Sample Activity Report for the Data Protection Officer, as proposed by the CNIL

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

This document is a report template provided for informational purposes only and is not binding.

You are free to adapt it and structure its content according to the specific needs of your organization. The format—writing style, graphic layout, inclusion of tables, etc.—is up to you.

In your report, you may address the following key topics:

- Strategic issues identified by the DPO regarding data protection

The organization and conditions for performing the role of DPO within the organization

- Compliance measures implemented
- An assessment of the actions taken and the outlook and needs for the coming year

The logo shown is also available in a female version on the CNIL website: https://www.cnil.fr/fr/logo-delegue-la-protection-des-donnees-et-ses-conditions-dutilisation

[Please remember to delete this page once you have reviewed the recommendations]

April 2026 version

Délégué à la protection des données

Activity Report of the Data Protection Officer

[Identity of the DPO and contact information]

[Organization(s) that appointed the DPO]

Publication date (or period covered):

Other authors and contact points:

Document confidentiality/distribution level: e.g., Executive Committee, local government…

Key Points

Objective: to summarize the key information in the activity report

At the beginning of the report, to highlight the essential information, you may include a short summary (1 to 2 pages maximum) covering:

- the strategic issues identified regarding data protection
- key messages and figures to remember and share within the organization
- the major achievements of the year and the main activities on which the DPO has focused
- the main alerts/risks
- outlook for the coming year

This summary can be used for internal communication with business units and senior management.

If possible**, prioritize visual presentations (tables, bar charts, etc.) to highlight the status of compliance, the activities carried out, and your recommendations.**

You may attach relevant documents as appendices (e.g., a summary of a Data Protection Impact Assessment).

The information and figures provided in this report pertain to the selected reporting period (specify whether annual, quarterly, or other).

Organization and conditions for performing the DPO role within the organization

Objective: to clarify the DPO's role within the organization and assess the efforts made to ensure they can best fulfill their duties.

This section of information is relatively stable but must be updated as changes and adjustments are made.

Attach any relevant documents (e.g., terms of reference; procedures regarding the DPO's involvement in identifying processing activities, conducting impact assessments, and managing data breaches; list of the "Data Protection" network of contacts).

For shared DPOs, you can of course adapt the exercise and further summarize the key information for each organization for which you are designated.

The DPO is a key player in personal data protection. Their role encompasses information, advisory, and oversight functions. They serve as the point of contact for individuals and for the CNIL.

The DPO must act independently and enjoy sufficient protection in the performance of their duties. They must be free from conflicts of interest and report directly to the highest level of management. To ensure the effectiveness of their duties, the organization must provide them with the necessary resources to carry out their tasks and facilitate their access to personal data and processing operations.

By coordinating efforts to ensure compliance with data protection rules, the DPO safeguards the organization against increased cyber and legal risks and helps build relationships of trust with employees, customers/citizens, external partners, and others.

For more details, see the Data Protection Officer Guide published by the CNIL.

Appointment of the DPO: date and context

- First appointment for the organization / replacement of a previous DPO (specify date of first appointment)
- Voluntary appointment / mandatory under the GDPR

Scope of the appointment

- Number of entities covered (number of subsidiaries, etc.)
- Number of employees or public officials concerned

Qualifications of the DPO

- Training, professional experience
- Certification of the DPO's competencies, if applicable
- Other professional certifications

Status, role, and position within the organization

- Reiterate the mandatory and necessary nature of the DPO's independence and, if possible, provide examples of its application; measures taken to ensure the DPO's independence
- In-house/external DPO, shared, full-time or part-time (specify the percentage of time allocated and any other role performed, if applicable);
- Content of the terms of reference/job description (objectives, priorities, action plan if applicable) and communication activities carried out by the organization regarding the role
- The DPO's position within the organization (if an in-house DPO). E.g., reporting to the legal department under the general secretariat
- Emphasize the absence of conflicts of interest and, if necessary, the remedial measures taken
- Is it possible to add an organizational chart if one exists?

The DPO's main responsibilities

- Specify how these are carried out in practice to help management understand what is actually done on a day-to-day basis
- Indicate the time spent on each major type of task to understand what is prioritized (or what should be) and/or time-consuming

Resources made available to the DPO

You can present the following here:

- Your team, if applicable
- Your "GDPR" contacts/internal liaisons and other key points of contact (e.g., CISO, archivist, PRADA—person responsible for access to administrative documents) and the procedures for communication
- How you are involved in all matters related to data protection within your organization, for example: regular participation in meetings where strategic projects involving personal data are defined, immediate notification in the event of a data breach, etc.
- The resources at your disposal (e.g., dedicated or available budget, dedicated infrastructure, access to internal communication tools, databases, and the services that manage them; access to continuing education and professional development programs, etc.)

Communication procedures with the organization

- Who is your primary point of contact? (e.g., CEO, COO, Deputy CEO, Executive Committee);
- What are your communication protocols? Type and frequency of communication (e.g., monthly, bi-monthly, quarterly

Cross-functional nature of the DPO role

- Here you can specify which departments you work with and on which projects. The idea here is to highlight the DPO's 360° perspective on data processing and their ability to collaborate (e.g., procurement strategy, archives, cybersecurity, etc.)

- Highlight the networking you do both internally and externally (identified internal contacts and how they work; specify if you are part of a network of DPOs and highlight your contributions within that network…)

Compliance actions carried out

Objective: to present the various actions carried out with departments, external partners, and, where applicable, the CNIL.

Numerous activities should be included in this section of the report (awareness-raising, supporting departments on projects involving the use of personal data, etc.).

As much as possible: provide details on the time spent by activity category; present this information in a visual and graphical format (tables, etc.); you may include a summary highlighting the main actions taken and key projects with key figures: this allows decision-makers to access key information by section.

Organization of awareness-raising and training initiatives (by the DPO or at their initiative)

Have you organized awareness-raising and/or training initiatives? YES / NO

If applicable:

- Specify the activities carried out with departments, the number of sessions organized, and the approximate number of people reached/trained (e.g., organizing information sessions, sending data protection news/updates via email, providing resources, etc.)
- Specify the actions carried out with decision-making bodies (e.g., presentations to the Executive Committee)

Implementation of procedures and document templates for compliance management

Do you have procedures in place and document templates available to manage your organization's compliance? YES / NO

- List the governance documents developed or updated, e.g., *privacy policy, information system security policy, IT charter, new employee orientation booklet, etc*.

- List existing internal procedures (or those currently being developed) If the document is currently being developed/updated, specify—if possible—the date by which it is expected to be finalized.
    - Consultation with the DPO and their internal contacts
    - Maintenance of the record of processing activities
    - handling requests to exercise rights,
    - Management of personal data breaches,
    - handling CNIL audits,
    - other.

- List the compliance document templates (contractual clauses, privacy notices, AIPDs, etc.) that are currently in use or under development. If the document is currently being developed or updated, specify the expected date of completion.

Presentation of the progress status of the processing register

Indicate the status of the processing activities register:

- Is the processing register complete? How often are the entries in the register updated?
- Which business units were involved in completing or updating the register?
- What are the next steps regarding the register?

Main topics on which you have been consulted

If applicable, in addition to quantitative information, the following table can be used to highlight the main topics addressed (e.g., sensitive processing, etc.).

Department(s) involved	**Processing**	**GDPR issue**	**DPO's opinion** (may refer to an attached document)

Focus on the DPIA(s) conducted

List the data protection impact assessments (DPIAs) that have been conducted and the main measures taken or to be taken for processing operations likely to result in high risks to the rights and freedoms of individuals

Focus on the audits conducted and the corrective actions taken

Department(s) involved	**Process(es)**	**Scope of the audit**	**Number of anomalies identified during the audits**	**Corrective measures taken**	**Comments from the DPO** (may refer to an attached document)

Examples of corrective measures

- Addition of new information notices for data subjects
- Measures taken to facilitate the exercise of rights and ensure compliance with request processing deadlines
- Deletion of data retained for an excessive period
- Strengthening of certain physical, logical, and/or organizational security measures
- Revisions to contractual frameworks (e.g., inclusion of required clauses in the event of subcontracting, signing of the European Commission's standard contractual clauses governing data transfers outside the EU)
- Updating the processing register based on findings (creation/deletion of processing operations or changes to their implementation conditions, e.g., exclusion of a data category, reduction of retention periods)

Requests from external entities regarding personal data protection (e.g., business partners, authorized third parties, etc.)

The objective is to keep a record of new requests and the responses provided in order to maintain a history for reference.

Regulation of data transfers outside the European Union

In particular, standard contractual clauses, BCRs, and certifications

Management of personal data security

What cyber threats have been identified? Which ones had to be addressed? What is the collaboration between the security officer and the DPO?

Provide a summary here and feel free to consult the organization's CISO.

You may include, if available, the contents of the breach register.

Management of personal data breaches

- Is there a data breach management policy and standard documents?
- What is the decision-making and information-sharing process internally (particularly collaboration between the CISO and the DPO) and externally (liaison with processors and competent authorities) for managing data breaches?
- Is the process to follow in the event of a breach clear, well-known, up-to-date, and effective? How is the DPO involved?
- Indicate the number of data breaches and whether this number is increasing or decreasing compared to the previous period.
- For each breach, indicate its nature, the number of individuals affected, the identified risks, and the measures taken.

- Specify whether a notification was made to the CNIL and whether the affected individuals were informed.
- What improvement measures have been taken or are being considered?

You can use this table to summarize the various data breach incidents

Date the DPO became aware of the breach	**Nature of the breach**	**Level of risk to the rights and freedoms of the data subjects**	**Number of data subjects**	**Notification to the CNIL**	**Date of notification to the CNIL**	**Notification of data subjects** (date, method of communication, number of individuals informed)	**Measures taken**
		HIGH/MEDIUM/ LOW/NONE		YES / NOT AFFECTED			

Handling of requests to exercise data protection rights and complaints investigated by the CNIL

- Is there a procedure for managing requests to exercise rights? And for managing complaints?
- If so, what is the decision-making and information-sharing process?
- Is the procedure clear, well-known, and effective? Indicate the number of requests to exercise rights and whether this number is increasing or decreasing compared to the previous period.
- Do you handle a large number of complaints?
- Is the subject of these complaints always the same?
- Please describe the measures taken to respect individuals' rights and reduce the number of complaints received
- Feel free to describe any complex cases encountered that warrant being included and retained in the report

You may use this table to summarize the various requests to exercise rights

Type of right	Measures taken to facilitate the exercise of these rights	Number of requests received	In connection with which processing activity(ies)?	Action taken	Processing time
Right of access				Granted in X% of cases Denied in X% of cases for such-and-such a reason	
Right to rectification					
Right to erasure					
Right to object					
Right to data portability					
Right to restriction					

You can use this table to summarize the different types of complaints

Date of the complaint	Subject	Subject	Internal follow-up	Measures taken by the CNIL

Tracking of operations related to a CNIL audit, a formal notice, a sanction procedure, or other corrective measures

You can use this table to summarize information related to a CNIL inspection or sanction

Date	Event (CNIL intervention)	Engagement of a law firm	Documents to be provided	Deadlines	Internal follow-up	Outcome
		YES/NO				

Evaluation, outlook, and needs for the coming year

Objectives:

- Assess the organization's maturity in data protection
- List upcoming priority projects, strategic objectives, and the resources needed to achieve them.

To conduct a comprehensive assessment, feel free to use the tool provided by the CNIL to measure the evolution of the organization's maturity level in data protection management (it is up to you to determine how often it would be appropriate to update your organization's maturity assessment)

This section may be particularly useful for raising awareness among management and your colleagues

Points of satisfaction regarding the planned objectives

What are the main successes you identify in terms of data protection? Were the set objectives achieved? If not, why? If so, what were the factors contributing to success? How do these elements build on the previous year? What connections exist between the actions taken and current developments in data protection (work by the CNIL, legal changes, etc.)?

Examples of points to highlight: improved organizational maturity regarding the legal framework for outsourced operations; greater staff involvement in data protection management due to an increase in the number of cases referred to the DPO.

General and specific points of attention regarding processing compliance

What are the main compliance risks identified by the DPO? Have these alerts been shared and addressed? What actions are planned to address them?

Examples of items to note: an increase in data breaches indicating the need to strengthen technical and/or organizational security measures; a general issue regarding the management of retention periods; failure to conduct a PIA for certain processing operations.

Proposals for improvement regarding the performance of the DPO's duties and the organizational measures taken to ensure the organization's compliance

To be completed

Include the proposed roadmap for the coming year

What are the objectives for the coming year? What actions will need to be implemented to achieve these objectives? Which projects should be prioritized, and what new projects will be undertaken in light of your organization's priorities (strategic plan, annual objectives, integration of a new department or information system, etc.)? What are the main themes and processing activities you will be working on?

Examples of items to include: prioritizing the topics of "individual rights," "security," and "retention periods" in overall compliance management; strengthening awareness campaigns and audits; conducting data protection impact assessments (DPIAs) for specific processing operations, etc.

Detail the resources required

What resources (human, technical, financial) are required to implement the roadmap for the coming year?

Examples of items to include: budget, training, appointment of a deputy and/or points of contact, increased working hours or use of ad hoc services, membership in a professional association for data protection, etc.

Appendices

If necessary.

Additional information may be included in the appendices to the activity report to clarify certain sections of the report.