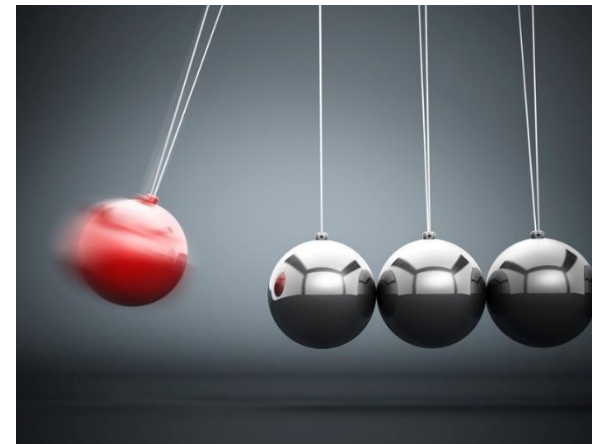
Finally, the DPO must check that DPIAs are carried out. He can also be consulted and give recommendations in this area.

WP29's guidelines indicate that the DPO will be doing more than mere checks. Indeed, the supervisory authorities recommend that the DPO's advice be sought to:

- determine whether a data protection impact assessment is required;
- determine the analysis methodology to be followed;
- define the measure to mitigate the risk to the rights and freedoms of natural persons.

It is worth noting that if the DPO's recommendations are not taken into account, the impact assessment report must state the reasons for which the controller overlooked them.

The DPO must also have data security skills.

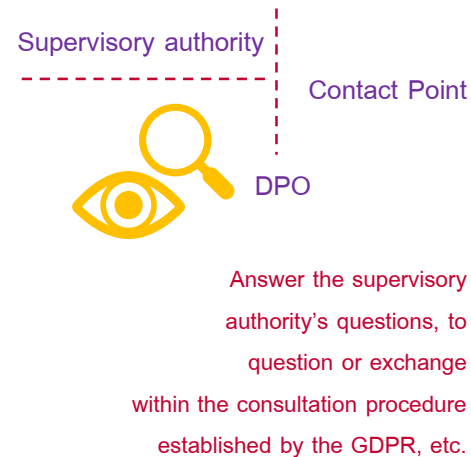


The **DPO's visibility** will be enhanced through the publication of his or her contact information to the public (institutional website, commercial website, intranet accessible to employees and/or to stakeholders, documents issued by the entity, etc.). In this respect, the DPO will interact with the data subjects seeing as they can ask him or her any question regarding the processing of their data and the exercising of their rights.

WP29 stresses the fact that the GDPR does not require that the DPO's name be given to data subjects. However, the Working Party deems that it would be good practice. The DPO and the entity having designated him or her must decide this issue.

Lastly, the DPO will be the point of contact with the supervisory authority with which he or she must collaborate.

For this reason, the GDPR provides that the DPO's contact details must be communicated to the supervisory authority.



How to prepare the designation of a DPO?

To best prepare for the designation of a DPO, it could be interesting to **raise the awareness of members of the decision-making bodies** on his or her role and tasks. It would allow the members to comprehend the extent of their requirements under the GDPR (providing the necessary resources, maintaining knowledge etc.).

Interviews with employees, agents and the different departments could also be conducted to better understand how data protection is perceived. This would help identify areas for improvement and draft a personal data protection policy with the DPO.

Furthermore, the CIL may facilitate the transition towards designating a DPO. Indeed, the CIL raised awareness about personal data protection in some companies³⁶. As such, the latter are better prepared for the GDPR and to accommodate the DPO.



³⁶. Garance Mathias, Amandine Kashani-Poor et Aline Alfer, *Le Délégué à la protection des données (DPO)*, Les essentiels de la banque et de la finance, Revue Banque, 2017.

Although today's CILs will not necessarily be tomorrow's DPOs, the CIL's work may be a valuable starting point for the DPO. For example, under the French Data Protection Act, the CIL had to keep the record of processing activities. It is of great value to have an insight into how the company functions and what steps have been taken to protect personal data. It will give the new DPO an overview of the personal data processing activities and help him organize his or her missions.



Sheet n°10: The data processor's obligations reinforced

The application of the GDPR will strongly impact the relationship between the data controller and data processor. Up until now, the data controller was responsible to the supervisory authority for the protection of personal data for regulatory breaches. In this respect, the data processor was protected from the sanctions imposed by the Cnil.

The GDPR tends to rebalance the relationship between both operators by placing obligations directly on the processor and reinforcing his or her contractual obligations. The Cnil namely published a guide regarding data processors which covers key points such as his or her obligations or the contractual relation with the data controller. It also holds practical advice on how to comply with the GDPR³⁷. The GDPR also provides that supervisory authorities may sanction a data processor for his or her non-compliance.

Obligations directly borne by the data processor

The data processor must bear several obligations.



First of all, if the data processor is not established within the European Union, he or she shall designate in writing a representative in the Union. This will be the case if the processor processes personal data of data subjects who are in the Union and whose processing activities are related to the monitoring of their behavior or to the offering of good or services³⁸.

Directive

Versus

Regulation

What about data processors'?

 Article 17 of Directive 95/46/CE	 Data processor's obligations (appointing a representative in the EU, designating a DPO, maintaining a record of processing activities, security obligations, etc.).
The contract between the processor and the controller must stipulate that the former acts only on instructions from the controller.	Data processor's contractual obligations are reinforced.
The contract between the processor and the controller must stipulate that the former has obligations pertaining to the protection of personal data.	Supervisory authorities can sanction data processors.

The processor will also have to designate a **DPO**³⁹.

Without this being a novelty, the processor must also **provide sufficient guarantees** (namely knowledge of the field in which he or she is involved, reliability or necessary resources) to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR. These guarantees are a criterion which must be taken into account by the data controller when choosing a processor⁴⁰. For example, this requirement will be fulfilled when the processor applies a **code of conduct** approved by the supervisory authority. If the data controller does not already do so, he or she must carry out checks, if only to ask the prospective processor for his or her **personal data protection policy**.

Furthermore, the data processor is also under the obligation to maintain records of processing activities. Indeed, **he or she shall maintain a record of all categories of processing activities carried out on behalf of the controller**⁴¹.

³⁷. https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

³⁸. Recital 80 and Article 27 of the GDPR.

³⁹. Sheet n°9: the DPO's key role in compliance.

⁴⁰. Recital 81 and Article 28§1 of the GDPR.

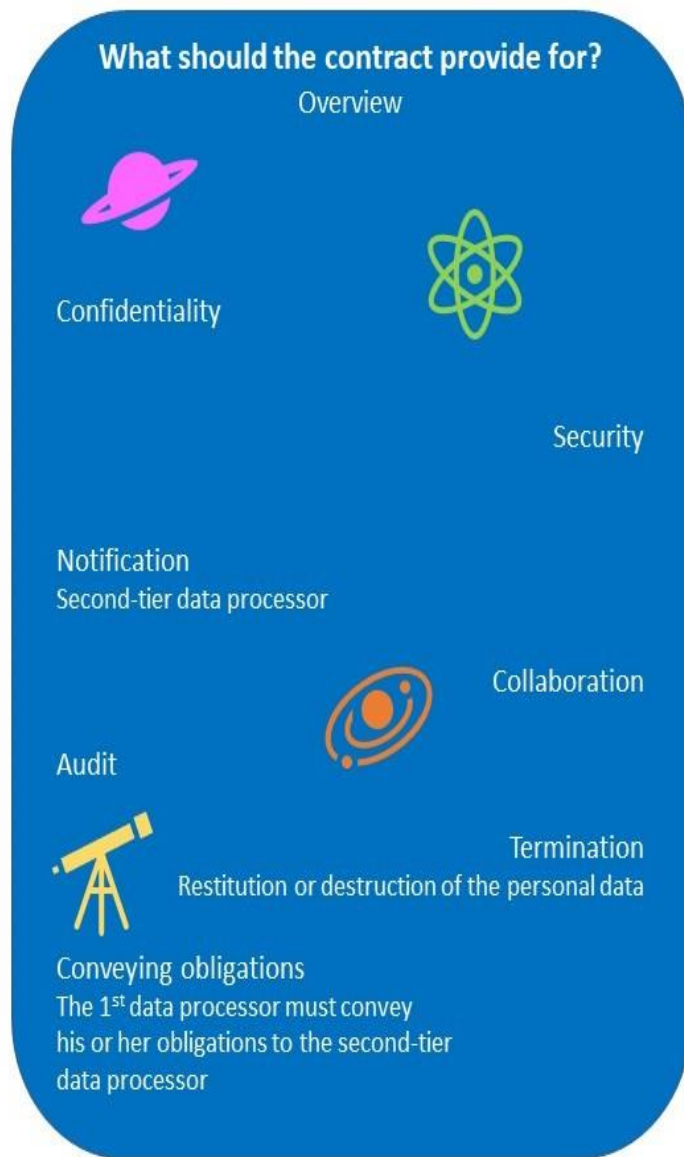
⁴¹. Article 30§2b of the GDPR.

Under Article 32 of the GDPR, the processor must ensure an **appropriate level of security** and is under the obligation to cooperate with the supervisory authority as well as with the controller⁴².

In view of the obligations to be met by the processor, the GDPR expressly provides that he or she can be sanctioned for his or her non-compliance. The maximum amount of the penalties will be the same as that incurred by the controller⁴³.

Reinforcing the data processor's contractual obligations

The GDPR considerably enriches the clause relating to the protection of personal data in the contract between the controller and the processor. Note however that certain of the GDPR's requirements were already included in the contract by practitioners.



❖ *Provisions on the processing of personal data outsourced to third parties*

The GDPR requires that the contract specify the subject matter, purpose, length and the nature of the processing. It should also set out the categories of personal data processed and the categories of data subjects.

❖ *Provisions on the processor's tasks*

The data controller must ensure that the contract specifies that the processor processes the personal data only on documented instructions from the controller. The novelty is that these instructions will have to be documented. As such, the specification could be useful tool. The instructions must also be in the appendix to the contract.

The contract must also provide that the data processor shall ensure that the persons processing the data (namely employees and consultants) shall respect the confidentiality of the data or are subject to such an obligation.

⁴². Articles 28 et 30 of the GDPR.

⁴³. Sheet n°15: The deterrent effect of sanctions.

Pursuant to the GDPR, and as previously stated, the data processor will be bound by a security obligation. Thus, he or she must implement appropriate technical and organisational measures to protect the personal data he or she processes on behalf of the controller (encryption, anonymization, etc.). Nevertheless, this obligation will have to be put in the contract.

Furthermore, the clause on the protection of personal data must specify that the processor shall not engage another processor without prior specific or general written authorisation of the controller.

In the event of a general authorisation, the data processor will be subject to a duty to inform.

The same data protection obligations as set out in the contract or other legal acts between the controller and the processor shall also be imposed on that other processor by way of a contract or other legal acts under Union or Member State law. Moreover, the GDPR provides that where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

The data processor is also under a contractual duty to cooperate with the data controller seeing as he or she must assist the latter in responding to requests for exercising the data subject's rights.



Audits can be carried out insofar as it is important for the data controller to verify that the data processor meets his or her contractual obligations. Furthermore, the data processor must demonstrate by any means that he or she meets his or her obligations (see Sheet n°6: Accountability).

The GDPR also governs the end of the provision of services relating to processing. It provides that the processor must delete or return the personal data and delete existing copies.

Use by the processor of the personal data entrusted to him or her

The future GDPR expressly provides that “if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing”⁴⁴. This would be the case if the data processor reused the personal data entrusted to him or her, in breach of the contract with the data controller, in order to carry out a processing operation for which he or she is the only one to define the purposes and means.

In such cases, the data processor is liable to the data controller but he or she would also incur criminal and administrative penalties.

Sheet n°11: Joint controllers⁴⁵

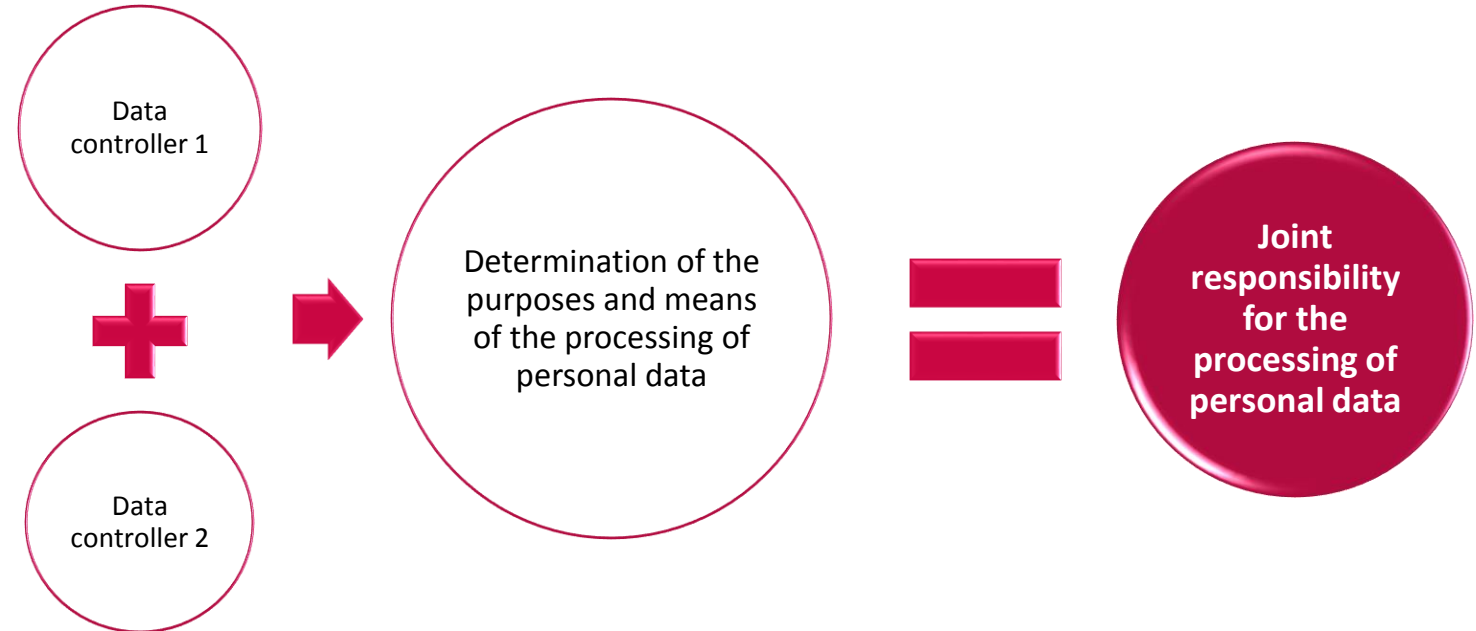
Directive 95/46/CE⁴⁶ had already taken into account joint responsibility for the processing of personal data. It was characterized when **several data controllers** jointly determined the purposes and means of processing. This definition was certainly practical in the sense that it allowed atypical conjectures to be taken into account. In practice however, it could have led to the concurrent enforcement of several Data Protection Laws according to the country in which the data controllers were established.

That being said, the French legislator did not establish joint responsibility for data processing when the Directive was transposed in 2004.

However, it should be noted that in the **cloud computing** sector the Cnil had considered applying joint responsibility between the customer of a cloud service and the provider. This would particularly be the case for standardised service offers subject to membership contracts⁴⁷.

It should be specified that if the data processor can be considered as having control over the processing means, he or she does not define the purposes of the use of the cloud

computing service and does not determine the nature of the personal data processed or the length of time during which the data is kept.



Thus, the GDPR is not innovative regarding the definition of joint liability for data processing activities. However, it does define the applicable regime. It should be underlined that the GDPR is applicable throughout the territory of the European Union and as such the risk of applying several national laws disappears.

⁴⁵. Article 26 of the GDPR.

⁴⁶. Article 2, d) of Directive 95/46/CE.

⁴⁷. Cnil, Cloud computing the 7 key steps to ensure data confidentiality, July 1st 2013.

An agreement between joint controllers

Each joint controller processing personal data will be subject to the GDPR (accountability, privacy by design, privacy by default, etc.).

However, joint responsibility implies that they must define their **respective obligations**. This allocation of responsibility must be the subject of an agreement and must specify the respect of the right of individuals and the obligation to provide information. A practice could be to consider that the data controller who collects the personal data informs the data subjects, organises the procedures for obtaining consent or even manage the data subjects' rights.

Furthermore, if a data processor is hired, the data controller whom is a party to the contract must ensure that the processor provides sufficient guarantees, that the contract complies with the GDPR...

Additionally, data controllers will have to collaborate order to be able to comply with their obligations (records of processing activities, cooperation with the supervisory authority, notification of personal data breaches...).

The availability of the agreement

Under the GDPR, the "essence of the agreement" must be made available to the data subject. However, it does not specify how to make it available.



Sheet n°12: Strengthening data subjects' rights and enshrining new rights

The digital economy provides new services that require the collection of users' personal data. However, the susceptible users' trust to use such services may have waived in the light of numerous media attacks.

In view of this finding, the enshrinement of new rights and the reinforcement of pre-existing rights has become necessary.

Transparency and the right of data subjects

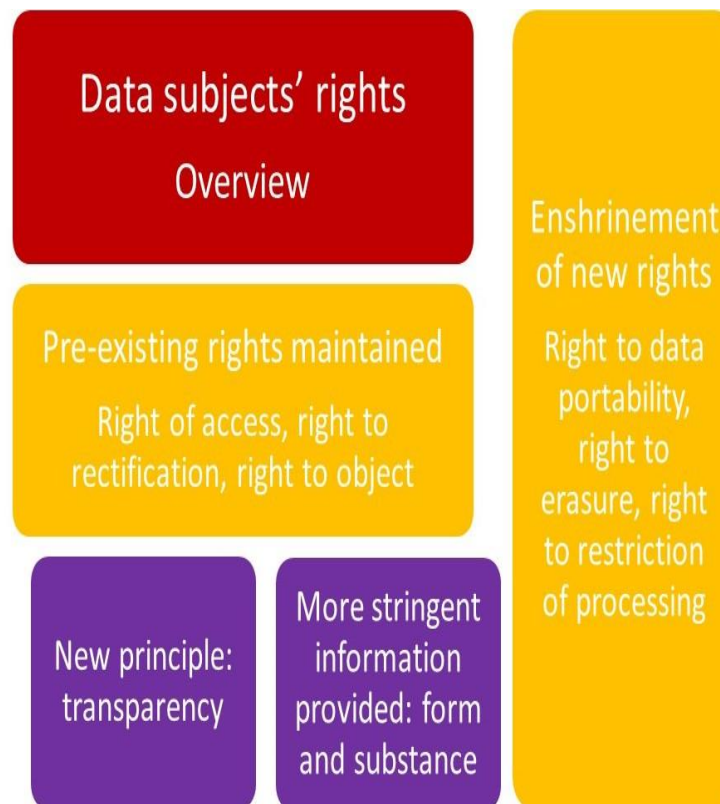
Let us first underline that the European institutions have inserted a **principle of transparency** in the GDPR (Article 12). This principle postulates that the data controller shall provide information to the data subjects in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**.

This principle is not limited to the information provided to the data subjects seeing as it also compels the data controller to **facilitate the exercise of data**

subjects' rights. The controller must inform the data subject of the action taken on a request or of the reasons for which no such action was taken without undue delay and in any event within one month of the receipt of the request.

As such, European institutions have shortened the response time, which is now of two months, in accordance with the application decree implementing the French Data Protection Act.

A review or even an adaptation of the procedures for processing incoming mail, whether postal or electronic, must therefore be carried out so that the controller can ensure that the deadlines set for him or her are respected. A procedure for managing such applications should also be adopted.

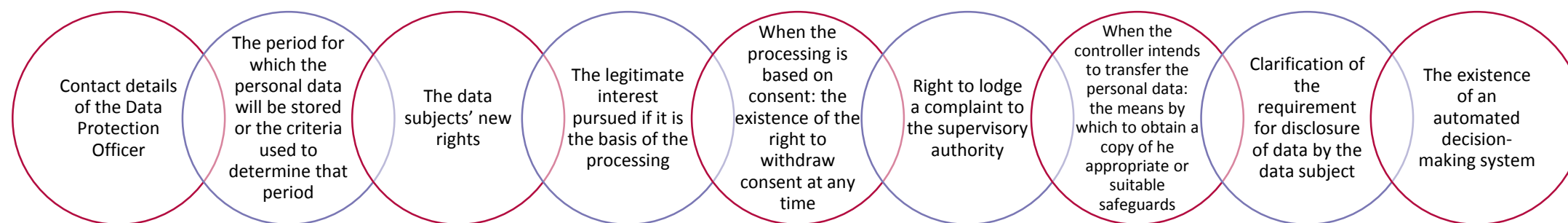


A wider scope of the obligation to provide information to data subjects

Articles 13 and 14 of the GDPR, while taking up the requirements of Article 32 of the French Data Protection Act, extend the scope of the information to be provided to the data subject, whether the data is directly or indirectly collected. If the data is directly collected, the data controller shall provide further information. Moreover, new pieces of information must be provided regarding the data subjects' new rights.

By exercising this right, data subjects will be able to retrieve the personal data that **they have provided**. For example, they can download the data or request its transmission from one data controller to another through APIs.

As another example, the user of an email service should be able to obtain all the emails he or she sent and received, as well as the list of contacts he or she has established, in a digital format.



The new rights

The GDPR consolidates the data subjects' pre-existing rights (right of access, right of rectification and erasure, right to object). Therefore, we have chosen to focus on the new rights and their consequences for the data controller.

The **right to data portability**⁴⁸ undoubtedly represents the archetype of power that the institutions wanted to give back to individuals over their personal data. The enshrinement of this right should, a priori, lead to competitive tendering of service providers. Indeed, the European institutions assume that the people will choose service providers which are the most committed to the protection of personal data.

In the WP29's guideline adopted on December 13th, 2016⁴⁹, the Working Group insists on the fact that the new data controller must in turn comply with the GDPR and respect the principles of Article 5.

In addition, it should be noted that the exercise of the right to data portability should not affect the data subject's freedom to exercise his or her other rights under the GDPR. Thus, for example, the exercise of the right to data portability should not impair the right to erasure.

That being said, the right to data portability is not boundless, as shown in the following diagram.

⁴⁸. Article 20 of the GDPR.

⁴⁹. https://www.cnil.fr/sites/default/files/atoms/files/wp242rev01_fr.pdf

Right to data portability: 2 cumulative conditions

The processing is carried out by automated means

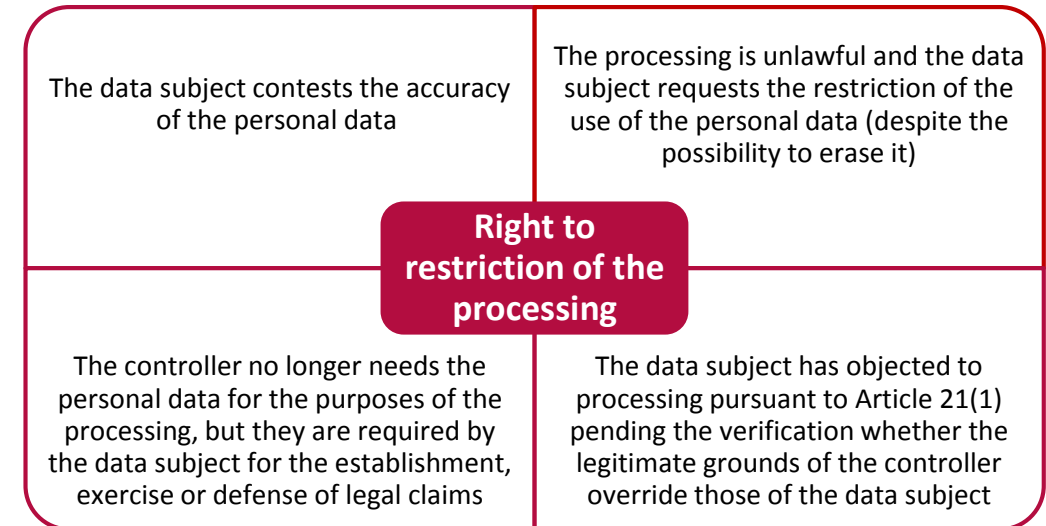
The processing is based on consent or a contract to which the data subject is a party

According to the WP29's guidelines, three conditions must be met for the data to be within the scope of the right to data portability:

- The personal data must concern the data subject: only personal data is within the scope of this right ; anonymous data or data which does not concern the data subject are not covered by this right.
- The data must be provided by the data subject: in particular, are namely concerned personal data deliberately communicated by the data subject (email, surname, first name, etc.) as well as data generated by the use of a terminal or service by the data subject (search history, traffic data, location data, etc.). Conversely, data provided by the data subject and inferred by the data controller (for example, after an algorithmic processing) or inferred from the data supplied by the data subject do not fall within the scope of this right.
- The right to data portability must not adversely affect the rights and freedoms of others: for example, the “new” data controller must not process the data for another purpose than the one initially determined so as to not adversely affect the rights and freedoms of third parties. **These include business secrecy and intellectual property according to the WP29.**

The right to data portability will also have **technical implications**. Recital 68 of the GDPR specifies that “data controllers should be encouraged to develop interoperable formats that enable data portability”. Operators will therefore have to find solutions to ensure that the data are returned to users in an open and standard format. This way, the data can be read by any type of material, in their entirety, without compromising their integrity. Thus, arises the **question of the cost** borne by companies. In addition, controllers will have to inform data subjects of their right to data portability in a clear and understandable manner.

The **right to restriction of processing**⁵⁰ is also a novelty. It is an illustration of the power given by the GDPR to the data subjects. In practice, the GDPR restricts the scope of this right in that it enumerates the circumstances in which it may be exercised.



⁵⁰. Article 18 of the GDPR.

Sheet n°13: Transfers of personal data

Transfers of personal data outside the European Union and more specifically in the United-States has been at the forefront of news.

The vast majority of the rules currently in force regarding the transfer of personal data are set out in Article 44 et seq. of the GDPR.

Standard contractual clauses et BCR: two strengthened tools

The existing tools to transfer personal data are not called into question. Thus, standard contractual clauses and BCR can be used under the GDPR. For the sake of simplification, the GDPR provides for the

removal of the authorisation mechanism by the Cnil for transfers governed by these tools.

New tools such as certification mechanisms and codes of conduct will also be developed to regulate transfers.

Contracts, *a priori* separate from standard contractual clauses, may be concluded between controllers or between controllers and processors for the purpose of supervising transfers. However, these contracts will be subject to the Cnil's scrutiny. This verification mechanism already exists today. It comes into play each time a data controller modifies the standard contractual clauses of the European Commission.

Let us specify that the transfer authorisation obtained from the Cnil, after submission of clauses differing from those of the European Commission, will remain valid when the GDPR will be applicable. However, the modifications will be subject to the requirements set out in the GDPR.

The data controller may refer to a list of countries established by the Cnil on which the level of protection of personal data provided by each of them appears⁵¹.

It should also be recalled that on January 1st, 2015, the European Commission adopted an adequacy decision, on the basis Article 25§6 of the Directive 95/46/CE, recognising that



the legislation of the following countries ensure an adequate level of protection : Andorre, Argentina, the Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and Canada. However, in view of the annulment by the Court of Justice of the European Union of the European Commission's adequacy decision on Safe Harbor, the above-mentioned list of countries can change at any time. **The European Commission's**

adequacy decisions adopted pursuant to the GDPR will be reviewed every four years in order to take into account the developments that may have taken place in third countries.

Data transfers required by administrative or judicial authorities

All personal data transfers carried out on the basis of a decision rendered by a court or an administrative authority of a third county to the European Union will be contrary to the GDPR unless an international agreement provides otherwise.

In practice, data controllers will therefore have to determine whether the decision falls within the scope of an agreement before any data transfer takes place.

⁵¹. Cnil, [Transferts hors UE: Liste des pays et niveau de protection des données](#)

Sheet n°14: Supervisory authorities – With the removal of prior formalities, what is their role?

The supervisory authorities retain their primary tasks of verifying the correct application of the rules on the protection of personal data, raising public awareness and supporting controllers and processors. In principle, these tasks will be accomplished in the territory of the Member State in which the entity is established.

However, the collaboration between personal data protection authorities is the subject of a new organization, in particular because of the introduction of the one-stop shop mechanism. WP29 adopted guidelines for identifying a controller or processor's lead supervisory authority on April 5th, 2017⁵².

One-stop shop system

❖ When is it necessary to identify a lead authority?

A lead authority must be identified only where cross-border processing is being carried out, i.e. processing by a controller or processor established in several Member States and/or processing which substantially affects data subjects in several Member States. According to WP29, “substantially” and “affects”, which are not defined in the GDPR, should be interpreted on a case-to-case basis taking into account the context of the processing, the type of data, the purpose of the processing and certain other factors such as possible damage that the processing may cause, likely effects on rights, etc.

❖ How to identify the main establishment of the controller or processor?

Regarding the data controller, the main establishment is the “central administration in the Union”. This definition seems to indicate that the competent authority will be that of the country of the Union in which the controller's head office is located.

⁵². http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

One-stop shop system in the EU

Lead authority

Supervisory authority of the Member State
in which the main establishment or the
single establishment of the data controller or
processor is



- Head office;
- Main processing activities (if there is no head office);
- Lead authority as a single interlocuter;
- Residual competence of other supervisory authorities (complaint);
- Cooperation between the lead authority and other supervisory authorities (exchange of information, mutual assistance, joint operations, etc.)

However, if it is found that the decision making power relating to determining the purposes and means of a given processing operation is exercised in another establishment, competence will be given to the supervisory authority of the country in which that establishment is located for that processing operation. Thus, in certain hypotheses, it would seem that several lead authorities could be identified.

Regarding the data processor, the principal place of business shall be defined by reference to the “central administration in the Union”. In the absence of a central administration, this establishment shall be the one where “the main processing activities” are carried out. WP29 guides us on the criteria to be taken into account in order to determine this place of processing: the place where decisions are actually carried out, the place where decisions are finally taken, the place where the company is registered, etc.

The burden of proof as to where the processing is carried out rests with the controller or processor.

❖ *Once the main establishment has been identified, what will be the practical consequence of this new organisation ?*

The lead supervisory authority will be the sole point of contact for the controller or processor.

However, the GDPR will uphold a residual competence for the other supervisory authorities. Indeed, each national supervisory authority shall remain competent to entertain a complaint lodged with it if its subject matter concerns only an establishment situated in the Member State to which it is subject or in the event of an infringement of the GDPR if it affects only the data subjects in the Member State to which it is subject.

The lead authority shall be informed of any such claim or violation of the GDPR and may then decide whether or not to handle the case.

❖ *How will the supervisory authorities cooperate?*

The GDPR organises the cooperation between supervisory authorities in so far as the authorities shall provide each other with relevant information and **mutual assistance**, even conduct joint operations (namely investigations and inspections)⁵³. They will have a discretionary power to decide which of the authorities will be the lead authority.

The authorities' powers

Supervisory authorities' have numerous powers. They have **investigative powers** enabling them to obtain access to any information or access to all data necessary for the performance of their duties and to the premises of the bodies. They may also conduct audits of entities acting as data controllers and data processors.

They may **adopt corrective measures**, such as notifying a controller of the non-compliance of the processing operations implemented with the GDPR. Furthermore, they may instruct entities to satisfy requests by individuals for the exercise of their rights.

When a prior consultation with the supervisory authority is necessary (DPIA revealing an infringement of the rights and freedoms of individuals or if the national law of a Member State so provides), the supervisory authorities will have **consultative** and, where appropriate, **approval powers**.

⁵³. Articles 56, 60 et 61 of the GDPR.



The creation of a European Data Protection Committee

This Committee will bring together all the presidents of the supervisory authorities of each Member State and the European Data Protection Supervisor. This Committee will replace WP29 established by Article 29 of Directive 95/46/EC.

As the WP29 is currently doing, this Committee will be able to publish documentation (guidelines, recommendations, good practices, etc.). It may also examine questions relating to the application of the GDPR.

This Committee will pay particular attention to the uniform application of the GDPR throughout the European Union. Thus, it will have to be consulted, in order to render an opinion, prior to any decision by a supervisory authority to adopt a list of processing operations subject to the obligation to carry out an impact assessment or to adopt standard contractual clauses.

It will also be responsible for analysing any question concerning the general application of the GDPR or any question which may produce effects in several Member States.

This Committee will also be able to issue binding decisions (in the event of disagreements as to the designation of the lead authority for example).

Sheet n°15: The deterrent effect of sanctions

The lack of deterrence and disparate sanctions imposed by the supervisory authorities have long been criticized.

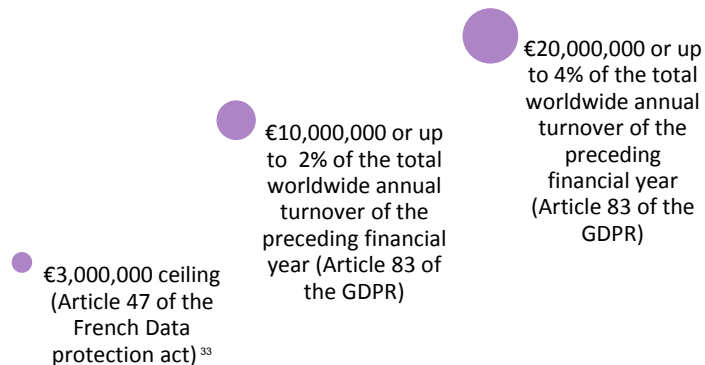
The maximum fine⁵⁴ of €150,000 rendered by the Cnil against Google has been greatly publicised. However, it did not force the American giant to inflect its personal data protection policy and it did not deter the other entities of the GAFA⁵⁵. This is evidenced by the recent public formal notice issued by the Cnil to Facebook concerning its numerous breaches of the legislation in force⁵⁶.

It is probably for this reason that the European institutions have insisted on specifying in the GDPR the fact that fines imposed for infringements of the applicable rules must be “effective, proportionate and dissuasive”⁵⁷.

Which entities will be subject to penalties ?

In accordance with current French and European regulations, only the controller is liable to administrative sanctions imposed by the Cnil. The processor has no other obligations than those laid down in the contract with the controller with regard to he security and confidentiality of personal data.

The GDPR changes this matter. Indeed, subject to obligations under the GDPR, the processor may be sanctioned by the Cnil in cases of infringement.



The criteria taken into account

The GDPR enumerates a series of criteria which the supervisory authority must take into account when imposing a penalty on a controller or processor. They include in particular the nature, seriousness and duration of the infringement, deliberate or negligent commission of the infringement.

What fine for what offence ?

The European institutions created two types of sanctions.

Certain infringements are subject to administrative fines up to €10,000,000, or up to 2 % of the total worldwide annual turnover of the preceding financial year (non-compliance with the principles of privacy by design and privacy by default, lack of data security, failure to report data breaches, failure to keep a record of processing activities or failure to comply with the rules on the designation of the DPO).

Other infringements will be subject to administrative fines up to €20,000,000 or 4% of the total worldwide annual turnover of the preceding financial year (non-compliance with the principles of personal data protection, breach of consent rules or infringements of provisions on the transfer of personal data outside the EEA).

⁵⁴. This fine was recently re-evaluated to €3,000,000, see Sheet n°16.

⁵⁵. [La formation restreinte de la CNIL prononce une sanction pécuniaire de 150 000 € à l'encontre de la société GOOGLE Inc.](#) » (confidentiality rules) or « [Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l'encontre Google](#) » (right to dereferencing).

⁵⁶. <https://www.cnil.fr/fr/la-cnil-met-publiquement-en-demeure-facebook-de-se-conformer-dans-un-delai-de-trois-mois-la-loi>

⁵⁷. Article 83 of the GDPR.

Sheet n°16: The changes brought by the Law for a Digital Republic

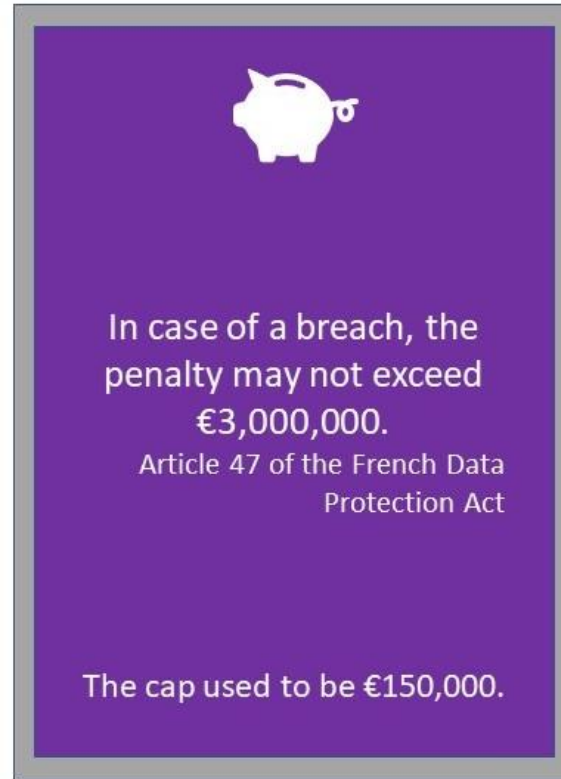
Law n°2016-1321 of October 7th, 2016 for a Digital Republic aims at ensuring a better protection of citizens in the digital society. This Law anticipates certain provisions of the GDPR, in particular individual rights and sanctions.

A reassessment of the maximum amount for a financial penalty

Since October 9th, 2016, the Cnil's ceiling for sanctions of € 150,000 has been raised to €3,000,000. The national legislator wanted to anticipate the increase in the maximum amount of administrative fines provided for by the GDPR.

It should be noted that the application of this new Law and the GDPR will have no influence on the criminal sanctions in Articles 226-16 to 226-24 of the Penal Code⁵⁸.

In addition, the distinction between the maximum amount of the fine depending on whether the controller was sanctioned for a first instance of non-compliance with the regulations or whether he or she reiterated facts already sanctioned by the Cnil was **abolished** (€150,000 for the first instance of non-compliance and €300,000 or 5% of turnover if the same fact is repeated within 5 years).



Informing data subjects

The Law for a Digital Republic also provides that the French supervisory authority (*Commission Nationale de l'Informatique et des Libertés*) may order that the sanctioned individuals each inform, and at their own expense, each of the data subject of the penalty⁵⁹. Initially, the Law only provided for the publication of the sanction or a formal notice. This possibility of publication by the supervisory authority has been maintained.

What is the relationship between the national regime and the GDPR ?

The French legislator specified that the new penalties prescribed by the Law for a Digital Republic will apply **until May, 25th 2018** (date of the coming into effect of the GDPR). Article 83 of the GDPR will then become applicable. However, the new sanctions provided by the Law for a digital Republic will remain applicable as from 25 May 2018, for breaches of the protection of personal data committed outside the scope of Article 83 of the GDPR⁶⁰. Thus, it would seem that the non-observance the individuals' right to define guidelines on the situation of their data at their death could be sanctioned on the basis of Law n°78-17 of January 6th 1978, since this right is not provided for in the GDPR.

⁵⁸. Fines ranging from €100,000 to €300,000 depending on the violations.

⁵⁹. Article 46 of the French Data Protection Act.

⁶⁰. Article 84 of the GDPR and Article 65 of Law n°2016-1321 of October 7th, 2016.

Informing data subjects

Information concerning the storage period of the personal data

Information regarding their rights to manage their personal data post-mortem

If the data was collected electronically, then the rights must be able to be exercised by electronic means. An e-mail address must at the very least be communicated to the data subject (Article 43 bis).

The right to recover data

The Law for a Digital Republic amends the Consumer Code by creating a right to data recovery for consumers. The Law specifies, confusedly, that consumers will be able to recover their data under the conditions laid down in Article 20 of the GDPR on the right to portability⁶³. Article 48 of the Law will come into application at the same time as the GDPR on May 25th, 2018.

However, it must be underlined that the Law for a Digital Republic only applies to providers of a public online communication services. The latter will also have to offer consumers a free functionality enabling them to retrieve the files they have uploaded online or the data resulting from the use of their user account.. The implementation of this measure should be specified by a decree published in March 2017.

⁶¹. Article 32 of the French Data Protection Act.

⁶². <http://www.economie.gouv.fr/republique-numerique>

⁶³. See Sheet n°12.

The situation of post-mortem data

Any person may define guidelines regarding the storage, erasure and communication of personal data after his or her death⁶. Thus, controllers will have to inform data subjects that they have the right to define the situation of their data post-mortem. The decree organising this "digital death", and in particular the directory of guidelines, should be published in March 2017, according to the government⁶².

Period for which the personal data will be stored

Article 32 of the French Data Protection Act now states that the data subject must be informed of the period for which the categories of personal data processed will be stored.

Data subject's rights

Right to specific erasure

For data subjects whose personal data was collected when they were minors (Article 40, II).

Data erased within 1 month of the request for erasure.

Right to manage personal data post mortem

All data subjects have the right to define guidelines regarding the storage, erasure and communication of personal data after his or her death (Article 40-1).

As a result, there is a specific right of access for heirs.

Sheet n°17: The changes brought by the Law for the modernisation of the XXIst century's justice

In France, the scope of class actions, a mechanism inherited from US law, is expanding. Initially limited to the fields of environment and health, Law n°2016-1547 of November 18th, 2016 on the modernisation of the justice system of the XXIst century expands the scope of class actions namely to the field of personal data protection. The legislative decree n°2017-888 of May 6th, 2017 sets down the procedural rules for class actions before the administrative and judicial judge.

Who is concerned by class actions?

	Judicial judge	Administrative judge
Competent court	<ul style="list-style-type: none"> Regional High court (Tribunal de Grande Instance, TGI) of the place of the defendant's residence; High court of Paris if the defendant resides abroad. 	<ul style="list-style-type: none"> Administrative court if the individual complaints would have fallen within the competence of a single jurisdiction; Council of State if the individual complaints would have fallen within several jurisdictions.
Status of the party having failed to meet his or her obligations	No particular requirements.	Legal person governed by public law or a private entity in charge of managing a public service.
Status of the injured party	Several persons, in a similar situation having suffered a harm caused by a data controller or data processor and the common cause of which is a similar failure to comply with the provisions of the French Data Protection Act (Law n°78-17 known as the "Law and freedoms" law).	
Persons with standing	<ul style="list-style-type: none"> Associations regularly declared for at least 5 years with the statutory purpose of protecting privacy and the protection of personal data; Representative and authorised consumer protection associations where the processing of personal data affects consumers; Trade unions of employees or representative officials when the treatment affects employees or civil servants. 	

What is the aim of class actions? Is there a prerequisite?

	Judicial judge	Administrative judge
Purpose of the class action	Exclusively the termination of the breach.	
Formal notice – prerequisite for initiating the proceedings	Before initiating the proceedings, the person must receive a formal notice to cease the breach or cause it to cease or to make good for the harm suffered. The class action can only be brought after a period of 4 months has elapsed from the receipt of the formal notice.	
The summons – initiating the procedure	<p>The summons must include the following, failing which it will be void:</p> <ul style="list-style-type: none"> the court in front of which the claim is brought); the request to cease the breach with a statement of facts; an indication of the procedures for appearing before the court and an indication that, if the defendant fails to appear, a judgement may be rendered against him or her based solely on the evidence provided by the plaintiff; the individual cases presented by the plaintiff in support of his action. 	<p>The summons must include the following, failing which it will be void:</p> <ul style="list-style-type: none"> the legal person governed by public law or a private entity in charge of managing a public service against which the action is brought; the nature of the breach and of the harm; the elements enabling an assessment to be made of the similarity of the situations of the persons for whom the action is presented; the individual cases in the light of which the action is brought.

Sheet n°18: The contributions of the Bill on personal data

On December 13th 2017, the Government presented⁵⁸ a Bill on personal data⁵⁹ amending the French Data Protection Act to adapt the latter to EU law. This Bill should allow the adaptation of the French data protection law in light of the above-mentioned European texts as well as Directive 2016/680⁶⁰. An impact assessment study of the law⁶¹ was carried out on December 12th, 2017.

It should be emphasised that the GDPR is directly applicable. This is not the case with the Directive which needs to be transposed. Nonetheless, seeing as the GDPR refers certain aspects of compliance to national legislator, the French legal framework must be adapted. In this context, the Bill clarifies several point detailed bellow.

Strengthening the Cnil's powers and clarifying its missions

The Bill predictably identifies the Cnil as the “national supervisory authority” within the meaning of the GDPR. It entrusts it with new missions in view of the accountability approach adopted by the GDPR.

In this respect, Article 1 of the Bill states that the Cnil may namely establish and publish guidelines, publish baseline methodology for the processing of personal health data (the Cnil has already begun to do so in the research field⁶²) or certify persons, products, systems or procedures for the purpose of demonstrating their compliance with the GDPR and national law. Thus, as an illustration, the Bill seems to pave the way for the certification of the Data Protection Officer.



Furthermore, the Bill specifies the framework in which agents and members of the Cnil will intervene when monitoring the implementation of data processing activities (Article 4). Monitoring is limited to the professional sphere.

However, it should be noted that agents may be allowed to use an assumed identity when carrying out online controls. Thus, these agents may create a false identity of an average user for an effective control. It is specified that the use of an assumed identity does not affect the legality of the findings. This protects the controls from the risk of challenges being brought on the grounds of breach of the principle of loyalty in collecting evidence.

Secrecy will remain enforceable against agents in a very limited context. Only three secrets/privileges will be enforceable: professional secrecy applicable to the attorney-client relationship, the secrecy of journalistic sources and medical secrecy.

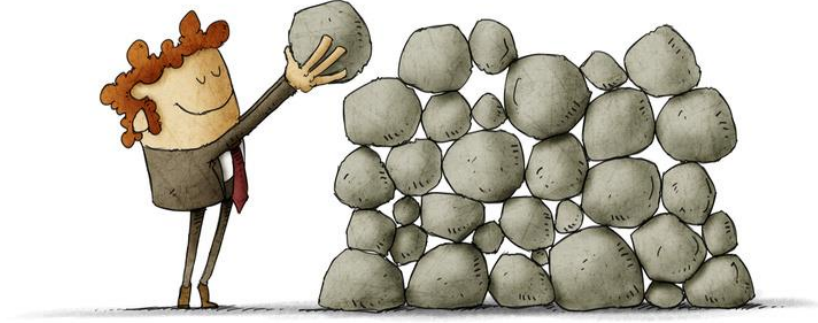
⁵⁸. <http://www.justice.gouv.fr/la-garde-des-sceaux-10016/projet-de-loi-relatif-a-la-protection-des-donnees-personnelles-31094.html>

⁵⁹. Projet de loi relatif à la protection des données personnelles (JUSC1732261L).

⁶⁰. Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. It must be transposed by May 8th 2018.

⁶¹. Etude d'impact du projet de loi relatif à la protection des données personnelles (JUSC1732261L/Bkeue-1).

⁶². <https://www.cnil.fr/fr/recherche-medicale-queelles-formalites-pour-les-theses-et-les-memoires>



Cooperation procedure between supervisory authorities

The GDPR provides for the cooperation between supervisory authorities (Articles 60 to 62). In this context, the Bill details the conditions of this cooperation procedure namely when joint operations take place on French territory. Therefore, “the members or authorised agents of the Cnil, acting as the host supervisory authority, shall be present alongside members and agents of the other supervisory authorities participating, where appropriate, in the [joint] operation” (Article 5). As such, members or agents of a European supervisory authority could be empowered by the Cnil to exercise the same powers of verification and investigation as the Cnil's members and agents.

It must be underlined that a specific procedure addresses the empowerment of agents of another Member State's supervisory authority. Indeed, the supervisory authority must request the empowerment of its agent beforehand. It must be specified that the President of the Cnil may only empower agents presenting similar guarantees to those required for agents of the Cnil.

When the Cnil acts as lead supervisory authority, it shall disclose the report of the rapporteur and all useful information for the procedure to the concerned supervisory authorities. However, the conditions for applying this procedure will be specified in a decree of the Council of State (*Conseil d'Etat*).

Data concerning offences

The Bill introduces an important development with regard to the processing of personal data relating to offences. Article 11 states that “natural or legal persons [may carry out personal data processing activities namely concerning offences] for the purpose of enabling them to prepare and, where appropriate, to bring and follow a legal action as, or on behalf of, a victim, a party to the proceedings and to have the decision enforced over a period proportionate to that purpose”. Thus, under certain conditions, a legal person governed by private law may be able to process personal data relating in particular to offences.

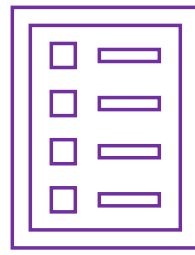
Conflict of laws

The GDPR gives Member States some leeway. For this reason, many countries have adopted or are in the process of adopting a law amending national data protection provisions. In the event of discrepancies between the Member States' national laws, the Bill provides that “national rules (...) apply where the data subject resides in France, including when the controller is not established in France” (Article 8).

The removal of prior formalities and the accountability of those involved in the processing of personal data

It may be recalled that the GDPR adopts an accountability approach for controllers, whom are subject to new obligations (ex: privacy by design, privacy by default, DPIAs, etc.) as well as for processors whom are subject to specific obligations, in particular regarding security requirements and cooperating with the controller. Data processors are also now liable for their breaches (Article 83 of the GDPR).

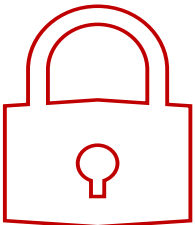




The Bill abolishes the system of prior declarations provided for in Articles 22 to 24 of the French Data Protection Act. Moreover, the current Article 25 of the French Data Protection Act would be repealed (Articles 9 and 10 of the Bill).

Nevertheless, a prior formality remains for processing operations requiring the use of the registration number of persons in the national identification register of natural persons (NIR). This type of processing may only be carried out after a decree rendered by the Council of State and a reasoned and published opinion of the Cnil.

In its deliberation n°2017-299 of November 30th, 2017 on the Bill, the Cnil stresses the practical hurdles raised by the authorisation by decree. For example, telemedicine solution providers, which must process the NIR for reimbursement purposes, could only do so after regulatory approval. This impedes the process and the development of innovative devices. The Cnil therefore considers it necessary to supplement the planned mechanism by reintroducing the possibility of allowing it to authorise the use of the NIR in the light of the information submitted by the applicant.



The available remedies

Article 16 of the Bill establishes a specific case of group action through a new Article 43 quarter inserted in the French Data Protection Act. The latter provides that a data subject may entrust an association or organisation with the task of making a complaint to the CNIL, a judicial appeal against the CNIL or against a controller or a processor on his/her behalf. This right is provided for in Article 80, 1° of the GDPR.

The association or organisation exercising the right must meet the requirements set out in Article 43 ter of the French Data Protection Act. It was created by Law n°2016-1547 of November 18th, 2016 on the modernisation of the justice system of the XXIst century and provides for the conditions of referral to the judicial or administrative judge for a group action for the purpose of putting an end to a breach to the French Data Protection Act.

In addition the Cnil also has a new remedy. Where a transfer of personal data to non-EU Member States or international organisations presents risks for the protection of the rights and freedoms of data subjects, it may request the Council of State to suspend or terminate the data transfer in question. The Cnil's request will be pending the assessment by the European Court of Justice of the validity of the adequacy decision or appropriate safeguards approved by the European Commission.

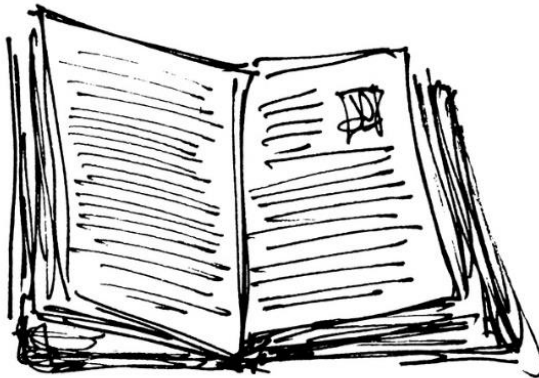


Focus on the intelligibility of data protection legislation

Article 20 of the Bill empowers the Government to take by means of ordinance the measures falling within the scope of the law that are namely necessary “to entirely rewrite Act n°78-17 (...) in order to make the formal corrections and adjustments necessary for the simplification and coherence of the provisions bringing national law into conformity with the GDPR, as well as for simplifying their implementation by the persons concerned”. Moreover, it also empowers the Government to take ordinances to establish coherency between these changes and “all legislation applicable to the protection of personal data”.

The purpose of these measures is to harmonize all legislation applicable to the protection of personal data. In view of the important changes brought by the entry into force of the GDPR, the coherence, intelligibility and transparency of all these legislations appear indispensable.

The Cnil’s opinion will be required for the rewriting order. The Government will have 6 months to table a ratification Bill before the Parliament as from the publication of the rewriting order.



The Cnil and Council of State’s opinions

The Cnil deems that “the Bill fully plays the game of the Regulation and the harmonisation sought by it” (deliberation n°2017-299 of November 30th, 2017)⁶³.

However, the Cnil points out the lateness of the Bill. This renders conformity by May 25th, 2018 all the more difficult. Moreover, it also raises the Bill’s lack of readability. It calls for the swiftest adoption possible by the Government of the ordinance rewriting the French Data Protection Act.

The same criticisms as the Cnil can be found in the Council of State’s Opinion n°393836 rendered December 7th, 2017⁶⁴. Indeed, the Council of State also raises the Bill’s lack of readability. It suggested two types of provisions to remedy this problem and namely an authorisation for the Government to take ordinances in order to organise and bring coherence to all legislation applicable to the protection of personal data. It seems that the suggestion was followed and incorporated into Article 20 of the Bill.

In order to ensure compliance as judiciously as possible, the Council of State is postponing the entry into force of the law until 25 May 2018.



⁶³. https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf

⁶⁴. <https://www.legifrance.gouv.fr/Droit-francais/Les-avis-du-Conseil-d-Etat-rendus-sur-les-projets-de-loi/2017/Projet-de-loi-d-adaptation-au-droit-de-l-Union-europeenne-de-la-loi-n-78-17-du-6-janvier-1978-relative-a-l-informatique-aux-fichiers-et-aux-libertes-JUSC1732261L-13-12-2017>

Do you have a question?

A team dedicated to achieve your ambitions will reply:

01 43 80 02 01

19, rue Vernier – 75017 – Paris

Find our lawyers' practical advice on twitter:

@GaranceMathias

You can subscribe to our Newsletter on the firm's website:

www.avocats-mathias.com