Advice paper on notification

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

Table of contents

1. Introduction 3
2. The current system 3
3. The future legal framework 5
3.1. Responsibilities and obligations under the future legal framework 5
3.2. The role of notification 5
3.3. A revised and simplified approach 8
3.4. A harmonised approach 13
3.5. Other considerations: exemptions and data protection officers (DPOs) 14
4. Conclusion 15

1. Introduction

The European Commission asked the Working Party to provide an opinion on the following question: how could the current notification system (Articles 18 and 19 of the Directive) be simplified and harmonised in order to limit the administrative burden for data controllers, while at the same time continuing to ensure effective protection for data subjects?

Notification cannot be considered in isolation; it must be looked at against the broader picture of effective data protection supervision, and its aims and how it is used. The Working Party previously looked into the various national notification systems in 2005 and the conclusions of its report (WP 106) are still valid today. It is clear that notification has been used in various ways by data protection authorities, organisations and individuals. This advice paper will set out some practical experiences of notification under the current Directive, and then suggest a revised and simplified approach for the future data protection legal framework.

2. The current system[1]

As was reported in WP 106, there are different approaches taken in member states. Some national laws provide for exemptions (when you don't need to notify); some provide a 'positive' list (when you do need to notify).

Those providing for exemptions do have some in common, such as those provided for in articles 18 (3), (4) and (5) of the Directive. Each national law provides for exemptions specific to the national situation.

The following information and figures are from information provided by 25 European data protection authorities.

In eight member states notification has a cost, and this provides some or all of the income for six of the data protection authorities. The fee charged ranges from €23.29 to €598.86. Some member states vary the fee depending on whether the data controller is a natural or legal person; is public or private sector; by numbers of staff and turnover; or by method of notification (paper or online). Two member states charge a fee for amendments to the notification. In some member states the fees are a one-off charge, in others they are an annual charge.

Six data protection authorities provided figures for the total annual revenue from fees, and this ranges from €9,855 to €15,795,000. For those who receive an income from fees, this ranges from 1.2% to 100% of their budget. In the eight member states that charge a fee, six data protection authorities collect this fee directly and receive an income from the fee; one authority collects the fee but then sends it to the Government and receives no income from it; and one authority does not collect the fee as it is paid directly to the Government by the data controller.

[1] See annex 1 for a summary of DPA responses to questions about the current system.

Data protection authorities make different use of the information they receive through notification. The most frequent uses are for inspections and audits; to contact the data controller; and as a transparency tool to assist or inform individuals. Authorities also use the information for prior checking; to issue opinions, instructions, guidance and so on; in complaints handling; and as an education and awareness-raising tool for data controllers.

In terms of the actual details provided through notification, data protection authorities find the purposes of processing and data categories to be the most useful information. Some DPAs find the description of security procedures to be the least useful information. Six authorities stated that all the information was useful; and four authorities stated that none of the information was useful.

Many authorities ask organisations for further information if needed and several have created template notification forms for specific sectors or types of processing, as well as standard wording or predefined fields on online forms.

Fifteen authorities link notification to prior checking, and 17 charge a fee for this activity. Several authorities stated that their national law mandates specific circumstances where prior checking is obligatory.

As previously mentioned, some authorities see notification as a useful transparency tool for individuals. However, many authorities do not collect information or statistics on the use made of the notification register, and those who do are not able to distinguish between use by individuals, by organisations, and by their own staff. The register is not directly accessible to the public in two member states. Data protection authorities vary in their opinions on how widely the register is consulted in their country.

The law enforcement sector is subject to notification requirements in 19 member states. In the six member states where they do not need to notify, this is either due to exemptions in the national data protection law or the existence of separate legislation to regulate processing by this sector.

In conclusion, the current systems of notification across the EU are quite varied and many differences arise from the specifics of the national law. Data protection authorities have many and varied uses for the information provided through notification, and by far the most common use is for enforcement activity. There are differing opinions on the usefulness of the notification register and its information for both individuals and other organisations, with some authorities reporting high levels of consultation and some reporting very little, if any, consultation of the register.

It is clear that for data protection authorities it is generally important to know and understand the purposes of the processing and the data categories, whereas they do not generally feel it is necessary to have details of the security measures organisations take.

As regards fees and income, a minority of member states charge for notification, but for those that do the situation is extremely varied, with some authorities receiving no income from the fees at all, and others receiving significant income. The Working Party does not intend to discuss different funding mechanisms in this advice paper, but is available to provide more information on this if required.

3. The future legal framework

Before considering how a notification system might work in a future legal framework, it is important to consider why such a system might be necessary, and where it fits into the broader picture of effective data protection supervision. What are the aims of notification and what purposes does it serve, for the data protection authority, the organisation and the individual?

3.1. Responsibilities and obligations under the future legal framework

Under the current legal framework, organisations have certain responsibilities and obligations to ensure they are compliant, and these will remain and be strengthened in the future legal framework. The Working Party has previously called for action to ensure that data protection requirements translate into effective mechanisms that deliver real protection.[2] In particular, it has called for an accountability principle to explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations of the Directive and demonstrate this on request. To be able to meet this requirement, organisations need to know and understand the details of their processing and the measures taken. This 'inventory' is a crucial first step for an organisation to be able to meet its responsibilities and obligations, and to demonstrate on request how it has done so.

Assuming that this requirement is in place, when and what information about their processing and measures should the organisation then notify to the data protection authority? Should the organisation be required to notify this information to the authority before data processing starts? What level of detail should the organisation provide?

Data protection authorities also have responsibilities and obligations under the current Directive, and will continue to do so under the future legal framework. Authorities have different views on what constitutes effective supervision, based on their national experiences, which in turn are affected by the legal, political, social and economic backdrop against which they regulate. It is clear that the information from notification is currently used in different ways and for different purposes.

Is it the task of the authority to approve processing operations? How does notification of information to an authority fit into their approach and strategy for effective data protection supervision? These questions are considered later in the advice paper.

3.2. The role of notification

This section of the advice paper looks at what role notification might have for individuals, organisations and regulators. Determining the role should help in developing a revised legal framework that meets the needs of all actors.

[2] In opinion WP 168 on the future of privacy, and in opinion WP 173 on accountability

For individuals

Individuals often do not have or feel they have control over who is using their personal information and for what purpose. Individuals want to know that organisations are looking after their personal data and not misusing it or disclosing it to others in a way they would not expect or want. Transparency is crucial to achieving this.

It has been argued that the notification register is a tool for achieving this transparency. However, the Working Party considers that while this may have been the case when the Directive was introduced, a public register is no longer the best and most appropriate way for individuals to understand what an organisation is doing with their personal data, and who to contact when things go wrong.

Where individuals have a relationship with an organisation that is processing their personal data, the organisation has an obligation to provide information directly on what data is held and being used for. Even in areas such as law enforcement, credit referencing and so on, where individuals do not necessarily have a direct relationship with the organisation, individuals are better served through existing and enhanced transparency measures. When things go wrong, individuals usually contact the organisation using information previously provided to them or obtained online.

Although some data protection authorities do see the benefit of a register for individuals, it is not necessarily the case that this mechanism can offer effective protection. Individuals should have more meaningful information about what an organisation is doing with their personal data and it is likely that this can be better provided in other ways directly by the organisation. Any requirements in the revised legal framework for organisations to demonstrate compliance and accountability should help reinforce a data protection culture in the organisation, which of course in turn benefits individuals. Organisations should see a competitive advantage in making it known publicly that they take appropriate data protection measures, and there is scope for this kind of proactive disclosure benefitting individuals to a greater extent than will ever be the case with the current notification system.

For organisations

Organisations processing personal data need to take appropriate steps to ensure they comply with relevant legislation, but they also need to be able to demonstrate this compliance to others, such as individuals and the regulator. Organisations who have gone further than the letter of the law also want to show that they are taking data protection seriously and will expect less attention from the regulator as a result. However, they also want to minimise the administrative burden that arises under the current Directive where many have to fill in a different form (or several forms) for each data protection authority, which takes time and resources.

Organisations may use different methods to demonstrate compliance and accountability to regulators from those they use for individuals. It has already been established that the current notification system is not the most appropriate tool for organisations to demonstrate compliance and accountability to individuals. It can be argued that the current system also does not provide adequate evidence for the regulator, as the information provided relates to broad categories and is quite vague. Whereas regulators need context-specific information where there are risks to individuals. Organisations need to be proactive in providing relevant

evidence to the regulator, as data protection authorities have limited resources and are not able to seek all the relevant information directly from organisations themselves. This is particularly relevant where the organisation is carrying out processing activities that pose risks to the fundamental rights and freedoms of individuals.

Notification has a positive role for organisations as it is often a starting point for a company to identify where data protection fits into their business and its importance. It raises awareness and helps the company spread a positive privacy culture within the organisation. To provide the information requested by the regulator an organisation has to examine its processing and this helps understand what personal information an organisation holds, which is an important first step to getting the data protection aspects right.

It also has a role in enabling an organisation to identify to the regulator who has responsibility for privacy and data protection, as well as provide meaningful information on what processing they are carrying out. It enables organisations to easily provide details on different aspects of their use of personal data (such as the nature of data, retention periods …), along with specific information as evidence to demonstrate compliance and accountability. This could include information on what internal policies the organisation has, whether they have carried out any PIAs and their results, whether they have BCRs or model clauses in place for transfers, in short – how they do data protection in the organisation in a way that complies with the legislation and shows they take it seriously.

Responsible organisations document the steps taken to ensure compliance as well as other measures that go further than the legislation requires. Many organisations regularly assess and review data protection measures, and in some sectors there is frequent change often driven by advances in technology and new ways to use personal data. However, under the current notification system, the information requested by the data protection authority can be quite different from that generated by the organisation itself and often requires the organisation to spend time and resources collating the details. Once the notification form is filled in, it is often forgotten about until there are significant changes or it has to be renewed.

Data protection authorities are in favour of a notification system that allows organisations to easily provide relevant and meaningful information to demonstrate compliance and accountability. Under the current system, many authorities have to request additional information from the organisations to be able to make decisions about compliance, supervision, enforcement and so on. Authorities are particularly concerned to have information about processing likely to pose risks to individuals.

For data protection authorities

To identify the role of notification for data protection authorities it is important to ask what information they need to carry out their role effectively. It is necessary to consider what roles the authority is required to carry out. It is clear that different authorities focus on different aspects of their regulatory remit and are guided by their national law, and the cultural and social backdrop against which they regulate. The Working Party considers that authorities generally have a role to play in supervision, enforcement, education and awareness raising, and resolving complaints. On this basis, to carry out these roles effectively, they need to know who they regulate and how to contact them. They also need to know about processing activities likely to pose risks to the fundamental rights and freedoms of individuals; and to have early sight of these activities and to be able to act accordingly. In addition, they need to

be able to request more information on processing activities and data protection measures in place; and to have sufficient and adequate information / evidence to take forward complaints and enforcement.

Notification can have a role in enabling an authority to know who they regulate - this is the 'know your customer' idea; how can an authority supervise organisations effectively if they are not visible? Knowing who processes personal data in a jurisdiction allows the supervisory authority to assess the national situation and allocate regulatory attention and resources accordingly. It allows them to contact the organisation about complaints, target newsletters and guidance, and know where to direct enforcement action. It also allows collection of a fee, if this is required. In short, it is a platform for client relation management.

Notification clearly has a role in enabling authorities to obtain meaningful information about processing activities where there are risks to individuals. Having this information allows authorities to carry out prior checking requirements if needed, as well as to better target organisations who are not taking data protection seriously. It allows them to assess whether they need to target certain organisations, sectors or types of processing at national level. The authority is also able to identify trends, such as new uses of technology, and to better predict where complaints might arise or where they might need to focus enforcement activity. Authorities should be able to identify whether any businesses would benefit from sectoral help, such as codes of practice or sector-specific standards, and work with business to achieve this.

3.3. A revised and simplified approach

Once the needs of authorities, organisations and individuals have been identified, the important question to ask is whether a notification system is appropriate to meet these needs, and how it might do so. This section of the advice paper aims to look at these questions and considerations and, where possible, provide options for solutions. However, there are many factors to consider and further work is needed in some areas. What is clear is that the notification system in the future legal framework needs to be revised and simplified to ensure it is fit for purpose and reduces undue burdens on both organisations and regulators.

As regards individuals, the Working Party considers that a notification system is not a useful or appropriate tool to provide information and transparency. Individuals are better served by other existing and enhanced transparency tools, such as privacy notices and strengthened rights.

For organisations, the current system is a way to provide more information to regulators and other interested parties on their processing activity; but there are questions over how useful a tool the current system is for this purpose. If the information provided was more meaningful, it would be a more useful tool for organisations to demonstrate compliance and accountability.

For data protection authorities it is important to be able to contact organisations processing personal data, and to have relevant, specific information about processing likely to pose risks to the fundamental rights and freedoms of individuals. It is also important to have information on the data protection measures taken by organisations.

A basic registration system

Data protection authorities favour a simplified approach that reduces burdens and focuses on processing that is likely to pose risks to the fundamental rights and freedoms of individuals. As such, they are generally not in favour of maintaining a mandatory basic registration system, particularly where this does not currently exist at national level, as this would impose additional burdens on business. However, some authorities see the benefit in keeping a single register of those they regulate and their contact details; whereas other authorities believe they can easily obtain this information elsewhere from other registers and databases.

Any future legal framework could provide for either:

- a mandatory basic registration system (or client register); or
- an obligation for authorities to know who they regulate, while leaving how this is done to national law.

Clearly the first suggestion would lead to greater harmonisation than the second, but is likely to impose additional burdens on both business and the regulator in some member states. The second suggestion would give authorities the flexibility they require to establish a 'client register' if they feel this is appropriate. However, it could lead to a situation where organisations are required to notify basic information in some countries and not in others, which would not achieve the Commission's stated aim of harmonisation. Furthermore, while it may lead to a reduction of administrative burdens in some member states, it would lead to an increased burden in others.

If a basic registration system is envisaged, the information provided by organisations should be limited to contact details; an indication of the nature of the business; and an indication of the processing, and / or personal data held.

A system for notifying risky processing

Data protection authorities believe a notification system for risky processing activities is a proportionate measure to meet their needs. However, further work is needed to define risky processing with reference to both types of data and purposes of processing. The experience of those authorities that have already taken steps in this direction can be a useful starting point. Further work is also needed on what information organisations should provide to the authority. This information needs to be meaningful to the authority to allow them to use it for supervision, enforcement, guidance and awareness raising, resolving complaints, and other activities as appropriate.

To achieve such a system, data protection authorities are in favour of a positive list of types of data and categories of processing considered to pose risks to the rights and freedoms of individuals. An organisation processing personal data in these circumstances would be required to notify details of their processing to the authority. This would require a list of risky processing categories to be agreed and clearly set out. As society and technology develop, there needs to be flexibility to add to this list, preferably with the involvement of the Article 29 Working Party. This means that it would not be advisable to have the list as part of the revised high-level legal framework. There are various options available that the Commission should explore, one of which is an instrument that sits beneath the framework.

It is also important to consider purpose. Categories of risky processing could also specify risky purposes – this fits with the context-based approach that processing personal data in some circumstances is more risky to an individual than in other circumstances. It would also allow personal data which in a revised legal instrument might in some circumstances be considered sensitive, such as financial data, to be included without simply listing all financial data processing as risky.

The list could stat with general categories relating to 'processing operations intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct'[3], or 'processing operations likely to substantially infringe freedoms or privacy of individuals or which is likely to have a discriminatory impact on data subjects'[4]. The list could then provide more specific circumstances that present a risk to individuals.

Examples[5] could include processing of:

- genetic data (to make decisions or determinations about individuals that could negatively affect them – so, for example, it wouldn't include processing of genetic data on request of the individual)[6];
- biometric data (a distinction is needed between raw data and the biometric algorithm that represents raw data; distinctions could also be made according to purpose);
- location information when processed via electronic networks;
- information on health or sex life (where processed for: assisted reproduction, provision of health care via electronic networks, epidemiological researches, surveys of mental or infectious diseases);
- information on sex life, health, race and ethnic origin (where processed to measure and demonstrate equality and diversity or non-discrimination; and where the information is used beyond mere statistics)[7];
- personal data processed electronically for profiling purposes (that have a direct adverse or discriminatory effect on the individual);
- personal data stored in databases and processed for monitoring creditworthiness, financial risk, fraud.

The list could also include specific processing operations carried out by law enforcement agencies, as well as processing of unique identity numbers in certain circumstances or for certain purposes.

Clearly there needs to be further work on the best forum and method for discussing and agreeing on the positive list, and to how to make it binding yet easily adapted as needed. While the Article 29 Working Party would provide valuable input, under the current Directive it would not be able to provide a binding document. It has been suggested that the current Article 31 Committee arrangement might provide a suitable forum. However, experience with Directive 2006/24/EC on data retention has shown the limits of a comitology procedure as regards issues of substance rather than technical details.

---

3 Taken from Regulation 45/2001.

4 Suggestion from the CNIL.

5 Most of the examples provided by the Garante (Italy) based on their national experience.

6 For example, it is becoming more popular and cheaper to send your DNA to a company to sequence your genomes.

7 There may be a case for exempting processing to comply with national law on ensuring equality and diversity or non-discrimination.

With regard to amending this list, consideration needs to be given as to whether it could be amended at EU level, at national level or both. There are also questions of who can amend the list, how they can do so, and on what basis. Empowering data protection authorities under national law to make amendments would lead to greater divergences across member states; it would though probably be a quicker process and better able to reflect the national situation. This is particularly relevant to the treatment of sensitive data which is affected by cultural differences across member states, as described in advice paper x on sensitive data.

What information should organisations provide?

Once a list of risky processing activities has been agreed, there is the question of what information about this processing organisations need to provide when they notify. To achieve harmonisation, this will also need to be agreed at EU level and set out in a binding instrument, but one derived from the revised legal framework rather than set out on the face of high-level legislation. This is because the level of detail required would not be appropriate for high-level legislation and may need to change over time to reflect current practice. It is clear that data protection authorities need useful, meaningful information from organisations, and practical experience shows that the current categories of information required are not always satisfactory. Authorities need detail on different aspects of the processing (such as the nature of data, retention periods …), and certain information as evidence to demonstrate compliance / accountability. It would also be more useful to integrate what organisations are doing in practice to safeguard personal data with the information they provide to regulators.

Organisations could provide individuals and regulators with the same information they already have and are routinely collating from their internal governance procedures.
This could include information on what internal policies the organisation has, whether they have carried out any PIAs and their results, whether they have BCRs or model clauses in place for transfers, in short – how they ensure data protection compliance in the organisation. Data protection authorities are looking for information and evidence that shows that an organisation carrying out risky processing is taking data protection seriously and has in place appropriate measures and safeguards. There is a clear link here to accountability. An accountable organisation needs to be able to demonstrate to regulators that it is compliant and so providing this information and evidence as part of a notification procedure will assist accountability. The Working Party has already done some work in this area by developing a checklist for BCRs. This, together with the work already done globally on defining the essential elements of accountability, could inform the further work needed to identify what information organisations need to notify.

The efforts made by the organisation and the information they can provide need to be relevant and proportionate to their size and function. So, for example, a multinational company is likely to have many and complex processing arrangements, including with processors and sub-processors, large numbers of staff located in different countries, as well as sophisticated data protection measures, such as BCRs or similar group-wide policies, and specialist data protection officers or teams. Whereas a small business is likely to have a few staff, a single database and data protection concerns dealt with by the manager or incorporated into an IT role. There are also differences between the private, public and third sectors in terms of resources, technology and function.

While large organisations in both the public and private sectors might be expected to be able to provide significant details of their processing arrangements and data protection measures, small businesses would be expected to provide simple details that are likely to reflect their business decisions.[8] This approach makes demonstrating compliance and accountability scalable and appropriate to the organisation, so reducing unnecessary administrative burdens.

Data protection authorities consider that all organisations processing personal data should be compliant and accountable. Given the current system of notification in some member states, limiting notification to only those carrying out risky processing is a significant change for some organisations and could lead to some who are not required to notify believing they do not need to put the same effort into demonstrating compliance and accountability. It is important that the future legal framework takes account of this and is clear about the obligations on organisations. For this reason, accountability as a concept needs to be introduced into the revised legal framework as a requirement for all organisations, with notification being just one way in which some organisations can demonstrate accountability.[9]

When to notify and what happens after notification

Once decisions are made on the categories of risky processing and the information required from the organisation, the next step is to consider when to notify and what happens after notification. A key issue here is the role of data protection authorities and the responsibilities and obligations they will face under the revised framework.
Key considerations are whether organisations should notify before the processing starts, how to deal with existing processing considered risky under the revised framework, and whether authorities have a role in approving processing activities.

As a general rule, organisations should notify their risky processing activities before they start or as soon as possible after they have started. As the notification information should include the data protection safeguards and measures taken, the organisation should have already done the work on analysing the processing, the risks it poses and how to reduce or mitigate those risks. This may include, for example, doing a PIA or consulting a data protection authority for advice and guidance.

Depending on the approach and strategy of the data protection authority, the notification may be the first time the authority is aware of the risky processing, or it may just be confirmation of what the authority already knows. This leads to the issue of what happens after notification and what the authority is expected to do with the information it receives.

As data protection authorities vary in size, resource, and approach, there needs to be flexibility as regards the use made of the notification information. It is clear that there are wide-ranging uses made of the information under the current Directive. Authorities have developed their approach to data protection supervision over the last fifteen years based on national experience and the legal, political, social and economic situation in their country. These are significantly different among member states and this has led to authorities developing the most appropriate strategy for their national situation.

---

8 For example, rather than having extensive formal security policies and procedures, the business has decided that no staff can take personal information out of the office on portable devices.

9 There is more detail on accountability in WP 173.

As a result, and given the Commission motto of 'united in diversity', the future legal framework needs to provide flexibility for authorities to make the best use of the information provided under notification. Based on their national situation, authorities need to be able to choose the extent to which they use the notification information to approach organisations for more information; to carry out prior checking; to target advice, guidance and stakeholder liaison; to target audit and enforcement activity; to identify trends; to better predict where complaints might arise; or even to do nothing with the information.

One example of this would be that where an authority is made aware of risky processing through notification, they may choose to carry out prior checking procedures; whereas where an authority has already been consulted as part of the process, they may choose to use the information to inform audit and enforcement activities.

The Art 29 Working Party could have a role in co-ordinating activity where a pan-European organisation has been identified as presenting particular risks.

3.4. A harmonised approach

As previously identified in the advice paper, there are several aspects of a revised and simplified notification system that would benefit from harmonisation. These include the decision as to whether to maintain a basic registration system; the categories of risky processing; and the information organisations are required to provide to the regulator.

One aspect that has near unanimous support for a harmonised approach, both from regulators and organisations, is the procedure and paperwork requirements. Organisations frequently complain about the administrative burden they currently face from having to compile information for each relevant authority using different forms in different languages, and that often request different information. Organisations would prefer to only have to provide the relevant information once, rather than separately to each authority. Data protection authorities are also in favour of a more harmonised system using a common form and online submission.

The Working Party urges the Commission to investigate technical measures as to how this could work in practice. One suggestion is for a central platform with an online form where organisations provide the requested information and tick against which countries they need to notify. On submitting the form the information is sent to the relevant authorities. This would clearly require investment in a central platform or interoperability with the systems in national authorities. There are also language implications and decisions need to be made about how a harmonised system and process could work in either one or several languages. It is also worth considering options for additional information to be provided according to the member state: the need to provide any fee, specific national exemptions and so on, if such national provisions are to be provided for in the revised framework.

Another factor to consider is the frequency of notification. Currently, some national systems require notification just once; others require it annually. This is an area that would benefit from harmonisation. The Working Party considers that organisations should only need to notify once, but that regular reviews should take place with the data protection authority contacted if there are significant changes or developments. The provisions in the future framework relating to compliance and accountability should require organisations to regularly review their processing.

3.5. Other considerations: exemptions and data protection officers (DPOs)

If the notification system in the new revised legal framework is set out as a 'positive' list idea, as described earlier, then there is less need for exemptions from notification than under the current system. However, the Working Party believes that a certain measure of discretion should be left to Member States in deciding whether to exempt additional processing operations from notification or to exempt from notification to the DPA altogether – in particular if a data protection officer (DPO) is appointed by an organisation (which is currently provided for in Article 19 of the Directive). At all events, if the positive list approach is adopted along with a "European" format of notification, such additional exemptions will have to be justified appropriately and notified to the Commission, in order to ensure that divergences are fully accounted for and kept to a minimum.

Some member states currently exempt from notification organisations with a DPO, and in some member states the appointment of a DPO is mandatory in certain circumstances. The Working Party has taken note of the Commission's intention to consider introducing a mandatory requirement to appoint a DPO as a measure to strengthen data controllers' obligations. In the Working Party's view, the experience gathered by those MS where DPOs are operating has proven quite fruitful and ensured greater compliance by data controllers whilst facilitating supervision by DPAs. However, there is a need to harmonise the criteria for such appointment (for example, the size of the organisation, or whether the DPO may be an external entity) and introduce safeguards in respect of their independence (for example, in some businesses they are reasonably senior, with significant responsibility and access to the board, whilst in others DPOs are junior members with no real influence).

The Working Party is doubtful of the advisability of introducing their appointment on a mandatory basis and would be in favour of a more flexible approach to take account of the complex scenario in which processing operations are performed at European level. It would be perhaps more appropriate to lay down strong incentives to the appointment of DPOs in national legislation, certainly by totally exempting those organisations that have a DPO from notification obligations but also - more importantly – by encouraging the appointment of a DPO as part of the accountability perspective supported by both the Commission and the Working Party to reduce red tape and administrative burden. This is especially so since a DPO should be required, as a minimum, to keep an inventory of all the processing operations in place in the given organisation - whether they are "risky" or not - and ensure that processing mechanisms and standards are in line with the law; as such, appointment of a DPO would be tangible proof of the organisation's accountability. Once again, the experience gathered by the DPAs of those Member States that have long relied on DPOs could be usefully integrated by the Commission (via the Working Party) in shaping the relevant legal framework.

Additionally, consideration needs to be given to how the regulator would know which organisations are relying on the exemption. The regulator might also reasonably need to know the contact details of the DPO. One option could be to make the inventory of processing operations kept by the DPO available to the regulator on request. Another option might be to have a register of DPOs – either at national or European level. In some member states there are associations of DPOs, and training of DPOs is performed on a regular basis with the

involvement of the DPAs. This is an area the Commission might want to look into in more detail, again by profiting from the experience gathered in some Member States. If the proposals on DPOs and notification lead to a scenario where organisations with DPOs do not need to notify any information of substance to a regulator, such as risky processing, then perhaps further reflection is also needed to make sure the regulator does not have an incomplete view of processing in their jurisdiction.

The Working Party also favours the idea that where the organisation makes information available publicly, they would not need to repeat the same information in the detailed notification, for example, a link to the information would suffice.

4. Conclusion

The Working Party acknowledges that current practice as regards notification is varied and that authorities have varying views as to how any future system might operate.
As a result, this paper attempts to highlight the factors to consider and the questions to ask, and makes suggestions where there is agreement between authorities. It cannot do more than this and we urge the Commission to further consider and develop the ideas in this paper, specifically the following.

- Data protection authorities are in favour of positive list approach whereby organisations are required to notify specified risky processing and the information given as part of that is more meaningful. There is a link between this and any accountability provision that might be introduced into the future legal framework. [plus any info from responses to letter to plenary on this point]
- Data protection authorities are in favour of flexibility and choice over how they use the information notified to them to carry out their roles.
- More work is needed on defining risky processing and on what information organisations have to provide.
- More work is needed on developing a common form and online submission to minimise burdens. Options include a single EU platform or website, or perhaps the interoperability of existing systems.
- A streamlined notification system benefits DPAs and organisations, it does not really benefit individuals. The Commission should look for other ways to achieve transparency for individuals in the future legal framework.
- The Commission should give further thought to provisions regarding ‘know your customer’ to achieve the balance between greater harmonisation and burdens on business. [plus info from responses to letter to plenary on this point]
- Current notification practice is extremely varied so the Article 29 Working Party are not able to provide a solution, but can only set out the questions to ask and the factors to consider.

Done at Brussels, on 4 April 2011

For the Working Party
The Chairman
Jacob KOHNSTAMM