Monitoring and Ensuring Compliance with Regulation (EC) 45/2001

Policy paper

Brussels, 13 December 2010

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

Contents

Monitoring and Ensuring Compliance with Regulation (EC) 45/2001

1. Introduction

This policy paper elaborates how the EDPS monitors, measures and ensures compliance with Regulation (EC) 45/2001 ("the Regulation"), and explains the nature of the various enforcement powers, as well as when and how the EDPS will use them. The paper reflects many of the current activities and actions of the EDPS in relation to monitoring and ensuring compliance, and sets out a comprehensive framework for all future work in this area. It is guided by the principles of proportionality, accountability and consistency, and aims to give transparency to what the EDPS does with the information gained from our activities (complaints handling, prior checking, monitoring, etc) as well as reflect general principles on how we will assimilate and act on this information and where applicable, the weight or severity we would accord to such information.

The policy seeks to encourage voluntary compliance and best practice, create sufficient incentives for compliance and facilitate targeted action where appropriate, by:

- emphasising where the responsibility for compliance lies
- explaining how the EDPS will support this compliance
- explaining what the EDPS will do in the case of non-compliance

In order to optimise the effectiveness of the existing framework, the policy aims to reflect the layered approach, provided by the Regulation, to guaranteeing data protection in the institutions and bodies of the EU: the institutions/bodies, controllers, data protection officers (DPOs) and EDPS all contribute to the application of and compliance with the Regulation. The policy therefore seeks to exploit these roles and responsibilities, and the underlying synergies in order to ensure effective compliance with data protection principles.

Further to the Lisbon Treaty, all Union institutions and bodies are bound by the fundamental rights to privacy and protection of personal data (see Articles 7-8 of the EU Charter and Article 16 TFEU). It is the task of the EDPS to monitor and ensure that these rights are respected in accordance with Regulation (EC) 45/2001.

Article 1.1 of the Regulation makes it clear that it is the responsibility of the institutions and bodies themselves to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

Furthermore, the EDPS is keen to see the institutions and bodies take a proactive approach to this responsibility by embracing the notion of

"accountability" (as recently elaborated by the Article 29 Working Party)[1] and by doing so fostering data protection in practice. Accountability requires institutions and bodies, and data controllers acting on their behalf, to put in place appropriate and effective measures to ensure that the principles and obligations set out in the Regulation are complied with and to demonstrate this to the EDPS upon request. The EDPS will then focus on his responsibilities for monitoring and where necessary ensuring compliance.

Within the EU institutions and bodies, DPOs will be key to any successful accountability program, and in this context the EDPS welcomes the DPO Network's "Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001" (October 2010).[2] The EDPS believes that this document provides a good basis on which to build new, more effective, data protection governance involving sound policies, effective implementation mechanisms and appropriate assurance programs.

The EDPS believes that this will enable a selective, targeted, risk-based approach to enforcement with emphasis on those institutions or bodies which demonstrate a clear lack of commitment and/or poor compliance records. This in turn will enable the effective use of our limited resources in the context of the existing EU data protection framework.

2. Compliance monitoring

There are a number of tools and mechanisms available to the EDPS to enable him to carry out his compliance monitoring function. Some of these are derived directly from provisions of the Regulation, whilst others are a result of different legislation or simply reflect best practice. The evidence gathered from all of these tools and mechanisms will be used to build up intelligence on individual institutions or bodies and this in turn will help inform any decisions in relation to formal enforcement action.

2.1. EDPS compliance tools

2.1.1. Raising awareness

In accordance with Articles 46d and 47(1)(b) of the Regulation, the EDPS will continue to invest time and resources in providing advice, guidance and training (both generic and bespoke) on matters related to data protection falling within his remit. He will publish and publicise this guidance where relevant in an appropriate manner. By doing so he hopes not only to encourage compliance but also the adoption of best practice within the EU institutions and bodies.

[1] Opinion 3/2010 on the principle of accountability (WP 173), adopted on 13 July 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf
[2] Available at http://www.edps.europa.eu/EDPSWEB/edps/Supervision/DPOnetwork

In the context of this policy, the EDPS expects any guidance or training provided to be implemented by the relevant institution or body, and expects controllers, and DPOs in particular, to play a significant and appropriate role in this in accordance with their responsibilities under the Regulation (see Article 24.1(a) & (c) in relation to DPOs). He will therefore take account of any relevant findings and evidence gathered during the course of his duties when considering potential enforcement action, and will monitor the demand and uptake of the training and advice/guidance provided in order to inform his decision-making in this regard.

The EDPS is currently developing guidance on certain topics in the form of thematic papers with the aim of adopting horizontal opinions for standard administrative procedures within agencies. These would then serve as a set of EDPS standards for institutions. Work in this field can be further developed in the form of workshops, and interactive seminars whereby the EDPS presents our position and experience in a particular field.

2.1.2. Prior checks

Article 27 of the Regulation empowers the EDPS to prior check processing operations likely to present specific risks to the rights and freedoms of data subjects. It also places a responsibility on DPOs to notify these prior checks to the EDPS. The opinion resulting from a prior check must in turn be notified to the controller, who has an obligation to modify the processing operation where requested or risk potential enforcement action.

When the EDPS started his activities, there was a backlog of ex-post prior checking cases relating to processing operations already in place. In 2004, the EDPS requested the institutions/bodies to produce an inventory of cases potentially subject to prior checking. With regard to ex-post prior checks, he adopted a thematic approach, setting priority themes (medical data, staff appraisals, disciplinary data, social services) and requesting notification for these themes. After this initial phase the EDPS invited the institutions to submit all notifications concerning processing operations already in place. The present situation is that the vast majority of ex-post prior checks in EU institutions have been notified to the EDPS.

Article 27 allows little leeway for a selective approach in relation to prior checking work, but where appropriate, the EDPS has limited its scope using Article 27.3 (which allows for consultation with the EDPS in case of doubt as to the need for prior checking). For example, the EDPS determined that the processing of personal data related to the use of mobile phones by EACI staff going on mission was not subject to prior checking because the purpose of the processing was to control invoices over 50€ and not to evaluate personal aspects relating to the staff members. In another case, the EDPS ruled that the processing of personal data to ensure that EMCDDA staff were granted education allowances was not subject to prior checking as it did not seek per se to exclude any individual from a right, benefit or contract.

Follow up to prior check opinions are a crucial element of the enforcement strategy of the EDPS. The EDPS usually concludes prior check opinions by stating that the processing operation does not violate Regulation (EC) 45/2001 providing certain recommendations are implemented. If these recommendations are not implemented and evidenced, the institution needs to be aware that it risks formal enforcement action. The EDPS for his part will set clear, concise recommendations and deadlines, and will consistently and thoroughly pursue the follow up in order to ensure compliance.

Prior checking work provides an opportunity to establish a preventive dialogue with institutions/bodies in the form of meetings or public consultations with the aim of promoting a positive and proactive culture in relation to data protection.

Prior checks also enable the EDPS to gain an insight into the activities of the EU institutions and bodies, and help identify key data protection issues and develop EDPS case law. The experience gathered in the application of the Regulation has enabled the EDPS to gain expertise and provide thematic generic guidelines to institutions and bodies.

The EDPS Video-surveillance Guidelines of 17 March 2010[3] should be seen as a pilot case both in terms of the provision of guidance to institutions and bodies, and in testing them with a shift of emphasis towards accountability. If a body respects the recommendations made by the EDPS, there is in principle no need for prior checking. However, once again, where an institution or body ignores the guidelines, misses the relevant deadlines or fails to implement the associated recommendations, the risk of formal enforcement action is increased.

2.1.3. Consultations

Articles 28.1 and 46d of the Regulation place responsibilities on the EU institutions and bodies to inform and consult the EDPS with respect to drawing up internal rules and administrative procedures in relation to the processing of personal data.

Article 28.1 stipulates that institutions and bodies shall inform the EDPS when drawing up administrative measures such as any implementing rules concerning the Regulation or the DPO (Article 24.8), as well as general internal administrative rules relating to the processing of personal data (e.g. use of e-mail, e-monitoring, archiving, etc.). Where appropriate, the EDPS will evaluate the draft measures and issue recommendations which should be implemented by the institution. The EDPS expects to be kept informed of progress in this regard and will conduct follow-up activities to ensure compliance.

Article 46(d) describes the advisory role of the EDPS in a broader manner as relating to *"all matters concerning the processing of personal data"* and adds

[3] Available at http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines

that the EDPS can give advice *"before [the institutions or bodies] draw up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data"*.

Although Article 46(d) overlaps with Article 28.1, it enlarges the scope to "all" other matters and therefore provides the basis to give advice on cases involving specific processing activities or abstract questions on the interpretation of the Regulation (for example on how to implement the right of access in particular cases that present practical difficulties, how to interpret and apply Article 9, etc.). When the consultations received are based on hypothetical cases or deal with interpretative matters, follow-up is limited, but cannot be excluded.

The EDPS welcomes any proactive consultation from an institution or body and will view it as a positive step towards compliance. Nevertheless he expects the institutions/bodies concerned to take appropriate responsibilities for effecting any changes, or implementing the advice or recommendations that result from these consultations, and cannot rule out formal enforcement action if this does not occur.

2.1.4. Complaint handling

Article 33 of the Regulation allows employees of EU institutions/bodies to make complaints to the EDPS regarding alleged breaches of the provisions governing the processing of personal data contained in the Regulation. Articles 46(a) & (b) require the EDPS to investigate or conduct enquiries into such complaints where appropriate. The investigation of complaints by the EDPS requires the cooperation of DPOs and controllers in particular, but may well involve other members of staff of the institution or body concerned where necessary for the investigation of any given case.

Complaints and the resulting investigations are an important source of information from a compliance monitoring perspective. The EDPS will continue to analyse this information in order to decide if it demonstrates wider compliance issues or whether it supports other evidence of poor practice or non-compliance gathered during the course of his wider supervision activities. He will then determine whether any further steps such as an inspection or formal enforcement action are appropriate.

The EDPS has adopted a complaints policy which enables selectiveness in relation to handling complaints. Criteria have been laid down in the internal complaints manual to determine first if, and then how, a complaint should be handled. These criteria will be further refined with experience, but the main elements of the policy have been published[4] to help potential complainants understand the EDPS approach and enable the EDPS to better manage their expectations.

[4] Available at http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Complaints

In addition, the EDPS is considering issuing guidance to both institutions and the public to the effect that, whilst a complaint can be brought directly to the EDPS, it would generally be best practice for both parties to attempt to resolve the matter bilaterally via an internal review procedure. Importantly, this implies providing the DPO with resources to be able to handle complaints. The implementing rules adopted under Article 24.8 of the Regulation provide for such powers in some institutions and bodies. Furthermore, the Network of DPOs' professional standards document endorses this approach[5], thereby contributing to the aims of increasing controller accountability and shifting responsibility for compliance to the institutions/agencies themselves.

2.1.5. Targeted monitoring and reporting exercises

The EDPS will undertake targeted monitoring based on the knowledge and evidence gathered from all of his supervision activities with a view to identifying themes or specific institutions/bodies deserving of more focussed attention. This will normally consist of correspondence-based enquiries in relation to specific types of data processing for all or some institutions or bodies, but if necessary it may involve an on-site visit - for instance in the situation where an institution/body repeatedly fails to respond or does not demonstrate sufficient regard for the provisions of the Regulation. Such exercises will usually lead to an agreed set of recommendations and deadlines, often in the form of a road map.

Failure to implement these recommendations and/or to respect the associated deadlines may lead to more formal action. As part of this process, the EDPS will expect and require the assistance and collaboration of the heads of institutions, controllers and of course DPOs, in accordance with Articles 47.2(a) and 24.1(b) of the Regulation.

2.1.6. General monitoring and reporting exercises

To date, the EDPS has twice sought to measure general compliance with the Regulation by writing to the heads of institutions and agencies and asking for written feedback on certain matters. The EDPS will continue to conduct these periodic "surveys" in order to ensure that he has a representative view of data protection compliance within the EU institutions/bodies, and to enable him to set appropriate internal objectives to address his findings.

Furthermore, on the basis of the responses and evidence he receives, the EDPS will provide individual comments to all institutions/agencies and set relevant, prescriptive targets in the case of non-compliance. The feedback may also be used to select institutions/bodies for inspections if appropriate. Where any targets are not met, binding decisions will normally be adopted

[5] See section 3.7 of "Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001"

including an obligation to report. Ongoing failure to comply with the Regulation is then likely to trigger formal enforcement action (see below).

In addition, it should be noted that some institutions oblige their DPOs to draft activity reports in their implementing rules. These reports often indicate the level of compliance within the institution and as a result are clearly of interest to the EDPS. The EDPS would therefore welcome copies of such reports[6] but would obviously approach any issues highlighted in a collaborative, informal manner so as not to discourage the practice in general. However, if the institution fails to implement any resulting EDPS recommendations or advice, formal enforcement action cannot be ruled out.

2.1.7. Inspections

Articles 41(2), 46(c) and 47(2) of the Regulation provide the broad powers, including those of inspection, enabling the EDPS to perform his function as a supervisory authority.

A specific inspection policy is currently being developed. However, given the significant time and resources required to carry out inspections, the EDPS is keen to ensure a selective approach to their use, limited to two general types (standard and thematic) and prompted by evidence and facts gathered as a result of the other tools outlined in this section.

Standard inspections are designed to investigate and ensure compliance with EDPS decisions in the frame of prior check opinions or complaints, and more generally to ensure compliance with the Regulation in those cases where regular monitoring exercises have given serious indications that the compliance mechanism is blocked. They should therefore be viewed as the final stage before formal enforcement action.

The EDPS will also carry out thematic inspections where the approach will be to provide guidance in a particular area/theme and to set deadlines by which institutions and agencies are expected to comply with the data protection standards and recommendations set in this guidance. Failure to meet such deadlines or to implement the required standards/recommendation will make formal enforcement more likely.

Inspections will, by their nature, be tailor-made and be structured around specific requirements and objectives. However, the EDPS is likely to wish to involve and obtain the cooperation of the directors and senior staff of the institution/body, the appropriate data controllers, the DPO[7] and any other relevant staff in the process.

---

[6] Section 4.1 of "Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001" endorses the provision of a copy of these reports to the EDPS.

[7] The role of DPOs in inspections carried out by the EDPS will be developed in the EDPS inspection policy.

2.2. External compliance tools

Privacy impact assessments, security breach notifications and internal compliance reports are mechanisms which can be used by EU institutions and bodies themselves to promote compliance with data protection responsibilities and indeed to help demonstrate a spirit or practice of "accountability". Not all are yet supported by legal obligations but they should be viewed as significant tools within the environment in which the EDPS operates, as well as important indicators of culture and sources of compliance evidence. Where they are relevant and appropriate they will therefore be encouraged by the EDPS, for instance by the issuing of guidance.

Accordingly, where such initiatives have been voluntarily implemented, the EDPS will take a constructive and supportive approach to any compliance issues identified as a result, resorting only to more serious and formal action when such collaboration fails.

Two further tools that could increase the effectiveness of the EDPS' compliance monitoring activities are audits and privacy risk assessments, although as yet these have still to be developed.

2.2.1. Privacy impact assessments

The EDPS should encourage institutions and agencies to conduct privacy impact assessments in relation to any new processing operations involving personal data. The EDPS is therefore considering issuing guidance on this matter to indicate either that we expect PIAs to be carried out by default, or specifying the type of data or processing where we would expect PIAs to be carried out. An alternative approach to support this compliance tool would be for the EDPS to carry out an initial assessment of whether a PIA is required and if so to push this action back to the institution.

PIAs are significant as they allow institutions and bodies to gain better insight into relevant privacy risks and ways to address these risks. They may also lead to notifications and possibly prior checks, recommendations and follow-up.

2.2.2. Security breach notifications

The EDPS should also encourage institutions to adopt internal security breach procedures (in line with the e-Privacy Directive and practice at national level) that involve notification by the controller to the DPO and/or the EDPS. The Commission implementing rules on security (notification to DPO) should be seen as a first step in this regard.

The EDPS response to such notifications will obviously depend on a number of factors including the seriousness of the breach, the type and volume of data involved, the numbers of data subjects affected, the location of the

recipients, etc. The EDPS response will also reflect the difference between self-reported breaches and those coming to his attention via complaints, the press or other means.

2.2.3. Internal compliance reports

The EDPS should consider issuing guidance to encourage EU institutions and bodies to compile internal data protection compliance reports. Not only are these a useful monitoring tool, they also help to shift responsibility for compliance to the institutions themselves, thereby encouraging accountability. The EDPS could incentivise institutions and bodies to proactively engage in such reporting by, for instance, allowing appropriate exemptions from our general monitoring surveys.

2.2.4. Audits

The EDPS could explore cooperation with Audit Services so that compliance issues discovered as part of their work can be followed up appropriately by the EDPS. This will almost undoubtedly require some sort of MoU to clearly define roles, responsibilities and procedures. Institutions and bodies would also have to be made aware that where appropriate such exchanges of information would take place.

2.2.5. Privacy risk assessments

To facilitate a selective, risk-based approach, and support a more effective and targeted programme of work, the EDPS could try to develop criteria and regular stock taking (e.g. bi-annually) to determine which areas and subjects should receive particular focus and attention.

3. Enforcement

3.1. Introduction and background

The enforcement powers of the EDPS are set out in Article 47 of the Regulation. They are relatively broad in scope ranging from offering advice to delivering warnings and imposing bans on processing. This policy aims to bring clarity and consistency to the application of these powers.

Taking into account the inter-institutional framework within which the EDPS operates, he has to date not adopted a punitive approach to enforcement, preferring to make recommendations and encourage compliance rather than warn or admonish the controller or make legally binding orders. However, following five years of such activity, it is time to signal a change of approach.

Whilst the EDPS will continue to encourage compliance and good practice by informal, collaborative means, he will now take a proactive and holistic approach to formal action in cases of serious, deliberate or repeated issues, or where his advice has been ignored. We are mindful that failing to act where we have evidence of non-compliance conflicts with our aims of being accountable and consistent , and risks undermining the authority of the EDPS.

As stated earlier in this policy, when deciding whether or not to embark upon formal enforcement action, the EDPS will carefully consider all the evidence and supporting facts gathered from the full range of his supervisory activities. This intelligence will inform not only his decision to resort to enforcement action but also what type of action to take.

3.2. Types and definition of enforcement action

There are a number of different types of enforcement action available to the EDPS. The most effective action will be chosen bearing in mind the results that it can achieve, and the possible deterrent or educative effect for the institution or body, and for other institutions and bodies. In the context of this policy, formal enforcement action is defined as that set out in Articles 47(1)(c) to (h) of the Regulation, under which the EDPS has the power to:

- order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 13 to 19;

- warn or admonish the controller;

- order the rectification, blocking, erasure or destruction of all data when they have been processed in breach of the provisions governing the processing of personal data and the notification of such actions to third parties to whom the data have been disclosed;

- impose a temporary or definitive ban on processing;

- refer the matter to the EU institution or body concerned and, if necessary, to the European Parliament, the Council and the Commission;

- refer the matter to the EU Court of Justice (subject to the relevant conditions).

Although in practice the use of these powers is likely to be rare, the EDPS intends to take a more proactive and robust approach to exercising them in future. For illustrative purposes, some example scenarios are outlined in section 3.4.

3.3. Triggers for enforcement action

The EDPS will adopt a selective and proportionate approach to initiating and pursuing enforcement action that is consistent with his limited resources. As mentioned above, the inter-institutional framework favours a cooperative approach opting for actions based on Article 47(1)(b) (referring to the controller and making proposals to remedy a breach). Therefore, in most cases, any formal action will be driven by concerns about significant actual or potential detriment caused by non-compliance with data protection principles or repeated, serious or deliberate non-compliance with EDPS recommendations.

The initial drivers for enforcement action will usually be:

- concerns raised within the complaints we receive;
- concerns that become apparent through our supervision and/or monitoring activities;
- concerns that become apparent through our consultation activities.

In determining whether to take action, the form of that action and the extent to which we pursue it, we will consider the following criteria:

- is action needed to clarify an important point of law or principle?
- is action justified by the likelihood that the adverse impact of a breach will have an ongoing effect or that a breach will recur if action is not taken?
- is the practice of the institution or body representative of a particular activity to the extent that it creates the need to set an example?
- does the failure of an institution or body to follow guidance provided by the EDPS (position paper, guidelines, recommendations, etc) support a case for action?
- does the attitude and conduct of the institution, body or DPO, both in relation to the specific case and more generally in relation to compliance issues, suggest a deliberate, unhelpful or uncooperative approach?
- is the level of public interest in the issue sufficient to support a case for action?
- can pursuing specific enforcement action be justified given the resources required and the competing demands on these resources?
- what are the risks to the reputation and credibility of the EDPS of taking and not taking action?

- would it be more appropriate or effective for action to be taken by other means or bodies (e.g. by the European Ombudsman or before the Court)?

3.4. Enforcement action examples

The following are some examples of the types of conduct which are likely and unlikely to lead to the EDPS using his formal enforcement powers. Where action is likely, the examples also indicate potential outcomes. The examples are intended to be illustrative rather than exhaustive or binding.

3.4.1. Action likely (especially after warning)

- denial of subject access, where it is reasonable to suppose that significant information is held, may result in an order for access to be granted;

- repeated failures to respond to the EDPS or to implement his recommendations in relation to a processing operation, may result in the issuing of a warning to the controller. This could involve a letter to the Director (or senior official) concerned, and/or publicity of the failure and citation in the EDPS' Annual Report;

- collecting and retaining detailed or sensitive personal information for significantly longer than necessary or for unspecified purposes (particularly where it impacts on career prospects), may result in an order for erasure or destruction;

- unanswered concerns or doubts as to the lawfulness of the processing may result in the EDPS imposing a temporary or definitive ban on the processing;

- deliberate unauthorised disclosure of or access to personal data may result in a referral to the European Parliament, Council, Commission or in certain circumstances even to the Court of Justice, as well as subsequent publicity.

3.4.2. Action unlikely

- “Accidental” non-compliance with the provisions of the Regulation which is acknowledged and followed by prompt, effective remedial action;

- Non-compliance which is not particularly intrusive and has not caused significant detriment, unless it would raise larger issues;

- Non-compliance where other pressures such as negative publicity and damage to reputation, may be swifter and more effective than formal enforcement action by the EDPS.

4. Transparency and publicity

The EDPS believes that transparency in relation to his activities is important both for his stakeholders and in terms of good governance. He therefore makes relevant information available on the EDPS website and in his annual report. He also uses press releases to highlight important actions, decisions and opinions, and to bring attention to significant contemporary issues in the area of data protection.

In relation to his enforcement activities, the EDPS will normally publish information regarding any official referrals he makes to the Parliament, Council, Commission or EU Court of Justice. In addition, he will consider, on a case-by-case basis, whether it is appropriate or beneficial to publish information via suitable media in relation to any of the other enforcement actions outlined in section 3.2 above.

Where the EDPS intends to publish or publicise details or summaries of his formal enforcement actions, he will inform the relevant institution or body beforehand to enable them to consider and prepare a public response if they feel this is appropriate.