Europäisches Patentamt
European Patent Office
Office européen des brevets

Data Protection Office

# Data Protection Oversight

## How the Data Protection Office conducts DP Audits and DP Inspections

# Data Protection Oversight

## 1. Background

The Data Protection Rules (DPR) foresee under Article 43(1)(d) the possibility for the Data Protection Officer to carry out data protection audits (DP Audits) and investigations (conducted in the form of DP Inspections or Ad hoc Queries).

## 2. Terminology and Definitions

In addition to the definitions included in the DPR, the below terminology is used in this document:

(a) **Auditee(s)**: is (are) the organisational unit(s) determining the purposes and the means of the processing operation(s) that is (are) being audited. In this context, Auditee(s) are the Delegated Controller(s) and the staff appointed by the Delegated Controller(s) that serve as focal point in ensuring that appropriate evidence is made available to the Audit Team to allow assessment of the compliance with the DPR.

(b) **Personal Data Breach**: a security incident involving personal data that compromises the confidentiality, integrity or availability of the personal data involved, such as the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data stored, transmitted, or otherwise processed.

(c) **Infringement of rights**: an Infringement of data protection rights of a data subject can occur, *inter alia*, following a Personal Data Breach or an Incompliance with the DPR, such as unlawful processing.

(d) **Irregularity**: occurs when a processing operation or aspects thereof are likely to violate the DPR, but the actual violation of the DPR has not materialised. If not addressed, the Irregularity may lead to an Incompliance.

(e) **Incompliance with the DPR**: a violation of the DPR (for example, the processing of personal data is occurring in the complete absence of information to the data subjects).

(f) **Findings**: information discovered as the result of a DP Inspection. The Findings are provided to the Delegated Controller for comments. The DPO may amend the Findings upon the comments received by the Delegated Controller.

(g) **Conclusions**: legal analysis by the DPO resulting in an interpretation of the Findings in the light of the applicable rules. When Incompliances are found, the Conclusions and the Recommendations are submitted to the DPB for validation.

(h) **Recommendations**: based on the Conclusions, Recommendations for preventive, mitigating or corrective measures are provided to the Controller to prevent, mitigate and/or correct an Irregularity or Incompliance. The DPO may recommend, i.a. (i) that the Delegated Controllers bring their processing operations in compliance with the DPR; (ii) that the Delegated Controllers comply with data subjects' requests to exercise their rights under the DPR (iii) that the Delegated Controllers communicate a personal data breach to the data subject(s), (iv) that a particular data processing operation is suspended; or (v) that the data flow to specific recipients is suspended.

(i) **Data Protection (DP) Audit Report**: based on the DP Audit process, the DP Audit Report summarises the Findings, Conclusions and Recommendations in a written document.

(j) **Data Protection (DP) Compliance Report**: based on the DP Inspection process, the DP Compliance Report summarises the Findings, Conclusions, and Recommendations in a written document.

# 1) Data Protection Audits

## 1. Background

The DPO conducts DP Audits in accordance with Article 43(1)(d) Data Protection Rules (DPR).

The performance of DP Audits is beneficial for:

- monitoring the documentary and implementary compliance with the DPR
- identifying data protection risks and detecting areas to be improved, thus enabling the Office to address the risks with specific technical and organisational measures
- raising awareness and knowledge on data protection, general information security and cyber security
- demonstrating the Office's commitment to the importance of data protection and individual rights
- independently assuring the data protection practices and procedures established in the records and privacy statements
- highlighting Office best practices that can be extended to other areas for continuous improvement

## 2. Transparency and co-operation

(1) The DP Audit methodology is based on the principles of clarity, transparency, and cooperation.

(2) The scope of each DP Audit will be communicated to the responsible Delegated Controller in advance and may take into account any data protection issues or risks which are specific to the Office, the organisational unit, and/or identified by the DPO.

(3) The methodology will be explained to the persons participating to the DP Audit before the interviews.

(4) Risks will be evaluated on the basis of an objective assessment of the impact/risk of the processing operation on the rights and freedoms of data subjects by virtue of their nature, scope, context, and purposes.

(5) If the circumstances so require, the DPO may request other units to assist or assign external experts to assist in or to carry out the DP Audit in part or in full, for example when specific expertise (e.g. IT security) is needed.

(6) The draft report will be shared with the Auditee(s) with the aim of reconciliating the results, clarifying concepts and filling any gaps.

(7) The final DP Audit Report will be shared with the Delegated Controller and with the President (or the President of the Boards of Appeal, where applicable) as the Controller.

(8) After every DP Audit, the DPB is informed by the DPO on the outcome and can then request to see the DP Audit Report.

(9) The DPB can comment or request a supplementary investigation on an issue emerged during a DP Audit, for example an Irregularity.

(10) Information on the DP Audits performed during the relevant year is submitted to the President, the President of the Boards of Appeal, the DPB, and the Administrative Council yearly, as a part of the DPO Annual Report.

## 3. Annual DP Audit Plan

(1) The DPO, in consultation with the DPB, prepares an **Annual DP Audit Plan** and submits the same to the President for approval. The approved Annual DP Audit Plan is submitted to the DPB for information. The DPB can, at any time, formulate suggestions on areas on which the Office should perform a DP Audit. In case the processing activities to be audited are under the responsibility of the Boards of Appeal as Controller, the draft Annual DP Audit Plan is also submitted to the President of the Boards of Appeal.

(2) In the planning of the DP Audits, priority shall be given to processing activities constituting high risks to freedoms and rights of data subjects.

(3) The Delegated Controller(s) will be informed of their specific audit only.

## 4. Phases of the DP Audit procedure

(1) **Communication to organisational unit** will occur with the notification of the imminent DP Audit to the Delegated Controller, including information on the methodology prior to the planned commencement of the DP Audit.

(2) **Opening Meeting**, marking the commencement of the DP Audit, will take place with all parties involved. This meeting will provide an opportunity to discuss the scope of the DP Audit, identify the Interviewees, and answer any questions that the Auditee(s) may have about the process.

(3) **Preliminary self-evaluation of the Delegated Controller** and transmission of all relevant documentation: after the Opening Meeting, the DPO will provide to the Auditee a standard catalogue of questions to answer on the processing operations that are to be audited (self-evaluation questionnaire) and indicate what further documentation should be provided by the Auditee such as data protection records, data protection statements, policies, procedures, guidelines, work instructions and all relevant documentation linked to the processing of personal data within the scope of the DP Audit (audit documentation) to the DPO for review.

(4) **Analysis of the preliminary self-evaluation questionnaire and audit documentation**. The DPO analyses the preliminary self-evaluation questionnaire and prepares a list of topics on which clarification is needed.

(5) **Meetings/interviews with staff selected by the Delegated Controller (including DPL)**, aimed i.a. at collecting information about how data processing and checking the measures it has in place, can take place on site or remotely. With a view to allow the Audit Team to obtain sufficient, reliable, relevant and useful audit reference to achieve the DP Audit's objectives, in selecting the staff members to interview, the DP Auditors may use the criteria of representative sampling or random sampling, as the techniques to help ensure that the data collected for the DP Audit is enough and free of bias.[1]

[1] A representative sample is a group or set chosen from a larger statistical population according to specified characteristics. A random sample is a group or set chosen in a random manner from a larger population.

(6) **DP Audit Report**. the DPO drafts a DP Audit Report on the basis of the documentation reviewed, the answers and clarifications provided by the Auditee(s) and the preliminary self-evaluation questionnaire. The DP Audit Report shall include:

(a) **Findings**.

(b) **Conclusions**, which may reflect the following:

(i) No Incompliances nor Irregularities were found.

(ii) *Compliant with Suggestions for Improvement:* the audited processing was found overall compliant, but some aspects could be improved.

(iii) *Irregularity*

(iv) *Incompliance*

(v) *Noteworthy Effort (best practice):* any aspects of the processing that constitute best practice and could be applied in other processing operations.

(c) **Recommendations (preventive, mitigating or corrective measures)**

(7) **Reconciliation**. the DPO will send the draft DP Audit Report to the Delegated Controller for comments for ensuring that the draft report accurately reflects the evidence collected and the findings.

(8) **Closure Meeting** will take place to clarify any outstanding issues on the DP Audit Report. After correction of any inaccuracies where needed, the DP Audit Report is resubmitted to the Delegated Controller for final comments, if any. Comments, if any, by the Delegated Controller will be attached to the DP Audit Report.

(9) **Submission of the DP Audit report to the President** (and the President of the Boards of Appeal in case they are the Controller). The DP Audit Report is always submitted to the President for information. In case Irregularities are found, the DP Audit Report is also submitted to the Controller for endorsement of the Recommendations and/or Suggestions for Improvement.

(10) **Submission of the DP Audit Report to the DPB**. In case the DPO assesses an Incompliance with the DPR, the DP Audit Report is submitted to the DPB for validation of the Conclusions and Recommendations. Upon validation by the DPB of the DPO Conclusions and Recommendations, the latter become binding and are submitted to the Controller for implementation. In case of disagreement by the DPB with the Conclusions and/or Recommendations formulated by the DPO, the DPB submits its comments in writing to the DPO, which amends the Conclusions or Recommendations accordingly. The DPO may engage in a follow-up audit or an extension of the DP Audit if the consultation with the DPB highlights elements that need further clarification.

(11) **Remedial Measures and Implementation Plan**. the Delegated Controller formulates a plan with remedial measures for implementation of the Recommendations which have been endorsed by the President or by the DPB.

## 5. DP Audit Follow up

(1) The DPO shall verify that the remedial measures have been implemented (normally after 6 months, variable on the basis of the timeline to implement the identified remedial measures).

(2) An annual report will be sent to the President for information regarding the status of the implementation of the DPO's Recommendations.

# 2) Data Protection Inspections

## 1. Background

In accordance with Article 43(2) Data Protection Rules (DPR), the Data Protection Office (DPO) can examine data protection compliance issues related to one processing operation or a group of processing operations that have come to its attention by way of information received from data subjects, third parties (stakeholders and partners, processors, press releases) or any body under the legal provisions of the Organisation, or motu proprio on a risk-based-approach, for example, in case there are repetitive or serious complaints received with regard to a certain processing operation, or the introduction of new systems or technological solutions.

## 2. Investigative activities

The DPO investigative activities on the compliance with the DPR can be conducted in the form of:

a) **DP Inspections** triggered by a specific request/mandate of the Office, e.g. by the President, the President of Boards of Appeal, a Delegated Controller, or an EPO statutory body, including DPB, or initiated *motu proprio* by the DPO on the basis of e.g. repetitive complaints related to a certain processing operation or other justifying occurrences under a risk-based approach.

b) **Ad-hoc DP Compliance Queries (Ad-hoc queries)** for the assessment of specific occurrences, procedures and practices, which may become necessary in order to analyse and respond to internal and external consultations, or other types of requests that cannot be channelled through the legal redress mechanisms, e.g. because they do not impact directly the rights of the complainant.

## 3. Scope of DP Inspections

(1) The DPO will only make use of its investigative powers if it concerns a real or potential, thus not hypothetical, Incompliance with the DPR of a processing operation. The DPO shall decide on the relevance and how to examine a processing operation by means of a DP Inspection, based on a risk analysis (necessity and proportionality), considering i.a.:

a. the nature and gravity of the alleged Incompliance(s) with the DPR;
b. the severity of the damage that one or more data subjects have or may have suffered as result of the Irregularities or Incompliances;
c. the potential overall severity of the case, also in relation to other factors;
d. in the case of potential Incompliances, the likelihood of them having occurred;
e. the date on which the relevant events occurred and whether and when the conduct in question stopped generating effects, the effects were removed or an appropriate guarantee of such a removal is identifiable or was already evidenced e.g., the unlawful processing has ended.

(2) The DPO in a DP Inspection examines the compliance of a certain processing operation (or of aspects thereof) and seeks to prevent, alleviate or correct potential data protection Irregularities or Incompliances and to mitigate risks to the rights and freedoms of individuals and for the Organisation, and therefore does not assess individual responsibilities. Consequently, if an Irregularity or Incompliance is found in a processing operation, the accountability is first and foremost institutional and the responsibility to implement preventive,

mitigating or corrective measures lies with the Delegated Controller, and ultimately with the Controller.

## 4. DP Inspections Procedure

(1) **Initiation of a DP Inspection**. The DPO is formally mandated by the President, a Delegated Controller, or a statutory body to look into matters of suspected DP Irregularity or Incompliance or starts a DP Inspection *motu proprio*, on its own initiative.

(2) **Fact-finding activity**. DP Inspection activities may comprise, depending on the complexity of the case and in accordance with Article 46 DPR:

(a) Requesting (documentary and testimonial) information from the responsible Delegated Controller or any other relevant Delegated Controller (and/or processors).

(b) Obtaining access, if necessary, to all personal data processed by the Delegated Controller (including access to any data processing equipment and means of processing).

(c) Organising on-site or remote interviews when it is necessary to gain practical knowledge about how data processing is done by the Delegated Controller or to check the measures that are put in place. The scope of the interviews is defined by the DPO on a case-by-case basis and the interviewees are informed of the interviews with a notification. Following the interviews, the DPO will send a summary of the discussion to the interviewee.

(3) **DP Compliance Report**. The results of the investigative activities and evidence collected are recorded in a document. At the conclusion of the investigative activity, the DPO prepares a DP Compliance Report that includes the Findings, the Conclusions and Recommendations on preventive, mitigating or corrective measures to the Controller for due implementation.

(4) **Opportunity to comment on the Findings**. In case an Irregularity or Incompliance is found, the responsible Delegated Controller is afforded the opportunity to comment on the DPO Findings. The responsible Delegated Controller is also provided the opportunity to comment on the draft DP Compliance Report. The DPO, if the case, revises the Findings and the DP Compliance Report which in the opinion of the DPO are warranted further to the comments provided by the Delegated Controller. The comments made by the Delegated Controller are annexed in their entirety to the DP Compliance Report issued by the DPO.

(5) **Submission of DP Compliance Report to the President**

(a) In case no Incompliances are found, the DP Compliance Report, including the DPO Findings, Conclusions, Recommendations, and an annex of any comments made by the Delegated Controller, is submitted to the Delegated Controller for implementation and further action as deemed appropriate and to the Controller for information. Unless the Inspection was started *motu proprio*, the DPO responds to the enquirer.

(b) In case no Incompliances are found, the DP Compliance Report, including the DPO Findings, Conclusions, Recommendations, and an annex of any comments made by the Delegated Controller, is submitted to the Delegated Controller for implementation and further action as deemed appropriate and to the Controller for information. Unless the Inspection was started *motu proprio*, the DPO responds to the enquirer.

(c) The DPB is informed by the DPO on the outcome of any DP Inspection and can then request to see the DP Compliance Report. The DPB can comment and/or request a supplementary investigation on any issue emerged during a DP Inspection.

(d) In case the DPO assesses an Incompliance with the DPR, the DP Compliance Report is submitted to the DPB for validation of the Conclusions and Recommendations. Upon validation by the DPB of the DPO Conclusions and Recommendations, the latter become binding and are submitted to the Controller for implementation. When the DP Inspection was not started *motu proprio*, the enquirer is informed accordingly.

(e) In case of disagreement by the DPB with the Conclusions and/or Recommendations formulated by the DPO, the DPB submits its comments in writing to the DPO, which amends the Conclusions or Recommendations accordingly. If necessary, the DPO and the DPB engage in consultation. The DPO may engage in a follow-up inspection or an extension of the DP Inspection if the consultation with the DPB highlights elements that need further clarification.

## 5. DP Compliance Report

The DP Compliance Report should normally include the following elements:

i. Title
ii. Addressee
iii. Scope of the DP investigation, including the time period covered
iv. Identification or description of the subject matter
v. A summary of the activities performed during the DP Inspection
vi. Findings
vii. Conclusions
viii. Recommendations of preventive, mitigating and corrective measures and/or actions (as appropriate)
ix. Report date

## 6. Ad-hoc Queries

(1) In the framework of data protection advisory activities, i.e. questions and consultations submitted to the DPO for opinion and advice, the DPO may be required to gather information on the processing operation or the implementation of the DPR from, e.g. the Delegated Controller, the DPL, the processor if relevant and further actors as necessary to respond to the consultation.

(2) The DPO may decide on a case-by-case basis on the measures that are most appropriate, necessary, and proportionate to conduct the fact finding in the course of the advisory activity, including initiating a DP inspection, in which case the related procedure will apply.

## 7. Obligation to provide assistance and information to the DPO

(1) In accordance with Article 46 DPR, every employee and all organisational units of the Office and bodies of the Office are required to assist the DPO in performing its duties, including investigating into DP matters.

(2) To enable the DPO to assess compliance with the DPR, all employees must provide the DPO with information in reply to questions and allow the DPO to inspect all documents and all data stored in files and/or any data processing programmes. They must also permit and facilitate access to all information, including personal data as well as processing operations, required to perform the DPO tasks and provide and facilitate access of the DPO to all EPO offices, data-processing installations and data carriers.

(3) The DPO shall cooperate with the respective Delegated Controller with a view to find the most appropriate actions/measures to (re-)ensure DP compliance.

(4) If necessary, the DPO may be assisted by staff from other organisational units or external providers (for example when a specific expertise is needed, e.g. in IT security).

## 8. Follow-up

(1) The need to follow up previously reported instances of Irregularity or Incompliance may be decided by the DPO on the basis of the nature of the subject matter, the nature of the Irregularity or Incompliance identified, the preventive, mitigating and corrective measures, if any, and the particular circumstances. The follow-up may form part of the subsequent year's DP Audit Plan.

(2) An annual report will be sent to the President for information regarding the status of the implementation of the DPO's Recommendations stemming from DP Inspections.