PRACTICAL GUIDE GDPR

DATA PROTECTION OFFICERS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr

The objective of this guide is to support both organisations in setting up the function of Data Protection Officer (DPO) and such officers in the exercise of their profession.

This guide is a living tool which will be enriched by best practices reported by professionals to the French Data Protection Authority (CNIL).

TABLE DES MATIÈRES

FOREWORD

The job of Data Protection Officer ("DPO" in this guide) has become essential since the entry into application of the European General Data Protection Regulation (GDPR) on 25 May 2018. This regulation, which harmonises formerly national obligations at the European level, concerns organisations in all their activities: human resources management, prospecting, relations with customers or users, etc. From now on, the processing of personal data is a fundamental component of most business lines.

It is therefore natural that the GDPR devotes three of its articles to outlining the profession responsible for advising data controllers on the protection of such data. Consequently, the DPO takes on a new qualitative and quantitative importance compared to its predecessor in France, the *Correspondant Informatique et Libertés* (CIL).

This development is qualitative, first of all: the spirit of the regulation is to **make the DPO the "orchestra conductor" of the management of personal data in the organisation which designates them**. The hierarchical position of the DPO must bear witness to this, and their resources must be adapted, so that they can fully accomplish their job and their role of compliance coordinator. They should not work in a vacuum, but be fully integrated into the operational activities of their organisation. **The DPO is an essential link in data governance**, in conjunction with the CISO (Chief Information Security Officer) and the IT (information technology) department.

The job of DPO has also changed from a quantitative point of view. Indeed, the number of DPOs has increased considerably, due to **the designation obligation** to which many organisations are subject. Thus, while 18,000 organisations had a CIL, **more than 80,000 organisations had designated a DPO in 2021 in France**, including 26,000 in the public sphere.

Fully aware of this development, the CNIL has adapted its support strategy for DPOs, mainly by orienting it on the development and backing of DPOs' networks. Organised by sector or region, they respond to a first level of questions from the field, with the CNIL only intervening with such representatives and federations in a second phase.
This guide aims to support both organisations in setting up the function of the data protection officer and DPOs in the exercise of their tasks.

The DPO guide is divided into 4 chapters:

- The role of the DPO;
- Designating the DPO;
- The exercise of the DPO's tasks;
- CNIL support for the DPO.

Each theme is illustrated by **concrete cases** and **frequently asked questions** related to the subject being dealt with. The reader can also rely on FAQs and practical tools, such as the mission statement.

This guide, which has been drafted on the basis of three years of practical support for DPOs, will provide you with the keys to making the most of the presence of a DPO, being recruited as a DPO or more generally improving your compliance.

WHAT ARE THE CNIL'S MISSIONS?

The Commission Nationale de l'Informatique et des Libertés (CNIL) is the French data protection authority. It pursues four main missions:

Informing and protecting rights

The CNIL responds to requests from individuals and professionals. It carries out communication actions with the general public and professionals, whether through its networks, the press, its website, its presence on social networks or by providing educational tools.

Anyone can contact the CNIL in the event of a difficulty in exercising their rights.

Supporting compliance and advising

In order to help private and public bodies to comply with the GDPR, the CNIL offers a complete toolbox adapted to their size and needs.
The CNIL oversees the search for solutions allowing them to pursue their legitimate objectives while strictly respecting the rights and freedoms of citizens.

Anticipating and innovating

To detect and analyse technologies or new uses that may have significant impacts on privacy, the CNIL provides dedicated monitoring.

It contributes to the development of technological solutions protecting privacy by advising companies as early as possible, with a view to privacy by design.

Oversight and sanctioning

Oversight allows the CNIL to verify the concrete implementation of the law. It can require an actor to bring its processing into compliance (formal notice) or impose sanctions (fines, etc.).

FOR FURTHER READING

On cnil.fr, in French:
- CNIL's missions
- Status and organisation of the CNIL

THE ROLE OF THE DPO

The GDPR places the DPO as a key player in the personal data governance system. Indeed, the missions assigned to the DPO establish their role as manager of the permanent and dynamic compliance process which organisations must put in place.

FOCUS: THE TEXTS DEFINING THE FUNCTION OF DPO

The function of the DPO is regulated and precisely defined in Articles 37 to 39 of the GDPR. This guide is based on that regulation, the French Data Protection Act, and its implementing decree, as well as the guidelines on the DPO of the European Data Protection Board (EDPB). At the end of each section, a reference to the relevant passages of those texts is provided.

Advising and supporting the organisation

The DPO has an advisory and support role at several levels :

- bringing their expertise to management so that it can ensure compliance of processing;
- disseminating the personal data protection culture and rules to all the individuals who process personal data within the organisation.

The DPO can thus identify and formalize the key moments during which they **would like their intervention or presence to be systematic**, for example for each:

- draft decision to create or upgrade existing processing (particularly to ensure compliance with the principles of data protection by design and by default);
- considering of the need for a data protection impact assessment (DPIA) and the actual completion of one;
- drafting or keeping of a record of processing activities;
- drafting and updating of internal data protection rules or policies;
- personal data breach, in order to advise on the measures to be taken as well as on the notification to the authority and to the data subjects.

The DPO raises awareness and supports the actors involved in each department processing data::

- by ensuring the adoption by all of a personal data protection culture (e.g., through internal training courses on the main principles of data protection);
- by carrying out communication and awareness-raising actions on subjects relevant to the organi-

sation (use of posters and practical guides accessible from the intranet, reminder of safety rules on the occasion of a sanction or a data breach reported in the media, false "phishing" campaigns for training purposes, etc.);

- by presenting themself as the internal point of contact for any question in terms of data protection, and through intermediaries if necessary.

Therefore, the DPO has above all a mission of information, advice, and oversight. **The DPO is not responsible for the compliance of the organisation**, keeping the records, carrying out impact assessments, or notifications of data breaches. However, the DPO is in a position to be a key player whose skills will be very useful to the head of the organisation to help them comply with their obligations.

FOCUS: COMPLIANCE MANAGEMENT BY THE DPO

Ensuring compliance with the GDPR is an active process which consists of anticipating and organising the interventions of the DPO within the organisation.
The steps to be taken can, for example, be the following:

- formalizing the DPO consultation cases;
- setting up, with the departments concerned, a "GDPR committee" responsible for arbitrating and guiding actions concerning data processing;
- being involved in the development and updating of governance documents (IT system security policy, IT charter, welcome booklet, internal rules, etc.);
- maintaining regular contact with operational staff who process personal data, being receptive to them and providing support to them;
- providing for an internal procedure in the event of CNIL audit (reception procedures, individuals to be notified, information to be obtained), a personal data breach (immediate information to the DPO), or internal blockage (alerting the data controller and/or resolution of the conflict);
- planning the modalities for responding to external requests (drafting response templates, informing the departments in contact with the public):
- providing a contact individual in the event of absence or impediment who can receive requests and be the internal point of contact vis-à-vis the data subjects, but also the CNIL;
- identifying the relevant departments for the regular activities and training procedures, with the help, if necessary, of competent internal or external contacts;
- keeping a dashboard of the activities carried out, in order to stock a regular update (management meeting) as well as a regular activity report for the management of the organisation;
- being active in their professional network by identifying and collaborating with the relevant contacts (internal contacts, joint data controllers, service providers);
- maintaining their technical and operational knowledge in connection with the organisation's processing activities through monitoring (on case law, publications by supervisory authorities, etc.) and during training and experience sharing (the DPO's geographical and/or professional network).

Monitoring the effectiveness of the rules

The DPO is responsible for monitoring compliance with the GDPR.

This mission must take the form of verifications organised by the DPO (external audit or internal contact), or carried out by the DPO personally, in collaboration with other key functions such as the CISO (Chief Information Security Officer). It must be accompanied by monitoring of the corrective and ongoing action plan.

Depending on the priorities, the purpose of these controls or audits may consist of:

- verifications of the accuracy of the information contained in the record of processing operations implemented by the organisation (inventory of processing activities, scope of purposes, data subjects, nature of the data processed, recipients and possible transfers outside the European Union, retention periods, security measures);
- verifications of the compliance of the most sensitive processing operations, taking into account the impact assessments conducted (particularly with regard to the implementation of measures intended to reduce the likelihood and severity of risks);
- the implementation of tools for tracking and monitoring the use of processing (analysis of logs, detection of prohibited data, verification of compliance with retention periods, etc.);
- monitoring the effectiveness of the technical and organisational data protection measures that the organisation has undertaken to implement.

Being the organisation's point of contact on GDPR matters

With the CNIL

The DPO is, on the one hand, required to cooperate with the supervisory authority and must therefore play a role of "facilitator" during discussions with the CNIL (responding to requests during an onsite investigation, investigating a complaint, consulting within the framework of a DPIA, notification of a data breach, etc.).

On the other hand, the DPO can consult the CNIL on all questions relating to the protection of personal data or their function. The data controller or the data processor is prohibited from submitting these questions for validation or from prohibiting them.

In addition, according to the Professional support charter (in French) that it published in February 2021, **the CNIL does not respond to requests for advice sent to it by organisations that have not taken care to consult their DPO** on the question they wish to ask.

The majority of the CNIL's onsite investigations are unannounced. However, on an exceptional basis, the organisation and the DPO may be notified a few days in advance. The DPO may, during an onsite investigation, be "responsible for the premises" where the processing takes place that is the subject of the verifications. The DPO is then the privileged, but not exclusive, point of contact of the investigation delegation and is responsible for verifying and signing the minutes drawn up at the end of the day. The data controller remains able to comment on the minutes when it receives them.

On the other hand, the DPO cannot represent the organisation alone with the CNIL during a summons for hearing, as this would represent a conflict of interest for the DPO. However, they can accompany a representative of the organisation to provide their expertise and answer questions.

With the data subjects concerned by the processing of personal data

The DPO is also the point of contact for individuals whose data is processed by the organisation that designated them. As such, they can take charge of organising the processing of their requests to exercise rights (access, portability, etc.) so that a complete response is provided within the allotted time. The DPO may also be requested by the data subjects (employees, agents, customers, suppliers, students, users, etc.) regarding any question relating to the processing of their personal data.

WARNING

As part of a response to a complaint, the DPO acts as a point of contact with the data subject and the CNIL agents. **This does not authorise the DPO to communicate the direct contact information of the CNIL agents to third parties** (including the data subject). Such contact information is intended solely for the recipient of the messages sent and for their co-workers.

Ensuring the documentation of data processing

Documentation plays a dominating role in the new logic of accountability under the GDPR. Now compulsory, it allows the data controller or data processor to guarantee and demonstrate compliance with its obligations as well as the steps taken.

Many elements can be included in the documentation, such as the record of processing activities, DPIAs, record of data breaches and measures taken to remedy them, informational notices, evidence of the collection of consent, procedures relating to the exercise of rights, data processor contracts, tools for supervising transfers outside the European Union, written analysis on the DPO's lack of conflicts of interest, etc. This list is not exhaustive insofar as any element making it possible to justify compliance and to steer the actions to be carried out may be included in the documentation.

Documentation is an essential tool for the DPO because it makes it possible to have an exhaustive knowledge of the processing operations implemented and to plan their management. The DPO must therefore ensure that this documentation is kept, i.e., to ensure its relevance and oversee its updating.

With regard to **keeping a record of processing activities**, Article 30 GDPR provides that the obligation to keep a record weighs on the data controller or data processor. However, in practice, the activities of the DPO may lead them to take charge of this task.

Indeed, the keeping of the record constitutes a tool for monitoring and supervision of the processing operations implemented, allowing the DPO to have the most exhaustive possible knowledge of processing operations and to propose the measures necessary for their supervision. In any case, the

DPO must be able to consult it at any time.

Note: it is recommended that the DPO's mission statement stipulates that keeping the record constitutes one of their tasks (if that is indeed the case) and indicates that the information relating to each processing will be communicated to them by the individuals who are responsible for them or who implement them

For more information on the processing record, the CNIL has published a factsheet dedicated to the record on its website, which contains in particular a simplified record template, spreadsheet form, in open format, freely reusable and which can be adapted to many data processing cases, as well as an example of records of processing operations.

Frequently Asked Questions

How should the DPO prioritize their tasks?

If all of the missions presented above must be implemented by the DPO, the GDPR specifies that the DPO "shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing" (Article 39.2). This means that the level of vigilance and resources must be all the higher the greater the risks presented by the processing operations (rigorous monitoring of sensitive data processing, training of particularly involved employees, internal audit on security measures, etc.).

Does the DPO have to personally respond to all external requests?

While the CNIL and any data subject must be able to contact the DPO in the cases provided for by the regulations, the DPO is not required to systematically generate the response. However, they must ensure that each request will receive appropriate treatment by the competent service within the allotted time.

Is the DPO responsible for compliance? Are the DPO's recommendations binding?

The DPO is not personally liable in the event of a breach of the obligations provided for by the GDPR. It is the organisation that is responsible for compliance with the GDPR (see Factsheet 6 on the status of the DPO). It is impossible to transfer to the DPO, by delegation of authority, the liability incumbent on the data controller or the obligations specific to the data processor.
If the DPO's recommendations are not followed, the data controller or the DPO can usefully document the decisions that have been taken as well as, if applicable, the reasons why the DPO's opinion was not followed.

Can the DPO perform other tasks than those provided for in Article 39 of the GDPR?

It is quite possible to entrust the DPO with other tasks provided that this does not hinder the performance of the tasks which are specifically assigned to the DPO by the GDPR (including by depriving them of the time necessary for the performance of those tasks) and does not constitute a conflict of interest.

Certain tasks appear to be adapted, by nature, to the function of the DPO and could be usefully assigned to them, such as keeping the record of processing activities, participating in the performance or evaluation of impact assessments, if they have required competency, or the supervision of personal data breaches.

It should be noted that none of these tasks can be carried out by the DPO alone, who must necessarily be able to work with the teams processing or determining the processing of personal data. In addition, these obligations remain the responsibility of the data controller or the data processor.

OFFICIAL TEXTS

- Articles 38 and 39 GDPR on the function and tasks of the DPO.
- Articles 82 et seq. of the implementing decree of the French Data Protection Act, Légifrance.fr.

DESIGNATING THE DPO

Factsheet 1: In which cases should a DPO be appointed?

Whether they are data controllers or data processors, the designation of a DPO is **mandatory** for:

- public authorities or organisations (with the exception of courts in the exercise of their judicial functions);
- organisations whose basic activities lead them to carry out regular, systematic monitoring of individuals on a large scale;
- organisations whose core activities lead them to deal with large-scale sensitive data or data relating to criminal convictions and offences.

BEST PRACTICE

Even apart from these three cases, **the designation of a DPO is recommended as soon as the organisation encounters problems relating to the protection of personal data**. This makes it possible to entrust an expert with the identification and coordination of the actions to be taken in terms of data protection.

What does the term, "public authorities and organisations" encompass?

These are national, regional and local authorities, but also organisations such as higher education structures, hospitals, health agencies, independent administrative authorities , public administrative establishments , etc.

BEST PRACTICE

Private organisations entrusted with a public service mission retain their private law status and are therefore not required to appoint a DPO. However, as pointed out in the DPO guidelines of the European Data Protection Board (EDPB), **the designation of a DPO is encouraged for these bodies**, even in cases where it would not be mandatory under the other criteria.

“Core activities”: what does that mean?

The core activity of an organisation corresponds to its core business. If the processing of personal data is essential to achieve the objectives of the organisation, then this criterion is met.

Example: the core activity of a clinic is to provide care for the patients it supports. This activity necessarily involves processing of data relating to health (patient medical records). The processing of such data must, in this case, be considered a core activity of the clinic.
However, the support or “auxiliary” activity (e.g., compensation of employees, IT support) is not a core activity of the clinic.

How should the concept of “large scale” be assessed?

“This should in particular apply to large-scale processing operations 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” (Recital 91 GDPR).

There is no threshold applicable to all situations, beyond which a processing is considered to be implemented on a “large scale”. A case-by-case analysis is necessary to assess this point. This analysis, and the reasoning behind it, can usefully be incorporated into the documentation.

It must consider a set of factors:

- the number of individuals involved, in absolute or relative value (in relation to the population concerned, and not in relation to the scale of the organisation);
- the volume of data and/or the spectrum of data processed;
- the duration or permanence of the processing activities;
- the geographic extent of the processing activity.

EXAMPLES

The following constitute large-scale processing:

- the processing of patient data by a hospital as part of the normal course of its business;
- processing of the travel data of passengers using urban public transport (tracked by tickets, for example);
- the processing of real-time geolocation data from customers of an international fast food chain for statistical purposes by a data processor specializing in the provision of such services;
- the processing of customer data by an insurance company or a bank as part of the normal course of its business;
- the processing of personal data by a search engine for targeted advertising purposes;
- the processing of data (content, traffic, location) by telephone or internet service providers[1].

The following do not constitute large-scale processing:

- the processing of patient data by a local doctor working on an individual basis if the patient population is less than 10,000 people per year (see the standard for medical and paramedical practices (in French) ;
- the processing of personal data relating to criminal convictions and offences by an individual lawyer.

What is "regular and systematic monitoring"?

The GDPR does not define the notion of "regular and systematic monitoring" of individuals, but gives the example of online tracking and profiling for the purposes of behavioural advertising (Recital 24 GDPR). The EDPB indicates that one or more meanings are to be considered for the expression "regular and systematic":

- "Regular" should be understood to mean:
  - continuous or occurring at regular intervals over a period of time; or
  - recurring or repeating at fixed times; or
  - taking place constantly or periodically.
- "Systematic" should be understood to mean:
  - occurring in accordance with a system; or
  - pre-established, organised or methodical; or
  - taking place as part of a general data collection program; or
  - carried out as part of a strategy.

1 All of these examples come from the EDPB guidelines about the data protection officer?

Examples of regular and systematic monitoring of data subjects:

- marketing activities whose personalization is based on personal data;
- profiling and scoring for risk assessment purposes (credit risk assessment, establishing insurance premiums, preventing fraud, or detecting money laundering, etc.);
- geolocation by mobile applications;
- loyalty programs;
- behavioural advertising;
- monitoring of wellness, health, and fitness data using portable devices;
- closed circuit television systems;
- connected devices such as cars and smart meters, home automation, etc.

EXAMPLES OF APPOINTING OF A DPO

Political parties: basic activities involve the processing of special categories of data (political opinions). Therefore, in view of l'article 37.1.c du RGPD, the criterion remaining to be assessed to determine whether the designation of a DPO is mandatory is the "large-scale" nature of the processing.

For political parties active at the national level and with a large membership base, the large-scale criterion is likely to be met. On the other hand, for small parties or local parties, this criterion might not be met. An analysis should be carried out on a case-by-case basis.

Retailer or mass marketer: the marketing of products, the collection of payments, and possibly the management of loyalty programs could be considered basic activities. However, such activities may not require regular and systematic monitoring of the data subjects. It is therefore necessary to carry out an analysis for each processing to verify whether that is the case, particularly in the case of loyalty programs, and thus to determine whether the designation of a DPO is mandatory.

REFERENCE TEXTS

- Article 37.1 GDPR on cases of mandatory designation of the DPO.
- Recital 97 GDPR on the concept of core activities.
- Recital 31 PR on the concept of large scale.
- Recital 24 GDPR on the concept of monitoring the behaviour of people.
- EDPB guidelines on the data protection officer (p. 6 et seq.).

Factsheet 2: Who can be designated DPO?

Although there is no typical profile to serve as DPO, the GDPR requires the DPO to have a certain level of expertise. The organisation must also ensure that there is no conflict of interest with the appointee's other missions.

The DPO's knowledge and skills

The person approached for the function of DPO must have a certain **level of knowledge**, i.e.:

- Legal and technical expertise on data protection;
- knowledge of the business line, industry regulations and the organisation of the structure for which they are designated;
- an understanding of processing operations, IT systems and the organisation's data protection and security needs;
- for a public authority or a public body, good knowledge of the applicable administrative rules and procedures.

If the person approached does not have the expertise on all this knowledge before taking office, it will be necessary to mobilize internal expertise and develop their knowledge in the very short term through training.

The individual must also present the personal qualities necessary for this function: integrity, high level of professional ethics, ability to communicate, popularize, and convince.

Note: the level of expertise required varies according to the sensitivity, complexity, and volume of data processed by the organisation. This knowledge and skills can be acquired through a training plan adapted to the profile of the future DPO (see the question "How can a DPO be trained?").

FOCUS: DPO CERTIFICATION

Certification is the procedure by which a third party certifies the compliance of a product, a service or a skill with a standard or a reference.

Since 2018, the CNIL has approved organisations that issue a **DPO skills certification** on the basis of its reference system, and keeps a list of such organisations. Such organisations offer a test, in the form of a multiple-choice quiz of at least one hundred questions relating to regulation, liability, and security.

Certification is only accessible after 2 years' professional experience in data protection, or 2 years in any field and at least 35 hours' training on the subject. It is then valid for 3 years.

For its holder, certification constitutes a proof of their adequacy with the level of knowledge requirement imposed by the GDPR. For organisations looking for profiles of data protection experts, certification represents a guarantee of confidence. **However, it is not mandatory to be certified in order to be designated DPO**.

Absence of conflicts of interest

The DPO may perform other duties within the organisation (part-time DPO). However, in the context of their other duties, they should not have **decision-making power over the determination of the purposes and means of processing**: the DPO should therefore not be "judge and jury".

The existence of a conflict of interest is assessed on a **case by case basis**. It is advisable to document the analysis leading to the exclusion of the existence of a conflict of interest for the designated DPO.

Examples of duties likely to give rise to a conflict of interest: Managing Director, Chief Operating Officer, Chief Medical Officer, Marketing Department Manager, Human Resources Manager, IT Department Manager, etc.

WARNING

Positions at a "lower" hierarchical level within the organisational structure are also likely to give rise to a conflict of interest if, **in practice, the person participates in determining the purposes and means of the processing**.

FOCUS: DOCUMENTING THE CHOICE OF YOUR DPO

When an organisation designates a DPO, it must be **able to prove that their DPO meets the requirements of the GDPR** (knowledge and skills, absence of conflicts of interest, etc.).

The CNIL does not verify these requirements at the time of designation. According to the principle of accountability, it is up to the body that designates a DPO to assemble internal documentation to certify that the DPO designated meets the requirements of the GDPR. In the event of a CNIL audit, the organisation may be asked to present such documentation.

Examples: CV, job description, written analysis on the absence of conflict of interest, any certifications, etc.

Frequently Asked Questions

What profile do you need to have to be a DPO?

There is no typical profile for a DPO. Indeed, according to the study on DPOs carried out by AFPA in partnership with the CNIL[2], around 28% of DPOs have an IT profile, and the same percentage a legal profile, the remaining 43% coming from administration, finance, compliance, audit, etc.

Does a DPO need to have a particular degree?

Obtaining a specific degree or following a specific training is not required to be designated DPO. However, the DPO must have adequate skills and knowledge to perform their duties.

Thus, if the DPO does not have a degree specializing in data protection, they often will have supplemented their academic training with professional experience or continuing education in computer security, law, or any other subject relevant to the performance of their duties.

A data controller recruiting a DPO must ensure that the successful candidate has the required specialist knowledge and must enable them to maintain and supplement their knowledge.

DPO and CISO: a conflict of interest?

A chief information security officer may be designated DPO if they do not have decision-making power as CISO in determining the purposes and means of the processing of personal data implemented by their organisation.

DPO and personnel representative: a conflict of interest?

A personnel representative may be called upon, as part of a vote, to take a position on certain subjects or projects related to the processing of personal data, particularly personnel management. In this case, there may be a risk of conflict of interest with the position of DPO.

According to the same reasoning, a DPO can appear on an ethics or professional conduct committee if it does not create a risk of conflict of interests.

2 "Délégué à la protection des données (DPO): un métier qui se développe, une fonction qui se structure (Data Protection Officer (DPO): a developing profession, a function that is taking form)" , Study conducted by AFPA's prospective business department, at the request of the Ministry for Labour, Employment and Inclusion (DGEFP), in partnership with the CNIL and AFCDP (2020).

Can the representative in the European Union of a data controller or processor established outside the Union be designated DPO?

The representative of a data controller or processor who is not established in the EU cannot, in principle, be designated DPO for that organisation as it would constitute a conflict of interest.

Can a legal entity be a data processor and a DPO for the same organisation?

There is no automatic prohibition on a service provider, who is also a data processor[3], being designated DPO for their client. This would then be a separate provision of services which would not be carried out within the framework of the data controller's instructions. This could be the case, for example, of an organisation offering digital services and an outsourced DPO.

However, a **case-by-case analysis** must be carried out to assess whether the situation is likely to compromise the independence of the DPO in the performance of their duties. Such an analysis is part of the data controller's and the data processor's documentation.
In some cases, it is necessary to implement measures to guarantee this independence. It is then advisable to pay attention to:

- the status (public or private) of the actors in question, with public actors not being subject to the same profit constraints;
- the possibility of providing different points of contact with the service provider (one as a data processor, one as a service provider/DPO);
- the possibility of providing for two separate contracts.

In order not to find themself acting as both judge and jury, and thus to be free from conflicts of interest, the individual serving as DPO must not, however, serve either as manager or principal within the organisation.

Can the same person be DPO for a data controller and their data processor?

The GDPR does not prohibit a DPO from being designated for a data controller and its data processor.

However, according to a reasoning similar to that presented above and taking into account the independence requirement, it is recommended to assess whether the organisation and the measures taken make it possible to guarantee that independence. These elements must be included in the data controller's and their subcontractor's documentation.
In particular, it should be specified how that independence can be ensured at times when the two structures may have divergent interests, e.g., in the context of reviewing the contract between the data controller and the data processor.

Can the same DPO be designated for competing organisations?

An external DPO can be designated for organisations in competition, as long as these different missions and tasks do not give rise to conflicts of interest. Indeed, the DPO is subject to an obligation of confidentiality or professional secrecy and can thus work for competing employers without endangering the confidentiality of each of the parties.

---

3 A data processor processes the data on behalf, on the instruction and under the authority of a data controller (e.g., hosting, maintenance, etc.)..

Can a lawyer be designated DPO?

A lawyer can be designated DPO of an organisation on the basis of a service contract (external DPO). However, that lawyer cannot represent this organisation before the courts in cases involving subjects relating to personal data since such representation would constitute a conflict of interest.

Can a elected official be a DPO?

An elected official cannot exercise the functions of DPO for the community by which they are elected, due to a conflict of interest. Indeed, they participate in the decision-making on the data processing implemented by the community.

Can a town hall secretary be a DPO?

In small communities, town hall secretaries are often approached to take on the function of DPO. However, the performance of associated missions can sometimes come up against difficulties: lack of time to devote to the subject and a risk of conflicts of interest.

Thus, before proceeding with the designation, the mayor must ensure that the prospective DPO does not take part in decisions concerning the files used by the community (objectives and conditions of implementation, data processed, recipients, retention periods, security measures, etc.) and that they have sufficient time to accomplish their missions.

Can a trainee or apprentice be a DPO?

Although this possibility is not explicitly ruled out by the GDPR, it appears hardly compatible with the requirements related to the performance of the function. In addition to the difficulties that this designation could entail in terms of labour law (assignment of a trainee to a permanent job), it should be noted that:

- the DPO must have "expert knowledge" while the trainee/apprentice is on the job to learn;
- the trainee/apprentice should be able to benefit from advice and comments on their work, which contradicts the fact that the DPO should not receive any instruction on the performance of these tasks;
- The DPO's mission is a long-term one, both in the initial compliance of the organisation and in the monitoring of new projects, which is difficult to reconcile with the limited duration of an internship. As such, the EDPB guidelines on the DPO recommend favouring the longest possible contracts for this position.

How to assess the independence of the DPO?

The real independence of the DPO, in their role of providing analysis and advice, presupposes that two types of impartiality are respected:

- objective impartiality: the DPO is not judge and party, because they are not called upon to review what they have personally decided, alone or jointly;
- subjective impartiality: the DPO is immune to influences guided by divergent interests, which could alter the freedom of their positions.

What is the risk for an organisation that does not appoint a DPO?

An organisation that has not designated a DPO when such a designation is mandatory would expose itself to a sanction from the CNIL, which could in particular take the form of a reprimand, an injunction to comply, or an administrative fine of up to 10 million euros or 2% of worldwide annual turnover for the previous financial year, whichever is greater.

OFFICIAL TEXTS

- Article 37.5 GDPR on the knowledge and skills of the DPO.
- Article 38.6 GDPR on the absence of conflicts of interest.
- EDPB guidelines on the data protection officer (p. 13 et seq.; p. 19 et seq.).

Factsheet 3: Internal or external DPO? How can the function be shared?

Each organisation is free to organise the function of DPO according to its needs. This is a choice that belongs to the entity, depending in particular on the advantages and disadvantages of using an external or internal DPO, the internal candidates available and the structure's organisation.

Internal DPO

The DPO can be a staff member of the organisation. They can perform their duties full time or part time.

Advantages:

- knowledge of the structure's organisation, the services as well as the business line;
- proximity to internal contacts;
- better responsiveness in the event of internal solicitations on subjects related to data protection;
- Easier to plan for their presence in the event of a CNIL audit

Critical points:

- risk of conflict of interest if the DPO performs other duties;
- allocation of sufficient time to the DPO;
- adequate hierarchical positioning;
- a training plan adapted to the profile of the DPO is to be prepared.

External DPO

The function of DPO can be performed based on a service contract concluded with a natural person (e.g., consultant, employee of a group subsidiary, etc.) or a legal entity (e.g., law firm, consulting firm, management centre, mixed union, etc.).

Advantages:

- solution to the lack of internal human resources;
- using the experience and tools developed by the external DPO;
- specialization of the DPO in an industry;
- knowledge of best practices for similar organisations;

Critical points:

- organisation of exchange points and regular contacts with the highest level of management, as well as with business teams to maintain proximity;
- making contacting the external DPO as systematic, simple, and easy as contacting an internal individual;
- difficulty in choosing a provider and ensuring their expertise.

Shared DPO

Whether they are an internal or external DPO, a DPO can be shared, i.e., designated for several entities.

Advantages:

- smoothing of costs related to the designation of the DPO for entities in the same group;
- standardisation of procedures between the entities having pooled the function;
- cross-management of compliance between organisations with the same concerns.

Critical points:

- organisation of exchange points and regular contact with business teams to maintain proximity;
- risk for the DPO of not being kept informed of internal matters related to data protection;
- setting up an organisation to ensure efficient compliance monitoring (e.g., intermediaries, points of contact).

Pooling is possible under **certain conditions** which vary according to the type of structure:

- **for the private sector: :** a group of companies can designate a single DPO provided that they are **easily reachable from each place of establishment**.

EXAMPLE

In the case of a group made up of subsidiaries located in different Member States of the European Union, a single DPO (employee of one of the subsidiaries or external service provider) can be designated for the parent company and all the companies in the group, provided that an adequate organisation is put in place.

Not being physically present in each of the subsidiaries, the DPO can, for example, be supported by a network of "intermediaries" or "points of contact" responsible in particular for providing operational support to the DPO, while passing on questions to them that may arise.

- **for the public sector:** the DPO's function can be shared between several authorities or public bodies, **taking into consideration their organisational structure and size**.

Pooling is a particularly suitable solution for **the smallest local authorities**. It allows them to reduce the financial costs associated with the function, while benefiting from the services of professionals with data protection skills, knowledge of issues specific to the local public sector and the availability necessary for an effective performance of their tasks.

Pooling can particularly occur at the level of a public inter-municipal cooperation establishment, such as a community of municipalities or a metro region, or of a public operator of digital services, such as a departmental technical agency or a management centre of the regional public service accompanying the development of e-administration in its region.

Regional authorities, local public establishments and private bodies responsible for a public service mission which opt for pooling must conclude an agreement specifying the conditions under which it is performed.

Frequently Asked Questions

Internal DPO: part-time or full-time?

This is a decision left to the discretion of the data controller or the data processor appointing a DPO.

The designation of a part-time DPO requires an assessment of their workload in order to allocate them the time necessary for the performance of their duties (see Factsheet 5).

According to the study carried out by AFPA in partnership with the CNIL[4], only a quarter of internal DPOs carry out this mission full time.

Can a DPO be designated for a limited time?

Organisations for which the designation of a DPO is not compulsory may provide that the DPO, internal or external, performs their duties for a limited period. However, this must be sufficient to allow the DPO to carry out in-depth work on compliance which, in a large majority of cases, requires several months or even several years. Long-term temporal availability can be part of the resources that the organisation provides to the DPO. It is advisable to formalize this point in the mission statement or in the service contract.

External DPO: what are the requirements towards the employees of the body designated DPO?

When the DPO function is performed by an external service provider, a team of individuals working on behalf of that entity can, in fact, perform the DPO's tasks as a group. In this case, it is advised to include, in the service contract, a clear distribution of tasks within the team responsible for the DPO function and clearly identify the individual who acts as the contact in charge of the client.
It is also recommended that each employee of the service provider performing the functions of DPO fulfils all the applicable requirements (independence, sufficient resources and means, absence of conflicts of interest, etc.).

Joint DPO: how to designate one with the CNIL?

If the DPO function is pooled for a group of entities, each of these entities must fill out a DPO designation form, as data controller or data processor.

For entities with a large number of designations to be made, a specific designation procedure ("multiple designation") is proposed (for more information, contact the CNIL DPO service).

REFERENCE TEXTS

- Article 37.7 GDPR on the designation of the DPO with the supervisory authority
- Articles 83 and 84 of Decree No. 2019-536 of 29 May 2019 on the procedures for designating the DPO with the CNIL and the pooling agreement (in French)
- EDPB Guidelines on the designation of a lead supervisory authority by a data controller or data processor

4 "Délégué à la protection des données (DPO): un métier qui se développe, une fonction qui se structure (Data Protection Officer (DPO): a developing profession, a function that is taking form)", Study conducted by AFPA's prospective business department, at the request of the Ministry for Labour, Employment and Inclusion (DGEFP), in partnership with the CNIL and AFCDP (2020).

Factsheet 4: How to appoint a DPO?

Step 1: choosing the "right DPO"

An external DPO can be a natural person or a legal entity, but an internally designated DPO can only be a natural person (e.g., an employee).
The internal DPO designation procedure requires that you first ask questions about the individual approached for the position: in this regard, it is important to ask the right questions in order to be able to subsequently justify your choice.

The choice of an internal DPO must particularly take into account:

- the relevance of the person approached for the tasks of the DPO and their interest in data protection matters;
- their profile with regard to their qualifications and the absence of conflicts of interest (see Factsheet 2);
- the conditions for performing their tasks (sufficient resources, access to useful information and independence - see Factsheets 5 and 6).

DESIGNATING A DPO: THE KEY QUESTIONS

The document entitled, "The key questions to ask yourself when appointing a DPO" (Appendix No. 1) will help you verify that the GDPR requirements for a future DPO are met.

Step 2: formalizing the designation

It is recommended to formalize the tasks entrusted to the DPO through a specific document.
Examples: mission statement, amendment to the employment contract, job description, service contract for an external DPO, etc.

This document can also be an opportunity to specify the working methods of the DPO (resources allocated, intermediaries identified, frequency of meetings with the management of the organisation and the services processing the data, communication circuit, etc.) by describing how the obligations of the appointing body will be translated into practice.

SAMPLE MISSION STATEMENT

This guide provides an example of a mission statement to be given to the DPO (see Appendix No. 2). The latter must of course be adapted and clarified according to the tasks entrusted to the DPO and the performance conditions of their function.

Step 3: making your DPO known

The designation of a DPO should be accompanied by **communication actions** in order to bring visibility to the function and contact details of the DPO within the organisation, for example with regard to all employees (officials or employees), employee representative bodies and management committees or executive bodies.

Examples of communication actions: informational memo sent by management to all staff, internal memo published on the intranet or by posting, internal presentation to management bodies, publication of the mission statement, etc.

The purpose of this type of action is to communicate internally on the role of the DPO, their status, the resources allocated to them, and the procedures associated with the performance of their tasks. It is also an opportunity to recall the issue of compliance and to present the future projects that will be managed by the DPO.

Note: the DPO is in permanent contact with the services and departments of the organisation. This communication plan is therefore particularly important insofar as it provides the DPO with the most favourable conditions for taking up their post.

Step 4: designating your DPO with the competent supervisory authority

Before designating its DPO, an organisation working in multiple countries must ensure that the CNIL is the competent authority for the designation. If it is the CNIL, they can then carry out the online designation of their DPO.

The designation of the DPO with the CNIL can only be done online via the dedicated online service. No postal mail is processed and it is not necessary to send supporting documentation such as the deliberations of the municipal council appointing the DPO.

The 4 steps of the designation form are detailed in Appendix 3 of this guide.

Frequently Asked Questions

Can a DPO be partially designated?

The DPO is **designated for all processing operations** carried out by the data controller or data processor (Point 2.1 of the EDPB DPO Guidelines). Consequently, the partial designation of a DPO (e.g., designation of a DPO only for HR processing) is not possible.

Can the role of DPO be filled by several people?

An organisation can only designate one person as the data protection officer. However, the DPO can be supported by a team, working in collaboration with the other business lines of the organisation or have a network of "data protection intermediaries" able to help the DPO raise awareness on data protection issues or to forward questions, projects or requests to exercise rights to them.

Do the employee representative bodies have to be informed of the designation of the DPO?

Informing the employee representative bodies is not required by the regulations. However, it is still a good practice in order to ensure transparency and good visibility of the designation of the DPO within the organisation.

Local authorities: does the designation of the DPO require sending the CNIL deliberations or an order relating to the performance of the function?

No, no supporting documentation is required for notifying the designation of the DPO to the CNIL. For regional authorities, it is therefore not necessary to send the deliberation creating the job or the decree appointing the DPO. Only the online procedure is required to designate a DPO.

When does the designation of the DPO become effective?

The designation of the DPO is effective the day after the validation of the online designation form by the organisation.

Which supervisory authority in Europe should I designate my DPO with?

The determination of the authority with which the DPO should be designated does not depend on the DPO's location, or on the organisation's status as parent company or subsidiary. However, the nature of the processing implemented does have an impact:

- **For local processing** (implemented by an organisation's establishments in a single country and materially affecting only individuals from that country): the DPO must be designated with **the competent local authority** with regard to local processing (registered office of the data controller or data processor, which corresponds to the data protection authority of the Member State where the local processing is carried out).
- **For cross-border processing:** in the event that the data controller (parent or subsidiary) also implements cross-border processing, the DPO must be designated with **the lead authority**.

The lead authority is the authority of the country where the main establishment is located (location of the registered office or location of the establishment in which decisions will be taken relating to the purposes and methods of processing). Therefore, it is frequently also competent for certain local processing.

EXAMPLE

A DPO is shared for a group of companies whose parent company is in Italy and the subsidiary is located in France. As DPO of the French subsidiary, they must be designated with the CNIL with regard to local processing and cross-border processing for which the French subsidiary is the data controller. No action by the French subsidiary with the Italian authority is required. Likewise, the parent company in Italy must designate this DPO with the Italian supervisory authority for its local processing and cross-border processing for which it is the data controller.

This reasoning applies whether it is the same DPO designated for all the entities of the group (pooled) or a different DPO for each entity in the group.

Is it possible for an employee to refuse to be designated DPO?

General labour law rules apply here: in France, if this designation constitutes a substantial modification of the employment contract, then the individual must be put in a position to refuse it. In addition to this general rule, special rules can be added if, for example, the modification of the employment contract was provided for in the contract or if the employee is also a protected employee (e.g., employee representative).

The reasons leading an employee to refuse or to wanting to refuse the function of DPO (insufficient resources to organise the function, particularly in terms of time, insufficient knowledge, etc.) can be a **serious indication that the obligations incumbent on the organisation in the designation of the DPO have not been met.**

REFERENCE TEXTS

On cnil.fr, in French:
- Article 37.7 GDPR on the designation of the DPO with the supervisory authority
- Articles 83 and 84 of Decree No. 2019-536 of 29 May 2019 on the procedures for designating the DPO with the CNIL and the pooling agreement (in French)
- EDPB Guidelines on the designation of a lead supervisory authority by a data controller or data processor

PERFORMING THE FUNCTION OF DPO

Factsheet 5: what resources should be allocated to the DPO?

The DPO must have the means necessary to perform their duties, which means that they must be **involved in all matters relating to data protection and have sufficient resources**.

The involvement of the DPO in all matters relating to data protection

It is essential that the DPO or, where applicable, their team, is involved as early as possible in all matters relating to data protection. Informing and consulting the DPO as soon as a processing project is considered will facilitate compliance with the GDPR and encourage an approach based on data protection by design. **The DPO must be a natural point of contact within the organisation**, e.g., by being involved with working groups within the organisation dedicated to data processing activities.

For example, the organisation ensures in particular that:

- the DPO is invited to participate regularly in the organisation's strategic meetings which specify beforehand the projects involving personal data;
- their presence is recommended when decisions with data protection implications are taken;
- the DPO can dialogue and work with the functions playing an important role in data protection, such as the Chief Information Security Officer;
- all relevant information is transmitted to the DPO in due time to enable them to provide a relevant, informed opinion;
- the opinion of the DPO is always seriously taken into account. In the event of a disagreement, it is recommended, as a best practice, to record the reasons why the DPO's opinion was not followed;
- the DPO is immediately consulted when a data breach or other incident (report in the press, complaints, etc.) occurs.

The DPO's resources

The GDPR requires that the organisation must **provide the DPO with the necessary resources to carry out their tasks** (time required, access to financial resources, contributors if necessary); by **facilitating the DPO's access to data and processing operations** (facilitated access to other departments of the organisation) and by **allowing the DPO to maintain their specialized knowledge**.

The DPO's resources must be adapted to the size, structure, and activity of the organisation. Thus, the more complex or sensitive the processing operations, the more resources allocated to the DPO.

It is recommended to specify the type of resources allocated to the DPO in the mission statement, as the organisation's commitment to the DPO to enable them to best perform their missions.

EXAMPLES OF RESOURCES TO BE PROVIDED TO THE DPO

- Acknowledging and promoting **the function of the DPO by senior management** (e.g., at the board of directors level).
- **Sufficient time** so that the DPO can perform their duties. This aspect is particularly important when the DPO performs their duties on a part-time basis. It is also recommended to determine, together with the DPO, the estimate of the time necessary to perform their function (the need is more significant when starting in the function), that a work plan be defined and that the DPO's tasks be prioritized.
- Adequate support in terms of **financial resources** (hold their own budget or available for awareness-raising actions or to recruit a team temporarily or permanently) and **infrastructure** (facilities, installations, equipment).
- **Default access to legal documentation** engaging the organisation with third parties on matters of personal data processing (partners and subcontractors).
- **Official communication of the DPO's designation to all staff** so that their existence and function are known within the organisation.
- **Access to internal communication tools** in the performance of their duties in order to be able to raise awareness and train in the requirements of the GDPR (reminder of best practices, response in the event of fraudulent emails or data breaches, etc.).
- **Access to other departments**, such as human resources, legal, IT, security, etc., so that the DPO receives essential inputs and information from those other departments.
- **Continuing education**. The DPO must be able to keep their knowledge up to date with regard to regulatory and technical developments, particularly in the field of data protection. In order to constantly increase the DPO's level of expertise, they should be encouraged to participate in training as well as other forms of professional development, such as participating in forums on privacy protection, workshops, professional associations, etc.
- Depending on the size and structure of the organisation, it may be appropriate to form a **team around the DPO** for which the tasks and responsibilities of each member must be clearly established. Likewise, when the DPO function is performed by an external service provider, a team of people working on behalf of that entity can carry out the tasks of the DPO, under the responsibility of a main point of contact designated for the client.

.

Frequently Asked Questions

How to assess the resources to be allocated to the DPO?

The nature and volume of resources allocated to the DPO vary according to the size, structure and activity of the organisation. Consequently, the more complex the processing operations or the more likely they are to infringe the privacy of individuals, the greater the resources allocated to the DPO. For example, the analysis of complex projects by the DPO requires time to deliver relevant advice. The estimate of the workload must be proportionate to the established priorities. This assessment is essential for the proper performance of the DPO's tasks for the benefit of the body that designates them.

The allocation of a specific budget may be part of the material resources available to the DPO. To quantify this budget, different elements can be considered: for example, the training needs of the future DPO, any awareness-raising actions for the staff of the organisation, the use of service providers if necessary (lawyers, auditors, etc.) or the contribution of other departments within the organisation.

Are letters sent to the DPO confidential?

While the DPO may wish to have their mail opened for sorting purposes, they are also entitled to request the establishment of a strictly confidential communication channel (registered mail marked "confidential", which will not be opened, encrypted emails, etc. confidential telephone line, etc.) in particular for the purposes of communication with data subjects in a subordinate relationship with the organisation.

How to ensure the DPO's access to the organisation's data?

The DPO must, because of their duties, be able to access the organisation's IT systems, contractual documentation as well as the information processed. The data controller must ensure that the services under their authority facilitate this access at the request of the DPO. Because of the challenges in this area, it is advisable that the DPO and the data controller agree on a document formalizing the cases and the conditions under which that access will be carried out (e.g., audit, spot check, investigating a request to exercise rights, data breaches, etc.).

The DPO is subject to professional secrecy or a non-disclosure obligation, and their access to data is subject to the same general principles as all employees: it must be proportionate, justified and traceable.

These methods may be provided for in order to best adapt access to the needs of the DPO (read/write access to data, temporary access, possibilities of extracting a database, etc.). In certain specific sensitive cases (e.g., access to files on an employee's position, to emails, to highly confidential information) specific rules may be set with the DPO in order to guarantee the performance of their duties (e.g. verifications conducted by a third party).

This access must include files containing personal data as well as those not supposed to contain any (breaches of the GDPR in terms of retention and confidentiality are regularly observed by the CNIL in files that the organisations deemed to be free of personal data).

The organisation must ensure that these limits and accommodations do not prevent the successful completion of the DPO's duties.

OFFICIAL TEXTS

On cnil.fr, in French:
- Article 38.2 GDPR on the obligation to provide resources to the DPO
- Article 39.1 GDPR on cases of mandatory designation of the DPO
- Article 25 GDPR on data protection by default
- EDPB guidelines on the data protection officer (p. 16).

Factsheet 6: What is the status of the DPO?

The independence of the DPO in the performance of their duties

The GDPR provides for certain guarantees intended to ensure that the DPO is able to perform their duties with a sufficient degree of autonomy and independence with regard to the organisation which designates them.

This independence means that the DPO:

- **Must not receive instructions on the performance of their duties**, e.g., on how to deal with a data subject, how to investigate a complaint, on the results to be brought to an internal audit or even on the advisability of consulting the supervisory authority. Likewise, the DPO cannot be required to adopt a certain point of view on a matter related to data protection law such as a particular interpretation of the law.
- **Must not be subject to a sanction or dismissal for the performance of their duties**, for example if the DPO advises the data controller to carry out an impact assessment and the latter does not agree, or records a legal or technical analysis that conflicts with that adopted by the data controller. Note, however, that the DPO's functions may be terminated for reasons falling under usual labour law (such as: theft, harassment, other serious misconduct).
- **Reports directly to the highest levels of the organisation's leadership** so that the level at which decisions are made is aware of the opinions and recommendations of the DPO. Thus, the CNIL recommends that the DPO draw up and present to the highest level of the organisation a regular report (e.g., annual) on their activities. The DPO must also be able to speak directly to the highest level on a specific issue if they deem it necessary[5]. Note that this requirement to report to the highest level does not prejudge the DPO's "attachment" for which the GDPR does not contain a requirement.

Lack of liability for the DPO in the event of non-compliance with the GDPR

The GDPR provides that the data controller is the one required to ensure and be able to demonstrate that the processing is carried out in accordance with the GDPR. Likewise, the data processor is responsible for complying with its own obligations under the GDPR. Consequently, the DPO is not responsible in the event of non-compliance with the GDPR within the organisation that designated them.

It is therefore not possible to transfer to the DPO, by delegation of authority, the liability incumbent on the data controller or the obligations specific to the data processor under the GDPR. Indeed, this would amount to giving the DPO decision-making power over the purpose and means of the processing, which would constitute a conflict of interest contrary to the GDPR.

Non-disclosure/professional secrecy obligation

5 On this subject, the Luxembourg Data Protection Authority estimated in its Decision No. 23FR/2021 of 29 June 2021 that a direct reporting or the possibility of bypassing the intermediate line management levels could be proportionate measures to ensure the autonomy of the DPO.

The DPO must be subject to professional secrecy or a non-disclosure obligation with regard to the performance of their duties. Care should therefore be taken to include such an obligation in the employment contract or mission statement of an internal DPO or in the service contract of an external DPO.

Note: this professional secrecy or non-disclosure obligation does not prevent the DPO from contacting the supervisory authority to seek its opinion. Indeed, the GDPR provides that the DPO can consult with the supervisory authority on any subject.

Frequently Asked Questions

Can the DPO be criminally sanctioned in the performance of their duties?

The DPO is not criminally responsible for the compliance of their organisation. They may, however, be found criminally liable like any other employee or official, if they intentionally violate the criminal provisions of the French Data Protection Act or as an accomplice if they help the data controller or data processor violate those criminal provisions.

Can the DPO be sanctioned civilly in the performance of their duties?

An employee DPO cannot be held civilly liable: in accordance with the principle of the employer's liability for the actions of their employees, a civil action initiated by a data subject concerned by the data processing in question could only be brought against the data controller. However, with regard to an external DPO, if the latter were to commit professional misconduct leading the data controller to suffer harm, the latter could seek the liability of the external DPO and obtain damages. This is why some insurance companies offer professional liability insurance for DPOs.

Can the DPO be dismissed or relieved of their duties?

The DPO enjoys a specific independent status (see Factsheet 6). The DPO cannot be "dismissed or penalised by the controller or the processor for performing his tasks." (Art. 38.3 GDPR). This provision means that a DPO cannot be held responsible for analyses or comments based on data protection that they make concerning the processing operations of their employer. Thus, the unfair dismissal of a DPO would constitute a violation of the GDPR (as well as a possible industrial tribunal risk). However, the DPO is not a protected employee in the legal sense, and does not have a dedicated dismissal procedure provided for by the labour code.

They may, like any other employee or official, be dismissed for reasons other than the performance of their DPO duties, for example in the event of theft, bullying, or other similar serious misconduct.

Finally, an organisation that designates a DPO must ensure that the DPO has the qualifications and capabilities enabling them to perform their duties. They can therefore decide to withdraw the DPO duties from an employee who is unable to fulfil the duties assigned to him by the GDPR. This procedure is only possible if the employer has ensured that the DPO's difficulty in carrying out their duties does not come from insufficient resources - particularly in terms of time - granted to them. It must be documented and carried out according to the conditions set in the contract or by their status.

As for the external DPO, their service provider contract can also be terminated in accordance with contract or public order law and under the conditions set therein.

Should the DPO be attached to a particular department?

The GDPR does not specify the level of "attachment" of the DPO, who can therefore fall under the IT department, the risks department, the compliance department, the legal department or the general secretariat of the organisation. Regardless of which branch they report to, it is important that the DPO be able to report directly to the highest level of management in the organisation so that their advice may be known and taken into account.

Can the DPO receive instructions (such as "perform an audit every year") or be given objectives?

The DPO cannot receive instructions on the operational manner of performing their duties.

Thus, for example, an organisation cannot prohibit the DPO from contacting the CNIL for advice, force the DPO to approve a document, nor constantly distort or reject the communications that a DPO would like to send to employees or officials of the organisation. On this subject, the CNIL has already intervened with organisations to remind them of their obligations.

It is possible to send them requests (such as the production of an annual report, the drafting of an audit, etc.) as long as these do not prevent them from having the necessary resources, particularly in terms of availability, to perform other tasks that the DPO considers to be priorities. Such tasks could then be provided for in the mission statement.

They may also have evaluable objectives, accompanied by sufficient means to carry them out, as long as these are established in line with the actions that they have personally identified as priorities, particularly in the context of raising awareness among internal teams.

The DPO's independence should not, in fact, be interpreted to mean the possibility for the DPO to work in an opaque manner, without communicating with management or other departments on the elements that they have identified as priorities or on the measures that they plan to implement. That independence is reflected in the operational freedom to define these priorities and these measures: it does not mean the absence of links, but the absence of instructions which would have the value of an order or an injunction in the employee or hierarchical relationship.

Finally, the DPO can receive instructions on items that do not fall under the performance of their duties, such as an obligation to have their time off validated in an internal system.

Can documents produced by the DPO be "validated" or modified?

By indicating that the DPO does not receive any instructions concerning the performance of their duties and that they must be able to report directly to the highest level of management, the GDPR enables the DPO to produce any document (training materials, report, expertise, etc.) without interference, particularly concerning the substance.

However, they can decide for themself to submit preparatory work to their hierarchy or other services to receive comments or remarks that they may or may not choose to consider.

OFFICIAL TEXTS

- Article 38.2 and 38.3 GDPR on the function of DPO

Factsheet 7: What to do in the event of departure, leave or replacement of the DPO?

The DPO plays a central role in protecting the organisation's personal data, and acts as a point of contact for individuals as well as for the supervisory authority with which they must cooperate. Therefore, the departure or replacement of a DPO, whether permanent or temporary, must be anticipated and organised by the data controller as early as possible.

Managing the transition internally

Communicate internally: in the same way as when they were designated, the departure and replacement of the DPO must be relayed internally by all means (e.g., internal memo published on the intranet, information to employee representative bodies, etc.).

In the event of their replacement, this information will be used to communicate the name and contact details of the new DPO.

Follow up on current cases: it is essential to update the procedures making it possible to ensure the follow-up and the resumption of the cases in progress (e.g., follow-up on a request to exercise rights, conducting a DPIA in progress, etc.).

Transparency with regard to data subjects

In the event of their departure or replacement, the organisation must ensure that the information, which must include the contact details of the DPO, is up to date.

Note: to avoid this systematic updating of information, use "neutral" contact details (e.g., generic email address, telephone number, postal address, etc.).

Procedures with the supervisory authority

In the event of a permanent change

The data controller or the data processor must inform the CNIL as soon as possible of the end of the mission of their DPO. Operationally, to process an end of mission, it is requested to copy to the legal representative on the email informing the CNIL of the end of the DPO's mission (see address in the designation confirmation email).

If the DPO is replaced, the organisation must, within the same timeframe, appoint the new DPO (see Factsheet 4).

In the event of a temporary absence

- **If the absent DPO is officially replaced by another DPO during their absence**, a new designation with the CNIL is then required (by informing the CNIL at the same time of the end of the mission of the absent DPO);

- **If the DPO is not replaced**, it is necessary to provide for an update of internal procedures (e.g., routing of mail and calls) ensuring that requests from data subjects or from the supervisory authority are dealt with. In cases where the designation of the DPO is compulsory for the organisation, this vacancy can only be exceptional and very limited in time.

Note: when the CNIL makes contact with an organisation, it contacts the DPO officially designated with it, regardless of the internal reorganisations put in place. It is therefore important to manage the directing of calls and letters to the right individuals until a permanent designation can be made.

Frequently Asked Questions

Can a DPO request the end of their mission while remaining in the organisation?

The CNIL recommends that when taking up the post, the conditions and modalities of the end of the mission requested by the DPO employee be provided for in the mission statement or in the contract. This allows both parties to confirm that the DPO will not be penalised or hampered by their duties in their career development, and that they can benefit from the same opportunities for promotions or internal mobility as their colleagues.

OFFICIAL TEXTS

- Article 39 GDPR (duties of the DPO)
- Article 38.3 GDPR (independence of the DPO)
- Article 83 of the implementing decree of the French Data Protection Act (procedures for designating the DPO with the CNIL, in French)

HOW DOES THE CNIL SUPPORT DPOS?

The CNIL supports DPOs by providing them with various tools, which can be classified into the following two categories:

The tools for training

- **The website**, www.cnil.fr (and www.cnil.fr/en/ for the English version) : constantly updated, it contains a lot of information, classified in particular by procedures, themes, technologies or official texts. Regular publications of press releases and news help to keep knowledge up to date. A search engine and a "need help" tool also make it possible to respond to targeted requests.
- **Workshops or webinars:** those are accessible to all data protection professionals subject to prior registration via the CNIL website. They focus on a topic (marketing, human resources, health research, etc.) which they examine in depth, also leaving time for questions.
- **Online training (MOOC)**, relating to the fundamentals of data protection, "The GDPR Workshop", open to all and free of charge, was published in March 2019. Given the success encountered (more than 100,000 accounts created as of late 2020), this tool will soon be translated into English and enriched with specific thematic modules, starting with a module intended for regional authorities.

Tools for finding an answer

- **A hotline:** the agents of the DPO service are on duty Monday, Tuesday, Thursday and Friday from 10 a.m. to 12 p.m. at 01 53 73 22 22 (key 3), reserved for DPOs designated with the CNIL.
- **A dedicated email address:** the address of the DPO service (appearing in the DPO designation confirmation email) allows you to obtain a written response to requests for advice for which the DPO did not find the desired information on the CNIL website, or which has not already been dealt with by a network of professionals in their industry.

> Many of you contact us by email or phone: it is therefore essential to consult our website and conduct your own analysis before contacting us.
> In line with the CNIL support charter (in French), the DPO service will give priority to answering questions that cannot be answered on cnil.fr.

- **DPO professional networks:** these are good sources for answers to "field" questions. Organised by industry and by region, they can provide feedback or valuable advice. As part of its strategy of priority dialogue with "network heads", these professional networks are the privileged points of contact for the CNIL.

Compliance tools

- **A simplified record template:** DPOs are most often at the heart of the implementation of this tool, which is both mandatory and essential for monitoring compliance (see "The DPO and documentation"). The CNIL offers a reusable record template, in open format, comprising a tutorial form, a processing list form, a template for the form to be completed, and a sample form. It also has **published its own record (in French)**, which can be used as a concrete example to understand the issues and a possible way of using this tool.
- For carrying out the data protection impact assessment, the CNIL offers a ready-to-use PIA tool making it possible to run a DPIA from A to Z. It has also published guides to support data controllers and DPOs in this obligation, as well as processing lists (in French) for which DPIAs are mandatory or, conversely, not required.
- The CNIL publishes numerous documents, recalling the law in force, summarizing its doctrine or providing best practices. By visiting the CNIL site regularly, the DPO can check out the compliance packs (in French), repositories, guidelines, etc.
- Finally, being at the centre of compliance with the GDPR, the DPO may find some usefulness in all the tools published by the CNIL, to dialogue effectively with their colleagues (e.g., with the "GDPR Developer Guide") or to better understand the obligations incumbent on their organisation (as the "Practical guide to retention periods", in French, can help with).

FOCUS: "DPO: WHERE TO START?"

You have just been designated as a data protection officer: what should your first actions be? How to prioritize the different projects?

The page "DPO: where to start?" (in French) on the CNIL website offers you a working plan allowing you to proceed methodically to help organisations fulfil their obligations, particularly by proposing a support plan that allows processing to be mapped and the most urgent actions to be prioritized.

I am looking for a DPO for my organisation, what should I do?

A DPO can recruited internally or by calling on a service provider offering its DPO services (if applicable, this individual may also be the DPO of other organisations, we then speak of a joint DPO).

The organisation recruiting the individual should ensure that the person has specialized knowledge of data protection law and practices. It must therefore take into account the training courses, long or short, followed by the individual approached, but also their experience and knowledge of the industry. Degree courses in data protection exist, but they are neither compulsory nor the only way to become a DPO or to be trained on these subjects.

In addition, in order to support organisations in identifying the appropriate profile, the CNIL has set up a procedure for DPO skills certification based on a reference system developed by the CNIL. Certifications are issued by certification organisations approved by the CNIL. A list of such organisations is available on our website.

To verify that a DPO is truly certified, a recruiter can contact the certification organisation that awarded the certification. The CNIL does not hold a list of certified DPOs but publishes a list of approved certification organisations.

What does the designation of a DPO bring if my organisation already has a legal department responsible for data protection?

If an organisation encounters problems relating to the protection of personal data, the CNIL recommends the designation of a DPO even when it is not mandatory.

Indeed, a legal team, even a competent one, cannot replace the advantages of designating a DPO:

- they are an easily found and reachable point of contact, both internally and externally;
- they combine legal and IT security knowledge;
- their independence, defined by a legal text, ensures their impartiality and the freedom of their recommendations;
- they can benefit from the support and assistance of the CNIL.

Where should the DPO be located?

The GDPR does not set a requirement for the DPO's location. However, the DPO must be **easily reachable** by data subjects and the competent supervisory authorities. It is therefore recommended that the DPO be located in the European Union, whether or not the data controller or data processor is established in the European Union.

If the organisation does not have an establishment in the European Union, the DPO may be established outside the European Union, provided that they can effectively perform their duties.

What language should the DPO speak?

The DPO must be able to communicate effectively with data subjects and cooperate with the competent supervisory authorities. This means that such exchanges will have to be conducted in the language or languages used by the data subjects and the supervisory authorities.
To meet this requirement, the DPO can, for example, be assisted by a team of local intermediaries who will be able to respond in the language of the data subjects.

WARNING !

Companies canvass professionals (businesses, administrations, associations), sometimes aggressively, in order to sell a GDPR compliance support service.

As a reminder, the CNIL never charges for a GDPR compliance service. It never asks for the immediate payment of a sum of money in the context of an audit.

Is the title of "data protection officer - DPO" reserved for persons designated with a Data protection authority?

Yes, this title can only be used by individuals who are DPOs within the meaning of the GDPR, and, in particular, designated with a Data protection authority. The designated individual has the right to use the "DPO" logo (trademark protected by the CNIL) in the performance of their duties.

Data controllers, except in cases of compulsory designation, who do not wish to appoint a data protection officer (DPO) on a voluntary basis, may employ an external individual or consultants, responsible for duties related to the protection of personal data.

In this case, it is important to ensure that there is no confusion as to their title, status, duties, and missions. Therefore, it should be clearly stated on any communication within the company as well as with data protection authorities, data subjects and the public (in the broadest sense) that this individual or consultant does not does not have the title of Data Protection Officer.

How can a DPO be trained?

To acquire the skills and knowledge necessary to perform the job of DPO, the DPO can in particular rely on all the resources available on the CNIL website.

The CNIL also offers GDPR presentation days and thematic information workshops (security, health, DPIA, etc.), sometimes delivered in the form of webinars. To view the dates of these events and register, an agenda is available on the CNIL website.

In March 2019, the CNIL launched its MOOC, "The GDPR Workshop", free of charge and intended for all audiences, but rich enough to interest DPOs in training. It will soon be translated into English and enriched with new thematic modules.

The DPO can also focus on long courses offered by universities or schools (see, among others, the list of DPO training courses carried out by AFCDP[6] and the dedicated page on the SupDPO website[7], in French).

According to the study on DPOs carried out by AFPA[8], the main topics DPOs want to be able to be trained on are elements of IT security (encryption, strong authentication, traceability, etc.), conducting the first impact analyses and knowledge of IT systems (databases, the cloud, Cookies, API, etc.).

6 Association française des correspondants à la protection des données à caractère personnel.
7 Association of DPOs working in Higher Education, Research and Innovation.
8 "Délégué à la protection des données (DPO): un métier qui se développe, une fonction qui se structure (Data Protection Officer (DPO): a developing profession, a function that is taking form)", study carried out by AFPA's prospective business department, at the request of the Ministry for Labour, Employment and Inclusion (DGEFP), in partnership with the CNIL and AFCDP (2020).

Appendix No. 1: key questions to ask when appointing a DPO

- ☐ Does the individual approached know the issues and have an interest in data protection and the duties of a DPO?
- ☐ Have you checked that the position or the pre-existing duties of the individual approached do not give rise to a conflict of interest?
- ☐ Does the individual have the level of knowledge (legal and technical expertise in data protection, knowledge of the practices of the organisation and the business line, etc.) and the necessary skills (ability to communicate, etc.)?
- ☐ If necessary, is a training plan scheduled for this?
- ☐ Have you established documentation to justify the choice of your DPO (e.g., CV, possible certification, etc.)?
- ☐ Are there plans to communicate internally (employees, employee representative bodies, etc.) on the designation of the DPO?
- ☐ Are the duties and conditions for performing the DPO's duties formalised in a mission statement or service contract?
- ☐ Are there any guarantees in place to ensure the independence of the DPO (not to be sanctioned for the exercise of their DPO duties, not to receive instructions in the context of the performance of their DPO duties)?
- ☐ Is an organisation in place to allow the DPO to report directly to the highest level of the company?
- ☐ Has an assessment of the DPO's workload and material needs (infrastructure, additional staff, etc.) been carried out?
- ☐ Will access to data and processing operations be facilitated? Will the DPO be able to access useful information?
- ☐ Have contact methods allowing data subjects to easily reach the DPO been put in place (dedicated email address, telephone line, etc.)?
- ☐ Is the scope of the DPO's duties defined? (e.g., keeping the record, drafting data processing clauses, etc.)?
- ☐ Have you defined a governance (adequate level of pooling, establishment of intermediaries or points of contact, formalisation of the duties of such intermediaries, etc.)?

Appendix No. 2: mission statement template to be given by the organisation to the DPO when they take up their post

NOTE

This document is a generic mission statement template that an organisation may give to its DPO. It must be adapted to the specifics of the context (legal nature of the organisation, type of activity, profile and positioning of the DPO) within the limits of the role and duties of the DPO specified by the GDPR.

[Name of the organisation] has designated with the CNIL, on [date], Ms/Mr [First name, Last name, title if applicable], as Data Protection Officer (DPO) as defined in Articles 37 et sec. of Regulation (EU) 2016/679 of April 27, 2016 on data protection (GDPR). A receipt for this designation was sent by the CNIL on [date].

As such, Ms/Mr [First name, last name of the DPO] is in charge of ensuring compliance with the principles and obligations in force for all processing of personal data carried out by [Name of the organisation] or on its behalf. In performing their duties, the DPO takes into account the risk associated with processing operations, considering the nature, scope, context and purposes of processing.

As part of their duties as DPO, Ms/Mr [first name, last name of the DPO] reports directly to [the organisation's management body/authority]. They have access to personal data and processing carried out by [Name of the organisation] or on its behalf. They do not receive any instructions with regard to the performance of their duties nor can they be penalised in their career because of those duties.

Other duties and tasks may be assigned to Ms/Mr [First name, last name of the DPO] only insofar as they are not likely to create a conflict of interest or deprive them of the resources necessary to carry out their duties as DPO.

Ms/Mr [First name, last name of the DPO] is subject to a [professional secrecy/non-disclosure] obligation. This obligation should not, however, prevent them from seeking advice, in the performance of their duties, from any competent authority or individual.

Responsible for ensuring that personal data processing operations comply with the provisions relating to the protection of personal data, the DPO's mission is to:

- inform and advise the data controller or the data processor as well as the employees,
- monitor compliance with these regulations and the data protection provisions,
- provide advice upon request with regard to the data protection impact assessment and verify its execution,
- cooperate with the supervisory authority,
- act as a point of contact on matters relating to the processing of personal data.

[Insofar as this does not preclude the performance of the aforementioned duties, the DPO is responsible for the following additional duties, with the assistance of the departments concerned:

- keeping an up to date record of the processing activities carried out by [Name of the organisation] or on its behalf by a data processor,
- participating in carrying out impact assessments,
- participating in making notifications of personal data breaches,
- providing the data controller with a monthly/biannual/annual report on the activities carried out every year.]

In order to allow the accomplishment of these duties, [name of the organisation] undertakes that the DPO will have adequate and sufficient resources. As part of the performance of their duties as DPO, Ms/Mr [first name, last name of the DPO] must:

- access all the information on projects having an impact on the methods of processing personal data from the outset (attendance at cross-functional and business meetings, etc.);
- access the highest management level of the data controller;
- access all the IT systems giving rise to the processing of personal data by the organisation;
- benefit from regular training allowing them to maintain their specialized knowledge in the field of data protection,
- *[have the means to cover the material and human needs necessary for the accomplishment of their duties.]*

A copy of this mission statement will be distributed to [all staff and/or employee representative bodies and/or decision-making bodies of the structure].

[Confirmation of acceptance of this mission statement must be made by post accompanied by a signed copy of this letter.]

Signature of organisation's legal representative **Signature of the DPO**

Appendix No. 3: the DPO designation form

The designation form involves **4 steps:**

- Step 1: information on the organisation designating a DPO;
- Step 2: information on the DPO designated;
- Step 3: public information on the DPO;
- Step 4: summary and sending to the CNIL

The designation form can be completed by the legal representative of the organisation designating the DPO, or by any other person specifically authorised by the legal representative.
Warning: the designation of a DPO has legal consequences. Failure to comply with one of the provisions relating to the DPO is liable to be penalised. It is therefore imperative that the legal representative of the data controller or of the data processor that designates the DPO be informed of the process for designating a DPO for their organisation.

WARNING

The designation of a DPO has legal consequences. Failure to comply with one of the provisions relating to the DPO is liable to be penalised. It is therefore imperative that the legal representative of the data controller or of the data processor that designates the DPO be informed of the process for designating a DPO for their organisation.

Step 1: information on the organisation designating a DPO

OPTION 1: THE ORGANISATION HAS A SIREN NUMBER

Information about your structure is automatically generated from the SIRENE directory of the National Institute for Statistics and Economic Studies (INSEE).

This information cannot be modified on the form. There may be variations in the workforce and the business line, without this having an impact on the designation of the DPO.

In the event of incorrect information (e.g. address), contact the INSEE services or consult its website www.insee.fr (section "register a business, change its situation or declare its cessation").

OPTION 2: THE ORGANISATION DOES NOT HAVE A SIREN NUMBER

Tick the corresponding box.

You must manually fill in the information about the structure designating the DPO.

Note: the "CNIL contact" field: if it is not the legal representative themself, it must be a person in contact with the latter (e.g., assistant, deputy director) that the CNIL can contact if necessary to contact the legal representative.

This "CNIL contact" cannot be the DPO.

Step 2: Information on the DPO designated

OPTION NO. 1: THE DPO DESIGNATED IS A NATURAL PERSON.

OPTION NO. 2: THE DPO DESIGNATED IS A LEGAL ENTITY

- If the organisation has a SIREN number: the information on the organisation is automatically generated from the INSEE SIRENE database (see step 1).
- If the organisation does not have a SIREN number: the information must be entered manually.

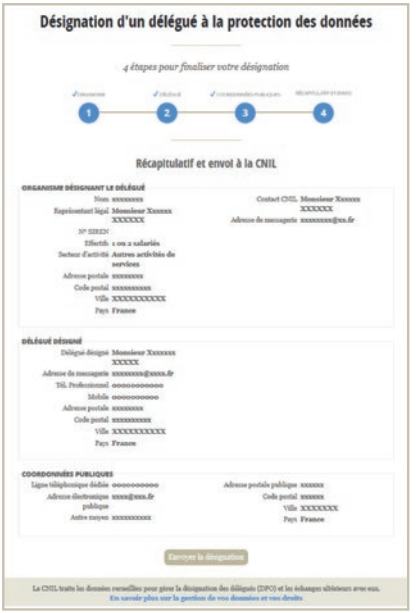
Note: "*Contact details of the individual responsible for the designation*" this refers to the internal natural person who performs the DPO's duties.

Step 3: the DPO's public information

In this step of the form, you are asked to fill in two ways to contact the DPO. One of them must be an email address or an online form.

This information **is made available to the public (open data) from the CNIL website.** Thus, in order to avoid receiving too many requests, it may be preferable to include the URL of an online form as an electronic point of contact.

In any case, these public contact details do not have to be identical to the contact details only accessible to the CNIL.



Step 4: summary and sending to the CNIL

Before validating the designation, remember to check the information provided on the form.

After validation, you can download a summary of the designation in PDF format.

Note: the legal representative of the body designating the DPO, the organisation's contact for the CNIL and the DPO designated will receive a confirmation email.

ATTENTION

it is not necessary to send any additional document to the CNIL (e.g., mission statement, decree, deliberations, etc.).

In the event of an error on the form, you can request its correction by sending an email to the DPO service (whose address appears in the DPO designation confirmation email).

Appendix No. 4: Glossary

DPIA: Data protection impact assessment

API: Application Programming Interface

EDPB: European Data Protection Board

DPO: Data Protection Officer

GDPR: General Data Protection Regulation

CISO: Chief Information Security Officer

Commission nationale
de l'informatique et des libertés
3, place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
Tél. : 01 53 73 22 22

www.cnil.fr
www.educnum.fr
linc.cnil.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

www.cnil.fr