ARTICLE 29 DATA PROTECTION WORKING PARTY

01269/07/EN
WP 137

Report 1/2007 on the first joint enforcement action: evaluation and future steps

Adopted on 20th June

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 1995[1],

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

having regard to Article 255 of the EC Treaty and to Regulation (EC) no 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents

having regard to its Rules of Procedure

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

FIRST JOINT ENFORCEMENT ACTION
PRIVATE HEALTH INSURANCE COMPANIES

REPORT

First part:

The first joint enforcement action: evaluation and future steps

I. Background – Enforcement

In its First report on the implementation of the Data Protection Directive (COM (2003) 265 final), the European Commission called upon the Article 29 Working Party (WP29) *"to hold periodic discussions on the overall question of better enforcement… and consider the launching of sectoral investigations at EU level and the approximation of standards in this regard"* with the objective of understanding the level of implementation and providing guidance to sectors, improving compliance in the least burdensome ways possible.

In response, the Working Party mandated the Enforcement Task Force (ETF) in June 2004 to discuss an EU strategy and criteria for enforcement. In November 2004, in its Declaration on Enforcement (WP101), WP29 announced its commitment to "*developing proactive enforcement strategies [and] increasing enforcement actions"* and identified six criteria to consider in identifying a sector for collaborative enforcement.

The combination of the criteria identified in WP101 pointed to the selection of a sector with highly harmonised activity and furthermore, whose impact on the protection of personal data would be equally high. WP29 therefore selected private medical insurance as the object of this first synchronised intervention, specifically in the provision of health assistance insurance.

The Commission recently reaffirmed the commitment to harmonising data protection practices and reducing divergence in national legislation, calling upon WP29 to continue its contribution and upon national Data Protection Authorities "*to adapt their domestic practices to the common line they decide at the Working Party*" (Communication on the follow-up of the Work Programme for better implementation of the Data Protection Directive (95/46/EC), COM (2007) 87 final, adopted on 7-3-2007). The Commission also noted that to the extent that divergences arise *"within the Directive's margin of manoeuvre,"* they do not generally create problems in the Internal Market; however, greater convergence continues to be desirable as a means to permit simplification and self-regulation initiatives that could potentially diminish the enforcement burden on supervisory authorities and increase compliance sector-wide (for example, through the use of binding corporate rules).

In this same Communication, the Commission made express reference to this joint investigation, then in progress, in the context of arguing against the modification of the Directive. However, whether this enforcement action truly satisfies the goals of the Work Programme established in the Commission's First Report on the Implementation of the Data Protection Directive (COM (2003) 265 final) depends upon its results. But even the results do not speak for themselves; alone, they are insufficient to evaluate the success of this joint enforcement action or to justify a new, similar action immediately. In order to improve the effectiveness of future activity of the Article 29 Working Party in this field, it is important to reflect critically not only upon the results, but also upon various other aspects of this first experience with joint enforcement actions.

II. Conclusions of the enforcement action

A. Reflections on the current enforcement action

1. The investigation was carried out by the Data Protection Authorities of: *Austria, Belgium, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovenia, the Slovak Republic, Spain, Sweden, and the United Kingdom.*

The action was initiated in March 2006 with a request for information from Data Protection Authorities (DPAs) to data controllers in their respective nations. It lasted 13 months, ending with the presentation of survey results that accompanies this report. The chosen approach was a joint analysis of responses to a common questionnaire issued by each participating DPA to selected data controllers under its jurisdiction. This method was selected in order to avoid creating asymmetry with respect to the quality and depth of investigation among the various European DPAs, with their distinct responsibilities and enforcement capabilities.

From the outset, this approach imposed an important limitation on the exercise of the DPAs' supervisory function with respect to the *in situ* review of facts and documents. This approach precludes the possibility of direct, immediate access to the solicited responses and direct conversations with data controllers; these are essential elements to any inspection action or audit.

This limitation prevented some of the responses that were not satisfactory from being studied in greater depth. In other cases, situations emerged that could be subject to a more in-depth national investigation. Such focused study, however, is not possible at the common European level, precisely because this kind of investigation requires direct access to data controllers to provide clarification (for example, what kind of genetic information is being collected, to what end, and on what legal grounds).

2. Another methodological aspect that could be improved is the essential instrument around which this action revolved: the common questionnaire, developed collaboratively by all the participating DPAs. The development of the questionnaire constituted a large part of the Enforcement Task Force's work (from January 2005 to March 2006), because of the effort required to combine, in just one document, all of the questions corresponding to the needs of divergent national data protection laws. This rendered the text of certain questions incomprehensible or irrelevant to data controllers in countries with different data protection systems and structures.

A less exhaustive and complete questionnaire could possibly be a more effective instrument, if combined with the possibility of deepening the investigation in a more direct, practical way (such as auditing or inspection). For this reason, it is absolutely necessary that all DPAs are empowered to take such direct action and are allocated sufficient resources to do so.

One positive aspect of this first synchronised enforcement action that we should emphasize is the inclination it has generated among the participating DPAs to take collective action in the realm of enforcement. The advantages and results obtained through this joint action have put coordinated enforcement on the table as a new and effective strategy in the supervisory sphere.

Another important and positive factor was reliance on collaboration with representative associations from the insurance sector, both at the national and European levels. The contact initiated by the European Commission with the European Insurance and Reinsurance Federation (Comité Européen des Assurances, CEA) made this collaboration possible and productive. CEA relayed to its associates the advantages of participation in this experience and the potential for its results to assist in improving their data management techniques. At the same time, this direct link to representatives from the sector permitted a greater understanding and awareness of the industry's needs and practices, and how they affect the processing of insurance beneficiary data.

Concerning the presentation of the results a significant point was whether the final findings should be state or company oriented. Should the percentages given for every question refer to the practice in the MS or to the practice by the companies in European level? In this first investigation, we opted for the first solution for purely technical reasons, since the national reports did not refer every individual company, but gave concentrated results concerning the practice in the MS. The opposite would be also difficult because the results within every MS did not represent equal percentages of the market or companies of equal sizes (it could be that there is a high number of non compliant organisations but they belong to a small number of countries). In future actions this point has to be decided in advance, in order to set the relevant criteria and to adapt the questionnaires accordingly.

It is important to underscore that this enforcement action was conducted within the scope of confidentiality rules with respect to the public presentation of results; results are comparative and do not identify the data controllers who were investigated. The confidentiality decision, adopted along with the agreement that selected the common questionnaire approach, should not present an obstacle to enforcement. If necessary, national DPAs will continue supervisory actions and take corrective measures as appropriate.

B. Evaluation of the investigation

1. On the basis of the numeric results of the survey, this investigation was positive. In each group of answers the situation in the majority of the MS was found in compliance with the criteria raised in the questionnaire, which reflected the general principles of the Directive. Accordingly, one can assume that, in general, the processing of personal data by the private health insurance companies is in compliance with the principles and provisions laid down in Directive 95/46/EC on the protection of personal data.

Nevertheless, one would need to highlight two major issues:
- Even if the general outcome is positive, numbers show that in respect with specific issues, compliance has achieved lower rates in several MS and that, even in those MS with high rates of compliance, there were specific problems related with the practice of specific companies.
- The results of this investigation reflect the feedback collected through a specific questionnaire, according to the criteria set up by the WP29. This investigation should, consequently, lead not only to the evaluation of the compliance of processing in the MS, but also to the evaluation of the means.

2. Pursuant to the findings, some specific issues can be highlighted, concerning concrete elements that need to be taken into account by the WP29 and the DPAs for future actions:
- It is necessary to include a question referring to the period of storage of personal data collected and processed by the investigated data controllers.
- With respect to the types of data processed, it was proved necessary to have more information on all potential applications, in order to allow more specific results on the necessity or lawfulness of processing of some particular types of data.
- Regarding security measures, the future questionnaires should be more prescriptive on the specific security measures applied by the data controllers. They should also be more detailed on the different positions of employees who are dealing with different types of data or who have access to different kinds of applications and, consequently, need different kinds of information.

3. Even considering the operational and methodological limitations of the enforcement approach, this action has identified a series of problems – some of them rather serious – in the processing of data by some controllers. These problems are identified in the second part of this report and must be corrected, whether by a separate initiative or by executive action on the part of the respective DPAs. This is the essence of any enforcement action; the primary objective has been completed, but beyond that, the action can have an anticipatory, exemplary ripple effect on those data controllers who were not directly subject to the investigation. They can improve their practices in light of the recommendations generated by the experiences of other, similarly-situated data controllers.

III. A strategy for the future: joint enforcement actions to improve global compliance and harmonise standards.

The overall outcome of the first joint enforcement experience undertaken by the WP29 was generally positive. The advantages of synchronised auditing with uniform criteria, of comparing results and promoting best practices in a given sector, are unquestionable. This precise function constitutes one of the essential abilities of the European DPAs, in accord with Articles 28 and 29 of Directive 95/46/CE.

These joint enforcement actions can and should improve and become more like true audit actions, which require the power to directly verify the truthfulness of responses. It is furthermore necessary to institute random checks on the selected data controllers as an integral part of such investigations.

The selection of new sectors or concrete practices on which to focus such audits should be based on an assessment of the risk a given sector or activity poses to the rights of data subjects, and should keep in mind the advantages of undertaking co-ordinated intervention at the European level over an individual action. This selection and evaluation is a new job for the WP29 and at the same time constitutes a challenge to the European DPAs to improve their own approaches, efficacy, and collaborative abilities.

In a similar vein, we should also consider the possibility of future collaboration between WP29 and other international entities or organisations with privacy enforcement abilities and

the ability to cooperate internationally (FTC, OECD, APEC, etc.) and in this way, contribute to a global improvement in data protection. Such cooperative efforts are not merely hypothetical; the OECD Working Party on Information Security and Privacy (WPISP) is engaged in discussions to adopt recommendations for cross-border cooperation in the enforcement of laws protecting privacy.

The WPISP recommendations closely mirror the collaborative framework used by WP29 and the lessons generated by this first joint enforcement experience. They call for the adjustment of domestic systems and the empowerment of domestic authorities to facilitate collaboration, as well as the development of international mechanisms for cooperation much like those in place in WP29. WPISP also recommends implementation of a reliable system of mutual assistance that parallels the cooperative duties imposed on European DPAs by Article 28 of Directive 95/46/EC. Finally, the WPISP recommendations suggest an open discussion with stakeholders – such as the relevant industry associations that proved so helpful in this enforcement action.

WP29 has the institutional knowledge, experience, infrastructure and legal mandate to sustain collaborative enforcement – not just at the European/regional level, but also globally. We are, therefore, uniquely positioned to participate in such international efforts and to ensure that joint enforcement approaches continue to be refined and improved with critical assessment of techniques and strategies. In-depth analysis of actions such as this one can inform cooperative enforcement in the international context, helping to accelerate the attainment of adequacy status by third countries and generating progress toward a global standard of data protection and the unimpeded flow of information across borders.

Second part:

Findings of the Investigation

This part of the report contains the findings of the private health insurance investigations, as reflected in the respective national reports. We chose to interpret compliance from a state level than from a number of companies level. This option was guided for practical reasons, since the penetration in the market and the size of the companies differed from one MS to

another. Accordingly, the numbers refer to MS and the percentages to the percentage of companies within the MS found in compliance, according to national reports.

The results of the questionnaire are structured around 5 categories of findings: type and cooperation of companies, processing of data, information to the data subject, communication to third parties and security.

A. Companies

1. Type of companies

Three types of companies were addressed: those covering (i) individuals, (ii) groups of persons (such as employees within a company) and (iii) families. The type of coverage is an important element, because it is related to the products offered and the types of data collected.
In 10 MS the survey was dealing with companies offering all types of insurance.
In 5 MS the survey was dealing with companies covering individuals and groups.
In 4 MS the survey was dealing with companies insuring only individuals.
In 2 MS the survey was dealing with companies covering individuals and families.

Since only in 4 MS the survey was dealing with companies insuring only individuals, we can consider that from the point of view of coverage the survey was rather high representative.

2. Market penetration

In 9 MS the investigated companies represented 90-100 % of the market. In 5 MS the level of penetration was 60-80%. In 3 MS the level of penetration was around 50%.

Given that the WP29 guidelines suggested contacting companies representing at least 50% of the market, we may conclude that representation was also in high levels concerning the penetration of the questioned companies in the market and that, accordingly, the survey was successful from this point of view.

3. Cooperation

According to the evaluation accomplished by the DPAs themselves, cooperation was positive or very positive in 15 MS. Cooperation was evaluated as negative in 3 MS and as medium in only 1 MS. This allows us to conclude that the cooperation of the investigated companies during the survey was highly positive.

But the general impression revealing from most of the national reports is that questions were not always sufficiently understood by the companies. Across most countries such companies are likely to have legal teams or specific data protection officers. Consequently whilst there might be some disagreements in interpretation, most companies will have a reasonably good understanding of the legislation and the issues will be down in part to the questions and in part how much effort was made in giving full and comprehensive answers.

The questionnaire dealt with complex matters and would have required a reasonable amount of time and effort to provide comprehensive and meaningful responses. The quality of the responses had more to do with the time and the effort necessary to answer the questionnaire reasonably well, rather than any inherent compliance issues.

In evaluating the cooperation of the companies one should consider that, in the vast majority of MS, responding to an investigation procedure by the DPA is part of the supervision system providing for in the national DP legislation and thus mandatory by law. It would be interesting to specify in which MS cooperation was not good although implied by law. This is an interesting issue to be addressed in future investigations.

In several MS the investigation was accomplished through the respective national association of insurance companies. Experience from those DPAs which had contacted their national associations was very positive. This highlights the importance of cooperation with the national associations in such investigations. It is always important to try to contact the associations of companies in national level in order to have a more global approach on the matter. This should be taken into consideration for future surveys.

B. Processing

1. Type of data

All companies in all 25 MS process personal information and health data. This appears to be expected. But if processing of general personal information is considered normal, we need to reconsider to what extend companies can ask for health data? Health data is sensitive information protected by stricter rules in European and national levels and it is not always obvious that this information is in close relation with the purpose of processing (management of the insurance contract). Health data is rather related to parallel purposes such as risk assessment. This does not mean that this practice is not in compliance with national legislation in a number of MS. The role of the proportionality principle has to be highlighted here.

Financial data are processed in 23 MS. The purpose of this processing is mainly the payment of primes and indemnities.

Insurance history data is processed in 17 MS. This is a rather high percentage. The processing of this data is mostly related with risk assessment, so that the company can evaluate whether a contract is beneficial for the company or to calculate the primes. Nevertheless, in some MS the law does not permit the insurance companies to refuse a contract, mainly for reasons of non-discriminated access to health insurance. In that cases, processing of information dealing with risk assessment should not considered justified even with the data subject's consent.

Processing of family information is taking place in 17 MS. This is justified only if the members of the family are covered by the contract. Two main issues are related to that:

(i) Consent and information of the members of the family, especially if they are not minors.

(ii) The type of family information. From the national reports it is not always clear if family information deals only with general personal information necessary for the management of the contract or if it includes medical (or even genetic) information. In that cases, see comments on the respective issues.

Collection and processing of genetic data is taking place in 6 MS. This is a rather important rate. Processing of genetic data is related with risk assessment but has much more considerable implications on data protection and compliance with the relevant applicable legal instruments in European and national level. According to the *WP 29 working document 91 on*

the processing of genetic data, adopted on 17th March 2004, this is permitted only if provided by law. The relevant *Recommendation of the Council of Europe of 2002* is also applicable on the matter. In most MS where processing of genetic data is practised, consent was noted as the main legal ground to do so. Consent cannot be a sole valid legal ground to process genetic data. This should be approached from a more global point of view.

As a general remark concerning the type of data processed, one could consider that the types of data processed are directly related to the nature of the product and the insurance risk. The questionnaire did not allowed to go further in depth in that matter. It would be useful for future actions to include in the questionnaire a full analysis of all applications and supporting forms in order to better assess the compliance.

2. Purpose of processing

In 22 MS contract management is the main purpose of processing. This is a compliant situation. In some national reports identification and communication are mentioned among the main purposes of processing (15 and 6 MS respectively). This should be read in the same context as contract management, as identification and communication are necessary to deal with the contract.

Risk assessment is at high level in 20 MS. There is a need to reconsider the compliance of this practice in respect with non-discriminated access to private health insurance services. On the other hand, in those MS where risk assessment is not prohibited by law, preventing insurance companies to proceed to it, may lead to significant increase of premiums. (See comments on processing of medical and genetic data above).

Among the main purposes of processing follow direct marketing (6 MS), fraud prevention (4 MS), statistics (1 MS) and consultancy (1 MS).

In general processing of personal information for other purposes, especially when those purposes are not always closely related to the main purpose, has to be evaluated in relation with a number of factors, such as national legislation, compliance of national legislation with the Directive, consent of data subject, quality of data subject's consent (free and informed)

and the possibility to provide the client an opt-in/opt-out option. The latter is a compliant practice according to some national legislation.

3. Legal grounds

Consent appears to be the main legal ground for the collection and further processing of the data by the insurance companies. In 18 MS the consent rate is at 100% and in 5 MS is at very high percentage. This can be evaluated as a positive result. It is not clear, however, whether the consent is always free and informed. Free and informed consent should be one of the main criteria for the evaluation of the companies' compliance in this field. Recommendations should be addressed to this direction.

Concerning the application of exceptions to the concept principle, the issue was not very clearly specified in the national reports, which makes the evaluation of this legal ground difficult. Only in 3 MS exceptions from consent constitute legal grounds for the collection and the processing of the data.

The same problem is posed concerning the right to object. Information given in the national reports is not always sufficient or clear to make a thorough evaluation in this field. Only from 4 MS we have a positive input in this question. This unclearness is maybe related to the definition of "further processing" towards which the holder has the right to object. It may be necessary for the DPAs to specify the sort of this processing (direct marketing etc.).

Finally as a general remark we should underline that evaluation of the legal grounds for collection and processing should be done only in relation with the relevant provisions of national legislation. In some legislation the collection of specific data for the main or/and further purposes may be mandatory by law. This is also related with the legitimacy or not of risk assessment in some MS. In those cases consent may have no major impact as a legal ground as law remains the main legal ground.

C. Information

1. Information on rights

Compliance concerning information given to the data subject achieves high percentages throughout most MS. In 12 MS companies inform about the rights of the data subject at a percentage 90-100% (100% in 10 MS). In 5 MS 75-90% of the companies inform about the rights of the data subject and in 3 MS 50-75% of the companies do so. Only in 2 MS the percentage of informing companies is lower that 50%.

Information of the data subject is a fundamental obligation provided in section IV of the Directive (art. 10-11). Nevertheless, this is not always the case in all MS. The information of the holder and other titular and beneficiaries of the insurance contract is part of this fundamental obligation. Although rates are rather high, the question is why the percentage of information is not in 100%, at least in those MS where information is mandatory.

2. Who is informed?

In 23 MS the holder of the insurance is informed. Nevertheless, only in 5 MS the titular of the contract (if he is other than the holder) or any other beneficiary of the contract is informed. This is a very important issue to address, since the capacity of the data subject has no impact, in the legal frame of the Directive, on the obligation of information. Every data subject should be duly informed, upon only criterion of processing of its data. Since personal information of any kind is processed, the company has the obligation to provide the subjects with this information and with all related documents.

3. Given information

Three types of information to the data subject were addressed: (a) information about the recipients of the data, (b) information about the processing of the data and (c) information about the potential international transfer of the data.

a) In 17 MS 100% of the companies inform the data subject about the recipients of the data. This rate is rather high.

b) In 17 MS 100% of the companies provide information about the general processing of their data. Unfortunately, there is no sufficient information from the national reports to evaluate the level and quality of specific information provided for automated processing.

c) Concerning information on international transfer of data, in 18 MS the companies claim that they do not transfer data. For the rest of the MS, the rate of companies that inform about international transfer of data is very low, not exceeding 30%.

D. Communication

1. Communication to third parties

According to the national reports, insurance companies in the totality of MS communicate personal information to third parties. In a high majority of cases, this is either inherent to the processing of the data or in compliance with national legislation, regarding specific categories of recipients.

These are the main categories of recipients of personal data, based on the answers given in the national reports. The numbers refer to MS:

Insurance related / reinsurers	25
Medicals	15
Related services (consultants, intermediaries, mailing, printing)	12
Banks	10
Other companies (within/outside the group)	7
Legal actions (lawyers, notaries, courts)	6
Providers of any kind of services	5
Public authorities (police, supervisors, other)	5
Social security	4
Insurance Associations	3
Parallel purposes (creditworthiness, direct marketing)	2
Family	2
Employer	1
Other	1

According to the above table, insurance related persons, medicals (within or outside the company), services related to those provided by the insurance companies and banks are the main categories of recipients of the holder's data in a vast majority of MS.

Regarding these specific categories of recipients, the communication is justified, as these recipients are more or less acting in fields related to the management of the contract and the obligations arising from that.

Information is not sufficient about medicals, as it is not always clear if the numbers refer to medicals acting within the company or having a specific contract with it, or if they refer to medicals that act on their own behalf. In any case, the respective national legislation on data protection and medical ethics is applied.

Apart from that we could see that there is a broad communication of the data to a numerous of recipients dealing with activities which are parallel, but not always directly related, with the main purpose (direct marketing, information trading, creditworthiness, law enforcement etc.) The lawfulness of such disclosure should be evaluated according to the national legislation and in relation with the principle of purpose.

2. Purpose of communication

In 20 MS the main purpose of the communication of the data to third parties is the accomplishment of the company's obligations arising from the insurance contract. In 10 MS risk assessment figures among the purposes of communication. In 7 MS, companies communicate personal information for direct marketing purposes, in 5 MS for fraud prevention purposes, in 3 MS for purposes related to justice and in 2 MS for taxation purposes. In very few cases (1 MS per purpose), data are communicated for purposes as consumer dispute, research, crime prevention and trading of personal information.

3. Legal grounds for communication

According to the national reports, the main legal ground for the communication of personal data to third parties is the law (7 MS), while in 6 MS the data subject's consent is necessary.

Three points have to be highlighted concerning communication to third parties:
- If it is not provided by law, communication to third parties should be done only upon consent of the data subject.
- Even communication upon consent should be examined under the purpose principle.
- Compliance of communication should be evaluated (i) according to proportionality principle and/or (ii) if this is in the interest of the data subject.

E. Security measures

1. Security measures

In 17 MS security measures are applied by 100% of the investigated companies. In 2 MS the rate of companies applying security measures is 70-90% and in 1 MS the percentage is 60%. Although the percentage is rather high, DPAs should enforce against companies to improve the situation in some MS in order to achieve 100% compliance in all MS. This is an achievable target.

Concerning application of security measures, in future actions the questionnaire should be more prescriptive, in order to receive more standardised replies. Specifically, questions should refer not only to whether the data controllers apply security measures, but also to the kind of measures applied and whether these measures are compatible with the relevant standards.

2. Information of employees

In 18 MS companies inform their staff on security issues at a percentage of 100%. This is a very high rate as far as it concerns information of the employees.

Again, at this point should, in future actions, be clarification in the questionnaire of the different positions of employees who need different type of information.

3. Types of security measures

According to the national reports, in all 25 MS, companies apply access control at 100%. Back-up is applied by companies in 24 MS (100% in 22 MS), among which in 20 MS daily. Security measures concerning remote access of data are applied in 20 MS (100% of the companies in 12 MS).

Companies apply special security measures for the processing of sensitive data in 19 MS (100% of the companies in 12 MS).

Among the security measures access control and daily back-up are the most frequently used in all MS. Security measures for remote access are also at high rates. This is a very positive sign as far as it concerns security in general.

Although security measures for the processing of sensitive data are applied in 19 MS, companies fully apply specific security measures in only 9 of those MS.

For the Working Party

The Chairman
Peter SCHAAR