**Charter of Deontology**

**for Data Protection Officers**

*Version 1.0*

[1. Preamble 1](#_Toc527781437)

[2. General Dispositions 2](#_Toc527781438)

[2.1 Definitions 2](#_Toc527781439)

[2.2 Purpose 3](#_Toc527781440)

[2.3 Approval of the Charter 3](#_Toc527781441)

[2.4 Adhering to the Charter – scope 4](#_Toc527781442)

[2.5 Release and application 4](#_Toc527781443)

[2.6 Updating the Charter 5](#_Toc527781444)

[3. The Data Protection Officer profession 5](#_Toc527781445)

[3.1 Definition of the profession 5](#_Toc527781446)

[3.2 Missions of the DPO 5](#_Toc527781447)

[4. The DPO ethics 8](#_Toc527781448)

[4.1 Personal qualities 8](#_Toc527781449)

[4.2 Professional qualities 11](#_Toc527781450)

[4.3 The DPO responsibilities 12](#_Toc527781451)

[4.4 End of mission 12](#_Toc527781452)

[5. The DPO relationship 12](#_Toc527781453)

[5.1 With the data subject 12](#_Toc527781454)

[5.2 With the controller/processor 12](#_Toc527781455)

[5.3 With the hierarchy 13](#_Toc527781456)

[5.4 With data protection authorities 14](#_Toc527781457)

[5.5 With other Data Protection Officers 15](#_Toc527781458)

1. Preamble

Personal data cannot be treated like any other data, and its processing entails a series of obligations.

Data Protection Officers (DPO) play a crucial role in this regard, providing guidance to data processors and controllers in order to make sure that the fundamental rights and liberties of data subjects are protected.

With this important goal in mind, the *Association Française des Correspondants à la protection des Données à caractère Personnel* (AFCDP) drafted this Charter of Deontology (hereinafter: the Charter), which aims to promote a culture of ethics among the DPO designated to one of the European Data Protection Authorities in accordance with the General Data Protection Regulation.

This document comprises of rules of conduct for the actions of the DPO. Thus, the present Charter contributes to the good implementation of Regulation 2016/679 of 27 April 2016 and of the Guidelines on the DPO adopted by the Article 29 Working Party on 5 April 2017 (WP 243), which was endorsed by the European Data Protection Bureau on 5 May 2018.

DPOs create value: they help various kind of organisations, whether public or private, to reach their strategic goals while protecting their intangible assets and ensuring that actions and processes are abiding by relevant regulations on personal data protection.

As a result, it is both relevant and necessary that the profession creates a Charter of Deontology for itself, in order to cultivate the trust between itself and the organisations it serves, and to guarantee the confidentiality, the quality, and the integrity of its work and advices.

The DPO contributes to risk reduction for the data processor. As such, the Charter is also beneficial to data processors and controllers, insofar as it allows them to know what they should expect from their relationship with the DPOs, and also how they should participate in making their mission a success.

By signing this Charter, the Data Protection Officer makes strong commitments. These cannot be achieved without the support of the data processor or controller, hence the requirement for them to sign this Charter as well.

1. General Dispositions
	1. Definitions

*AFCDP: Association Française des Correspondants à la protection des Données à caractère Personnel* (French Organisation of Data Protection Officers)

*Charter of Deontology*: a charter of deontology (hereinafter “Charter”) rules a way of practicing a profession or activity with the goal of abiding by an ethic. It is a set of rights and duties for the practice of a profession, those that exercise it, and the relationship between them and the public. Contrary to a code of deontology, a charter of deontology is not sanctioned by the State. Rather, it is drafted and adopted by the parties that seek to protect the interests of a non-regulated profession.

*Data subject:* a natural person identified or identifiable whose personal data are processed, according to the definitions found in article 4 of the GDPR.

*Data Protection Officer*: a natural or legal person, officially appointed by a data processor or controller to monitor and advise on its compliance with the GDPR and other national and European Union data protection laws, and registered with one of the European Data Protection Authorities, either mandatorily (under article 37 of the GDPR) or voluntarily.

*Data controller*: a natural or legal person that determines the purpose and means of the data processing, according to the definitions found in article 4 of the GDPR.

*European regulation or GDPR*: European Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (hereinafter “GDPR”).

*Prime Contractor*: a natural or legal person receiving support from a professional (this applies specifically to external DPOs). The relationship between those two parties is defined by the provisions governing their civil, administrative, commercial and work relations.

*Processor*: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, according to the definitions found in article 4 of the GDPR.

* 1. Purpose

This Charters aims to provide guidance regarding the conduct and behaviour of data protection officers designated to the national data protection authorities, in accordance with the GDPR.

This Charter may find its place among a set of documents constituting professional standards, including, among other things, good practice guidance stemming from guidelines published by the Article 29 Working Party – including the one on the DPO.

* 1. Approval of the Charter

The Charter is approved by secret ballot by the AFCDP board of administrators upon proposal of the President.

The Charter is made public by all means, including publication on the AFCDP website (www.afcdp.net).

It becomes applicable one month after its publication, even if modified.

* 1. Adhering to the Charter – scope

Accession to the Charter is voluntary, full and *in extenso*, free and does not require the AFCDP membership.

The following categories of people can sign the Charter:

- Internal Data Protection Officers (employee of an organisation);

- External Data Protection Officers (natural person or representative of the designated legal person), acting as a service provider;

- Shared Data Protection Officers (natural person or representative of the designated legal person) appointed by several data processors or controllers.

The loss of the DPO status triggers an automatic removal of the accession to the Charter.

In order to be valid, the Charter must also bear the signature of the data controller or processor and be sent to AFCDP for registration.

DPO (whose appointment has been notified to one of the European Data Protection Authorities) can rely on this charter in their relationship with a data controller, a data processor, internal or external partners of their organisation, the data protection authority, colleagues, as well as data subjects (as defined in article 4 of the GDPR).

Accession to the Charter is made by sending one signed copy to the AFCDP. The copy must be signed by the DPO and the data controller or processor which made this appointment. An online offer available on the AFCDP website makes it possible to materialise this commitment and to communicate the DPO contact details, in order to be informed of the Charter’s evolution. By signing this document, the DPO and the processor/controller commit to abiding by its principles.

This accession can be materialised by the affixing of a specific logo (available to download on the AFCDP website). This logo is the intellectual property of the AFCDP and must not be used in an ostentatious manner, in particular in terms of occurrences and relative size. By no means can the logo be interpreted as proof of quality or a value judgment made by the AFCDP on the professional using it. Every time this logo is used on a website, a link must be made to the page presenting the Charter, so that anyone can know which commitments were made.

For those interested, the list of DPOs who have signed the Charter is available on the AFCDP website (www.afcdp.net).

* 1. Release and application

The Charter can be (among other things):

- brought to the knowledge of data subjects;

- made available to the whole organisation (staff union, employees, etc.);

- put in the annex of the DPO’s employment contract;

- sent to the data protection authority at the time of the nomination of the DPO, including as a guarantee of absence of conflict of interest, of the independence of the DPO, and of the support that he or she will enjoy from the processor;

- used as a reference in the context of initial or continuous training related to personal data protection;

- referenced in contracts made with clients (for external DPOs);

- mentioned by recruiters in job offers for a DPO position;

- used by a processor to prove to a controller that he provides sufficient guarantees (according to article 28 of the GDPR).

* 1. Updating the Charter

This Charter will be revised and updated by AFCDP. Improvements will be made periodically so as to adapt the document to applicable legislation and best professional practices.

These updates will be made public by all means at the discretion of the AFCDP president. They take effect for those concerned, that is to say data protection officers and data controllers and processors who signed it, one month after their publication.

Signatories will be informed of those updates via the contact details that they have communicated during their online registration. By default, and without the parties asking otherwise, signatories are deemed to be maintaining their adhesion to the Charter’s rules. If they do not agree with the update, they have to inform the AFCDP President, and withdraw the logo from their documents.

1. The Data Protection Officer profession
	1. Definition of the profession

In the framework of this Charter, any « professional » natural or legal person whose nomination has been notified to the CNIL *via* the online form, in accordance with the GDPR, is considered a Data Protection Officer.

If the DPO is external, a major part of their professional activity is done in all the domains linked with conformity with regulations on data protection applicable in Europe, and in particular with Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 (GDPR).

This document makes it clear when some rules only apply to a particular category of Data Protection Officers.

* 1. Missions of the DPO

The Data Protection Officer must:

a) Inform and advise the data processor/controller;

b) Advise on and monitor compliance with the GDPR*;*

c) Establish and maintain (or supervise the creation and maintaining of) documentation related to personal data processing (including the register or processing activities), in accordance with the accountability principle[[1]](#footnote-1) and the Article 29 Working Party’s guideline of 5 April 2017 on DPO (endorsed by the EDPB);

d) Analyse, investigate, audit, control;

e) Provide recommendations and warnings, and request arbitration if needs be;

f) Inform and raise awareness of the staff;

g) Present an annual report to their organisation’s legal representative, as indicated in the Article 29 Working Party Guidelines of 5 April 2017 on the DPO (WP 243) endorsed by the EDPB;

h) Be the point of contact for data subjects.

*3.2.1 To take part in the conformity of the processing and to ensure independently its compliance*

The DPO must make sure that all the processing activities put in place by the data controller or processor are compliant with the GDPR and all the other legal texts related to personal data protectionin France.

To this end, they can make all the necessary recommendations to the data controller/processor as long as the all the conditions for the lawfulness of the processing are not met.

*3.2.2 To establish and maintain the list of processing activities (“records of processing activities”)*

The DPO can handle the documentation that the data controller/processor has the obligation to establish, according to article 30 of the GDPR, and, in particular, list the personal data processing, as is indicated by the Article 29 Working Party guidelines on the DPO of 5 April 2017 (WP 243).

*3.2.3 Analysing, investigating, auditing, controlling*

The DPO leads or supervises, in an independent and controlled manner, any action allowing to judge the state of the organisation's conformity, and to pinpoint the non-compliant processes and items (their seriousness, their possible impacts for data subjects, their origin and its responsibility, etc.).

To fulfil these tasks, the DPO has the data controller / processor communicate to them all necessary information, and is granted all the necessary means and resources.

The Data Protection Officer is, among other things, significantly involved in the following subjects: Data Protection Impact Assessment (as required by guidelines (WP 248) on DPIA adopted by the Article 29 Working Party and endorsed by the EDPB), data breaches notification and privacy by design (i.e. taking into account, as the conception goes, how the processing impacts privacy).

*3.2.4 Providing recommendations and warnings*

The DPO advises the data controller/processor and expresses documented and reasoned opinions and recommendations.

They also reply to any query for information or opinion addressed to them. The DPO must be consulted before the implementation of a new processing or the substantial modification of an existing one, and they can make any recommendation to the data controller/processor.

*3.2.5 Informing and raising awareness. Spreading the data protection culture*

The Data Protection Officer:

- makes sure that data subjects are informed of their rights and of any processing made by the organisation involving their personal data;

- heads or supervises actions for the awareness of the direction and colleagues on the rules to be observed with regard to personal data protection;

- presents in a favourable and positive manner the efforts to comply with data protection requirement in a way that builds trust in data subjects and/or differentiate the organisation.

*3.2.6 Preparing the annual report*

The DPO reports on its action every year to the data processor, as provided for by the guidelines on the DPO adopted on 5 April 2017 by the Article 29 Working Party (WP 243). This report shall be a faithful representation of their action throughout the past year, and states the progresses made, as well as the difficulties encountered – if any.

*3.2.7 Being a contact & coordination point*

The DPO receives complaints and demands from natural persons whose personal data are processed by the data controller/processor. The DPO makes sure that their rights are respected.

They treat those demands with impartiality and implement the procedures providing for their fair treatment.

*3.2.8 Giving the alarm if necessary*

The DPO informs without delay the data controller/processor or theprime contractor if staff initiatives or the lack of observance of their recommendations would put at risk the organisation or its leaders.

The professional sees to it that a procedure is implemented in order to inform directly the data controller/processor in case of a significant non-compliance.

*3.2.9 Supporting the controller or processor*

In order to fulfil their missions, a Data Protection Officer must:

- be informed upstream of any project involving personal data, so that they are able to analyse the compliance of the project and give advice. They shall be consulted at each stage of those projects;

- see their detailed and informed recommendations be taken into account. If this was not the case, the reasons for it shall be documented;

- be able to lead or to head, any action allowing to judge the degree of compliance of the organisation, and to objectivise non-compliances (seriousness, possible impacts on data subjects, origin, responsibility, etc.). To complete these tasks, the DPO have the data controller/processor communicate to them all the information necessary to maintain the registry of processing/category of processing or make sure that this registry is maintained in compliance with Article 30 of the GDPR;

- be consulted prior to any data protection impact assessment and be able to verify it – or make it. If necessary, they must be able to recommend the carrying out of an analysis;

- be closely involved in all things related to notification of data breaches (preparation, analysis of incidents and decision to inform the data protection authority and data subjects, *ex-post* analysis, calling into question previous measures to secure data, etc.).

*3.2.10 Reaching the DPO*

The Data Protection Officer must be reachable easily and directly, whether it is by a person inside their organisation, or by an external person. To this end, their contact details (such as: postal address, telephone number, dedicated email address) will be communicated by all appropriate means (intranet, extranet, or institutional website, for instance). The DPO and the data controller/processor can also decide to publicise similarly the name of the Officer, as provided for by the guidelines on DPOs adopted by the Article 29 Working Party on April 5, 2017 (WP 243) endorsed by the EDPB.

If the DPO is shared between several organisations, they must be easily reachable from each place of business, whether it is by data subjects or data protection authorities, and also by each organisation for which they act as a DPO. Thus, they must make sure that their contact details are shared appropriately.

If the DPO acts in several countries, they must be able to communicate with data subjects and to cooperate with data protection authorities in their languages.

1. The DPO ethics

Data Protection Officers acceding to the Charter must:

- behave with honesty, precision, equity and independence;

- provide only the professional services for which they have a full implementation capacity, inform appropriately data controllers/processors of the nature of the missions and services they provide (including any concerns or potential risks they meet);

- treat confidentially any information they encounter during their work;

- prioritise, in all their action and considerations, the protection of data subjects’ personal data.

* 1. Personal qualities

*4.1.1 Probity*

Data Protection Officers act at all times diligently, loyally, responsibly, honestly, according to their knowledge and their expertise, in the service of the data controller/processor or of the prime contractor for whom they work.

As a result, Data Protection Officers cannot use illicit or unethical means while carrying out their mission.

External Data Protection Officers are particularly careful about the use of names, brands or resource material from organisations for which they have worked, in the making of business references, and make sure to obtain, before any use, a clear authorisation from the prime contractor**.**

*4.1.2 Impartiality*

Impartiality entails the following elements: objectivity, independence, neutrality, equity, balance in judgments, absence of conflict of interests, absence of prejudices, and resistance to abusive influence.

*Objectivity*

Data Protection Officers acceding to the Charter:

- show a high level of objectivity in their analysis, their evaluation, and their communications with data processors or prime contractor on the subject of the organisation's compliance;

- carry out their task impartially, i.e. fairly and without prejudice for or against a party in all their actions;

- make a fair evaluation of information and documentation they have received, and make their judgment uninfluenced by their interests or those of others.

*Independence*

Data controllers/processors must define and publicise means to guarantee the independence of the Data Protection Officer. They must abstain from interfering and must put the DPO in a situation where they are guaranteed their independence, including with regard to the means they have access to.

Consequently, the Data Protection Officer can interact directly and in all independence with the higher rank of the direction and with the data controller/processor or their representative, in accordance with article 38 of the GDPR.

The DPO is not accountable to their hierarchical superiors in the exercise of their mission. They have the full control of the decisions they take, and how they organise themselves for their mission.

They act independently, do not receive instruction in the line of duty and make decisions relating to it on their own. This freedom does not mean that they act alone or without consultation.

They are free to consult the data protection authority within the limits of their office and missions.

In the case of part-time data protection officers, data controllers/processors will:

- limit other tasks for which the DPO are responsible in their other missions;

- make sure that the data protection officer are not prejudiced by the carrying out of their other missions during the annual assessment of his/her work (for human resources purpose);- ensure that, once the DPO’s mission is finished, they are able to pursue in their organisation at least the career they would have had, had they not became DPO.

Similarly, in the case of an external Data Protection Officers, the data controller/processor must abstain from interfering, especially while the renewal of the DPO’s contract is at stake. Data controllers/processors which have chosen an external Data Protection Officer will favour a long mission duration, which is fit for the DPO independence.

*Absence and avoidance of conflicts of interests*

Besides avoiding conflicts of interests as defined by article 38.6 of the GDPR, the Data Protection Officer must ensure that they avoid conflicts of responsibility in their missions.

If the Data Protection Officer does not undertake this mission full-time, their other tasks and responsibilities must not lead them to take decisions on data processing activities put in place by their organisation.

Moreover, the Data Protection Officer:

- cannot work for more than one client in the same legal matter if there is a conflict (or serious risk of conflict) of interests between the clients or representatives;

- do not carry on their mission if a conflict of interests arises, if professional secrecy is at risk or their independence cannot be fully guaranteed;

- cannot accept a mission proposed by a new client when information provided by a previous client is put at risk or the knowledge of this information favours the new client;

- has to inform the data controller/processor or prime contractorof all interests that might influence their judgment or compromise the equity that they must demonstrate.

External Data Protection Officers will, with all due transparency, evaluate with data controllers/processors if they can be employed by another organisation that could be seen as a “competitor”.

*Resisting abusive influences and prejudices*

Data Protection Officers are aware of other parties that may try to influence them, their analyses and opinions. The principle of objectivity entails that they will not compromise their judgment on the ground of prejudices, conflict of interests or other undue influences.

*4.1.3 Social skills*

The Data Protection Officer will make sure of gaining, developing and maintaining skills related to communication, negotiation and conflict management.

* 1. Professional qualities

*4.2.1 Professional secrecy*

The Data Protection Officer is bound by professional secrecy, as foreseen in article 8.5 of the GDPR.

Except for cases provided for by law, the professionals treat information, processes, uses, complaints and litigations that they encounter during their work as strictly confidential information.

They shall not use internal documents or information acquired during their mission from a prior data controller/processor or prime contractor without their express consent. Likewise, they will not use information for other purposes than those defined by the prime contractor.

This confidentiality also applies in the social environment of the Data Protection Officer and goes on after the end of their mission.

*4.2.2 Dedication*

A Data Protection Officer acceding to the Charter:

- shows their competencies and professionalism in the carrying out of their missions. They act with caution and take informed decisions in all the situations encountered;

- found their judgment on expertise and experience.

*4.2.3 Skills, Knowledge, Know-how and good conduct*

The Data Protection Officer must have the adequate knowledge, skills and experiences to carry out their mission and professional activities. When applying for a job opportunity or a mission as a DPO, the professional shall not claim to have a skill they do not possess.

The GDPR states that the Data Protection Officer is a person with the qualifications needed for carrying out the mission. When the DPO is a legal person, this condition must be met by the professional designated by it to complete the mission.

The skills must concern IT and new technologies as well as Regulations on the protection of personal data. They must also be relevant to the Industry concerned.

When the Data Protection Officer does not meet all the skill requirements at the time of appointment, they must acquire them before taking office.

The Data Protection Officer have to maintain their skills and knowledge in the area relevant to their missions, and must take care of improving and expanding constantly their legal, technological and societal watch, including by a continuing education if needs be. As required by article 38.2 of the GDPR, the data controller/processor must support them in this effort.

* 1. The DPO responsibilities

In regard to the necessary independence and the absence of conflict of interests that the Data Protection Officer must have, the data processor/controller cannot delegate its power on personal data protection to the DPO.

Moreover, the Data Protection Officer cannot be penalised or relieved of their duty by the data controller/processor on the ground of the exercise of their mission.

Like any employee or service provider, the Data Protection Officer may see their civil liability, if any, and their criminal liability engaged under local law.

The DPO will take out a professional indemnity insurance covering all the risks linked with their activity.

* 1. End of mission

At the end of the mission, the Data Protection Officer commits to:

- provide all the documents concerning the mission to the data processor/controller;

- in the time that they can give to this task, to inform their replacement on on-going proceedings (for an external DPO, this can be subject to billing if it was not included in the mission).

The data controller/processor will make sure that the internal DPO carry on a normal career in the organisation.

When the Data Protection Officers remains an employee of the organisation after the end of this mission, the data controller/processor must ensure that the progress of their career is not impeded by the fact that they were Data Protection Officer.

1. The DPO relationship
	1. With the data subject

The Data Protection Officer gives priority to the minimisation of risks for data subjects.

In all their relations with data subjects, the Data Protection Officer acts in an appropriate and respectful manner.

* 1. With the controller/processor

The relationship between the Data Protection Officer and the data controller/processor is based on trust and frankness and demands that the professional’s endeavour is honest, loyal and diligent.

This entails that the Data Protection Officer:

1. accept a nomination as a DPO only if they deem themselves competent for the task, which means that they have the knowledge and resources necessary to hold office in the best conditions possible. In cases where they perceive a deficiency, the DPO commits to ask the data controller/processor for adequate resources and to gain the required knowledge before taking office;

2. have an easy and unconditional access to the data controller/processor or their direct delegate and reports to the highest level of management;

3. are provided by the data controller/processor the adequate means and resources for the proper carrying out of their tasks and will notify clearly and without delay any deficiency in this regard (including but not limited to);

a. Information and documentation which are sufficient, relevant, and reliable, so that they can base their advice, conclusions and recommendations on them;

b. easy access to interlocutors having the required skills and authority in the organisation;

c. help, formation, tools and budget;

d. reduction of their other tasks.

4. head the production and enforcement of policies, guidelines, processes and rules of control for an efficient personal data protection and protection of data subjects’ fundamental rights by the data controller/processor;

5. bring to the attention of the data controller/processor, in the framework of their missions and activities, their evaluation of the organisation's level of compliance. If they are aware of a non-compliance, they will make sure to notify the data controller/processor;

6. report to the data controller/processor on their mission, on non-conformity and potential risks, and proposes judicial, organisational, or technical measures to bring the organisation into conformity and mitigate or cancel risks;

7. commit to using the data controller/processor’s information and documentation confidentially, to make sure to securely keep them, and not to use them or store them outside of their mandate.

The Data Protection Officers cannot act alone. They must develop networks inside the organisation for which they ensure compliance and develop synergies with the information systems security managers, the information systems management, the legal department, the operational units, etc.

* 1. With the hierarchy

The relationship between the external Data Protection Officer and the prime contractor is based on trust and frankness and demands that the professional’s endeavour is honest, loyal and diligent.

This entails that the DPO:

1. will not contact potential clients through processes or means contradicting the trade’s dignity or affecting its image;

2. will make sure that contracts signed with theprime contractor define precisely the conditions and means of the delivery. In particular, they are mindful that the contract includes the requirements found in article 28 of the GDPR;

3. will refrain from giving their potential clients false indication regarding their capability and the human and material means at their disposal (to carry out the mission). They only accept the mission if they consider that they are competent for it, which means that they have the appropriate knowledge and resources in order to carry out the mission in the best possible conditions. In the cases where they identify a deficiency, they inform their interlocutor in order to find a way to remedy it, for instance thanks to additional training;

4. has to demand from the prime contractor the adequate and relevant means and resources for the proper carrying out of the mission, and notify clearly and without delay of any deficiency in this regard:

a. Information and documentation which are sufficient, relevant and reliable, so that they can base their advice, conclusions and recommendations on them;

b. easy access to interlocutor having the required skills and authority in the different parts of the organisation.

5. bring to the attention of the data controller/processor, in the framework of their missions and activities, their evaluation of the organisation's level of compliance. If they have the knowledge of a non-compliance, they will make sure of notifying the data controller/processor;

6. reports to the data controller/processor on its mission, on non-conformity and potential risks, and proposes judicial, organisational or technical measures to bring the organisation into conformity and mitigate or cancel the risks;

7. commits to using the prime contractor’s information and documentation confidentially, to make sure to securely keep them, and not to use them or store them outside of their mandate;

8. provides the prime contractor with detailed, transparent and honest invoices, avoiding distortion of amounts, and never tries to fraudulently obtain grants or subsidies;

9. does not keep documents from the prime contractor with the aim to pressure it for bill collection.

* 1. With data protection authorities

The Data Protection Officer shall:

1. reply diligently to queries by any European Data Protection Authority and comply with their summons. their declarations to them will be sincere;
2. maintain a loyal relationship with the data protection authority and its staff;
3. be free to contact independently the data protection authority. However, if they deem it necessary, they will inform the data controller/processor;
4. only communicates what is strictly necessary to the data protection authority about the activities of the data processor/controller;
5. ensure that procedures are put in place allowing them to:
6. be informed of any communication from the DPA to the data controller/processor (claim, request for information, summon, audit of documents, etc.);
7. be informed of any communications from the organisations’ departments to the DPA;
8. loyally collaborate with inspections carried out by the DPA. They make available, respecting legal and regulatory provision on privacy and secrecy, updated documents requested for immediate consultation, or without any undue delay. They facilitate the copy of those documents by the agents and inform the data controller/processor.
	1. With other Data Protection Officers

The relationship between Data Protection Officers is governed by this Charter.

The professionals shall, among other things:

1. create contacts with their fellow DPOs to favour exchanges of experiences and the sharing of good practices;
2. maintain relationships based on mutual respect and fellowship. In this spirit, they seek the amicable settlement of any dispute;
3. do not discredit or denigrate the occupation, this Charter, or their colleagues;
4. ensure the respect of loyal competition. They refrain from unfair competition or smear campaigns aiming to harm a peer or take their place in one of their mission;
5. act for the general interest of the profession, and in particular of its public recognition;
6. get involved in the transmission of their expertise to interns or apprentices that they may have;
7. do not accept from the data controller/processor working conditions unfit for the profession or the efficiency of a mission. They do not offer or impose such working conditions to themselves, or their principals, or their own colleagues.

Signed by the Data Protection Officer and the data controller or data processor.

 Yes, I (as Data Protection Officer) accept that my commitment to the "AFCDP Charter of Deontology for Data Protection Officers » is mentioned on the AFCDP website ([www.afcdp.net](http://www.afcdp.net/)). The website will only display my name, the organisation for which I am designated, the country and the date of signature.

*Personal data collected in this document are processed for the purpose of managing commitments to this Charter. They are kept for as long as is necessary for this goal. You have a right to access, modify or suppress the data, as well as a right to opposition or limitation of the processing. These rights may be exercised via a signed letter accompanied by a copy of a signed identity document sent to " AFCDP– 1, rue de Stockholm 75008 PARIS, FRANCE ".*

|  |  |  |
| --- | --- | --- |
|  | The Data Protection Officer | The Data Controller / Processor |
| Date |  |  |
| Signature(and stamp of the organisation) |  |  |
| Surname & First name |  |  |
| Email address |  |  |
| Address and Country |  |  |

*Then to be sent by email to* *back-office@afcdp.net*

1. The accountability principle entails the mandatory establishment by organisations of mechanisms and internal procedures allowing to demonstrate the compliance with rules related to personal data protection [↑](#footnote-ref-1)