Revisiting Sensitive Data (1999), by Mr. Spiros SIMITIS

Professor at Johann Wolfgang Goethe University of Frankfurt am Main, Director of the Research Centre for Data Protection (Germany)

Review of the answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) (Strasbourg, 24-26 November 1999).

I. Premisses

Reflections on both a conclusive definition and a convincing delimitation of "sensitive data" as well as on the consequences of any such classification of personal data for an efficient protection of the data subjects are all but unusual. They have in fact accompanied data protection from its very first days. The early Norwegian attempts to elaborate methods permitting to distinguish personal data according to their sensitivity are as significant for the importance attached to a series of data whose processing was deemed to be particularly risky for the persons concerned as the clearly articulated demand of the French legislators to simply prohibit the use of such data.

While however the initial discussions were, as illustrated by the history of the German data protection laws, first and foremost debates on whether "sensitivity" really is a valid criterion for determining the conditions of the processing, both the context and the purposes of the debates were set anew by the adoption of the Council of Europe's data protection convention. It explicitly (article 6) sanctioned the quest for a particular regulatory regime of sensitive data, a position that since then has been over and over underscored by the Council's recommendations. The consequence is easily discerned. The existence of per se "sensitive data" ceased to be contested. The Convention officially acknowledged them as a pivotal element of all further regulations regarding the use of personal data. Hence, the sole relevant question was, from then on, how to best achieve the Council of Europe's definitely restrictive expectations for the use of the sensitive data enumerated by the Convention.

As a result, the reference to sensitive data was ritualised. Not a single law passed after the Convention disregards or even questions the inclusion of a provision phrased on the lines of the Convention. As obvious as the differences between, for instance, the British, the Dutch or the Spanish data protection acts may otherwise be, the consensus as far as sensitive data are concerned can hardly be overlooked. They all grant sensitive data a special status. Thus, when in October 1995 the EC Data Protection Directive was adopted, the majority of the member States had, not least under the influence of the Council of Europe, already subjected sensitive data to particular rules. It was therefore not surprising that the Directive joined the by then long list of regulations in the view of which sensitive data must be treated in a clearly distinct way.

But the Directive chose a more radical approach. Instead of sticking to the flexible wording of the Convention it just interdicted the processing of the sensitive data mentioned in article 8 para. 1. In order to correctly estimate the range of the prohibition the structural differences between the Convention on the one hand and the Directive on the other must be taken into account. The Convention is lastly no more than an offer. The States are given the opportunity to inhibit the risks stemming from the processing of personal data by applying an internationally approved regulatory model. The Convention does however not prejudice their decision. They are in other words perfectly free to enact a regulation corresponding to the Convention's principles, to elaborate rules better fulfilling their expectations or even to abstain from any restriction. Not so in the case of the Directive. Its clauses are not proposals but prescriptions and to the extent that alternatives are tolerated they must fit into the regulatory frame established by the Directive. Where a common regulation is both the incentive and the aim, conformity necessarily prevails.

Discrepancies such as the obviously contradictory perception of sensitive data can therefore not be maintained. Countries, like Austria and Germany, that had consistently rejected all abstract categorisations of personal data and instead focused on a context-oriented appreciation of the data, must consequently abandon their long-standing practice and for the first time expressly recognise the existence of sensitive data. Thus, the new Austrian Data Protection Act lists in accordance with the Directive the sensitive data (sect. 4, para. 2) and specifies, again in agreement with the Directive's expectations, the conditions of their use (sect. 9). Similarly, the draft for the transposition of the Directive into German law confirms the readiness to revise the hitherto defended views with regard to sensitive data and incorporates provisions addressing their processing.

All in all, the Directive finishes what the Convention had begun. Sensitive data are both nationally and internationally seen as a constitutive element of any regulation concerning the use of personal data. As paradoxical as it may however sound, the longer the list of laws grew that attach a particular importance to sensitive data, the more critical questions regarding the precise range of sensitivity and the credibility of a pointedly prohibitive approach were raised. The routinely inserted clauses in an ever greater number of regulations did thus not dissipate queries and doubts. But the rather general remarks increasingly gave way to a detailed analysis of sensitive data.

As long indeed as the request for a distinctly restrictive regime repeated similar statements either contained, like in the case of data revealing the racial origin, political opinions or religious beliefs, in the national constitutions, or, as in the case of data related to the state of health, traditionally dealt with by specific regulations, there seemed to be no need for further considerations. The data protection laws simply emphasised well-known demands and at the same time underscored their expectation that the use of all such data be excluded. Once however this intention has to be transformed into concrete directions for the various processing operations, abstract references to sensitive data quickly prove as untenable as a strictly prohibitive policy. All existing regulations are therefore notwithstanding their differences marked by two basic dilemmas also illustrated by nearly every answer to the questionnaire:

a. The persistent claim that sensitive data can and must be defined in an exhaustive manner collides with constant attempts to either bypass or to review the apparently definitive list.

b. The categorically declared intention to radically limit the processing of sensitive data is contradicted by a virtually endless list of exceptions.

II. Regulations and experiences

1. The relativity of the lists

For most data protection laws the enumeration of the sensitive data is comprehensive. Thus, neither the French nor the Austrian, British, Czech, Estonian, Finnish, Greek, Hungarian, Italian, Spanish, or Swiss laws hesitate to explicitly qualify the list they contain as exhaustive. Only very few laws, as, for instance, both the Danish acts and the Icelandic law, consider their lists as merely indicative. But what at first appears to be an undeniably exceptional attitude expresses in reality a conviction shared by all legislators. The large majority of the actual laws may certainly suggest that the attribute "sensitive" is reserved to an exclusive class of data carefully selected by the legislators. None of these laws contents however itself with the statement that its list is exhaustive. On the contrary, they all provide ways and means to reopen the apparently definitely closed list.

a. The proviso of a legislative intervention

It is probably easiest to declare, as, for example, the Estonian act does, that the list can be supplemented by law. What looks like a superfluous truism has in fact a strategic function. The legislators may at all times exercise their privilege to determine the content of the law but the individuals can be sure that there is only one way to alter the composition of the list and thus modify the access to their data, the adoption of a law. The change is hence bound to a strictly formalised process that guarantees a maximum of transparency and stability and therefore also protects them against too quick and too many changes. The legislative intervention has however also another equally important side. It demonstrates that there is no definitive list of sensitive data. The still widespread assumption that the lists contain no more than a few once and for all fixed data is a pure fiction. The best that one can expect is that at least some of these data will be included in most enumerations. The legislative intervention illustrates and embodies the variability of the list.

That the legislative intervention is all but a theoretical means to question and review the composition of the list is demonstrated by the answers to the questionnaire. Thus Finland amended the original enumeration in order to include trade union membership, an extension also envisaged by the Netherlands and Norway. Both countries intend besides to revise the actual enumeration, the first by striking out psychological data, the latter by redefining the reference to family affairs. Portugal, finally, renounced, as did Estonia, a special protection of data related to the property and to the financial situation of the data subjects, but included genetic data in its list. Each of these cases demonstrates that the enumeration of sensitive data is throughout understood as an ephemeral indication.

Legislators act, as also the T-PD stressed in its fourth meeting in May 1990 on the application of Art. 6 of the Convention, under the proviso of a re-examination of the list in view of both the experiences with the use of the individual data and new exigencies.

The inclusion of trade union membership is a typical example of an alignment with rules developed by the courts in discrimination cases as well as in connection with questionnaires used by employers. As to the elimination of the data regarding financial situation, the abandonment of their special status is not least a result of the growing impact of sunshine laws, whose main purpose is to increase the transparency of financial activities. That the access to information regarding the financial situations, and consequently the creditworthiness of the data subjects must nonetheless be limited is best illustrated by the crucial role of data protection laws in connection with the processing of consumer data. But, as necessary as restrictive measures are, they obviously do not, as for instance the Danish Private Registers or the Irish Data Protection Act show, justify their incorporation into a sensitive data list. There is, lastly, no better example for the need to update lists than genetic data. They were hardly noticed when the first lists were put together. By now, however, there can be no doubt that no other data provide such comprehensive information on the persons concerned. Never before were the risks of the processing of personal data therefore so evident. Irrespective of whether the opportunities to be employed, the chances to obtain health insurance, or the limits of a rapidly expanding commodification of the individuals are at stake, the accessibility of genetic data determines the answers. No list of sensitive data can henceforth disregard genetic data without questioning its seriousness.

b. The interpretation process

Modifications of the lists may certainly also be achieved through the interpretation of the items already included. The answers to the questionnaire show that the interpretation process has indeed affected the range of the lists. While most of the data are part of all lists, their understanding is clearly not common. Thus Estonian, French and Norwegian law agree that the restrictions applicable to the processing of data related to race or ethnic origin are irrelevant as far as nationality is concerned. They all, in other words, regard nationality as a clearly "non-sensitive" datum. The Austrian law adopts a more lenient position. Nationality is in its view a "less-sensitive" datum. The CNIL is in contrast obviously not willing to really "declassify" nationality data. It in fact demands that the necessity to process them should in any case be thoroughly scrutinised. The Dutch law definitely goes further. According to the explanatory memorandum of the Dutch sensitive data decree and to the opinion of the Data Protection Authority, a correct application of the rules governing the use of data indicating race or ethnic origin presupposes a broad interpretation that must necessarily also cover nationality.

Genetic data are another equally significant example. Interpretation assumes in their case, because of the lack of an explicit reference in the lists of sensitive data, a particularly important role. It can indeed help to close the gap. The difficulties should however not be underestimated. There are certainly cases in which it is perfectly possible to regard genetic data as health or medical data. But it is nonetheless not justified to conclude that

genetic data can under all circumstances be entered into either of these two categories. Most laws have therefore avoided a general classification and instead put the accent on the specific uses of genetic data. Their growing importance makes it, however, difficult to maintain such a carefully differentiated approach that inevitably leaves an ever greater number of processing operations uncovered. The initial hesitations were hence gradually given up. Genetic data were, as the example of Austrian, Icelandic, Norwegian, Portuguese and Swiss law, but also of the Recommendation R (97) 5 on the Protection of Medical Data shows, simply subsumed in the health or medical data. And even where doubts persisted, the repeated legislative interventions unmistakably restricting the use of genetic data were, as in France, seen as proof of their particular sensitivity that fully justifies treating them like all other sensitive data.

c. The impact of the context

Considerations such as those underlying both the legislative proviso and the interpretation process culminate sooner or later in a standpoint exemplified by the British, Danish, French and Swiss answers to the questionnaire. Sensitivity is no more perceived as an a priori given attribute. On the contrary, any personal datum can, depending on the purpose or the circumstances of the processing be sensitive. All data must consequently be assessed against the background of the context that determines their use. The specific interests of the controller as well as of the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its possible consequences for the persons concerned are factors that, put together, allow both the range and the effects of the processing to be discerned and thus to determine its degree of sensitivity. An evaluation of the sensitivity requires hence more than a mere look at the data. It may very well be that, for instance in the case of genetic data or of data concerning criminal convictions, the risks for the data subjects are more or less obvious. However, the sensitivity can in the end only be affirmed if all the elements typical of the particular processing operation are taken into account.

The relevance of the context is also illustrated by two rather unusual examples that are both mentioned in the questionnaire. The first is images and sounds. Austria, Denmark, France, Iceland, Italy, the Netherlands, Norway and Switzerland answered in exactly the same way. They all stressed the connection between the circumstances of the processing and any attempt to classify the data. And indeed: for most laws it is by now clear that it makes no difference whether the data are stored in a computer, collected in a file or contained on a video as long as they can be ascribed to an identifiable person. The next step depends however once more on the context. Its characteristic elements either pave or bar the way to rules that tighten the restrictions. Thus, for instance, data on photos and videos can, as the Dutch, Italian and Norwegian answers remark, be sensitive any time they reveal information on the race or the sexual behaviour of the persons concerned. The legislators may, as shown by the French answers, limit, for instance, the control competence of the supervisory authority in the case of video-surveillance of public spaces. No such regulation affects however the assessment of the data. On the contrary, the monitoring of public spaces is, as exemplified by police videos of demonstrations, a particularly pertinent example of the sensitivity of the data gathered.

Similarly, the use of personal identificators is, irrespective of their form, inevitably linked to the processing of personal data. Moreover, the sensitivity of at least some of the identificators seems to be out of the question. Genetic fingerprints, social security and personal identification numbers are the most salient examples. Context-oriented considerations prevail again nonetheless. A clearly limited use for purposes exhaustively defined by law and a deliberate exclusion of numbers providing information on their own on the data subjects are, as illustrated by the Dutch, French, Portuguese and Swiss answers, amongst the measures that allow, but at the same time reduce, the use of personal identificators to a few precisely indicated processing operations under clearly prescribed conditions.

The same distinctly context-oriented approach predominates, finally, whenever personal data are put together to dress either a general or, as in the case of traffic data, a mobility file. That profiles are especially sensitive when based on an automated processing of personal data is demonstrated by provisions such as articles 15 of the Directive or 2 of the French Data Protection Law. Reflections on the profiles do however not substitute considerations on the data employed. Each of them must on the contrary also be assessed in view of its possible use for a particular profile. For exactly this reason the processing of traffic data, for instance, is subject to mandatory restrictions delimiting their employability. In sum, absolute classifications of personal data are here as elsewhere supplanted by a distinctly situational assessment. Sensitivity is no longer an attribute granted once and for all but a characteristic determined by the context of the intended use that therefore has in principle to be constantly reappraised.

2. Diversity of the data

The assumption that certain data are per se sensitive furthers the view that the data concerned are part of a small nationally and internationally acknowledged group of data, an understanding promoted by the wording of both the Convention and the Directive. The answers to the questionnaire convey, however, a different picture. They confirm in fact a tendency visible since the earliest years of data protection. Although it is true that the recognition of the data enumerated by the Convention as well as by the Directive transcends by far national boundaries, it is also correct that these data are no more than the hard core of national lists. National legislators have amplified the primary list by a whole series of very different data. They have however one thing in common: the choice of the supplementary data reflects problems typical of a particular country or society. While, in other words, the hard core is based on enumerations closely related to international human rights conventions, the additions renationalise at least to a certain extent the legislative intervention.

A first, rather surprising, example are the data regarding trade union membership. The Convention did not include them, the Directive cites them expressly. The divergence is all but accidental. At the time of the Convention especially the Scandinavian States saw no reason to mention them. In their view such a reference is simply superfluous once collective bargaining functions in a both efficient and frictionless way. For those however who advocated the inclusion, the decisive argument was that in their experience

unionised workers were still discriminated and should consequently be protected by inhibiting the collection of data revealing trade union membership. That the standpoints still differ is illustrated by the Austrian answers. They fully coincide with the position defended in the late seventies and early eighties, in particular in Norway and Sweden.

A second, equally characteristic example are the references to social security data as, for instance, contained in both Greek and Swiss law. The wording of the Danish and the Icelandic law is broader. Instead of addressing social security they speak of data related to "social problems". What they mean, however, is information related to the support provided in economically, physically and psychologically critical situations. But even in countries in which, as in Germany, the law has up to now deliberately renounced enumerating sensitive data, the processing of social security data is subject to a markedly restrictive regime. Few other barriers are as high as "social secret". The background is the same everywhere. To the extent that individual risks are socialised, the transparency of individual behaviour increases. The condition for providing support is an ever growing amount of data meticulously depicting both the problems and the general situation of the data subjects. Where therefore social security systems are institutionalised and continuously expanded, the data they process quickly reach the top of the sensitivity scale.

Social changes are also at the origin of the third example. Drugs and addiction generate their own data basis. It ranges from an extensive documentation of the personal history of the persons concerned and information on the various forms of help provided to police data and criminal convictions. As necessary as collection may be, it inevitably accentuates the vulnerability of the data subjects. Laws such as the Icelandic and the Norwegian data protection acts have therefore expressly included data related to drug or alcohol addiction in their sensitivity lists.

3. Degrees of protection

The logic of sensitivity seems to imply that all data concerned should be subject to the same degree of restriction. Consequently, most answers to the questionnaire categorically rejected the idea that the degrees of protection may differ. The plain denial was sometimes underscored by a statement permitting the decisive argument to be discerned. Thus, the Italian answer draws the attention to the structure of the relevant provision in the data protection law. As in all other similar regulations, the law simply juxtaposes the various data and hence chooses a wording that disavows all attempts to treat whichever of the data differently.

The opposite is however the case. Already three of the laws that at least "in principle" favour uniform rules tolerate distinctions. The Austrian, French and Italian answers point to the high degree of sensibility of genetic data and the ensuing necessity to secure an equally higher protection. The Hungarian answer goes further and openly advocates a split. Especially the data concerning racial or ethnic origin, political opinions, party affiliations or religious beliefs are deemed to be more sensitive. Danish law intensifies also the protection of data related to "political matters", but only partially. As long as they have not been accessible to the general public their processing is prohibited.

The tendency to relax the restrictions for some of the sensitive data is no less common. Criminal convictions are the classic example. Interestingly enough neither the Convention nor the Directive include them in the actual list. They are cited and, in the case of the Directive, also treated separately. But irrespective of whether they are directly placed on the list of sensitive data or only mentioned in connection with it, no law has ever considered prohibiting absolutely the processing of criminal convictions or even assimilating the restrictions on their use to what is in general thought to be an appropriate standard for sensitive data. On the contrary, all laws opt for a system carefully channelling the access.

Criminal convictions thus confirm and underline the Dutch answer to the questionnaire. There are finally no special categories of sensitive data. There is merely a special regime for each of these data. Their use may be generally regarded as a possible source of particular risks for the data subjects. However, whether and to what extent these risks justify an exclusion of their processing, is a question that can only be answered separately for each of these data and in consideration of the circumstances characteristic of the specific use. Both the relativity of the restrictions and the necessity of a situational approach are hence once more confirmed.

III. Conclusions and recommendations

1. Increasing flexibility

The readiness to develop and enforce rules intensifying the protection of data subjects in accordance with the degree of sensitivity of the data processed is evident. But there is neither a generally accepted exhaustive list of sensitive data nor can their use be unconditionally prohibited. The sources of the lists vary as much as their content. International agreements and national constitutions are just as specific demands of particular branches of the national laws and the emergence of new social and political problems at the origin of their components.

Besides, sensitivity is no more than a mere alarm device. It signals that the rules normally applicable to the processing of personal data may not secure adequate protection. Its primary consequence is therefore to incite a reflection process the purpose of which is to locate the shortcomings of the existing regulations and to establish the improvements needed. Both the starting point and the range of all considerations are determined by the potential contexts of the processing. They permit the specific risks to be discerned and the antidotes to be designed. Prohibition is hence a possible but by no means a compelling consequence. And even where it appears justified to forbid the use of certain data, the prohibition remains a reaction confined to the context that legitimates and at the same time limits the exclusion of the processing.

In the interest of a both credible and transparent regulation, two conditions must therefore be respected. Firstly, omnibus regulations must definitely renounce statements declaring expressly or implicitly that any processing of sensitive data is prohibited. All they can ask for is an adequate protection. Secondly, sensitivity lists must be phrased in a way that

unmistakably indicates their purely exemplary character. Their components can hence always be complemented or replaced.

Both requirements reveal and underscore however also the limits of omnibus regulations. If the context is really to be the primal criterion for restating the prerequisites of an adequate protection, the conditions of the processing must be fixed in a sectoral regulation. Only where the legislators can fully concentrate on a specific context, are they also able to reach a degree of precision that appropriately responds to the particularities of the processing circumstances. A situational approach is, as experience at both the national and the international level have time after time demonstrated, necessarily also a sectoral approach.

2. Securing a reliable protection

Distinctly context-oriented rules are however only one of the prerequisites of a both conclusive and efficient regulation of sensitive data. The other equally decisive requirement is the reduction of the present lists of exceptions to a few exhaustively enumerated and precisely defined cases. Almost none of the actual dispensations can therefore be exempted from a thorough review. Already the seemingly incontestable exception heading every list, the consent of the data subject, is anything but convincing. Consent is, contrary to still widespread views, not a master-key opening all doors to any data potential controllers are interested in. Employment relationships are only one of many examples demonstrating that consent does not necessarily guarantee a participation of the data subjects enabling them to freely decide whether their data should be processed for purposes known and approved by them. The chances of interfering and influencing the processing depend essentially on the circumstances in which the data subjects are asked to agree and, more precisely, on their particular position with regard to the processor. Employment relationships underscore therefore the fallacies of the assumption that consent incorporates and secures the data subjects' power to determine the use of their data. Hence, both national laws and international documents such as the ILO Code of Practice on the Protection of Workers' Personal Data deliberately exclude consent whenever the employer intends to use, for instance, data regarding criminal convictions or genetic data. It is the law and not the parties that in each of the cases conditions the access.

But probably the most critical item on the exception lists are clauses that legitimate access for public interest reasons or in order to combat criminal activities and to safeguard public security. Terms like public interest or public security are de facto a carte blanche allowing all restrictions finally to be bypassed. The references to both are therefore usually followed by a statement specifying that the conditions of the access have to be regulated by law. However, all such provisions address merely the form but not the substance of the prospective rules. Public interest and public security remain consequently an inexhaustible source of interventions adapting the processing of sensitive data to government policies. Thus, the crisis of the traditional social security systems steadily intensified efforts to obtain an ever greater number of health data, not only with the intention of establishing a solid data basis for the urgently needed reduction of the growing costs, but also in view of measures meant to prompt the data subjects

individually to buy less medicine and to substantially diminish the number of doctors' visits. The impact of these policies on attempts to enact special rules for the processing of sensitive data can be easily traced in the Directive.

All in all, provisions containing no more than a few very general terms burden the data subjects with the risk of access to their data, the conditions and limits of which are indiscernible. Moreover, they openly contradict the legislators' intention to seriously restrict the processing in the case of sensitive data. Sensitivity is reduced to a merely ornamental function where the access can be broadened without any difficulties. Exceptions can certainly not be avoided. But as justified as they may appear, they are intolerable as long as their wording is not precise, their purposes and consequences not clearly determined, the data asked for not confined to really necessary information and the use limited to unmistakably defined controllers.

3. Extraterritorial effects

Regulations subjecting sensitive data to a particularly protective regime especially draw the attention to transborder flows. The more sensitivity is emphasised, the more it appears only natural to safeguard the use of sensitive data regardless of where the data are processed. At least as long as sensitivity is understood as an emanation of fundamental, universally acknowledged values such as the respect of political opinions and religious beliefs, or the rejection of racial and ethnic discrimination, special rules for transborder flows are seemingly a compelling complement of the provisions governing the processing of sensitive data within national boundaries.

However, before extending the special regime, the effects of the normally applicable standards should be carefully considered. Their basic principle has already been developed by the earliest data protection laws and since then over and again affirmed by all national regulations and stressed by many of the answers to the questionnaire. A transfer can only take place if an equivalent protection is secured in the addressee's country. The quest for such protection applies to all personal data. It does furthermore not imply the existence of identical provisions. All it demands is a functionally equivalent regulation. It is in exactly this sense that the Directive (article 25) not only requests an adequate level of protection but also enumerates against the background of the experiences of the national data protection authorities some of the criteria that have to be taken into account in order to correctly assess the rules in the addressee's country.

In short, neither the course and the result of the evaluation are determined by abstract considerations but by the circumstances characterising the specific processing operation. The attention focuses, in other words, entirely on the individual case. Whenever hence the processing involves data subjected to special treatment, the admissibility of a transfer depends on the existence of a similarly privileged protection in the country of destination, a view obviously also shared by the T-PD in its eighth meeting in January 1993 on the interpretation of Art. 6 of the Convention and especially of the "appropriate safeguards" demanded by the Convention for any use of such data. The case by case approach secures thus a degree of flexibility that permits adapting the requirements in order to ensure

protection corresponding to the risks of the particular transfer. Additional provisions specifically addressing the transborder flow of sensitive data are therefore not needed.

It may however be advisable to complete chapter III of the Convention by provisions explicitly dealing with transmissions of personal data to countries that are not parties to the Convention. All the more because the actual regulation obviously also incites misinterpretations, particularly in the case of sensitive data. A rule such as article 12 para. 3 is only understandable against the background of common standards regulating the processing of personal data. But precisely this assumption does, with a few exceptions, not apply to states that are neither parties to the Convention nor members of the European Union.