Advice paper on the practical implementation of the Article 28(6) of the Directive 95/46/EC

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 06/036.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Analysis of the Article 29 Working Party on the practical implementation of the Article 28(6) of the Directive 95/46/EC

The Commission has asked the Article 29 Working Party to provide an an answer to the following question: How do DPAs make use, in practice, of article 28(6) of the Directive? Is its implementation currently problematic and, if so, how could it be improved?

The legal context for the analysis of this question is defined by both Directive 95/46/EC, and by Convention 108, which dedicates 5 articles and a substantial part of the explanatory memorandum to international cooperation. Article 28(6) reads as follows: "Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred to it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State. The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information."

As follows from the application of article 4(1)a of Directive 95/46/EC, and as can be inferred from its wording ("whatever the national law applicable to the processing in question"), article 28(6) aims at bridging the possible gap between applicable law and supervisory jurisdiction, in such cases where the territorial scope of a DPA does not coincide with the applicable law of the country of jurisdiction.[1]

There are complex and problematic aspects to the implementation of article 28(6) Dir 95/46/EC. There are different forms of involvement of various DPAs: DPAs have some experience with joint investigations, where each applies its own law in its own jurisdiction. In practical terms, these are most probably the easier forms falling under article 28(6) of the Directive. The main issues here are issues of cooperation (information sharing, practical cooperation and secrecy obligations etc) and the more complex procedural question of ensuring a harmonised approach.

Furthermore, DPAs ask each other to provide assistance in handling cases. That may happen, for example, when they need to gather information from sources outside their own jurisdictions, in order to carry out a proper analysis of a specific case. In general terms, DPAs evaluate such existing cooperation in a positive way, mainly due to the goodwill of their colleagues from other MSs to provide assistance. Cooperation, however, is carried out mainly on an informal basis: as can be deduced from a consultation recently carried out (see the Addenda), most of DPAs have not established specific procedures to deal with cooperation issues, nor have designated concrete contact points to more efficiently handle such proceedings. Some concerns have also been detected with regard to the language in which cooperation is conducted, to the fact that time limits differ from one country to another, and even to the lack of response in some specific cases.

Legally, the situation will be more complex when jurisdiction and applicable law do not coincide. This is the case when DPAs will need to apply their own procedural/ administrative law, while the material aspects of data protection legislation correspond to another Member State. The main issues here are of a legal nature (what is the applicable law with regard to the

[1] See in this respect the Opinion 8/2010 of the Article 29 Working Party, on applicable law.

material processing, but also what is the applicable law with regard to the procedural aspects), and of a procedural nature (what are the respective roles, responsibilities and powers of each DPA involved, the application of sanctions, etc).

In the current context, where data protection issues become global, it is expected that cooperation matters under art. 28(6) increase in the coming years, both in number and complexity. At the same time, and although up to now bilateral cooperation is the general trend, multilateral cases will be ever more common in future. Bearing in mind these facts, ensuring harmonisation, not only of the powers of DPAs but also of the substantial implementation of the new legal framework, is of major importance. On the other hand, practical conditions, such as time limits or translation issues, are also going to have a greater impact. In that sense, existing legal texts (such as the Regulation (EC) No 2006/2004, of 27 October, on cooperation between national authorities responsible for the enforcement of consumer protection laws) could be used as reference documents in order to adequately face administrative cooperation issues in the data protection enforcement context.

This advice paper shows the most common scenarios of cooperation in which art. 28(6) is currently applied, and provides suggestions for solutions in relation to the difficulties arisen from such cooperation and from the involvement of several DPAs/ national laws. It focuses mainly on the procedural issues, thus questions related to what the applicable law is with regard to the procedural aspects of international cooperation, and issues such as what are the respective roles, responsibilities, tasks and powers of the involved DPAs. Furthermore, the advice paper addresses issues of cooperation. This advice paper intends to take as a given the applicable law (on the material aspects), since we do not know yet how the (material) applicable law regime will be in the new data protection framework. The Article 29 Working Party opinion on applicable law will be taken as a starting point.

The body of the draft advice paper discusses three different scenarios of cooperation, and the main issues that come into play under these three scenarios. We also note here that there is a fourth scenario of “vertical” cooperation between national DPAs and a European body such as the EDPS (for example in the case of Eurodac). This scenario is not further elaborated in the advice paper. The Addenda contains a report summarising the replies received to a questionnaire circulated among DPAs, which tries to reflect the current situation in this field.

SCENARIO 1
Investigation and sanctioning of a controller established in various Member States

This is a scenario EU national DPAs have dealt with several times recently, and concerns cases relating to multinational companies, and the joint investigations undertaken in the context of the Enforcement Subgroup. This scenario occurs when national DPAs undertake supervisory activities concerning a specific processing at a data controller established in their country, and other DPAs are undertaking within their jurisdictions similar investigations at the establishment of that same (internationally operating) data controller.

Main issues to be addressed under scenario 1:

Law

As the law of each Member State applies, each DPA can decide on the basis of its own national law how to apply the substantive principles, about the undertaking of supervision activities and about sanctions.

Insofar national implementations of Community data protection law differ among themselves and lead to different conclusions, the national application of the law by DPAs could seriously affect coherence across the European Union. This could be solved only by ensuring that national differences in implementation are diminished in the new framework.

CONCLUSION NO 1:
In order to ensure a uniform application of the substantive data protection principles across the EU, the new framework should reduce the bandwidth for national divergence of the substantive principles to the minimum compatible while respecting the legal culture and administrative traditions.

Sharing information and practical cooperation

There is a duty for DPAs to cooperate to the extent necessary for the performance of their functions (article 28(6) Dir 95/46/EC[2] and article 13 of Convention 108).

The current provisions have to date provided a basis for cooperation between DPAs in specific cases; the current article 28(6) of the Directive allows for the necessary cooperation between DPAs. For example, in the context of a subgroup of the Article 29 Working Party, for a particular investigation undertaken in several Member States, a coordinator was appointed, members developed a contact list of persons within DPAs involved in the investigation, an ad-hoc information sheet on the state of play of those investigations was developed, and bilaterally best practices with regard to investigation methods were shared. However, without a clear and more formalised format for information exchange and practical cooperation, up-to-date information exchange and practical cooperation remain complex in practice.

As to the legal provisions underlying cooperation, the extent of the current legal duty defined in article 28(6) of the Directive seems to be not sufficiently developed: it is formulated in very general terms, not providing for specific obligations. As an example, this provision does not oblige DPAs to engage in specific forms of practical cooperation. Neither would the current

[2] For the text of the provision, see above in the introduction.

provisions seem to involve an obligation to share information in the cases described under this scenario, which can, strictly speaking, be dealt with adequately at national level. Furthermore, it cannot be deduced from the current articles that there is an obligation for DPAs to inform – before the case is publicised – its European counterparts of the outcome of the investigations they are carrying out within their own national jurisdictions, when it could have significant cross-border implications.

In the context of the national investigations taking place, DPAs would have to ensure they exchange the necessary information with other DPAs involved, and that practical cooperation is facilitated. This would start with DPAs informing each other that they are investigating a particular case and facilitating that DPAs can reach each other quickly with their questions and information on the matter. Information needs to be exchanged on the scope of the investigation, the methods used to collect information, the time frame, what DPAs will publish on the case etc. As to practical cooperation between DPAs, there has to be agreement on the language in which documentation is shared. Furthermore, particularly in case of technically complex issues, the sharing of formats and methods used for the investigation is both useful and ensures uniformity in the analysis.

In order to facilitate information exchange and practical cooperation, more specification of the general cooperation duty of article 28(6) should be provided in the new framework. This concerns on the one hand more specification of the rules.

As to a further specification of the cooperation obligation, the Commission could consider an obligation for Data Protection Authorities to notify national supervisory cases to the other authorities and provide them without undue delay with all necessary information, when such cases have significant repercussions at EU level and/or affect the other authorities as well. Other authorities are affected, for example, when the same controller undertakes similar activities within their territories.

As to providing information on request, the Commission could consider giving DPAs explicitly the power to request other authorities to provide them without undue delay with any information that is necessary for them to carry out their tasks. Furthermore, use could be made of 13(3) of Convention 108 that states that an authority shall at the request of another authority furnish information on its law and administrative practice, and shall upon the request of that authority take all appropriate measures for furnishing factual information relating to a specific automatic processing. What exactly “all appropriate measures” are could be further elaborated.

CONCLUSION NO 2:
The Commission could consider developing rules providing authorities with the right to ask from other authorities all relevant information and cooperation, and committing authorities to inform, on request and at their own initiative, other authorities without undue delay of any supervisory information that would have significant repercussions at EU level or significantly affect the other authorities.

Furthermore, the Commission should consider whether it would be useful to set up a technical system through which Data Protection Authorities can, in a pre-defined and structured manner, provide information. Depending on the type of case and the DPAs involved, specific information exchanges between specific DPAs could then take place through that system.

Such information exchange could include very specific issues such as investigation methods and technical formats and scripts used for inspections.

CONCLUSION NO 3:
The Commission should consider whether the new data protection framework should ensure the setting up of a case handling system to be used by Data Protection Authorities to exchange information and facilitate practical cooperation.

The extent to which the exchange of information is limited by confidentiality obligations needs further clarification. Article 15 (1) and (2) of Convention 108 provide safeguards for the sharing of information between DPAs, with regard to the prohibition to further use, and ensuring the appropriate level of secrecy. As to the sharing of personal information, Directive 95/46/EC – and its successor – applies to the exchange of information. These measures are sufficient to ensure that sharing of information can take place in principle. Clarification is however needed on the extent of information that can be shared, and the authorities with which information can be shared.

Furthermore, the use that DPAs can make of the information received also deserves particular attention. It should be clarified whether this information could be incorporated into a specific procedure, even as factual basis for decision-making. And subsequently, it would be desirable to consider strengthening its evidential value, for example by presuming its accuracy to the same extent that the information obtained by national officials in the context of an investigation has. DPAs should also keep this information as secured and confidential as the records they collect in the performance of their supervisory duties.

CONCLUSION NO 4:
More clarification is needed on the extent to which national confidentiality obligations could limit the duty to exchange information and practical cooperation.

Procedure
In light of the vast increase of cross-border data processing, the need for a uniform application of national laws within the EU, in particular in the types of supervision and enforcement cases, becomes ever more pertinent. Even if the substantive principles of the EU legislation would be sufficiently harmonised, and the exchange of information and practical cooperation between DPAs would function properly, the fact that some DPAs can use their margin of appreciation for deciding if and how to deal with a particular case, can also result in the EU data protection principles being applied differently across the EU.

For example, because of predefined criteria, such as the number of complaints, the subject matter or the amount of detriment, some DPAs might not find it opportune to start an investigation, whereas others do. Furthermore, in their investigations, DPAs can focus on different aspects of the same issue. DPAs could also come to different conclusions as to the legality of the processing, or evaluate differently the need for sanctioning. If different appreciations by DPAs of cases with a cross-border, EU dimension, occur at a regular basis, it could have serious ramifications for the credibility of the EU data protection framework, both within the EU and at a global level. It makes the framework unnecessarily vulnerable for criticism and could ultimately undermine the strength of the EU data protection framework, both within the EU and towards other countries.

It is of utmost importance to the effective and harmonised implementation of the new framework that the above mentioned aspects of cross-border cases are coordinated at EU level. A solution should thus be sought in facilitating and ensuring closer coordination between DPAs. At a basic level, the Commission could in this context consider developing specific rules, such as an obligation for DPAs to inform other authorities that could be affected of its reasons for a decision to start (or not) an investigation, and to consult with the other authorities with regard to that decision, while introducing appropriate and realistic deadlines in order to guarantee that the consultation process is swift enough to meet the time-limits laid down by the relevant national legislation. The same type of obligation could be developed with regard to the decision on the legality of the processing and the decision on sanctioning: here as well, there should be a duty to consult with DPAs that are affected by that decision.

In order to ensure a harmonised approach towards the investigation across the EU, further rules could be developed. DPAs could be required to seriously endeavour to take up cases with repercussions at a cross-border level. As to coordination, DPAs could be required to seek to conduct simultaneous investigations and enforcement measures.

Furthermore, possibly a more effective form of coordination, through collective decision making, could be envisaged. This collective decision making could consist of delivering a joint opinion on the cross-border supervision case. In this context, the Article 29 Working Party could play an important role. Its aim should be to stimulate coordination of supervisory activities and cooperation between supervisory authorities in these situations, and its position vis-à-vis the national domain should be strengthened to ensure that. Currently, the Working Party delivers opinions on matters in more general terms. One could foresee a situation where the group delivers opinions on concrete cases.

Furthermore, the legal nature of these opinions and its influence on the national level should possibly be clarified and reinforced, while respecting the independence of DPAs.

CONCLUSION NO 5:
The new regulatory framework could specify that DPAs should act consistently with the opinions of the Article 29 Working Party, or explain why that is not possible.

Furthermore, the Article 29 Working Party could play a more operative procedural role. The following approach could be envisaged: in case a significant number of members of the Working Party cannot agree on the supervision strategy in a case that has repercussions at an EU level, the Working Party could be asked to issue a written opinion on the case. The Working Party could be given the power in this context to explicitly ask DPAs to undertake an investigation. Furthermore, there could be a provision allowing authorities to report to the Working Party recurrent difficulties concerning cooperation and coordination in these cases, including a request to issue a written opinion on the matter. If authorities would decide not to follow the coordination agreed between authorities, or the opinion of the Working Party, they should inform the Working Party without undue delay of this decision, and of the reasons for it.

CONCLUSION NO. 6:
The Article 29 Working Party should support the coordination among DPAs as to concrete cross-border investigations.

SCENARIO 2
Handling complaints where the data controller is established in another Member State

This scenario broadly covers two different situations. On the one hand, traditionally, this scenario is related mostly to relatively "simple" complaints of individuals involving two DPAs, for example in cases of cross-border direct mailings. On the other hand, nowadays this scenario will occur more and more in the online context, where data subjects resident in one or more Member States make use of, and have a complaint about the data processing of, a service or application provided by a multinational company operating throughout Europe but having its place of establishment in one of the EU Member States. More and more, therefore, scenario two will involve more than two DPAs and covers potentially "big" data protection breaches, in terms of numbers of complaints, the controller involved, the matter at hand and the societal stir about it. This type of situation is likely to involve broader data protection policy issues. The second situation under scenario two thus differs from scenario 1 in the fact that the controller is only established in one Member State, but the data subjects are resident in several Member States.

We start from the presumption that the applicable law is the law of the place of establishment of the controller (rather than law of the place of residence of the data subject or the country which the service provided by the controller is targeted to).

Main issues to be addressed under scenario 2:

Practical cooperation

First and foremost, in an increasingly complex on-line environment, where it is increasingly unclear for data subjects who is the controller for what part of the processing, it should not be in the hands of the data subject to find out where to exercise his rights. Data subjects should therefore always be allowed to turn to their own DPA and ask the DPA to take up the matter, in case that such complexity creates problems in exercising their rights. Convention 108 of the Council of Europe has already provided some basic rules in this regard that could also be envisaged in the new data protection regulatory framework. In particular, it provides for the right to use one's own authority, and provides the basic information elements that authorities should exchange in the case of assistance in cross-border cases (see article 14, annex 3).

In the context of the so-called "Case Handling Workshop" under the aegis of the Spring Conference of European Data Protection Authorities, several years ago a cooperation form was developed. The function of this cooperation form was to structure the information exchange between two DPAs involved in a cross-border case, and at the same time to inform other DPAs of the case at hand, so that it could be verified whether the case was a broader issue across the EU. The formalisation of the use of such a form, through a case handing system (see conclusion no 3) could be envisaged in the new framework.

Procedure: possible difficulties in upholding EU citizens' rights

In both the traditional and the modern day situations under scenario two, as the material law of the Member State of the place of establishment of the controller applies, it would be logical to consider that that DPA is the "lead DPA". As lead DPA, it would decide about matters such as whether or not supervision activities ought to be undertaken, the application of the substantive principles, and about sanctions.

However, in such cross-border cases, the decisions on the processing of personal data by the controller, and the decision of the DPA on the action to be undertaken, have consequences in the other EU Member State(s) involved. So, from both an applicable law as from a jurisdiction perspective, for the exercise of their rights, citizens of other EU Member States are dependent upon the situation in a particular Member State, which could lead to an unbalanced application of rules across the EU.

Under situation one, this could entail for example that a complainant has to be informed his case is not dealt with, because the foreign lead DPA does not deal with (particular types of or all) "simple" complaints, or the result for the individual is different from what he would have expected under his own national law. Differences in supervision for relatively small and simple complaint cases could be justifiable from a perspective of the margin of appreciation of DPAs, and the bandwidth that exists for national data protection law.

However, in case of more complex and bigger complaints as described under situation two, the ramifications for a consistent and uniform EU data protection regime of the decisions of the lead DPA are potentially bigger and more harmful. One particular implementation of EU data protection law could thus have broader, unbalanced, policy effects throughout the Union.

To ensure a harmonised EU approach, in such situations, the possibility should be considered to guarantee that the other involved DPAs have a role in the decision making process.

A more effective form of coordination, through collective decision making, could in such cases be envisaged. As explained above under scenario 1, the Working Party could play an important role here, both as to deliver a joint coordination opinion on the cross-border supervision case, as in a more operative procedural role (see above).

One could also imagine that discussions arise as to who is the supervisor best placed to lead the investigation. The Working Party could also provide an opinion on these matters and ask the authorities to accept that the one is better placed than the other to lead the investigation.

SCENARIO 3
Collecting factual information and evidence of data processing for another DPA and imposing sanctions

This scenario covers situations where one or more DPAs are asked by another DPA, undertaking an investigation into a controller established on the territory of its Member State, to gather facts and evidence for its investigation. This situation could occur for example when servers of the controller are established in other Member States. A concrete example of this is the Swift case, where WP29 concluded that the controller was established in Belgium, whereas the servers were run in the Netherlands. This situation also occurs when the controller makes use of a processor in another Member State. The imposition of sanctions could consist of blocking the processing of personal data, erasing certain data etc. This situation has not occurred yet in practice. The analysis will therefore be "theoretical", and will need further refinement if and when more concrete experience has been gained under this scenario.

We start from the presumption that the substantive applicable law to be applied by all DPAs involved would be the applicable law of the Member State of establishment of the controller

(rather than the law of the Member State where the processing takes place or where the processor is established, or the law of the place of residence of the data subject or the country which the service provided by the controller is targeted to).

Main issues to be addressed under scenario 3:

Law

Although the law of the requesting DPA applies from a substantive point of view as to procedural matters, the laws of the other DPAs should be applied in their Member States to the enquiries and investigations they might carry out as a consequence of the request. In this situation, it could be difficult to draw the line between the substantive law and procedural matters, and it seems necessary to establish criteria to strike an adequate balance when these are in conflict.

Procedural matters would be all matters related to the power of supervision and investigation of the DPA. This includes the territorial and substantive scope of the supervision powers, the criteria under which investigations can be undertaken, the types of supervisory activities that are allowed, the sanctions that can be applied, and the administrative arrangements such as possibilities for objection and appeal.

Practical cooperation and information exchange

It should be ensured that DPAs provide to other DPAs the necessary assistance, in order for other DPAs to be able to carry out their national priorities. To this end, as a specification of the general cooperation obligation of article 28(6) of the Directive, the new legal framework could provide for more specification of the obligation to provide assistance. Convention 108 provides a basis for that. Article 13(1) provides that "The Parties agree to render each other mutual assistance in order to implement this convention." Concretely, this should mean that DPAs would be in principle obliged to undertake an investigation, to gather the required information and furnish it without undue delay, and undertake on-site inspections if these are required for the investigation.

Procedure

How should DPAs cooperate in a situation where jurisdiction and applicable law do not coincide? The DPA of the Member State of the controller should be the "lead DPA" in the decision making process, as that DPA undertakes the investigation and makes the decisions about the application of the material principles and about investigation and sanctions. However execution of those decisions could have to be done by other DPAs. This could however be problematic in case of differences in powers between DPAs and in the case of the application of sanctions.

If sanctions have to be executed in the territory of other Member States (eg blocking the processing of data), the DPA of these other involved Member States should have a legal basis certain enough that empowers it to properly execute those sanctions. Once again, possible problems could rise from combining substantive law and sanctions of another Member State with the procedural law of the DPA's own country. Complexities are also envisaged in case decisions are objected to in court, also on substantive grounds. It might be appropriate to explore whether the drafting of unified criteria for mutually enforcing decisions adopted by other DPAs at a domestic level is feasible.

As to differing supervision powers, if DPAs are requested to undertake particular actions, for example, to do an on-site inspection in a particular case, they should have those powers at national level. However under the current data protection framework, not all DPAs have the same and effective powers of supervision and sanctioning powers.

CONCLUSION NO. 7:
It is therefore essential that the new data protection framework ensures harmonisation of powers of DPAs. These powers should include at least:

- The power to have access to any relevant information, in any form, and to require the supply of all relevant information by any person;
- The power to carry out compulsory on-site inspections;
- The power to require the cessation or prohibition of any data processing;
- The power to apply financial punitive sanctions for breaches of data protection law;
- The power to publicise the decisions taken by the DPA

Furthermore, it should also be borne in mind that those powers will only contribute to ensure a better coordination if they are implemented in practice. In that sense, DPAs should have sufficient resources to properly exercise them for those cases requiring international cooperation, whatever the relevant scenario, and this should also deserve the Commission's attention.

Aside from providing the possibility to execute the enforcement request of another authority, the new framework should also stimulate DPAs to indeed abide by the requests of other DPAs in this context. To this end, the Commission could consider inserting in the framework provisions stating that authorities shall take all necessary measures to execute the enforcement requests of other authorities, and that they shall to that end exercise the powers granted to them. The involved DPA would also need to have an obligation to consult each other on the enforcement measures, within appropriate and realistic deadlines in order to guarantee that the consultation process is swift enough.

Concluding summary

- As the first priority, it seems appropriate to struggle to avoid divergences in application and ensure smoother cooperation: first and foremost, need for a strong harmonising effect of the new EU legislative framework, both as to material principles and as to powers of DPAs.

- Develop in the new framework more specific rules for the exchange of information and practical cooperation: duty to inform each other of cases which affect other DPAs, duty to exchange all relevant up-to-date information on those cases with the relevant DPAs, duty to consult the relevant DPAs before taking a decision affecting those DPAs, duty to inform each other before publicising decisions made.

- Investigate possibilities for additional forms of international cooperation in cases of cross-border supervision and enforcement cases, including compulsory procedural duties. Investigate the possibilities of strengthening the role of the Article 29 Working Party in this regard.

- Explore the practical implications that may result from such cases in which applicable law and supervisory jurisdiction do not coincide, from the point of view of cooperation. In that sense, use the experience from established practice in other fields, such as consumer protection.

- Consider developing article 28(6) in a more detailed and specific way, in order to clearly cover existing issues, not leaving cooperation duties up to excessively restrictive interpretations.

- Analyse how practical issues, such as time limits or translation of documents, may be improved in order to facilitate cooperation. In that sense, the fact that small DPAs could have difficulties to deploy sufficient resources to deal with issues requiring international cooperation should also be taken into account, e.g. by stating international cooperation among their statutory powers, in order to ensure that they receive adequate funding to perform this task.

- For situations of (amongst others) joint investigations, establish better practical cooperation mechanisms between the DPAs.

- Provide clarity on the extent to which information can be shared between DPAs.

Done at Brussels, on 4 April 2011

For the Working Party
The Chairman
Jacob KOHNSTAMM

Addenda

Introduction

The Article 29 Working Party received, last October, a letter from the Commission requesting our opinion on three specific issues linked to the review of the European data protection legal framework. One of these issues is how national DPAs make use, in practice, of Article 28.6 of the Directive, whether its implementation is currently problematic or not, and how could it be improved.

As a result of the meeting of the Future of Privacy subgroup, held in Brussels on 12 November, the Working Party prepared and circulated a questionnaire on this topic. 25 replies were received, which can be summarised as follows:

Detail of the contributions

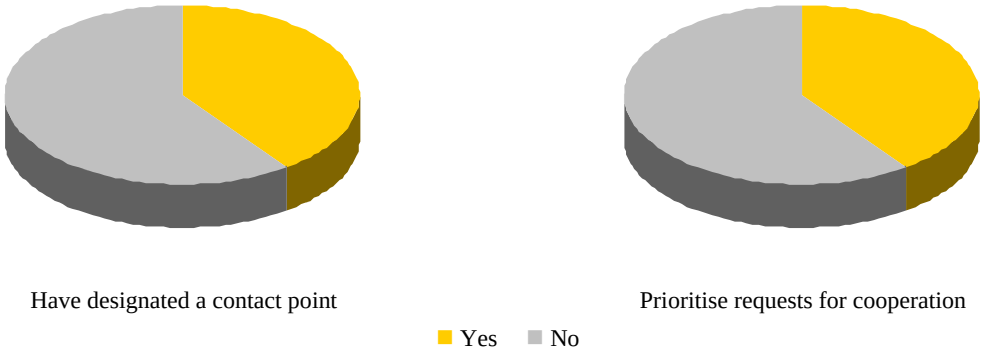
1. Practical use of Article 28.6

Virtually all DPAs have made use of Article 28.6. The amount of situations described, however, varies significantly from one Member State to other. Most mentioned countries are Spain, France, Germany and the United Kingdom.

2. Procedural issues

Only a small number of DPAs (concretely, 2) referred to have established specific procedures to deal with situations in which international cooperation is required. The rest of Authorities handle this kind of issues as they do with national ones. In that sense, just 8 DPAs have designated a contact point within their organisation, and the same number prioritises requests of cooperation lodged by DPAs from other Member States.

English is used as the cooperation language by all the DPAs that have answered this question. In any case, a pragmatic approach is applied, especially in relations between countries that share the same or a similar language (i.e. Belgium and the Netherlands, or Slovakia and the Czech Republic). Some DPAs have procedural restrictions that compel them to issue every decision in their national language, but they usually enclose a courtesy translation into English when sending information to their foreign colleagues.



3. Applicable law
Three main scenarios have been identified:

- The most frequent case happens when a complaint is lodged to DPA 1, with regard to a processing carried out by a controller based in the jurisdiction of DPA 2. In this case, DPA 2 usually applies its national law.

- Other common situation occurs when there is a request for cooperation by DPA 1, which is conducting a national investigation on the activity of a controller, in case that some evidences may be found within the jurisdiction of DPA 2. In this case, the law of DPA 1 is usually applicable.

- The third scenario takes place when a controller is established in several Member States, and consequently there are several applicable laws and jurisdictions. Each DPA should handle its own proceeding, but coordinating its activity (as far as possible) with its foreign colleagues.

Any response has been received describing a situation in which a DPA applied other Member State's law as a legal basis to issue a decision; indeed, some DPAs underlined this fact.

4. Role of the affected parties
Taking into account that the first scenario is more common than the others, in case of requests received from other DPAs, the party about which cooperation is requested is more likely to be a controller. On the contrary, in case of requests sent to other DPAs, the requesting party is normally a data subject. Processing carried out by information society service providers are the most referred ones, normally for direct marketing purposes.

5. Tasks carried out by the DPAs
The procedure is carried out in a very similar way:

- In case of incoming requests, DPAs check the applicability of their national laws to the specific case and then act in the same manner as with national complaints.

- In case of outgoing requests, DPAs verify the un-applicability of their national laws and try to identify the relevant foreign law, in order to request cooperation.

In both cases, DPAs share the relevant information with their foreign colleagues.

6. Efficiency of the current cooperation regime
In general terms, all DPAs that have answered the questionnaire appreciate the goodwill of their colleagues, and evaluate cooperation received in a positive way. However, some concerns have been raised regarding the lack of harmonisation among Member States, which in some situations could hamper an adequate protection of citizens.

7. Information sharing
All the DPAs have stated that, in general terms, they have no problem to send information to (with limitations, in some specific cases) or to use the information received from their counterparts within the framework of Article 28.6. Some of them, however, have pointed out that they are using Convention 108 as a legal basis for doing so, alleging that it is more certain from a legal standpoint.

8. Identified problems

Many DPAs have not identified any problem on applying this article. On the other hand, the rest of DPAs have highlighted a number of issues, such as follows:

- Lack of harmonisation with regard to investigation powers

- Lack of harmonisation with regard to substantive law

- Necessity to state a duty to reply and to inform about the outcome of the proceeding when a request for cooperation is lodged.

- Difficulties with respecting deadlines

9. Foreseen challenges

The following issues should be underlined:

- Problems derived from the aforementioned lack of harmonisation.

- Possible conflict of laws, which could arise from the increasing cross-European processing activities, especially when dealing with entities based in several countries.

- The possibility of appointing a lead DPA, to reinforce the role of the Article 29 Working Party or to draft FAQs has been suggested.

- Difficulties to enforce foreign data protection law at domestic level, and to execute decisions taken by other DPAs.

- Increasing number of cases in which cooperation will be necessary.

- Difficulties to small DPAs to deploy sufficient resources to deal with issues requiring international cooperation.