Bloomberg BNA

Privacy and Security Law Report®

What to Do When the Privacy Regulator Comes Knocking on Your Door? A Short Guide to Handling Inspections and Data Protection Audits in Europe

BY KARIN RETZER AND JOANNA LOPATOWSKA

Inspections and data protection audits from regulators are on the rise across Europe, and this trend is likely to continue. The latest figures for 2012 show that the French data protection authority (Commission Nationale de l'Informatique et des Libertés or CNIL) completed 458 inspections, a 19 percent increase from 2011.[1] The number of inspections has been steadily rising since 2004, when CNIL's enforcement powers—and later on, its budget—were significantly increased. The Bavarian data protection authority conducted 13,404 off-site audits and 20 on-site inspections in 2012, compared to 50 off-site audits and 12 on-site inspections during the previous year.[2] Perhaps not surprisingly, the number of sanctions imposed has quadrupled over the last five years. The Polish Inspector General for the Protection of Personal Data(GIODO) conducted 199 inspections in 2011,[3] and the U.K.'s Information Commissioner's Office (ICO) completed 58 audits in 2012/2013, and 42 audits in 2011/2012, compared to only 26 in the previous year.[4]

Companies need be proactive and take steps to dealing with a data protection audit. Any regulatory inspection is a burdensome undertaking, and inspections carry the risk of noncompliance being exposed, sanctions, adverse media attention and damage to reputation. Sometimes noncompliance is only identified after an inspection has been carried out. Even for fully compliant organizations, inspections bring disruption to the conduct of normal business.

This article provides organizations with recommendations on how to handle privacy inspections when the local data protection authority (DPA) comes knocking, and how to establish best practices to prepare for such checks and audits. It focuses specifically on on-site inspections, and describes the various steps, from the decision to inspect an organization to the final statement drawn at the end of an inspection.

I. Why Is an Organization Audited?

Organizations are usually selected for privacy audits for one or more of the following reasons:

- The organization or industry is identified for inspection as part of the DPA's routine (planned) compliance monitoring. This approach is often seen in France, Germany and Northern Europe,[5] where the DPAs annually publish a program indicating the sectors and data processing activities that are due for inspection in the coming year. For example, in the 2012 audit program, CNIL planned 450 inspections that focused on how telecommuni-

[1] CNIL, *Commission Nationale de l'Informatique et des Libertés: Rapport d'activité 2012* (2013), *available in French at* http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_RA2012_web.pdf (12 PVLR 793, 5/6/13).

[2] Bayerisches Landesamt für Datenschutzaufsicht (Bavarian data protection authority), *Tätigkeitsbericht 2011/2012* (March 2013), *available in German at* http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/dsa_Taetigkeitsbericht20112012.pdf (12 PVLR 617, 4/8/13).

Karin Retzer is of counsel to Morrison & Foerster LLP, in Brussels, where her practice focuses on electronic commerce and data protection, technology licensing and intellectual property law.

Joanna Lopatowska is an associate in the Privacy and Data Security Group in Morrison & Foerster's Brussels office.

[3] GIODO, *Sprawozdanie–Z Dzialalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2011* (June 2012), *available in Polish at* http://www.giodo.gov.pl/data/filemanager_pl/sprawozdaniaroczne/2011.pdf.

[4] ICO, *Annual Report and Financial Statements 2011/12* (July 2012), *available at* http://www.ico.gov.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/annual_report_2012.ashx (11 PVLR 1114, 7/9/12).

[5] The Nordic countries include Denmark, Finland, Iceland, Norway and Sweden.

 ISSN 1538-3423

cations operators and application developers use personal data collected from smartphones, as well as the processing of online health data (11 PVLR 709, 4/23/12). Sweden's Data Inspection Board announced in 2012 that it would monitor how local municipalities use tablet computers and e-readers to store and share official documents (11 PVLR 737, 4/30/12).

- An individual has filed a complaint with the DPA. In recent years, there has been an increase in complaints from individuals, which can be attributed to increased public awareness of privacy rights (in particular, the European Commission actively works on strategies to raise citizens' awareness of privacy and data protection issues). For example, in Bavaria, one of the 16 German Länder or states, there were 719 complaints in 2012 alone,[6] and there are similar figures for other countries.[7] Usually, when a DPA receives a complaint from an individual, it first reviews it, alerts the organization, and then requests explanations and information. Following this phase, the DPA may decide to launch an on-site inspection.
- Another public authority has alerted the DPA to an organization's suspected noncompliance (national authorities or those based in other countries, including public prosecutors, other DPAs or labor or consumer protection associations). Some DPAs have developed formal partnerships with other public authorities regarding privacy compliance cooperation. For example, based on an agreement signed in 2012, the Polish Labour Inspectorate must inform the GIODO about any privacy violations identified during a labor inspection. In France, based on a 2011 cooperation protocol, CNIL must be informed of privacy violations identified during inspections by the Directorate General for Competition, Consumption and the Prevention of Fraud.
- The inspection is voluntary, performed at the request of (or in agreement with) the organization. In the U.K., the ICO carries out consensual audits, *i.e.*, with the full agreement of the organization in question. The ICO can also perform compulsory inspections at central government departments and, as of 2011, telecommunications and Internet service providers.[8] In the latter case, the ICO's approach is to first seek agreement to a consensual audit. The audit will become mandatory if the service provider fails to agree to an audit ''without adequate reasons.''[9]
- Adverse media attention involving the organization, for example, when a major data breach occurs that has been made public.
- The inspection follows up on a registration or request for approval. Some DPAs also initiate an investigation after receiving requests for registrations or authorizations that reveal noncompliance in specific areas.
- Adverse findings from a privacy inspection of the organization's affiliate or at another (separate) organization in the same sector.

II. General Legal Framework and Jurisdiction

The enforcement powers of the DPAs are currently regulated in European Economic Area (EEA) member state laws implementing the EU Data Protection Directive (95/46/EC) (''Directive'').[10] These laws differ across the EEA, which consists of the 28 European Union member states and Iceland, Liechtenstein and Norway. Although this article will not discuss this in depth, we note that this diversity of law may change in a few years' time. The proposal for a draft ''General Data Protection Regulation'' published by the European Commission in January 2012 (''draft Regulation'')[11], and currently under the review of the European Parliament, harmonizes and strengthens sanctions and rules on enforcement.[12]

The Directive sets out that each DPA is competent to exercise its powers on the territory of its own member state. However, each DPA may be requested to exercise its powers by a DPA from another member state. Furthermore, the DPAs must cooperate with one another to

---

[6] *See* Bavarian DPA, *supra* note 2.

[7] In 2011 there were 5,738 complaints in France and 114 complaints in Poland, and in the 2011–2012 period there were 12,985 complaints in the U.K. *See* CNIL, GIODO and ICO, *supra* notes 1, 3–4. There were 1,161 complaints in Ireland and 3,668 complaints in Italy. *See* Irish Data Protection Commissioner, *Twenty-Third Annual Report of the Data Protection Commissioner 2011* (Apr. 2012), *available at* http://www.dataprotection.ie/documents/annualreports/AnnualReport2011.pdf; Garante per la Protezione dei Dati Personali (Italian DPA), *Annual Report For 2011—Summary* (Dec. 2012), *available at* http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/2148370.

[8] The ICO's powers to conduct mandatory audits of providers of electronic communications services were introduced under the U.K. Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2011, which transposed the 2009 amendments to the European Union e-Privacy Directive (2009/136/EC).

[9] ICO, *Audit: A Guide to ICO Privacy and Electronic Communications Regulations Audits* 4 (Aug. 2012) [hereinafter ICO *PECR Audits*], *available at* http://www.ico.org.uk/~/media/documents/library/Privacy_and_electronic/Detailed_specialist_guides/guide_to_ico_pecr_audits.ashx.

[10] Directive 95/46/EC of Oct. 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on Free Movement of Such Data, 1995 O.J. (L 281), 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML. The Directive is applicable to the EEA countries based on the Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 Amending Protocol 37 and Annex XI (Telecommunication Services) to the EEA Agreement, 2000 O.J. (L 296), 41, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:296:0041:0043:EN:PDF.

[11] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM(2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (11 PVLR 178, 1/30/12).

[12] For example, the draft Regulation provides for the ability to impose a fine for privacy violations of up to 2 percent of the organization's global turnover. *Id.* at Article 79(6). Sanctions imposed in one country will be enforceable across the EEA, and organizations operating in multiple countries will be subject to the supervision of one DPA in the country where the company has its main establishment. *Id.* at Article 79(1), Recital 98.

  PVLR ISSN 1538-3423

the extent necessary for the performance of their duties. For example, in 2012 the Estonian and Latvian DPAs published joint recommendations to an organization after they cooperated in inspecting the organization's employee and customer data practices in the two countries.

Despite the cooperation efforts, however, the DPAs' powers are still limited in territorial scope and do not extend beyond the territory of a member state.

Organizations that have executed Standard Contractual Clauses for transfers of personal data from controllers to processors outside the EEA,[13] or those that have adopted Binding Corporate Rules (BCRs), must also agree to submit their operations to a European DPA for inspection. The U.S.-EU Safe Harbor Framework mandates such cooperation for human resources data. However, even in such cases, the DPAs do not have sufficient resources to conduct on-site inspections of non-EEA parties. Therefore, even when there is a theoretical risk of an inspection under these transfer mechanisms, in practice, we see little to no foreign inspections. For example, in 2011, the Italian DPA, the Garante per la Protezione dei Dati Personali (''Garante''), decided that non-Italian call centers that collect information from Italian residents on behalf of Italian entities are subject to the same rules that apply to Italian call centers (10 PVLR 1160, 8/15/11). However, in practice these overseas call centers were not inspected by the DPA; the Garante officials said that the inspections should be carried out at the Italian company that contracted the offshore call center. Even if, in practice, the DPAs do not have jurisdiction to inspect the non-EEA organizations, they may—and do—inspect the EEA affiliates.

In light of increasing DPA powers, the rising number of inspections, and the risks of sanctions that may follow, organizations operating in the EEA are advised not only to prepare for a planned, notified inspection, but to establish best practices, policies and procedures on how to handle all inspections.

Below we provide guidance on what organizations can do when faced with an inspection, and we set out some best practices.

III. How to Prepare for and Handle an Inspection

Data protection audits are intended to evaluate whether an organization complies with local data protection laws and standards, including:

- registrations and authorizations;
- notice requirements;
- purpose limitations;
- transfer mechanisms for transfers outside the EEA;
- management of vendor relationships;
- adequate security measures and the establishment of privacy policies and procedures;
- access and correction policies;
- employee monitoring activities; and
- direct marketing.

Most local data protection laws only contain general provisions on the DPA's inspection powers, but some DPAs—for example in Ireland, the U.K. and Poland—have published guidance on procedures, sample questions and template documents and reports.[14]

A. Before the Inspection Takes Place

An organization's existing privacy measures and standards are key factors in handling the inspection itself. Organizations that are aware of inspection risks and are prepared for them will be able to undergo inspections with less disruption and better results.

Conduct an assessment. Knowing the status of your organization's compliance with local laws and implementing any necessary changes are the first steps. Basic compliance involves: providing privacy notices to individuals whose personal data are collected and processed; completing database registrations; implementing written policies and procedures (*e.g.*, on data security, data retention and access and correction); and where required, appointing data protection or data security officers. Most of these requirements take time, and cannot be implemented in a hurry right when the organization receives a notice of an inspection.

Therefore, it is prudent to regularly perform an analysis identifying and addressing any gaps in compliance as early as possible. In addition, it is useful to monitor the DPA's enforcement trends, especially in similar industries.

The DPA inspectors often run a preliminary inspection of an organization without actually visiting the premises. For example:

- In Ireland, inspectors will first: review case studies in annual reports and previous audit reports, focusing on organizations operating within the same sector; check the organization's existing registrations; review media articles and published reports; and check the organization's website to see what personal data are being collected online.
- In the Netherlands (College bescherming persoonsgegevens or the CBP) , the DPA will review

[13] Commission Decision of 5 Feb. 2010 on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39), 5, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF (9 PVLR 253, 2/15/10).

[14] *See* guidance on inspection and enforcement: Irish Office of the Data Protection Commissioner, *Data Protection Audit Resource* (Jan. 2009), *available at* http://www.dataprotection.ie/documents/enforcement/AuditResource.pdf; Irish Office of the Data Protection Commissioner, Offences and Penalties, http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/legal/4e.htm&CatID=23&m=e (last visited Sept. 11, 2013); ICO, *Information Commissioner's Guidance About the Issue of Monetary Penalties Prepared and Issued Under Section 55C (1) of the Data Protection Act 1998* (Jan. 2012), *available at* http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ico_guidance_on_monetary_penalties.pdf (11 PVLR 248, 2/6/12); ICO, *Auditing Data Protection: A Guide to ICO Data Protection Audits* (Aug. 2013) [hereinafter ICO *Auditing Data Protection*], *available at* http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/auditing_data_protection.pdf; GIODO, *ABC zasad kontroli przetwarzania danych osobowych* (Dec. 2011), *available in Polish at* http://www.giodo.gov.pl/plik/id_p/1053/j/pl/.

any notices, privacy policies, registrations or other information that was made public by the company, and take into account in its ultimate findings the extent to which the company complies with these statements.

- In Bavaria in 2011, the DPA reviewed more than 2,000 websites via an online tool to ensure compliance with German tracking restrictions.

A good level of privacy compliance will help prepare organizations and employees for investigations. In particular, regular training and awareness on general privacy obligations and employees' duties will minimize any compliance gaps.

Prepare a plan and organize training. Organizations may consider developing a plan that sets out how to react in an organized way to the DPA's visit. The plan may determine who should be notified about the inspection, establish an internal inspection or audit team, provide guidelines on handling the DPA's questions and requests for documents and set out procedures for actions during an inspection. It is helpful if the plan sets out the basic logistics, such as what offices and resources will be made available to the inspectors. Staff should be briefed on the role they may play during an inspection. For example:

- Employees should be trained on the role and powers of the DPA in order to know what to expect from them. The training may include topics such as: how to answer questions and provide documents, and the risks of obstructing the investigation, giving false or misleading information or making false statements.

- Receptionists and security guards should be briefed on how to greet inspectors and whom to inform about their arrival; they should contact the in-house counsel and privacy officer immediately—even if that means interrupting a meeting—and instruct inspectors to wait in a lobby or a conference room until a representative arrives.

Form an inspection team. Organizations may consider creating an inspection team that includes key individuals responsible for handling the inspection (*e.g.*, the data protection officer, the head of legal, the head of information technology (IT) and the heads of main departments such as human resources (HR) and marketing). It may be helpful to draft rules of procedure, including the composition of the team, their duties and responsibilities and the procedures that must be followed. These may include receiving and accompanying the inspectors throughout their inspection, responding to their questions, coordinating with other employees, attending interviews and coordinating daily meetings.

Members of the team should be informed immediately about the DPA's visit. Therefore, their phone numbers should be readily available to the front office in case the team members are out of the office when an unannounced inspection takes place.

Raise awareness among employees. An organization should ensure proper awareness amongst its staff about the likelihood of privacy inspections. Employees should be informed of such a possibility so that they know what to expect. When no inspections have occurred in the past, employees may not be familiar with the procedure, or may not be at ease when interviewed by the authorities. Therefore, prior notice helps to make them aware of the inspection process and its potential impact on the organization. Prepared employees are better able to respond to the DPA's questions and to locate the requested documents.

B. During the Inspection

Notice of the inspection. While some DPAs provide advance notice, others provide little or no warning of their intention to conduct an inspection. The notification period may be greater if the inspection is routine, as opposed to complaint- or inquiry-driven. For example:

- In France, before 2011, on-site inspections could be conducted without prior warning and without the opportunity to object. As of 2011, CNIL must now inform the organization of its visit and of the right to object.[15] The notice is usually served several days in advance, or on the morning of, the inspection. If the organization objects, the visit may only take place upon authorization granted by a judge. The approval must be rendered within 48 hours.[16] If justified by the urgency or seriousness of the relevant facts or by a risk of destruction of evidence, the visit may take place without warning (but only upon prior judicial authorization) and cannot be opposed.

- In the U.K. and Ireland, the majority of inspections are scheduled and dates are agreed in advance, often with several weeks' notice. Usually the organization will receive a letter providing a general outline of the inspection's purpose and the requested documents. Before the inspection, the ICO requests documents such as: data protection policy documents; operational guidance or manuals for staff processing sensitive data; data protection training modules; risk registers; information asset registers or information on governance and other similar structures.

- In Germany and the Netherlands it has been the practice of the DPAs in recent years to first send out to the company a written questionnaire, which the organization has to answer truthfully and completely within a certain time period. The DPA may thereafter follow up with an on-site inspection to review the accuracy of the answers provided, and to further investigate the organization's compliance with privacy law.

Authorization. Upon the inspectors' arrival, the first action should be to verify their identity and their specific accreditation to conduct the inspection. The accreditation should specify the subject matter and purpose of the inspection, and the inspectors will usually produce an explanatory note. The representative of the organization should determine the scope of inspection, in particular whether there is any particular area of concern (customer service, HR, *etc.*), whether the inspec-

[15] Article 44 of the Law on Processing Data Files and Public Liberty was amended by Law No. 2011-334 of March 29, 2011 (10 PVLR 521, 4/4/11).

[16] In 2011, three organizations objected to CNIL's on-site inspections. In each case, the judge authorized the CNIL inspection. CNIL, *Rapport d'activité 2011* 71 (July 2012), *available in French at* http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/Cnil-RA2011/index.html#/71/zoomed (11 PVLR 1148, 7/16/12).

  PVLR ISSN 1538-3423

tion is the result of an infringement or planned with regard to a specific industry, what the nature of the infringement is and the planned duration of the inspection.

Duration and timing of the inspection. The duration of the inspection can be a few days to several weeks, depending on its type, the size of the organization and the country.[17] Even routine inspections can take several weeks or more.

In general, the inspectors' agenda will govern the visit. The inspectors will indicate what they would like to do and when. It is helpful to discuss the agenda with them in advance because it allows the organization to better manage the resources necessary to gather the information and to schedule employees for interviews. Planning ahead will also help to minimize disruption to business activities, and allow employees needed for interviews to reschedule other meetings.

Generally, inspectors will arrive at the organization's premises during normal business hours. However, some laws allow inspections outside of business hours. In Poland, inspectors can enter the organization's premises between 6 a.m. and 10 p.m. and in France between 6 a.m. and 9 p.m.

The logistics. Once the inspectors have arrived, they should be shown to a room where they can work, but they should not be left out of sight. The room should be able to accommodate the inspectors as well as a similarly sized organization team; it should also have a worktable for the documents under review, as well as a telephone, paper and pens, *etc*. In addition to the actual inspection room, adequate work areas for copying and stamping documents (*e.g.*, date provided, confidentiality, *etc.*) should be provided.

It is also best to notify selected staff that the inspectors are on the premises, and that their assistance may be requested at short notice. It may also be useful to remind employees that they should not write any e-mails, memos or other documents about the inspection, unless asked to do so by their managers, the legal team or the inspection team.

Inspectors' powers. The DPAs have broad authority to carry out inspections. Generally, most laws specify that the inspectors may access any place, premises, surroundings, equipment or buildings that are used to process personal data for professional purposes, and specify that they are allowed to: look at and request copies of the documents, interview staff; review and print out data that are stored electronically; perform inspection of any devices, data carriers or computer systems used for data processing; and demand written or oral explanations.

Document requests. Many laws specifically provide for the ability to request access to the organization's documents. Requested documents might include a list of processing activities, the structure of the IT applications, a list of databases, screenshots from applications and software, extracts from data files, copies of internal policies (*e.g.*, privacy policy, data retention, technology use policy, IT security policy and access and correction policy), copies of privacy notices, copies of service and provider agreements and any information regarding the internal procedures for handling data access requests. Often the following requests cause the most concerns:

- The documents provided to the inspectors should be responsive to their requests but should not go beyond the information requested. Often, unless expressly requested, or unless the response would be incomplete without a document, questions can be answered without providing documents.
- The inspection team should identify any logistical problems with responding to a request, such as retrieving documents from remote locations. The inspectors often may not understand the architecture of the organization and the document management process. However, the organization's representatives should refrain from questioning the relevance of the document request. Rather, they should explain to the inspectors their difficulties and request an appropriate time frame to provide the documents.
- Despite their broad authority, the inspectors may request documents that are beyond the scope of their authority—for example, concerning financial information, trade secrets, privileged communication, employee performance or medical files, internal audit information, *etc*. The decision to provide or withhold a document should be made by the organization's representatives in consultation with legal counsel. It is helpful to draft a note describing any differences of opinion between the organization and the inspectors regarding documents considered out of scope. Alternatively, the organization may request that sensitive areas of the document be redacted, or propose that the documents be reviewed but not copied. Sensitive documents should be marked as ''confidential'' before being copied.
- The inspection team should keep records of what documents are provided to the inspectors, including the dates they were requested and provided. The team should also keep copies of all extracts, documents, *etc.* taken by the inspectors, as well as a list of anything requested by the inspectors but not released to them.

Interviews with employees. Inspectors routinely request interviews with the organization's staff. Inspectors may request to interview a specific person. This request should not, in general, be objected to; however, sometimes, following a suggestion from the inspection team or the unavailability of an employee, the team may agree to interview another person instead. However, failure to provide the requested employees for interviews may be regarded as hindering the inspection.

When anticipating requests for employee interviews, the inspection team should consider identifying employees who are likely to be called for an interview. Meetings should be scheduled with those employees to discuss the process and the areas of possible review, identify documents that may be responsive to requests and answer any questions that they may have. Organizations should consider preparing the employees through mock interviews. The inspection team should also be present during interviews.

The meetings. If acceptable to the inspectors, it is a good practice to begin and end each day with a meeting between the inspection team and the inspectors. These

[17] In Poland, the total duration of all inspections by any combination of state agencies cannot exceed 48 working days per year for large organizations, and 24 days for medium-size organizations.

meetings allow a review of the status of the inspection to ensure that the inspectors are satisfied with the information provided, to provide the inspectors with any requested documents and to discuss any new questions or requests. More senior members of the organization should attend the meetings, and members of the inspection team should be generally available throughout the whole inspection.

Minutes. It is helpful to record steps taken during an inspection, as well as any communication with the inspectors. The minutes should include each question or request from the DPA and a response to each inquiry, the name of the person who provided the response and whether the inspectors were satisfied with the response. Minutes create a record that can be used to dispute inspectors' conclusions (*e.g.*, inaccurate claims that the company withheld information or failed to answer questions), and can also be used to prepare for future inspections.

Hindering the inspection. There are certain areas where the organization has the right to object or the right to redact certain confidential information. However, objecting to the inspectors' requests, denying access to premises or documents or any other hindrance to the inspection of certain areas will likely be thought of as resisting the inspection and can lead to a negative outcome for the organization or its representatives. In some countries, obstruction of a DPA inspection or investigation may incur administrative or even criminal penalties:

- In Poland, preventing or hindering an inspection is a criminal offense punishable by up to two years of imprisonment or a fine. Individuals acting on behalf of an organization are subject to criminal liability.
- In France, preventing the inspectors from performing their duties, refusing to provide the information or documents requested or supplying false information is punishable by a penalty of one year of imprisonment and a fine of 15,000 euros (approximately $20,000).
- In Germany, failure to provide the requested information or to cooperate during an audit, or providing incorrect information, is subject to a fine of 50,000 euros (approximately $66,000).

C. After the Inspection

After the inspection, the members of the inspection team should: run a preliminary assessment to determine whether the explanations concerning any documents that were withheld or any other reservations made should be sent to the DPA; whether the documents supplied or explanations given were sufficient or whether further documents should be submitted; whether there are any factors relevant to the inspection that may not have been apparent to the inspectors; and whether it is necessary to correct any unfavorable inferences or impressions that the inspectors may have drawn.

Depending on the outcome of the inspection (and in particular if sanctions are likely), the inspection team will need to determine what actions must be taken in order to remediate the violations.

Protocol. At the end of the inspection, the inspectors will present a final protocol including the records and the findings of the inspection. Some laws, *e.g.*, French and Polish laws, include detailed content of such protocol.

The outcome of the inspection. The outcome of the inspection and its consequences may greatly vary among the member states.

- In the U.K., the organization is asked to agree to a set of recommendations and complete an action plan indicating how, when and by whom they will be implemented. The final report is then issued with an executive summary that is published on the ICO's website when the organization agrees.[18] The aim is to share good practices with other organizations, and let others learn from the outcomes of the inspections.
- In France, at the end of an investigation, CNIL sends a copy of the report to the organization, which then has 15 days to submit any comments or observations.

Following the inspection, the DPA may ask the organization for additional information. The DPA may also find that the organization has complied with the law. In such case corrective measures are not ordered, nor are sanctions imposed, and the organization is informed about the closure of the investigation. The inspection will, however, usually be followed by a DPA's decision, including the findings, recommendations or orders and, where necessary, sanctions. The following measures may be imposed or ordered:

- ***Warnings.*** In some countries, for example in France, Germany, the U.K. and Ireland, the DPA may issue a warning to an organization that fails to comply with the law. In the U.K., consensual inspections are supposed to be ''educative and not punitive,''[19] and in general it is not intended for them to lead to formal enforcement action, although enforcement powers may be used when the organization refuses to address the recommendations within an acceptable time frame.
- ***Orders and corrective actions.*** In most countries, the DPA may: further restrict data collection and processing until data protection or security violations are remedied; require remedy of the negligence, in particular to complete, update, correct and disclose or not disclose personal data; require adoption of additional measures protecting the collection or processing of personal data; suspend data transfers to countries outside the EU; require additional safeguards of the data to transfer the data to vendors or business partners; and require erasure of personal data that were improperly obtained.
- ***Financial penalties.*** In some countries, DPAs can impose monetary fines. For example:
  - In France, the sanction for a first breach cannot exceed 150,000 euros (approximately $199,000). For a second breach that occurs

[18] The ICO began posting executive summaries of data protection audits on its website in June 2010. *See* ICO, Audits, http://www.ico.org.uk/what_we_cover/audits_advisory_visits_and_self_assessments/audits (last visited Sept. 11, 2013).

[19] ICO *Auditing Data Protection*, *supra* note 14, at 12.

  PVLR ISSN 1538-3423

within five years of the first sanction, a second fine may be imposed. The second fine cannot exceed 300,000 euros (approximately $398,000) for natural persons or 1.5 million euros (approximately $2 million) for legal persons.

- In contrast, the ICO will not impose a financial fine as a result of noncompliance discovered in the course of a consensual inspection. Regarding compulsory inspections, the ICO may impose penalties of up to 500,000 pounds (approximately $784,000); however, according to the ICO, audits are mainly ''a means of encouraging compliance and good practice.''[20]

- ***Criminal actions.*** In some countries criminal actions may be initiated. In Poland, if the inspection reveals a violation of the Data Protection Act, the DPA has a duty to inform the relevant prosecuting body. In many countries, the results of the investigation can be—and sometimes are—made public. This acts as a deterrent to organizations and can be an indirect punishment for the organization if the outcome of the report is negative. For example, it can lead to the loss of customer confidence, influence stock prices, *etc*.

Any noncompliance identified should be promptly addressed, and in any case within any time frame provided by the DPA. The corrective actions should be documented. It is also wise to inform the DPA of the actions taken and of the implementation of the recommendations to limit the risk of a post-checking inspection.

Appeal. Generally, when the organization does not agree with the findings of the DPA or the sanctions imposed, it can question the decision in a court proceeding. However, this is not always the case. For example, in Poland in 2011, only 10 percent of decisions were appealed.

Follow-up. Organizations that have been inspected may expect to be contacted by the DPA to establish what actions have been taken to implement the recommendations as set out in the final audit report. Follow-up inquiries are often conducted in writing, and will usually involve the provision of additional documentation or sample data sets.

[20] ICO *PECR Audits*, *supra* note 9, at 12.