



10211/05/EN
WP 106

Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union

Adopted on 18 January 2005

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 D (Knowledge-based economy) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: www.europa.eu.int/comm/privacy

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995¹,

Having regard to Articles 29 and 30 (1) (a) and (3) of that Directive and 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

Has adopted the present Report:

¹ Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

INDEX

1. INTRODUCTION.....	PAGE 4
2. THE WORKS OF THE TASK FORCE “SIMPLIFICATION OF NOTIFICATION REQUIREMENTS”	PAGE 4
3. MAIN FINDINGS AS REGARDS NOTIFICATION REQUIREMENTS IN THE MEMBER STATES.....	PAGE 5
4. MEMBER STATES´ EXPERIENCES ON THE EXCEPTIONS TO THE DUTY OF NOTIFICATION.....	PAGE 7
5. MEMBER STATES´ EXPERIENCES WITH DATA PROTECTION OFFICIALS (AS A SUBSTITUTE TO THE DUTY OF NOTIFICATION)	PAGE 15
6. SIMPLIFICATION BY MEANS OF INTERNATIONAL CO-OPERATION: FIRST APPROACH TO A SIMPLIFIED SYSTEM FOR ORGANISATIONS WITH MORE THAN ONE ESTABLISHMENT IN THE EU.....	PAGE 20
7. RECOMMENDATIONS.....	PAGE 22
8. CONCLUSION.....	PAGE 24

ARTICLE 29 WORKING PARTY REPORT ON THE DUTY OF NOTIFICATION TO NATIONAL SUPERVISORY AUTHORITIES

1. Introduction

By means of this report, the Article 29 Working Party responds to the European Commission's invitation at its first report on the implementation of the Directive in the Community, to explore possible means to provide further simplification to the duty of notification in the Member States.

The research carried out over the last months by the Task Force "simplification of notification requirements" with the drawing up of a "Vademecum on notification requirements" has allowed the Article 29 Working Party to present a comprehensive overview of the situation in the Member States, both from the perspective of the notification requirements in place and the experience of the Member States with the different simplification efforts made at national level.

This report therefore identifies best practices as regards the duty of notification in the Member States (see chapters 2-4) including the role of data protection officials (see chapter 5); it also explores a possible system of simplification for organisations with more than one establishment in the EU (see chapter 6), and it issues some recommendations which the European Commission is invited to take into account if further harmonisation attempts were envisaged for the future.

The Article 29 Working Party would like to express its gratitude to the members of the Task Force for their work over the last months and express its hope that this report will be just the first contribution of this group on this issue.

2. The works of the Task Force "simplification of notification requirements"

The system of notification as set out in Articles 18-21 of Directive 95/46/EC reflects the different traditions in the Member States at the time the Directive was negotiated in the early nineties: whereas some relied heavily on notification and the keeping of registers, others sought to minimise these obligations or did have alternative systems in place.

In its first report on the implementation of the Directive, the Commission – also based on the criticalities pointed out in respect of the overall implementation of data protection legislation – recalled that the Directive sets out a system of possible exemptions that allows Member States to reduce notification requirements considerably. In view of achieving enhanced harmonisation and simplification of notification mechanisms, **the Commission called on the Article 29 Working Party to put forward proposals for a substantial simplification of the**

notification requirements in the Member States, which may need to include proposed amendments to national legislation.

In particular, the report on implementation of Directive showed that notification requirements entailed difficulties for both large-sized controllers – especially those with several establishments in different EU Member States – and SMEs, albeit on different grounds. It also pointed out that data subjects were not sufficiently aware of the existence of a system of notifications whereby any entity is entitled to verify the processing operations carried out in a given country by a given controller.

Based on the above premises, the Article 29 Working Party decided to entrust a subgroup (the “**Task Force Simplification of Notification Requirements**”) with the following **mandate**:

- Analysing the current system of notification in the 25 EU Member States** plus EEA countries, also in order to produce a web-based “**Vademecum**” explaining, in summary, the basics of the system in each country with a view to supporting data controllers in complying with the relevant requirements;
- Analysing the exemptions provided for in national laws** transposing the Directive, in order to point out possible avenues for harmonisation and simplification, including the use of data protection officials as provided for in the Directive;
- Exploring** the possibility of developing co-operation arrangements under Article 28 of the Directive to **simplify notification duties of organisations with more than one establishment in the Community**.

This report sets out the initial conclusions drawn by the group as based on the findings of the analysis of the situation in Member States and **puts forward some suggestions for future work on harmonisation and simplification** of notification requirements that the Commission should take into account if proposals for further harmonisation were considered in future.

3. Main findings as regards notification requirements in the Member States

The answers provided to a questionnaire circulated by the subgroup in January 2004 served as the basis for the assessment of the existing system. They were included into a **Vademecum that will be available shortly on the website of the Article 29 data protection Working Party, as a single-stop point for any entity interested in notification** to gather how the system currently works in the EU/EEA area.

The information contained in the Vademecum will be organised by country, with links to the relevant national legislation and the competent data protection authority; additionally, an English version of the notification form(s), where existing, and a sample filled-in notification form will be available for each Member State.

The findings of the survey carried out via this questionnaire also provided the subgroup with information on the main views held by national data protection authorities concerning notification. It should be remembered that the **differences in notification mechanisms in Member States are partly related to the historical development of data protection legislation**, which in some countries was a reality long before the European directive was adopted.

In particular, **the experience gathered by some countries (such as France, Germany, and Sweden)** in this sector ever since the '70s and the '80s should be mentioned here, partly because it has pointed out the important role of data protection officials in the implementation process. Indeed, it has been said that **data protection officials are a core part** of the success story of data protection in those countries.

Keeping this in mind, and having regard to the results of the questionnaire referred to above, it was found that:

Notification or the provision of information to the data protection officers is seen favourably in the overwhelming majority of Member States

Basically, as outlined more specifically in some answers, notification appears to serve three main purposes:

- it is helpful for data subjects** because it is a **major token of transparency** in respect of the processing of personal data and can be the starting point for lodging a complaint with the competent authorities, via the controls carried out in the Register of processing operations (or of notifications);
- it is helpful for data controllers** as it helps in **raising their awareness** of notification duties and keeps them “tuned” to the need for complying with data protection requirements;
- it is helpful for data protection authorities** because **it allows them to keep abreast of the data processing situation in their countries** (they can “feel the pulse”) and, at the same time, enables several analyses to be carried out (statistical or otherwise) with a view to refining the approach to recommendation, audits and inspections.

As for the latter point, it should be clarified that **a distinction should be drawn between notification for prior checking purposes** (as per Article 20 of the Directive) **and notification submitted for processing that is not subjected to prior checking** (as per Article 18 of the Directive). The former is actually reserved for specific categories of processing that are likely to present specific risks for the rights and freedoms of data subjects, is regulated by specific provisions laid down in domestic laws, and usually results into issuing of a prior opinion, an authorisation or permit by the competent data protection authority or an opinion by a data protection official who in case of doubt must consult the supervisory authority; the latter has a broader scope, although it appears – based on the answers collected through the Questionnaire – that the information it provides is often used by data protection authorities as the basis for additional investigations also concerning processing operations possibly falling within the scope of prior checking requirements.

Flexibility and simplification of the notification procedure are achieved on the basis of different approaches, which sometimes operate simultaneously:

- Use of electronic notification mechanisms** (in the majority of the Member States), at times enabling online filling-in of the notification (currently possible in a minority of Member States).
- Application of exemptions.** This is a major point, and there is actually no Member State where at least some partial exemptions from notification obligations have not been implemented. As indicated by several Member States, the exemption mechanism is useful in itself to allow data protection authorities to focus on really “dangerous” processing operations, i.e. those possibly jeopardising fundamental rights and freedoms.

It is worth noting that **not all MS availed themselves of the catalogue of exemptions set out in the Directive**, which might be regarded as a “minimum list” to be taken into account.

- Setting up of data protection officials.** In the five countries where such officers are provided for, the choice to introduce **this mechanism was found to be useful** as a means to suppress or at least reduce notification requirements (it being provided that notification to the DPA is unnecessary if a data protection official is appointed) and ensure that controllers were aware of their obligations.

4. Member States’ experiences on the exceptions to the duty of notification

Legal background: notification is the rule but large exceptions are possible

The general rule under the Data Protection Directive is that the duty of notification to the competent data protection authority is an obligation for all data controllers. However, immediately after this general obligation, **the Directive set outs extensive exemptions** whose application is left to the discretion of the Member States. This broad margin of manoeuvre left to the Member States is in the origin of the **important differences in the implementation of these exemptions** in the domestic legal systems detected by the Task Force.

Yet, the legal framework for the exceptions to the duty of notification is mainly provided for in paragraphs 2 to 5 of Article 18 of the Directive. Under these provisions, the Directive allows Member States to implement the following exemptions/simplifications:

- for certain categories of **processing operations which are unlikely**, taking account of the data to be processed, **to affect adversely** the rights and freedoms of data subjects,

- if a data **protection official** is appointed,
- in case of **public registers**,
- for **non-profit- organisations** (foundations, associations, etc.)
- in case of non-**automated processing** of personal data.

Recital 49 of the Directive explains that Member States are provided with the opportunity to exempt data controllers from the need to notify in order **to avoid unsuitable administrative formalities**, provided that the processing is unlikely to adversely affect the rights and freedoms of the data subject. **Member States keep different views on which should be those categories of processing operations likely to adverse rights and freedoms.**

Besides these general exceptions, **Article 9** of the Directive allows Member States to provide exceptions or derogations for the processing of personal data carried out solely **for journalistic purposes or the purpose of artistic or literary expression**. This might lead to an exception to the duty of notification in these cases.

National experiences: different approaches, positive feedback

Almost all Member States have availed themselves of **the right to exclude** certain categories of processing operations from the notification obligation. However, **the way in which the countries have exempted these latter categories varies a lot**; the taken measures range from small catalogues in the transposing law (Austria, Poland) to complicated systems of cross-reference (Denmark, Finland) or extensive lists adopted in secondary legislation, such as Decrees and Ordinances or regulations adopted by the Data Protection Authorities themselves (The Netherlands, Sweden, Belgium or France).

Despite these differences between the Member States, common **trends can be identified such as:**

- the existence in all Member States of exemptions for the processing of data with the sole purpose is the **keeping of a register** which according to laws or regulations is intended **to provide information to the public** and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest;
- the existence in several countries (about 50% of the total) of exemptions applying to the membership **processing** carried out in the course of its legitimate activities by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim
- the existence of **exemptions applying to processing for journalistic purposes** (most countries, though not all of them);
- and the existence of **exemptions applying to processing of data that is required by specific laws/regulations** (e.g. to comply with tax laws)

The Swedish case

In Sweden the Government has tried to make use of all the exemptions that the Directive allows. This was made clear in the **Government Bill** of the Data Protection Act where the Government stated that **what matters for data protection is that the data controllers respect the data protection rules** when they process personal data **and not that they send in papers to the Data Inspection Board.**

Sweden has had data protection legislation since 1973 when the old Data Act came into force. That Act was based on a system where those who created and kept a computerised filing system of personal data should notify the Data Inspection Board and get a licence. In many cases it was also necessary to get a prior check and permission from the Data Inspection Board.

The Government found that it could be assumed that those who obey the formal rules and make a notification also are the ones that best obey the rules that govern the processing of personal data. In fact, the system of notifications and licences was not a good basis for supervision activities of the Inspection Board and did not give individuals any information on which personal filing system they were registered in. Consequently, when the Government presented the Bill of the Personal Data Act of 1998, there was the general perception the system with notifications and licences should be abolished and the supervisory authority should concentrate its activities both on giving advice and spreading awareness about data protection and supervising compliance. This should not be mixed up with the mandatory notification of processing that is particularly sensitive as regards integrity (prior checking).

Sweden excludes from the notification duty such processing operations as would probably not result in an improper intrusion of personal integrity, if specified in rules issued by the Government or the Data Inspection Board. Under section 36, third paragraph, of the Personal Data Act. The Government or the authority appointed by the Government (the Data Inspection Board) may issue regulations concerning exemptions to the notification duty for such kinds of processing as would probably not result in an improper intrusion of personal integrity.

The Government has issued such regulations in the Personal Data Ordinance. Sections 3-5 provide exemptions from the general notification duty. Furthermore, **the Government has empowered the Data Board to issue regulations on exemptions from the duty of notification for such types of processing as will not be likely to result in improper intrusion of personal integrity.** The Data Inspection Board has issued such exemptions in section 4-5 of the Data Inspection Board Code of Statutes.

When the Data Inspection Board considered exemptions that should be made, it started out by trying to find out the purpose of the notification duty in the Directive (see article 18-19 and preamble 48-52) in order to, from that stand point, make general exemptions for all types of processing not likely to result in an improper intrusion of personal integrity. **The aim has been to make all the foreseeable and suitable exemptions that are allowed** within these limits and to be prepared to make further legally based exemptions if proven necessary. These exemptions are very much based on the experience that the Data Inspection Board has got through many years of being a supervisory authority under the old Data Act.

Further to these exceptions adopted **in Sweden, the notification duty does not apply to the following processing operations:**

- the processing of personal data that is undertaken pursuant to an authority's obligation under Chapter 2 of the Freedom of the Press Act to provide official documents,
- the processing of personal data that is undertaken by the archive authority pursuant to the provisions of the Archives Act (1990:782) or the Archives Ordinance (1991:446),
- the processing of personal data that is governed by specific regulations in a statute or ordinance in other cases than those mentioned in items 1 and 2 (there is a great number of specific Acts and Ordinances that regulate personal data processing in specific sectors),
- the processing of sensitive personal data that is performed under Section 17 of the Personal Data Act. Nor does the duty of notification apply to the corresponding processing by such an organisation of other kinds of personal data than sensitive personal data
- the processing that takes place with the individual's consent
- the processing of the following categories of personal data** if the data controller keeps a schedule of the processing operations (including the information that otherwise would have had to be notified):
 - personal data that relates to a registered person who has a link to the data controller of the kind that follows from membership, employment, customer relation or some other relationship comparable therewith, unless the processing comprises such sensitive personal data as is referred to in Section 13 of the Personal Data Act,
 - personal data processed by an employer concerning the sickness of an employee that relates to absence due to sickness, provided the data is used for the purposes of payroll administration or to determine whether the employer is liable to initiate a rehabilitation investigation,
 - personal data kept by an employer and revealing an employee's trade union membership if the data are used for the purpose of fulfilling obligations or safeguarding rights according to labour legislation or in order to establish, exercise or defend legal claims,
 - personal data that has been gathered from the registered person provided he processing is necessary to comply with a provision under statute or ordinance,
 - personal data that may be processed in the health care sector under Section 18 of the Personal Data Act,
 - personal data in the operations of an advocate that is of significance to conduct an assignment in the operation or to verify that a situation involving disqualification does not exist, and
 - personal data that takes place in compliance with a trade/industry agreement that has been assessed by the Data Inspection Board under Section 12 of the Personal Data Ordinance

The cases of the Netherlands, the United Kingdom, France and Poland

The supervisory authorities of these Member States have made **efforts to exempt from the duty of notification routine business activities** and similar activities (unsuitable administrative formalities) to the extent permitted in the Directive with the proviso that that the processing would not have any significant impact upon privacy. This has led to a **broad catalogue of exceptions and considerable simplification** in these countries.

The Netherlands is a good example of the extensive reliance on certain categories of processing exemptions. As stipulated in article 43 of the Exemption Decree, some combinations of exempted processing operations are also exempted. In addition to that, the Data Protection Authority and the Ministry of Justice are currently reviewing the possibility to further extend the list of exemptions.

Membership and patronage	(Associations, foundations and trade associations under public law, Spiritual societies),
Work and retirement	(Applicants, Temporary workers, Personnel administration, Salary administration, Compensation in case of dismissal, Retirement and early retirement)
Goods and services	(Subscriptions, Debtors and creditors, Customers and suppliers, Rental and leasing, Legal service providers and accountants),
Health and welfare	(Individual healthcare, Residential care homes and nursing homes, Child care facilities)
Education	(Pupils, participants and students Compulsory education, School transport)
Government	(Permits and reports, Decentralised taxes, Travel documents, Grave rights, Naturalisation, Change of name, Compulsory military service)
Archives and research	(Archival storage, Scientific research and statistics)
Management and security	(Document management, Network systems, Computer systems, Communications equipment, Access control, Other internal management Registration of visitors, CCTV supervision)
Other forms of processing	(Notices of objection, complaints and legal proceedings, Registers and lists, Former members and pupils, Communication files).

The situation in **France** can be summarised as follows:

Public registers/ Government	Exemption from notification for processing the sole purpose of which is the keeping of a register which, according to law, is intended to provide information to the public and which is open to consultation to the public
The most frequent categories of processing which do not present risk to rights and	Exemption or simplification based on one of the current 39 CNIL's regulations adopted in

freedoms	the following fields: work (personnel, administration, salaries, billing telephone, restaurant, access control to buildings, control of working hours), pensions, goods and services (customers and suppliers, banks, insurance, distant selling, housing, press), education (pupils), local authorities (various services), electoral lists and public statistics.
Membership and patronage	Exemption for organisations with a political, philosophical, religious or trade-union purpose and upon condition that the processing relates solely to the members of the organisation or to persons who are in regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects

In the **United Kingdom** the exemptions apply to data controllers who only process:

Work	Personal data for ‘staff administration’
Goods and services	‘Advertising, marketing and public relations’ (of their own business), ‘Account and records’
Membership and patronage	Some ‘not for profit organisations’ (charities, small clubs and associations),
Government	‘The maintenance of a public register’,
Other forms of processing	‘Manual data’ (paper based records only). personal data processed for ‘personal domestic and household affairs’,

In **Poland**, the obligation to register/notify data filing systems shall not apply to the data controllers as regards the following categories of data:

Government	Data constitute a state secrecy due to the reasons of state defence or security, protection of human life and health, property, security, or public order, Data were collected as a result of inquiry procedures held by officers of the bodies authorized to conduct such inquiries, Data are processed by relevant bodies for the purpose of court proceedings and on the basis of the provisions on National Criminal Register, Data are processed by the Inspector General of Financial Information,
-------------------	---

	Data are created on the basis of electoral regulations concerning the Diet, Senate, European Parliament, communal councils, poviatic councils and voivodship regional councils, the President of the Republic of Poland, head of the commune, major or president of a city elections, and the acts on referendum and municipal referendum, Data refer to persons deprived of freedom under the relevant law within the scope required for carrying out the provisional detention or deprivation of freedom,
Membership and patronage	Data relate to the members of churches or other religious unions with an established legal status, being processed for the purposes of these churches or religious unions,
Work and retirement	Data are processed in connection with the employment by the controller or providing services for the controller on the grounds of civil law contracts,
Health and welfare	Data refer to the persons availing themselves of data controller's health care services,
Goods and Services	Data refer to the persons availing of notarial or legal advice, patent agent, tax consultant or auditor services, Data are processed for the purpose of issuing an invoice, a bill or for accounting purposes
Education	Data refer to the controller's members and trainees,
Other	Data are publicly available, Data are processed to prepare a thesis required to graduate from a university or be granted a degree, Data are processed with regard to minor current everyday affairs. Data are processed for journalistic purposes

The Italian case

Mention should also be made of the approach adopted by Italy in the recently enacted Data Protection Code (June 2003). This new system of notification was the outcome of the experience gathered by the Garante in the 1997 to 2003 period; it is based on the analysis of the data related to the requests for authorisation of processing operations concerning sensitive data as well as of the data contained in the Register of processing operations. The purpose was to simplify notification as much as possible by eliminating any items of information that could be regarded as unnecessary though ensuring that significant information was retained.

In trying to achieve the above objective, it was decided from the start that the new IT technologies were to be used to the greatest possible extent by doing away with notification via filling in of a paper form and/or a form on a floppy-disk. The latter arrangements were found to be expensive to manage as well as time-consuming, in particular because of the need to enter the data contained in the filled-in forms into the Register of processing operations, which entailed the risk of introducing mistakes to be subsequently corrected and caused several difficulties in order to timely update the information with a view to publication of the Register on the Internet.

The system envisaged in Italy draws inspiration from the Community principle set out in Article 18(2) of the Directive, whereby notification should not be exempted “for categories of processing operations which are []likely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects”.

Based on the legislative approach adopted by Italy’s Parliament, this principle can also be implemented by means of a “positive” list of processing operations to be notified, i.e. by directly specifying the processing operations that are considered to be prejudicial for data subjects’ rights and freedoms.

Given this background, an initial “positive” list was provided for directly by the Data Protection Code, which however committed the Garante with the task of adding other processing operations, still in pursuance of the aforementioned principle, where they are found to be prejudicial to data subjects’ rights and freedoms – also in the light of scientific and technological evolution.

Since the categories of processing operations referred to in the Code are quite broad in scope, the Garante was also authorised to specify – within said list – some processing operations that may be exempted from notification because of their features.

Therefore, under Section 37 of the Data Protection Code notification is currently mandatory exclusively if the processing concerns any of the data categories reported below:

- a) genetic data, biometric data, and data disclosing geographic location of individuals or objects by means of an electronic communications network;
- b) data disclosing health and sex life for purposes related to assisted reproduction, provision of health care services via electronic networks in connection with data banks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure;
- c) data disclosing sex life and the psychological sphere by not-for-profit associations, bodies or organisations, whether recognised or not, of a political, philosophical, religious or trade-union character;
- d) data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services;
- e) sensitive data stored in data banks for personnel selection purposes on behalf of third parties, as well as sensitive data used for opinion polls, market surveys and other sample-based surveys;

f) data stored in ad-hoc data banks managed by electronic means in connection with creditworthiness, assets and liabilities, appropriate performance of obligations, and unlawful and/or fraudulent conduct.

It should also be pointed out that those controllers that are not required to notify their processing operations under the law “shall make available the information contained in the [notification] form to any person requesting it, unless the processing operations concern public registers, lists, records or publicly available documents” (Section 38(6) of the Code).

Notifications are included in a Register that is publicly accessible online.

In March 2004, some processing operations within the aforementioned categories were exempted from notification via an ad-hoc decision issued by the Garante as they were considered not to be prejudicial to data subjects’ rights and freedoms. This applies, for instance, to the processing of genetic and biometric data carried out in a non-systematic fashion by health care professionals if the data are not organised in a data bank accessible to third parties via electronic networks, as well as to the processing of these same data carried out in the exercise of the legal profession insofar as the data and operations are necessary to carry out investigations by defence counsel and/or to establish or defend a legal claim that is not overridden by the data subject’s one.

5. Member States’ experiences with data protection officials (as a substitute to the duty of notification to national supervisory authorities)

Article 18 (2) of the Directive allows Member States to exempt controllers from notification duties where “*the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:*

- *For ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive,*
- *For keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2) (...)*”

This alternative to notification provided by the Directive is currently implemented in five Member States: Germany, the Netherlands, Sweden, Luxembourg and France.

The German case

This part of the Directive was largely inspired by the German law on this field. In Germany, every private entity with more than four persons engaged in automated data processing is obliged to appoint a data protection official. Every public entity must appoint a data protection official without exception.

Data protection officers are familiar with the problems of the entity where they work and given their special status they can be very helpful to provide advice and solve any data protection problems. In cases where conflicts arise between the data protection official and the management board he/she is free to ask for support from the supervisory authority. It must be

stressed that the management board remains responsible for any decision regarding data protection within a given entity.

German data protection authorities are of the view that the system works well. There are several data protection publications addressed to these data protection officials and private or semi-private institutions offer seminars and lectures.

It is interesting to have a closer look on the German experience concerning the measures to guarantee transparency of data processing activities, because the German system has undergone the most dramatic changes.

At the time of preparation of the law the legislator was determined to make sure that for the data subject a way was provided for to identify anybody who was processing data relating to him. He also wanted to satisfy the interest of the public to know the structures of personal data processing. The concrete way finally chosen to achieve these aims was different for the public sector on one side and for the private sector on the other side.

In the public sector the supervisory authorities were given the task to keep publicly accessible registers of the processings (actually of the files) containing personal data; the controllers, i.e. the authorities, had to notify their activities accordingly. In the private sector the controllers had to inform the data subjects individually of the fact that their data were held in a file, as far as they were not already aware or were informed otherwise.

It is remarkable, that public registers and individual notifications were regarded as alternatives, not to be taken cumulatively as provided for later by the Directive. In the public sector, an individual who wanted to know which authorities processed data about him, was expected to consult the register of files, in order to learn which authorities potentially did so and then to turn to them and to ask for full information. Individual notifications were regarded as more comfortable for the individual but in the last resort, taking into account the cost-benefit-ratio, as not crucial.

In the private sector, beyond individual notification, a need for a general obligation to submit the structures of processing to (general) publicity like in the public sector was not regarded as adequate, taking into account the fact that knowledge of all data subjects was already guaranteed; the possibility of others to gain this information in an easy way was not seen as justifying the introduction of comprehensive public registers. The law therefore chose a limited approach. Only those controllers whose professional function was to process data in the interest of third parties, i.e. without an own interest to exploit the information contained in the data, were subject to publicise their data file structure. In practise this applied to data processing services, to opinion poll and marketing research companies and to credit reference services, an industrial sector for which the law also provided a set of special substantial regulations.

When the Directive offered the opportunity for the member states to choose the installation of independent data protection officers instead of a public registration scheme, in Germany the choice was not difficult. For all DPAs, whether the federal one or the Länder authorities, the keeping of the register had always been an unloved duty, something that the law required, but also something that did not help neither the authorities to discharge their tasks nor the data subjects to exercise their rights nor anybody else in the country to learn about the practices of controllers or the development of data processing in general. So the abolition was taken with

relief by the data protection professionals, and the public did not take more notice of the abolition than it had ever taken of the existence of the registers, which means it ignored it completely.

For insiders this was not surprising. The analysis of the information contained in the notification to the register had rarely been exciting. 99 % of it reflected the functions of the agency or the company just as you would imagine them. Even if it was different, it was mostly far from indicating an anomalous situation in data protection terms, requesting investigation. Mostly it derived from an input error or a misunderstanding. Implausible notification data were frequent. To get them corrected was cumbersome and time-consuming. But this was not regarded as a good investment, as the register was rarely consulted. The Federal Data Protection Commissioner's register e.g. used to be consulted by the public less than once per year. Never a consultation has had any follow-up, be it questioning of the activities described in the notifications, or mention in an article in a newspaper. For this reason, the DPAs in a joint effort have written a booklet which describes in a systematic approach all data processings important for individuals, covering all sectors of private and public activities. Since its first appearance in 1980 it has been very successful in numerous editions.

The DPA staff used the register - if at all - just once, but rarely again, because they did not find the information they sought. Not in terms of detail, notwithstanding the fact that the German BDSG required a more detailed description of the data fields than the Directive does, not in terms of technical and organisational information, as it necessarily is so abstract that an assessment cannot be based on it, and not in terms of identification of possible data protection violations, because – not surprisingly – controller did never present information on illegal or legally dubious activities, a self-incrimination they are legally not obliged to deliver. Finally the non-registration did by no means guarantee or at least indicate that a data processing activity did not take place; undoubtedly the registers were to a relevant degree incomplete, but no one could say whether to 10, to 50 or even more percent. So the registers never became the information resources as which they had been introduced. And the DPAs could easily live without them. All kinds of information that the registers could potentially have offered, could be gained by directly requesting them from the controllers, based on their legal obligation to respond. And the direct way revealed practically always to the better one, if detailed, focussed, up-to-date and reliable information was needed.

The limited role which the registers have played in Germany has also to be seen in the context of two specific aspects of the German supervisory system. The first one is the important role of the data protection officers in the implementation process, which makes them an information source of primordial value. Regarding – with the Directive - as an alternative to public registers, they may generally cause higher costs for the controllers, but certainly not their cost-benefit-ratio. Their functions are fundamentally different. They contribute to problem-identifying and problem-solving, whereas the registers are purely descriptive. The second one is the focus of DPAs on auditing of controllers at place, which in Germany from the early days of data protection has been regarded as the king way when quality information, effective correction and permanent improvements are sought. In terms of information turn-out for the time spent, auditing has proved as highly productive, and as delivering valuable information not only for the assessment of the individual controller audited but also as part of a general analysis of the practices or the developments in a given sector. In Germany, it is no the general view, that privacy protection officials are a core part of success story of data protection. A new profession has been created with its own education and important

information exchange activities in form of congresses, seminars, periodicals and other publications. The strength of the German data protection community was proofed in the Commission consultation on the implementation of the Directive, where nearly 50 % of all answers received originated from Germany, both for individuals as for corporate participants.

The Swedish case

In Sweden there is no obligation to appoint a data protection official (personal data representative in Swedish terminology): it is a voluntary arrangement. The personal data representative shall have the function of independently ensuring that the data controller processes personal data in a lawful and correct manner and in accordance with good practice pointing out any inadequacies to him/her.

If the representative had reasons to suspect that the data controller contravenes data protection rules and if rectification was not implemented as soon as practicable, the representative shall notify this situation to the supervisory authority. The representative shall also otherwise consult with the supervisory authority in the event of doubt about how the rules should be applied.

The Data Inspection Board provides specific seminars and other training facilities for appointed representatives. One member of the Board's lawyers is appointed as specific contact person for personal data representatives. This lawyer co-ordinates all contacts and activities towards the representatives. These representatives frequently turn to the Board by phone, e-mail or letter to ask for advice. There is also a specific part of the website aimed at serving to the personal data representatives.

If a personal data representative has been notified to the Data Inspection Board, the general notification duty does not apply. The representative, however, has to maintain a register of the processing that the controller implements and which would have been subject to the notification duty if the representative had not existed. The register shall comprise at least the information that a notification under Swedish law would have contained. The representative shall also assist registered persons to obtain rectification when there is reason to suspect that the personal data processed is incorrect or incomplete.

At the end of 2003, 5.324 controllers had notified personal data representatives to the Data Inspection Board. The Board keeps these notifications in a register that is available to the public. The number of notified personal data representatives was 3.133 at the end of 2003 (one representative may represent several data controllers). The Board's activity towards representatives has required quite a lot of resources but in return, experience shows that the representatives have improved the level of data protection within the organisations they represent. The Board's experience is consequently that the system of personal data representatives works very well.

The Dutch case

In the Netherlands, the law stipulates that a controller or (sectoral) organisation to which controllers belong may appoint its own data protection official (privacy officer in Dutch terminology). The statutory tasks and powers of the privacy officer give him/her an independent position in the organisation with respect to the performance of his/her duties. For example, the privacy officer may not receive any instructions from the data controller. He shall sustain no disadvantage as consequence of performing his duties and must be given the opportunity by the data controller to perform his duties properly.

The Dutch Data Protection Act stipulates that if there is a privacy officer, notifications can be done to the privacy officer (thus not to the data protection authority). The Dutch Data Protection Authority has developed a special notification programme for privacy officers. This adapted version of the notification programme offers the privacy officer the possibility to further process the notifications within an own database and/ or intranet of the organisation.

About 165 privacy officers are currently installed. The Dutch authority expects this number to increase further. They are active in all sectors of society. Examples are banks, insurance companies, trade unions, financial regulatory bodies, schools, hospitals, municipalities, ministries, and a variety of big and medium-size business.

The Dutch authority has a statutory task to maintain an up-to-date list of registered officers. This register is public and accessible from the website. The privacy officers have founded a branch organisation, '*Nederlands Genootschap van Functionarissen voor de Gegevensbescherming*' (Dutch Association for Privacy Officers). This branch organisation has as a purpose the furtherance of the quality and integrity of the privacy officers.

The Dutch data protection authority maintains good relations with the privacy officers. Every privacy officer is appointed a contact person within the data protection authority. The contact person, a legal adviser, can be addressed in case of questions or problems. The data protection authority further stimulates the organisation of meetings by privacy officers who work within the same sector, in order to share experiences and learn from each other. It advises on the programme or gives presentations at such meeting. The data protection authority also organises such meetings itself. Finally, it maintains a good working relationship with the Dutch Association for Privacy Officers.

Appointing a data protection officer will mean that the Dutch data protection authority will exercise restraint with regard to organisations in which this data protection officer functions properly. The Dutch data protection authority will, wherever possible, refer persons with questions or complaints to the data protection officer. However, as the national supervisory authority, the Dutch authority retains all powers with regard to organisations that have appointed a data protection officer.

The French case

The new French data protection law has introduced an exemption from the notification requirements based on the option for private enterprises and local governments to designate an independent and internal data protection officer, except in cases where the processing is subject to prior checking by the CNIL (the cases concerned are provided for by law).

The data protection officer's skills, missions and powers, independence and liability should offer a level of guarantee which can replace notification to the CNIL and constitutes a means of simplification for data controllers. The main aims of this new provision are to offer a network of correspondents to the CNIL, in order to supplement the action of the DPA, and to contribute to a better co-operation between the CNIL and the companies instituting them. Moreover, concerning public local authorities, the existence of data protection officers would be a precious help for the smallest authorities with limited legal expertise.

The Luxembourgish case

The Data Protection Act provides for an exemption of the notification duties for data controllers who appoint a data protection delegate/officer. Secondary legislation will enter into force only at the beginning of 2005. At the moment the data protection officer may not be a person employed by the data-controller but only at a third party (e.g. a lawyer, IT consultant, Auditor).

The idea of allowing also a member of the staff appointed by a data controller to act as data protection officer is discussed at present. An amendment of the law is necessary if this idea is adopted; it will then have to provide for a protection against dismissal or any harm by the employer as a consequence of the exercise of its function as data protection officer which is to be accomplished in full independence.

The data protection officer establishes a list of the personal data processing operations carried out by the company/entity he is appointed for. A copy of this list is to be communicated to the DPA and information about the data processing operations described herein is integrated in the public register accessible for citizen.

Other Member States' laws provide for data protection officials (e.g. Poland, Slovakia) but their tasks and legal position is not connected with any exemption from notification duty.

6. Simplification by means of international co-operation: first approach to a simplified system for organisations with more than one establishment in the EU.

At the occasion of the review of the Data Protection Directive in 2002, **business representatives were unanimously of the view that it should be possible to facilitate the notification duties of multinational companies** which, in accordance with current national laws implementing the Directive, must notify as many times as establishments they may have in different Member States of the European Union.

The European Commission shared this criticism to a large extent and invited the Article 29 Working Party to reflect on possible means to alleviate this burden, if necessary, by proposing amendments to national laws. The Task Force "simplification of notification requirements" has considered different proposals and it is currently working on a system whose main lines are described below.

It must be emphasised that at this stage of the discussions, many uncertainties remain. Although the Working Party fully supports these efforts, **it is uncertain whether or not some of the technical difficulties already detected by the Task Force could be overcome**. It is also uncertain whether or not the final result of these technical deliberations, which are very much influenced by the constraints of the national laws and their differences, will be able to provide the level of simplification sought by those expressing criticism at the time of the review of the Directive.

The main elements of such a simplified system could be the following:

1. Justification that a **notification has been completed in one Member State**, as a prerequisite to apply for a simplified procedure.
2. Similar processing operations would be a must. Processing operations in the country where the notification took place and in the country where the simplified system is being used should be very similar. Using the same information system, for example, would help the applicant to demonstrate the existence of similar processing operations.
3. The provision of information to other data protection authorities (by means of model fiche translated into all official languages) would be limited to **the content of Article 19 of the Directive + 3: time of data storage, information on the sources of the data and mechanisms made available to data subjects to exercise their rights**. Compliance with national law may also require identification of data transfers or prior checkings.
4. Data Protection Authorities may, on a case-by-case basis, request the provision of additional information, if the provision of such **additional information was deemed necessary in attention to the particular circumstances of the case at hand**.

Such a simplified procedure would work on the general assumption that a data protection authority receiving a simplified model (see number 3) could **always rely on the archives of the data protection authority where a successful notification** for similar processing operations was made.

Whether or not this can be deemed as a lawful notification in accordance with national laws still requires further reflection and consultation. This is particularly difficult in those cases where, as it is frequently the case, national laws do require the provision of more information than the limited information contained in the model fiche. Under the current legal framework, Member States do benefit from a broad margin of manoeuvre which makes different perceptions fully legitimate and therefore any harmonisation attempts face tremendous difficulties. There is also the **technical question of guaranteeing appropriate interface** between this new simplified system and those currently existing in the national data protection authorities.

In any case, the **Working Party would like to update** the data protection community about the results of these works over the last months **and reaffirm its commitment to keep on working** on co-operation mechanisms which may eventually simplify the notification duties of organisations carrying out similar processing operations in several Member States. **These**

reflections might also be taken up by the European Commission in the future if a European action on this field was found necessary and appropriate.

7. Recommendations

1. First of all, the Article 29 Working Party would like to endorse the **recommendations of the first Commission's report on the implementation of the Data Protection Directive (p. 24):** *"The Commission recommends a wider use of the exceptions and in particular of the possibility foreseen in Article 18(2) of the Directive, that is the appointment of a data protection officer"*.

The Article 29 Working Party invites the Member States to make good use of the possibilities for exceptions and simplification available under the Directive and, where this is not yet the case, recommends Member States to empower the data protection authorities with appropriate regulatory powers to implement these exceptions accordingly.

If amendments to the existing legal framework were envisaged, the Article 29 Working Party is of the view that **notification as a general requirement should not be eliminated**. The research carried out by the Task Force over the last months shows nevertheless that differences in the perception between the data protection authorities remain whether this notification should be made to data protection authorities (administrative notifications) or to data protection officials (internal notifications).

2. **This is particularly so with regard to those Member States where data protection legislation was introduced more recently;** indeed, the data protection authorities of such Member States regard notification as a means to also draw the controllers' attention to the need for abiding by data protection legislation. However, in order to comply with the spirit of the Data Protection Directive and as outlined by the concrete experiences expressed by the Member States in their answers to the questionnaire, **notification should not be a bureaucratic step**, i.e. to the submission to the data protection authority of a form with poorly meaningful contents.
3. The Article 29 Working Party also recommends **enhancing and pursuing the user-friendly approach** that is de facto adopted by Member States in dealing with notification requirements. This means enhancing the implementation of **electronic and online** notification mechanisms. Here, useful guidance might be provided by the Member States with more advanced experience in online/electronic submissions. Furthermore, the use of **ready-made lists of purposes/data categories** as already available in several Member States should be enhanced as this can reduce errors and harmonise notifications. Work might be done on a pan-European list of purposes/categories.
4. Data Protection authorities within the Article 29 Working Party agree on the need to **streamlining the exemption system** by inviting the Member States where some exemptions are not provided for to consider possible harmonisation attempts. It would be desirable that data controllers could benefit from the same catalogue of exceptions and simplification everywhere in the European Union. This should concern, **at the very least, the processing of data that are already the subject of exemptions lato**

sensu in the EC Directive, i.e. the exemptions applying to processing by associations and foundations, processing for journalistic purposes, and processing required to comply with existing legislation (in particular as regards data in the employment sector). Any harmonisation attempts should in any case take into consideration the existence of peculiarities in the national legal systems which may justify the existence of certain differences. The generalisation of regulatory powers to data protection authorities for this particular field is very likely to enhance a flexible approach and enormously facilitate international co-operation in this context, although there are doubts that within the current legal framework and the broad margin of manoeuvre left to the Member States further harmonisation can be achieved.

5. **A broader use of data protection officials as a substitute to notification duties**, at least with regard to certain industry sectors and/or in respect of larger organisations including those in the public sector, would be useful **in view of the positive findings reported by the Member States in which these data protection officials have been already introduced or have existed traditionally**. It should be kept in mind that **the establishment of data protection officials does neither reduce the information accessible for the data protection authorities where this information is needed, nor necessarily entails elimination of notification requirements** in respect of the data protection authority, in particular with regard to prior checking. In fact, it is an important item of simplification, and would help the supervisory authorities to be able to focus on other in-depth work on certain data processing or sectors more likely to be prejudicial for the privacy of individuals. When considering the opportunity of generalising data protection officials, that is, shifting from administrative to internal supervision, appropriate attention should be made both to the experience gathered by the Member States with the application of the law and to the local legal culture.

8. Conclusion

The Article 29 Working Party issues this report in response to the invitation made by the Commission in its first report on the implementation of the Directive in 2003. This report should be regarded as a first contribution for a better understanding of the role of notification duties and of data protection officials in the data protection system existing in the European Union and as a first step in the progress of providing further harmonisation and simplification to notification duties in the Community.

The Article 29 Working Party will continue working on this issue bearing in mind that the implementation of these provisions of the Directive by the Member States varies considerably. The Article 29 Working Party invites the European Commission to use the content of this report as a first contribution from this group to any proposals of further harmonisation or simplification of notification duties in the field of data protection.

Done in Brussels, on 18 January 2005

For the Working Party

The Chairman

Peter Schar