DATA PROTECTION AND EMPLOYMENT IN THE EUROPEAN UNION

An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and its Member States

By MARK FREEDLAND

Professor of Employment Law in the University of Oxford

Oxford 1999

Data Protection and Employment in the European Union

An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and its Member States

CONTENTS

Data Protection and Employment in the European Union

An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and its Member States

Executive Summary

1. Introduction - the Purpose, Methodology and Scope of the Study.

A Purpose and Methodology.

The purpose of this study is to seek to answer the following question, which has two parts. Firstly, what advantage is there, within the legal systems of the member states of the European Union, in having a data protection regime which applies specifically to employment relationships? Secondly, what if any action could usefully be taken at Community level to bring about, encourage, or give shape to such regimes? Firstly, we seek to identify the problems of data protection in the sphere of employment in a way which is specially responsive to the needs of the employment relationship. Secondly, we attempt to synthesise a scheme of analysis telling us what a robust overall structure of employment-specific data protection might look like. Thirdly and finally, we consider what role for Community action is implied by such a scheme of analysis.

B Definition of the area.

1 The concept of data protection.

The concept of "data protection" used to be focused upon the storage of and access to information in electronic form. We could say that this conception of data protection prevailed from the 1970s until comparatively recently - let us say until the early 1990s. It has, however, gradually been emerging that we could have a different, and more far-reaching, conception of data protection, which would extend to the full range of monitoring and surveillance practices which now exist in the employment sector

2 The concept of employment.

Equally, if, ten years ago, we talked about a sector-specific treatment of data protection for the employment sector, we probably still had in mind simply the traditional sphere of application of labour law. Now, by contrast, changes in the structure of the labour market and the practice and perception of employment relationships point towards a much looser less monolithic definition of "employment".

3 The Public Sector and the Private Sector.

There is another significant respect in which it has become appropriate in current conditions to adopt a more than previously flexible and inclusive approach to the definition of the scope of employment for the purposes of employment-specific data protection frameworks, namely in relation to the distinction between the public and the private sector.

II A Structural Analysis of Data Protection and Employment.

A Stage I - the Basic Rights, Expectations, and Public Policy Considerations.

1 The Basic Rights or Expectations of Workers in Relation to Data Protection.

1.1 The right to privacy and the right to private life. The evolution of coherent legal frameworks for data protection in relation to employment seems increasingly clearly to depend upon recognising that this right or expectation has to be expounded in its more ambitious form.

1.2 Other rights and claims of workers - health, safety and welfare at work, equality and freedom from discrimination. The heading of health, safety and welfare at work is relevant because in most legal frameworks that heading is increasingly recognised as extending to those forms of damage to health, safety and welfare which consist of or result in stress and psychological trauma. The heading of equality or freedom from discrimination is relevant as information technology increases employers' capacity and incentives to apply various forms of discrimination and inequality in, and in the formation of, employment relationships.

2 The Interests of Employers. These are claims to which great and increasing importance is attached in the legal and policy frameworks of the member states and of the European Union itself, namely the interest in conducting efficient, competitive and flexible enterprises or productive processes.

3 Public Policy Considerations. At the employment-specific level, we have to add that many member states now regard the employment sector (both public and private) as a crucial one for implementing their laws and policies about immigration, racial and ethnic integration, tax and social security fraud, and particular types of criminal or anti-social behaviour.

4 Conclusions to Stage I. Firstly, we found that the basic rights or claims to data protection in the employment sector are more extensive and more multi-faceted than is at first obvious. In particular, those rights or claims go beyond rights or claims to "privacy" as such. Secondly, we found that those rights or claims have to be balanced against an extensive range of countervailing interests of employers, and also against some distinct public policy considerations.

B Stage II of the Analysis - Areas Requiring Regulation

1 Method of holding or use of information - automated or non-automated. Latterly, the computerisation of information storage, in relation to employment as in other spheres of social

and economic life, has become so widespread and generalised that it has largely ceased to be a criterion of the requirement for regulation

2 Source of information and extent of transmission. These cannot be regarded as decisive criteria in the employment sector. As to the former, it is not realistic to expect to confine the employer's acquisition or use of information about workers to data obtained from the workers themselves. As to the latter criterion, we cannot regard this as a key indicator of the fact or extent of requirements for regulation in the employment sector.

3 Type or subject-matter of information. We might say that information is specially sensitive, therefore specially requiring rigorous data protection, if its subject matter is so intimate to the personality of the individual worker that its acquisition and use in and of themselves threaten the right to private life

4 The stage or aspect of the employment relationship. Although this criterion seems to focus special attention upon recruitment, it also, on further reflection, draws our attention in different senses to needs for data protection during the continuation of employment relationships as well as upon their termination.

5 Method of acquisition or assembly of personal information. It is quite helpful to list types of data transaction in the employment sector which seem particularly to threaten rights to privacy and private life, or rights to health, safety and welfare at work, according to the methods of gathering and marshalling information - thus, as different forms or ways of testing or monitoring workers or job-seekers.

6 The changing roles of personal data use in the management of employment relationships.

Essentially, there seems to be a general dynamic towards the broadening of the roles of personal information use from the relatively limited traditional roles of selection and discipline into a new set of functions which have to do with the motivation, incentivisation and acculturation of workers, and the control of their behaviour. The increasing centrality of *appraisal systems* of all kinds is a central, though not the only, illustration of this phenomenon.

C. Stage III of the Analysis - Establishing the Appropriate Regulatory Norms

1 Organising principles. It is suggested that the optimal approach can most nearly be arrived at by regarding the regulatory task as an *integrative* one. We will tend not to see and grasp this potential if we regard general data protection norms as hard-edged rules. We should rather regard them as *organising principles*, in the sense of principles which serve to organise a norm-making process which produces specific normative solutions to concrete problems in particular sectors and contexts. We can distinguish a group of principles which impose *qualitative* controls, and another group of principles which impose *procedural* controls upon the acquisition and use of personal data in relation to employment.

2 Qualitative controls

2.1 The principle of *confidentiality* can be expressed, in the employment context, as a norm requiring that in general personal data relating to workers or job-seekers should be regarded and treated as confidential to them.

2.2 The principle of *proportionality* is to the effect that the acquisition and use of personal data about workers or job-seekers shall take place so that the extent of its encroachment upon their basic rights, interests, and legitimate expectations is no more than is proportional to the need to achieve the purposes for which the acquisition and use of those data are allowed and established as appropriate.

2.3 The principle of *necessity* may be articulated as a requirement that in situations appropriately identified as specially sensitive ones, the acquisition and use of personal data about workers or job-seekers shall take place only to the extent and in the manner necessary to achieve purposes the pursuit of which is either sanctioned by law or otherwise identified as essential in the general public interest.

3 Procedural controls

3.1 The principle of *notification, access and verification* is that, in general, workers or job-seekers should be guaranteed, either personally or through appropriate representatives, access to and the opportunity to verify personal information about them which is acquired or used in the context of employment relationships.

3.2 The principle of *consent* is to the effect that, in general, workers or job-seekers should be given, either personally or through appropriate representatives, meaningful opportunities to decide whether to give consent to or withhold consent from the acquisition and use of personal information in ways which relate to them or affect them.

3.3 The principle of *information and consultation* is that, in general, workers or job-seekers should be informed and consulted, either personally or through appropriate representatives, about the acquisition and use of personal information by employers in ways which relate to them or affect them.

4 Conclusions to Stage III. There is a crucial continuity between the process of norm-making which we have just considered. and the process of implementation which we go on to consider in the next and final stage of our four-part analysis.

D Stage IV of the Analysis - The Implementation of Data Protection Norms in the Employment Sector.

1 Regulatory Functions. There seem to be *three main types of regulatory functions* to be covered, namely,

1.1_ adjudication of disputes and complaints,

1.2 registration and administrative regulation, and

1.3 the making and revising of codes of practice.

2 Institutional Arrangements. There seem to be *three main types of institutional arrangement* to be put in place, namely

2.1 judicial or quasi-judicial machinery

2.2 the appropriate administrative agency or agencies, and

2.3 machinery for self-regulation and social dialogue.

3 Conclusions to Stage IV. There is a complex task of combing these conclusions about implementation with the conclusions from the three earlier stages of the analysis. There are very many possible permutations between the findings at the different stages, and it would be very unwise to suggest that there was a single valid pattern. But merely to present a structure for systematic thinking about the options has some utility.

III The case for action at European Union level.

In this concluding section, it is suggested that the structural analysis of data protection needs and methods in the employment sector has indicated both a basis and rationale for action in this field at European Union level, and a set of ideas about the form which such action might take. The basic rights, claims and interests which are at stake in relation to data protection in the employment sector in particular, we find that they are all ones with which the European Union is seriously concerned - the right to private life by reason of its place in the European Convention on Human Rights, the right to health, safety and welfare at work as a matter of Social Policy, the rights to equality or against discrimination as the results of specific commitments at EU level to combat discrimination, and the interests in efficiency and competitiveness as a matter of employment policy in particular and economic policy in general. The assessment or auditing of employment data protection frameworks has to be a continuing and dynamic process. It will presumably be felt that such a process of assessment has to consist first and foremost of self-assessment by and within member states. Equally, it is to be hoped that there would be a consensus in favour of a reporting and reviewing process at European Union level.

Data Protection and Employment in the European Union

An Analytical Study of the Law and Practice of Data Protection and the Employment Relationship in the EU and its Member States

I Introduction - the Purpose, Methodology and Scope of the Study.

A Purpose and methodology.

The purpose of this study is to seek to answer the following question, which has two parts. Firstly, what advantage is there, within the legal systems of the member states of the European Union, in having a data protection regime which applies specifically to employments relationships? Secondly, what if any action could usefully be taken at Community level to bring about, encourage, or give shape to such regimes? [1]. This study is constructed around a set of tentative answers to those questions. That set of tentative answers forms a working hypothesis which is explored and tested in the course of the study.

[1] The author of this study wishes to acknowledge not only the full co-operation which he has received from DGV of the European Commission, but also the valuable research assistance at the preliminary stages of , and comments at later stages from, John Craig and Hazel Oliver, and also help from the staff of the European Documentation Centre of the Bodleian Library Oxford, especially Elizabeth Martin, in respect of access to published sources of material relevant to this study. However, the views expressed in this study, and any errors or omissions in detail, are to be regarded as the responsibility of the author alone.

That working hypothesis is formulated against the following background [2]. General legal frameworks for data protection are now relatively well established in the European Union, both within the legal systems of the member states, and at Community level by virtue of the Data Protection Directive 95/46/EC [3]. However, the development of specific legal frameworks for data protection in relation to employment is much less extensive at both those levels, and much less congruent and more "patchy" as between the member states. This is a matter for concern in that data protection raises extremely important, and somewhat specialised, issues in relation to employment. As we shall see in the course of this study, two sets of developments converge from different starting-points to produce that result . On the one hand, rapid changes in the field of information technology, and the evolution of the "information society", affect employment relationships in a of special ways. On the other hand, employment relationships themselves are undergoing very significant changes which have major implications for data protection.

The carrying out of the study has involved analysing the national responses to the questionnaire administered on this subject to the relevant authorities in the member states by the Commission [4]. All of the fourteen member states responding to the Questionnaire viewed themselves as having *general* legal frameworks which provided data protection in the employment sector, whether derived from general constitutional provisions, from general data protection legislation or from general employment legislation, and the fifteenth, Sweden, is to be viewed in the same way [5]. However, none of those (with the possible exception of France) can be regarded as having a comprehensive data protection framework which is specifically constructed for the employment sector, even if many have employment-specific measures of various kinds which are relevant to data protection, such as provisions about the powers of works councils, or about the use of medical records in relation to employment.

---

[2] The working hypothesis which is tested in the course of this study is comparable to the central ideas which are explored in Professor Spiros Simitis' extremely valuable thematic paper of February 1995, *Towards a regulation of the processing of employee data: Premises and Principles.* Although the detailed formulations diverge in important respects as between that paper and this study, and although the enactment of the Data Protection Directive in October 1995, anticipated in Professor Simitis' paper, changed the practical context quite considerably, this study owes an intellectual debt to that paper.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *Official Journal No L 281, 23.11.1995 pp. 0031 - 0050.* A fuller account of the general legal data protection framework provided at Community level by virtue of the Data Protection Directive is given at various points in this stuy where the extent and influence of Community action in this field is under consideration; see especially text at footnotes 13 to 17 below.

[4] European Commission DGV Questionnaire of April 1997 on the protection of the rights and freedoms of Workers, in particular their right to privacy with regard to the processing of data and the use of technical monitoring devices.

[5] See generally and for Sweden in particular, Flaherty, David, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, Chapel Hill and London, 1989) pp 1-15, Bennett, Colin *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, Ithaca, 1992) pp 1-11.

In that context, then, we put forward a working hypothesis which consists of three tentative suggestions. Firstly, it is suggested that a response or set of responses, to the needs identified in the previous paragraph, is already necessary and important within the European Union, and is likely to become increasingly necessary and important in the near and medium-term future as the dynamics described in the previous paragraph become more intensified. The second tentative suggestion is that action of a broad co-ordinatory kind at Community level would be helpful towards creating that response. The third such suggestion is that Community action of that broad co-ordinatory kind might be increased in validity by a clear and robust structural analysis of the problems of data protection in the specific context of employment relationships. The present study seeks to explore and pursue those suggestions.

The most appropriate way to fulfil the aims described in the previous paragraphs would seem to be to proceed in three stages. Firstly, we should seek to identify the problems of data protection in the sphere of employment in a way which is specially responsive to the needs of the employment relationship. Secondly, we should attempt to synthesise, from an awareness of those problems, and from the many positive examples of data protection measures within member states, a scheme of analysis telling us what a robust overall structure of employment-specific data protection might look like. Thirdly and finally, we should consider what role for Community action is implied by such a scheme of analysis. We shall proceed according to that methodology[6].

[6] This study is presented in the form of a *text*, which contains the principal arguments or observations, and an accompanying *commentary*, which provides supporting detail and examples and illustrations of the main arguments. The commentary is contained in a series of supplementary paragraphs which form two *sequences*, respectively numbered (i) and (ii). The first sequence develops the main arguments more fully at a *supranational* level and at the level of the *general* writings and debate about employment data protection, while the second sequence deals with the corresponding discussion at *national*, that is to say *member-state* level. For this purpose, a system of abbreviations will be used to refer to particular member states, as follows: Austria = A, Belgium = B, Denmark = D, Finland = Fi, France = Fr, Germany = Ge, Greece = Gr, Ireland = Ir, Italy = It, Luxembourg = L, Netherlands = N, Portugal = P, Spain = Sp, Sweden = Sw, United Kingdom = UK.

The central task of this study is therefore to conduct a structural analysis of the needs for and the patterns of development of legal frameworks for data protection in relation to employment in the European Union. This will be done by drawing upon a supra-national discourse which already has a real existence at a European level, and which offers valuable guidance as to how the logic of the national legal frameworks might best be developed in the employment sector. This European supra-national discourse derives from several sources. It comes partly from the pronouncements of the Council of Europe and of the ILO on the application of data protection principles to the employment relationship, that is to say, respectively, the Council of Europe Recommendation of 1989 on the Protection of personal data used for employment purposes[7], and the ILO Code of practice of 1997 on the Protection of workers' personal data[8]. But it can also be derived from the expertise which the European Commission has already assembled on this subject, which can now be related to, and can build upon, the general Data Protection Directive[9]. The discourse can also draw upon the more general policy documents and reports of and from the European Commission which relate to the information society[10], to issues of growth and competitiveness[11], and to the role and content of employment and social policy[12]. In short, one can embark upon a partly prescriptive structural analysis of data protection in relation to employment with the confidence that there is a body of wisdom on which to draw which has some objective status.

It will be useful at this point to identify the general purpose and effect of the Data Protection Directive, and to show how it provides a modern basis for the development of employment-specific data protection frameworks. DPD served to bring together into a single structural framework the main ideas and impulses which were shaping the evolution of general data protection frameworks in the member states. DPD takes data protection beyond the scope

---

[7] Recommendation No. R (89) 2 adopted by the Committee of Ministers of the Council of Europe on 18 January 1989 (Strasbourg, 1989), which will be abbreviated to CER. CER has an integral, authorised, Explanatory Memorandum which we shall refer to as CEREm.

[8] *Protection of workers' personal data - an ILO code of practice* (Geneva, International Labour Office, 1997), which will be abbreviated to ILOC; ILOC has an integral, authorised, Commentary, which we shall refer to as ILOCCom.

[9] The Directive will be denoted by the abbreviation DPD. It has a Preamble containing 72 recitals; the abbreviation DPDPre will be used to refer to the Preamble, followed where appropriate by numbers referring to particular recitals (for example, DPDPre 10).

[10] The best starting point for this discussion is the report known as the Bangemann Report, *Europe and the Global Information Society, Report of the High Level Group on the Information Society* (1994).

[11] The main starting point being the European Commission White Paper, *Growth, competitiveness, employment - The challenges and ways forward into the 21st century*, (COM (93) final, Luxembourg: Office for Official Publications of the European Communities, 1994.

[12] For this we could now refer, for instance, to the European Commission Communication, *The Social and Labour Market Dimension of the Information Society: People First - The Next Steps* COM (97) 390, 1997

of automatic processing into the realm of manually processed personal data in filing systems[13]. It lays down a set of "principles relating to data quality" such as those relating to fair and lawful processing, or to relevancy or accuracy[14], and a set of "principles relating to the reasons for making data processing legitimate" such as unambiguous consent of the data subject[15]. From the point of view of the present study, the Directive serves as an important confirmation that

> "data processing systems are designed to serve man; ... they must, whatever the nationality or residence of natural persons, *respect their fundamental rights and freedoms*, notably the right to privacy, and *contribute to economic and social progress*, trade expansion and the well-being of individuals"[16] , and that
>
> "the establishment and functioning of an internal market in which the free movement of goods, persons, services and capital is ensured require *not only that personal data should be able to flow freely* from one Member State to another, *but also that the fundamental rights of individuals should be safeguarded*"[17] .

It is that balancing or reconciliation of free and efficient trade and commerce with the fundamental rights of individuals which is the central task of data protection; however, the Directive does not develop rules for carrying out this task specifically in relation to the employment sector. An essential preliminary to that employment-specific analysis is to define the area under consideration.

B Definition of the area.

If we say that our area of concern in this study is that of data protection and employment relationships, that seems, on the face of it, to identify a clearly and precisely defined topic. However, on further examination the concepts both of data protection and of the employment relationship turn out to be somewhat imprecise. That is partly because the empirical content of

---

[13] Art. 3.

[14] Art. 6.

[15] Art. 7.

[16] Recital 2 (emphasis added).

[17] Recital 3 (emphasis added).

each of those two concepts is changing quite rapidly. Nevertheless, we need to establish some outlines at this stage, and we should do this by questioning firstly what we mean by data protection and secondly which social and economic relationships we regard as employment relationships.

1 The concept of data protection.

There is a real sense in which, at least in the English-speaking world and perhaps beyond it, the concept of data protection has come not merely to identify an area of concern but also to confer a certain kind of legitimacy upon legal regulation within that area of concern. This occurs because the terminology of "data protection" seems to describe a concept which is essentially technological or scientific in nature, and which thus avoids being political or ideological. It is, moreover, a terminology which suggests a concern with regulating access to or use of "data" as if those were disembodied, abstract items of technical information. The evolution of this concept was itself a reaction to the very rapid automation of the storing and processing of information which was brought about by the development of the computer. The concept of "data protection" was thus focused upon the storage of and access to information in electronic form.

(i) CER is very much a product of this phase in the development of data protection framework; it represented a sector-specific adaptation of Council of Europe Convention for the Protection of Individuals with regard to *Automatic* Processing of Personal Data of 28 January 1981[18] (emphasis added). CER 1.1 states that the principles of CER apply to automatically processed data, and to other data in so far as necessary to make automatically processed data intelligible, and CEREm 16 explains that CER "is essentially directed at personal data undergoing automatic processing" - though CER 1.1 did add that "Manual processing of data should not be used by employers in order to avoid the principles contained in this Recommendation" and 1.2 authorised member states to extend the principles to manual processing in general.

(ii). Where member states enacted general data protection legislation down to the early 1990s, that legislation was usually directed at *automated* data processing, as in A, Ge, Ir, L, P, S, UK.; but examples of a relatively early inclusion of manual data processing are to be found in D, Fi.

We could say that this conception of data protection prevailed from the 1970s until comparatively recently - let us say until the early 1990s. It has, however, gradually been emerging that we could have a different, and more far-reaching, conception of data protection.

[18] Council of Europe: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series No 108 (Strasbourg, 1981).

As we become more and more accustomed to the existence of all kinds of collection of data in electronic form, we become less attached to the idea of regulating those electronic data bases in and of themselves. We come to realise that "data protection" is an essentially elliptical notion which we have to expand, and of which we have to identify the constituent elements. Thus expanded, it becomes the idea of *regulating the acquisition and use of* data *for the* protection *of the individuals to whom the data relates.* In this expanded form, the idea is as evidently societal as it appears to be merely technological in its compressed from. In this study we adopt this wider, fuller, meaning of data protection.

(i) One of the main purposes of DPD was to carry the development of data protection beyond its old boundaries so far as the mode of data processing is concerned, and in particular so far as the distinction between manual and automatic processing is concerned. Compare, for example, DPDPre 14 which identifies "the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons" and the need to apply the Directive to such data. DPD did not, however, extend data protection to *all* manual processing, but to manual processing "of personal data which form part of a filing system or are intended to form part of a filing system" -DPD Art. 3.1 - compare DPDPre 15. For the further requirement that the filing systems must, if DPD is to be applicable, be structured according to specific criteria, see Art 2(c) and DPDPre 27. ILOC is applied, by s.4.2, to "the manual and automatic processing of all workers' personal data.

(ii) The member states which had not previously done so are generally in the course of enacting or implementing legislation to give effect to the extension of data protection so that it includes the manual processing of personal data, at least in or via filing systems, as DPD requires; consider, in particular, current or recent legislative activity in A, B, Ge, Gr, It, and UK.

2 The concept of employment.

In the previous paragraphs, we saw that, when we come to define the idea of "data protection and employment", the meaning and scope of "data protection" are by no means as clear and obvious as might at first be thought. The same is true of the "employment" element of that idea. If, ten years ago, we talked about a sector-specific treatment of data protection for the employment sector, we probably still had in mind simply the traditional sphere of application of labour law. That is to say, we meant the area defined by reference to the stereotype of the full-time permanent employment relationship constituted by a contract of employment and characterised by the clear subordination of the employee to the employer. We might have included the relationship between civil and public servants and their state or public authority employers, but it is unlikely that we would have had a wider stereotype in mind.

(i) Thus, it is not surprising to find that CER 1.3 used the term "employees" to identify the workers to whom the Recommendation was applicable; CEREm 15 suggests that the use of that relatively narrow terminology was uncontroversial at that time.

Now, by contrast, changes in the structure of the labour market and the practice and perception of employment relationships point towards a much looser less monolithic definition of "employment". That is to say, we now have to consider, as the result of the growth of a more "flexible" labour market, a variety of types of employment, involving many combinations of full-time and part-time work, permanent and fixed-term employment, and dependent and semi-dependent work relationships. Moreover, and as part of the same set of developments, employment relationships are no longer nearly as uniformly bipartite as they used to be. They may much more readily be multipartite, as where the "employment agency" has not merely an introductory role, as has always been the case, but also, as is now much more common than before, a continuing role as the co-ordinator of work for one or a number of client-employers. Again, we may find that the role of employer is distributed between the franchisor and the franchisee of a commercial activity. In these ways the scope of "employment" has become more ambiguous and controversial than it used to be.

(i) ILOC uses the term "worker", s.3.4 making it clear that includes "any current or former worker or applicant for employment". ILOCCom 3.4 comments that ILO instruments generally do not define "worker", leaving it to national law and practice. Whereas CER, in Art. 1.4, simply declares that its principles apply to the activities of employment agencies in their capacity as enabling the making of contracts of employment with prospective employers, ILOCCom 3.4 goes further, and declares that "because the code of practice covers workers and applicants for employment alike, both direct employers and employment agencies are subject to the principles laid down therein", specifically including "temporary workers who are referred [by employment agencies] to other employers". Compare also ILOC 13, to the effect that if an employer uses employment agencies to recruit workers, "the employer should request the employment agency to process personal data consistently with the provisions of this code". Very valuable insights into the impact of changes in labour market practice upon understandings of the personal scope of employment law are provided by the recent report of the Madrid Group of Experts[19].

(ii) Given that few if any Member States have yet enacted comprehensive data protection frameworks specifically for the employment sector, this has not yet been a major issue at national level. However, where national labour legislation does impinge upon the area of data protection, it would seem that it is generally framed around the category of "employees" rather than the somewhat more comprehensive category of "workers".

[19] *Transformation of labour and future of labour law in Europe,* Final report, June 1998, V/98/776 - see especially chapter 2 , "Work and Employment Status".

3 The public sector and the private sector.

There is another significant respect in which it has become appropriate in current conditions to adopt a more than previously flexible and inclusive approach to the definition of the scope of employment for the purposes of employment-specific data protection frameworks, namely in relation to the distinction between the public and the private sector. In the early development of general data protection frameworks, there was, although with some notable exceptions at national and sub-national level, some tendency to exclude the public sector, on the assumptions either that the interests of the state were systematically paramount over claims to data protection, or that state functionaries were in a position quite different from that of workers in general, in which it was less appropriate to accord them data protection. Certainly, many labour law systems used to distinguish totally between employees of the state and other workers. However, recent tendencies wholly or partly to privatise many previously state or public sector activities have eroded such distinctions to the point where they are not generally capable of being maintained in any coherent way. For the most part, the thinking about data protection in the employment sector has responded by envisaging a common regime for both public and private employment, no doubt with important reservations in respect of national security and other such considerations of state.

(i) DPD Art. 2(f) defines data controllers to include public authorities, though Art. 3.2 excludes processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in the areas of criminal law. Art 1.1 of CER ensured that the principles set out in the Recommendation apply both in the public and private sectors, in this respect like the 1981 Data Protection Convention from which CER is derived. Similarly, s. 4.1 (a) of ILOC declares that "This code applies to the public and private sectors", and ILOCCom explains that "The amount and kind of information retrieved may differ, but employers in both sectors gather data to assess the suitability of workers for a specific occupation or to evaluate their performance."

(ii) In so far as the data protection frameworks of the different member states depend upon the general employment legalisation of the country concerned, they may treat private sector employees and public functionaries in quite distinct categories, as for example in D, Fr, Ger, It; but all the member states with general data protection legislation seem to have accepted or to be in the course of accepting the need for that legislation to extend both to the public sector and to the private sector.

The foregoing discussion has a further purpose or message beyond its immediate one of defining the scope of the present study; it also serves to indicate a key feature of the content of this study. The conclusion which emerged from examining the two elements of the idea of "data protection and employment" was that each element was in its own way dynamic, a changing conception. It is this sense of being in the middle of the evolution of a sphere of regulatory activity, changing both in scope and content, that will be developed in the course of the present study. This is the main key to the structural analysis of the present state of affairs, which forms

the second part, and to the suggestions about a rationale and basis for Community action, which forms the third part, of this work.

II. A Structural Analysis of Data Protection and Employment.

The question from the previous chapter is, how might one best analyse the existing legal frameworks for employment-specific data protection and draw upon the supra-national or Europe-wide discourse in order to refine and improve that analysis? The purpose of this section is to suggest that this can best be done by considering employment-specific data protection as a regulatory system, the logic and functioning of which can be analysed in four distinct, though strongly inter-connected, stages. The four stages are:-

I Identifying the basic rights, legitimate expectations and public policy considerations which are at stake;

II Identifying the practices requiring regulation;

III Establishing the appropriate norms or regulatory conditions;

IV Establishing the appropriate processes for implementation.

This chapter is concerned with explaining more fully what each of these stages means or involves and how they relate to each other.

A Stage I - the Basic Rights, Expectations, and Public Policy Considerations.

We begin stage I of the analysis by indicating, or reminding ourselves, of the sense in which we are trying to identify the basic rights, expectations and public policy considerations which are to be recognised as being at stake in a rational and coherent framework of data protection for the employment sector. As we have previously acknowledged, that process of identification is ultimately a prescriptive or evaluative one. However, the intention is to carry out that analysis *reflexively*, so that it reflects the current practice and the logic of employment-specific data protection in the member states of the European Union. Viewed in that way, each of the stages of the analysis becomes an exercise in making a synthesis from the legal frameworks in the different member states, and identifying the main areas of convergent or divergent development. That involves, in particular, noting the employment-specific developments or trends. This process turns out to yield very interesting results at each stage of the analysis, not least as a result of separating out the different stages of the analysis from each other.

Using the approach outlined above, we find that, as compared with the typical general account of the rights and expectations which are at stake in data protection frameworks, the picture for the employment sector in particular needs to be more carefully drawn. Thus, a general account of the legal framework for data protection will usually concentrate on the right

of the data subject to "privacy", and will tend to view that right to privacy as more or less synonymous with the idea of the "right to private life". This right will normally tend to be seen as limited by reference to a few basic considerations such as those of national security or of the enforcement of the criminal law. In relation to the employment sector, we really need a more complex analysis, both of the rights which workers or job seekers have, and of the other or competing claims or considerations to be borne in mind. On the one hand, the basic rights which are at stake seem to go beyond privacy rights. On the other hand, the competing claims or considerations are also complex, and we have to distinguish between employers' interests on the one hand, and public policy considerations on the other hand.

(i) The focus on the right to privacy as the basic (though not exclusive) rationale for general data protection is reflected in DPD Art 1.1, which states as the Object of the Directive that "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".

(ii) The same emphasis is found in the general data protection frameworks of many member states, especially those where the basis for data protection is a constitutional one. Examples are A (refers to European Convention on Human Rights Article 8[20]), Fi (S. 8.1 of the Constitution Act protects the privacy, integrity and domestic peace of the individual), Fr (Law on Informatics, Computer Science and Freedom of 6 January 1978, s.1 - "Computer science must not injure human rights, private life and individual and public freedoms"), Gr (Law 2472 of 1997 transposes DPD "with a view to protecting the privacy and fundamental rights of natural persons"), It (Act No. 675 of 31.12.96 Art 1.1 - "the rights, fundamental freedoms and dignity of natural persons, especially as related to privacy and personal identity"), Ne (Basic Constitutional Law, Art 10 - Respect for personal privacy) Sp (Constitution of 1978, Art. 18(4) - "The law shall limit the use of information technology to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights).

[20] Article 8 of the European Convention on Human Rights and Freedoms ("ECHR8") states that
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

1 The basic rights or expectations of workers in relation to data protection.

Continuing, therefore, to a categorisation of the basic rights or expectations of workers in relation to data protection, it is suggested that we need to elaborate the general data protection framework in two main ways. Firstly, we need to recognise that the right to privacy or private life has become a complex conception in the context of employment, having a number of different aspects and needing to be sub-divided in order to understand its full extent and ramifications. Secondly - and this is equally important - we also need to acknowledge that, in the employment sector, the concept of privacy, even if articulated in a wide form, no longer provides a full account of the rights or expectations which are at stake. Only by making these two conceptual steps can we hope to capture the full range of issues about civil liberties, interest in the personality, and claims to social and economic freedoms which are at stake here.

1.1 The Right to Privacy and the Right to Private Life.

It seems to be widely accepted in the member states of the European Union that workers have a claim to be covered by a legal framework of data protection which derives from a right to privacy or private life. Sometimes a right of that kind is to be inferred from, or is closely linked to, the measures that member states have taken to respond to the development of computers. Where that is the case, the right tends to be formulated in terms of privacy as a claim to confidentiality or secrecy of personal data, or of seclusion of the individual from the surveillance of others. Sometimes, on the other hand, a right of that kind is derived from a larger, more general, set of constitutionally protected human rights. In that case, the claim will tend to be, more far-reachingly, formulated in terms of a right to private life, of the kind so significantly recognised in Article 8 of the European Convention of Human Rights when it declares that "Everyone has the right to respect for his private and family life ..." [21]. The evolution of coherent legal frameworks for data protection in relation to employment seems increasingly clearly to depend upon recognising that this right or expectation has to be expounded in that more all-embracing form.

(i) A useful set of discussions of this theme is to be found in the symposium of papers published by the Comparative Labor Law Journal in 1995 on the subject of the right to privacy in relation to employment; see, for general discussion, Professor Gerhart's Introduction and Overview on Employee Privacy Rights[22]; also, in the ILO *Special*

[21] See full text above, fn. 14.

[22] Comparative Labor Law Journal Vol 17:1 (1995) pp. 1 et seq.

Series on workers' privacy of the *Conditions of Work Digest* see Professor Simitis' analysis of issues surrounding workers' privacy [23]

[23] ILO, *Special Series on workers' privacy, Conditions of Work Digest*, Volume 10 No. 2 (1993).

(ii) The publications referred to in the previous paragraph also each have corresponding analyses for many of the particular member states of the EU. [24]

The ways in which "the right to private life" is more far-reaching than "the right to privacy" are especially significant to data protection in the employment sector; but in order to understand why this is so, we have to identify the different aspects of "the right to private life". Thus, it is particularly relevant to the employment relationship that "the right to private life" is widely seen as a recognition of the claims of individuals to respect for their *dignity* and *autonomy*. But even this degree of separation of distinct elements is not enough to give a clear guide to the content of "the right to private life". Indeed, we are unlikely to be able to be very precise in this respect. We are, after all, talking about broad principles rather than detailed rules. Nevertheless, we can observe that the idea of respect for the dignity and autonomy of individuals itself seems to break down into two main divisions. Firstly, it represents the notion of respect for civil liberties, especially those of freedom of expression, freedom of association, and freedom of religious or political opinion. Secondly, it also represents an idea of protection of the personal space which people need if they are to exist and develop as individuals in a meaningful way and choose their own lifestyle. It will be evident that employment relationships are a crucial location for the working out of those ideas.

1.2 Other rights and claims of workers - health, safety and welfare at work, equality and freedom from discrimination.

In many analyses, it is regarded as appropriate to expound the whole legal framework for data protection in terms of a basic right to privacy or private life. However, even given the wide construction of that basic right which we have outlined above, it does not seem that a complete picture can be provided for the employment sector in terms of that basic right alone. It does not even seem that the total range of rights and claims of workers can be satisfactorily brought under that one heading. There seem in fact to be two further headings or groupings of workers' rights or claims which we need to consider. The first is that of health safety and welfare at work. The second is that of equality, non-discrimination, and economic and social mobility. We proceed to expand briefly upon those headings.

In the case of these two headings, it is relatively uncontroversial that workers have these rights or claims in some shape manner or form. That is to say, the legal systems of all the member states of the European Union accord some degree of protection to workers in respect of their health, safety and welfare at work, and some guarantees of equality or freedom from various kinds of discrimination such as sex discrimination, or racial, ethnic or religious

[24] See also the very useful analysis by Professor Alpa of the linguistic and wider issues about the meaning of "privacy" which has been carried into Italian law in its English version - Guido Alpa, *The Protection of Privacy in Italian Law*, University of Oxford, 1997.

discrimination. More controversial is the proposition that such rights are significantly at stake in employment-specific data protection regimes. It is more appropriate to leave the detailed exploration of that proposition to stage II of this analysis; suffice it at this point to give some basic indications why these headings are relevant in general terms.

The heading of health, safety and welfare at work is relevant because in most legal frameworks that heading is increasingly recognised as extending to those forms of damage to health, safety and welfare which consist of or result in stress and psychological trauma. There are, it emerges increasingly clearly, various forms of data use in employment relationships which may impinge upon those rights or claims in that sense. The heading of equality or freedom from discrimination is, for its part, relevant as information technology increases employers' capacity and incentives to apply various forms of discrimination and inequality in, and in the formation of, employment relationships. That relevance is increased as further forms of discrimination are prescribed or controlled; in the area of employment, the specification of rights or claims against discrimination is a decidedly dynamic process as, for example, in the case of disability discrimination or discrimination based upon sexual orientation.

The previous few paragraphs have indicated how important it is, when analysing the basic rights, claims, and considerations which are at stake in data protection in the employment sector, to move from the general discourse of data protection - which as we have indicated tends to be led or dominated by developments in information technology - to a more authentically employment-specific discourse which will follow the contours and home in on the special features of the employment relationship. Thus, when identifying the workers' basic rights and interests, we moved, as it were, from the very general concern with privacy and private life towards a more employment-specific breakdown of those concepts, and so on to even more employment-specific claims, such as the claim to protection of health, safety and welfare at work. In similar vein, we need to be as employment-specific as possible when identifying the rights or considerations which are at stake *other than* those of the workers' themselves. This involves looking separately at, on the one hand, employers' interests, and, on the other hand, at public policy considerations.

2 The Interests of Employers

The employer as data user is exercising a general prima facie right or freedom to acquire and use information the acquisition and use of which is not specifically controlled - that is, a sort of general freedom of information or of action. It is, however, useful to articulate rather more specifically the basic claims which we regard employers as having to acquire and use information about workers, and to distinguish those claims from public policy considerations in favour of the acquisition and use of data. For these are claims to which great and increasing importance is attached in the legal and policy frameworks of the member states and of the European Union itself, namely the interest in conducting efficient, competitive and flexible

enterprises or productive processes. This basic claim provides a useful reference point for the further stages of this analysis.

A very useful articulation of the claims to efficiency and competitiveness in the context of the "information society" is provided in the European Commission White Paper on Growth, Competitiveness and Employment[25]:-

> "With easier access to information, it is becoming increasingly easy to identify, evaluate and compete with economic activities in all sectors. The pressure of the market-place is spreading and growing, obliging businesses to exploit every opportunity available to increase productivity and efficiency. Structural adaptability is becoming a major prerequisite for economic success. The growing interconnection of the economy is leading to major productivity improvements in the production of goods but also in relation to services, and the borderline between goods and services is becoming increasingly blurred. ... To be able to compete worldwide, European industry must exploit all possible ways of improving its competitiveness by making growing and effective use of ICTs (information and communications technologies)"[26].

This point is further defined as follows by the Communication on the Social and Labour Market Dimension of the Information Society [27]:-

> "The introduction of ICT together with organisational changes, in the context of a globalised economy, are driving forces for productivity gains and thereby for higher profits and real wages, which form the basis for further new demand and new employment. Employment is also affected through the changes in demand for more and broader skills and for fewer unskilled people. The more effective the transformation of profits into new investment and from old skills to new skills, the stronger the employment growth and the quicker the reduction of unemployment"[28].

(i) ILOC Preamble is also very useful in this respect in articulating the purposes for which employers collect personal data, with the implication that these are, generally speaking, *legitimate* purposes:-

> "Employers collect personal data on job applicants and workers for a number of purposes: to comply with the law: to assist in selection for employment, training and promotion; to ensure personal safety, personal security, quality control,

---

[25] See above, fn.11.

[26] At para. 5.1.

[27] See above, fn.12.

[28] At para. 39.

customer service and the protection of property." ILOCCom adds the further purpose, "and to organize the work process" (at p.16).

3 Public Policy Considerations

All the basic rights or claims so far discussed could be regarded as constituting, at least indirectly, public policy considerations in themselves. It is, after all, clear that there is a public or communal interest in the securing to workers of their civil liberties, their claims to health safety and welfare at work, or their claims to equality and against discrimination. In other words, there are clearly public policy considerations sustaining data protection in the employment sector. However, it is useful to distinguish, from those, as it were indirect, public policy considerations, a number of direct public policy considerations which in the law and practice of various member states of the European Union constitute important factors in favour of certain kinds of acquisition and use by employers of information about workers or job-seekers. Again, it is useful in identifying those factors to move from the level of general data protection to the level of data protection in the employment sector. At the general level, there are the usual, almost universal, considerations of national security, the upholding of the criminal law, and the maintenance of public health and safety. At the employment-specific level, we have to add that many member states now regard the employment sector (both public and private) as a crucial one for implementing their laws and policies about immigration, racial and ethnic integration, tax and social security fraud, and particular types of criminal or anti-social behaviour such as paedophilia or pornography. This often means that employers are expected to acquire and use information about workers or job-seekers for those purposes, as also for the purpose of ensuring that workers engaged in providing services to the public are doing so in a safe and satisfactory way. In short, there are significant public policy considerations, to which additions are being made quite rapidly, militating against, or at least limiting, the data protection accorded to workers in particular.

4 Conclusions to Stage I.

What provisional assessments can we take forward from stage I of the analysis to the subsequent stages? Firstly, we have found that the basic rights or claims to data protection in the employment sector are more extensive and more multi-faceted than is at first obvious. In particular, those rights or claims go beyond rights or claims to "privacy" as such. Secondly, we have, on the other hand, found that those rights or claims have to be balanced against an extensive range of countervailing interests of employers, and also against some distinct public policy considerations. Thirdly, by representing the task or agenda of employment-specific data protection as, at this basic level, a balancing process between competing considerations, we increase the likelihood that solutions or approaches to data protection which may be proposed on the basis of such an analysis will be accepted as balanced and well rationalised. So it is from that set of starting points that we move to consider what are the specific areas requiring data protection regulation in the employment sector.

B Stage II of the Analysis - Areas Requiring Regulation

This second stage of the structural analysis of data protection in the employment sector consists of identifying the particular areas requiring regulation, and also of differentiating between those areas in terms of the degree or intensity of regulation which is required. This will be done by building on Stage I of the analysis, in the sense that we shall consider in what ways different sorts of data transactions, or practices consisting of the acquisition or use of data, impinge upon the basic rights, claims or public policy considerations which we identified in Stage I. First we need to explain more fully what we mean by "areas requiring regulation" and "degrees of regulation".

If the analytical framework for employment-specific data protection is to be robust and convincing, it has to identify a field of operation which is narrower, and depicted in a more rationalised way, than the entire area of information transactions relating to employment. In the early phase of development of legal frameworks for data protection, it appeared as if data protection could satisfactorily be focused upon electronic or computerised information transactions, but it would now generally be accepted that we cannot solely focus upon that sphere. A coherent method of focusing upon areas requiring regulation has, instead, to be more sophisticated in several respects. Firstly, as we have already explained, it has to be related to the basic rights, claims, and public policy considerations identified in Stage I of the analysis. Secondly, it has to be multi-dimensional. Thirdly, it has to be employment specific. It has to be multi-dimensional in the sense that it has to analyse information transactions in a number of different ways, such as according to type of information, method of acquisition, storage, or communication, or the kind of use to which the information is put. It has to be employment-specific in the sense that those dimensions have to be related to the different stages or aspects of work relationships; are we, for example, concerned with recruitment, with the termination of employment, with the ongoing conduct of work relationships and so on.

The existing law and practice of general data protection supports a distinction between, on the one hand, personal data in general, and, on the other hand, specially sensitive personal data such as medical reports. In the context of employment, it seems important to recognise the need, which that distinction implies, to differentiate between degrees of intensity or rigour of data protection regulation, and to apply that differentiation to the different areas requiring regulation which we have identified. We suggest that, in the employment context at least, this requires a more complex analysis than is achieved simply by singling out "sensitive personal data". For, useful though that concept is, it may fail to reflect the fact that it is the way in which different dimensions combine or interlock which really identifies specially sensitive areas or situations requiring specially sensitive regulation. For example, it might not be satisfactory to say that information from drug tests constituted "sensitive data" in and of itself, but we might wish to say that where the information from drug tests was (a) used in decisions about recruitment, and (b) held and/or transmitted in computer files for that purpose, that combination

of factors did create a "specially sensitive data situation", requiring specially stringent regulation. The ensuing paragraphs pursue the analysis along those lines.

(i) Supranational as well as national formulations generally support the notion of specially sensitive data *types* rather than, as argued for here, a more complex conception of specially sensitive data *situations*, though perhaps there is some movement towards the latter approach. Thus CER 10 deals with particular categories of *data*, DPD Art 8 also creates "special categories of data"; ILOC 6, on the other hand, under the general heading of "Collection of personal data" in effect designates special data *situations*, particularly by going on to deal with forms of testing (6.10 - 6.13) and monitoring (6.14).

(ii) National formulations almost invariably identify a typical set of specially sensitive data types consisting of data relating to political, religious or other beliefs, trade union membership or activity, sex life, criminal record, and health record. There are some interesting variations around that typical pattern; examples are:- A includes pregnancy; D uses the notion of "data on an individual's purely personal circumstances"; Fr uses broad category of data on sickness and disability, not just health records; Gr includes philosophical with religious beliefs, and "social welfare" with sex life; It also includes philosophical beliefs, and, similarly to Fr, "health conditions" generally; Sp has a composite category of "ideologies, religion or beliefs".

1 Method of holding or use of information - automated or non-automated.

As has been indicated previously, the fact that data is stored or applied by automatic or electronic means, that is to say, generally speaking, on or by computers, used to be regarded as one of the strongest indications of a requirement for data protection regulation. The perception was that the computerisation of information storage, or of decision-making, was, in and of itself, threatening to the privacy or to the right to private life of the data subject. Latterly, the computerisation of information storage, in relation to employment as in other spheres of social and economic life, has become so widespread and generalised that it has largely ceased to be a criterion of the requirement for regulation - though it remains in the background as a reason for a general high level of concern with data protection, in the employment sector at least as much as in other sectors.

By contrast, it may be said that we would generally continue to regard the automation or computerisation of decision-making, that is to say the production of decisions by automatic, programmed, processing of data relating to workers or job-seekers as in and of itself threatening to their rights to private life, because of the extent to which it seems to deny their individuality or personality. On the other hand, there will be kinds of decision where we do not in fact regard this as problematical, because we regard the decisions in question as entirely in the nature of calculations - such as decisions as to the extent of liability to social security contributions out of payments of wages - and automation might even, up to a point, be an aid to the achievement of objectivity in the treatment of workers, and to the reduction of certain kinds of discrimination or

inequality. So automation of decision-making is thus to be regarded as a factor potentially requiring regulation, but to an extent which is contingent upon other factors such as the kind of information which is involved, and the role of the decision in the process of management - factors which we consider in later paragraphs.

(i) The concern with automated decision-making has been significant in supranational formulations. The main manifestation of this is in DPD Art 15 which expresses a strong principle against automated individual decisions. The theme recurs in ILOC 5.5 - 5.6, which advance the principles that decisions concerning a worker should not be based solely on the automated processing of that worker's personal data, and that personal data collected by electronic monitoring should not be the only factors in evaluating worker performance. But ILOCCom at p.27 makes it clear that there is an anxiety not to press these principles too far:-"The code thus rejects a purely mechanical decision-making process and opts instead for a clearly individualized evaluation of workers. It should, however, be clear that the accent is on the word *solely*. The code therefore does not reject the use of automated procedures. ... *[Not intended to have as wide a range as the EU Directive]"* (emphasis added) - an interesting illustration of balancing of interests in the employment context.

(ii) The concern with automated decision-making was not evident in the national responses to the Questionnaire, but this may be due to the fact that there were no questions clearly directed to that concern. In It, Art. 17 of Act no. 675 of 31.12.96 limits action involving the assessment of a person's conduct based solely on the automated processing of personal data aimed at defining the data subject's profile or personality.

2 Source of information and extent of transmission

In the search for satisfactory criteria to define the areas requiring data protection regulation, and to define the degree of regulation required, we need to consider some further possible criteria which are suggested by the general discourse of data protection, before moving on to criteria which are in their nature more specific to the employment relationship. Two such general criteria, further to those already considered, relate to the source of the information and the extent of transmission. Thus, as to the former of those, there are suggestions that we can treat it as a decisive criterion of the requirement for regulation that the information comes from a source other than the data subject himself or herself. As to the latter, there are, equally, suggestions that we can regard trans-border movements of data as requiring regulation in a way or to an extent that internal movements of data within national boundaries do not.

These cannot, however, be regarded as decisive criteria in the employment sector. As to the former, it is not realistic to expect to confine the employer's acquisition or use of information about workers to data obtained from the workers themselves - any such argument would seem to give insufficient weight to the employer's interests in efficiency and competitiveness. As to the

latter criterion, itself rendered more marginal than it previously was by the extreme internationalisation of data transmission by means of the Internet, we would have to say that, although no doubt the more widely data are disseminated, the more strongly the basic rights and claims to data protection are engaged, nevertheless we cannot regard this as a key indicator of the fact or extent of requirements for regulation in the employment sector.

(i) In supranational formulations, certainly in the employment context, there seems to be some evolution away from a strict notion that the data subject should be the source of the data; this is to be expected, in the sense that such a notion is scarcely practical as a norm for the employment sector. Thus, whereas both CER Art 4.1 and ILOC s. 6.1 declare the principle that personal data should be obtained from the individual worker, ILOC ss. 6.2 to 6.4 develop a set of exceptions which are more significant than the primary rule. The position concerning external communication of data and transborder data flows is somewhat more complicated. CER was specially concerned with the communication of data to public authorities - see Art. 8. ILOC has a rather wider set of concerns with external communication of data, which specifically extends, for example, to communication for commercial or marketing purposes - see generally s.10, and s.10.2 on the particular point. DPD is generally concerned to create or assume free movement of data within the European Union, subject to the appropriate standards of data handling, and concentrates its controls on external communication upon transfer of personal data to third countries - ie those outside the EU - not offering adequate levels of protection - see Arts 25, 26.

(ii) In general, and particularly with regard to transborder data flows, it would seem that the member states are tending to follow the patterns of evolution mentioned in the previous paragraph, and that in particular they are generally in the course of implementing DPD in respect of transborder data flows.

3 Type or subject-matter of information.

In relation to the employment sector, we can make progress towards more helpful criteria of the need for data protection regulation, and of the degree of regulation required, by concentrating on the type or subject-matter of the information which the employer may acquire or use. This is a criterion of considerable validity, not least because it links up very directly with the basic rights, claims, and interests identified in stage I of the analysis. Thus we can readily appreciate that information is "specially sensitive" in the sense that it impinges on the right to private life, considered in terms of civil liberties, if it relates to, for example, the political, religious, or trade union affiliations of the worker, or in the sense that it impinges on claims to equality which we wish to uphold, if it relates, for instance, to the medical history, criminal record, ethnic origins, or sexual orientation of the worker or job-seeker. Or, even in the absence of such specific concerns, we might say that information is specially sensitive, therefore specially requiring rigorous data protection, if its subject matter is so intimate to the personality of the individual worker that its acquisition and use in and of themselves threaten the

right to private life - as we might say, for example, of information about an individual's relations with, or communications with, his or her family or friends.

At the same time, we should beware of assuming that we can use even this criterion to guide us straightforwardly to the conclusion that we have identified a case for data protection regulation, or, a fortiori, for a specially rigorous degree of regulation. There are several reasons for caution in this respect. They can for the most part be generalised into the proposition that information of a type or subject-matter such that its acquisition or use threatens the worker's basic rights, for instance to private life or equality, may nevertheless also be of a type which it is crucial to the employer's interests, or to the wider public interest, to be open to acquisition and use by the employer. This might well be judged to be the case vis-a-vis, for example, information about the worker's criminal record, citizenship status, mental or physical health, or record of drug or alcohol abuse. We may even be approaching a situation where that might be judged to apply to genetic information about workers or job-seekers, as derived from genetic testing. So, although classification of information by type or subject-matter provides an important and quite highly employment-specific set of criteria for regulatory attention, it is not a conclusive or free-standing source of guidance. We need to press on in the search for further dimensions by reference to which to refine the analysis.

(i) The situation concerning supranational formulations of notions of specially sensitive data types was considered earlier at para. 43A above, but it is useful to consider in slightly more detail the position concerning genetic data obtained by genetic testing or screening, which is clearly becoming more and more critical. The key question is whether it is adequate and satisfactory in current conditions to address the issues about genetic testing under the general head of health or medical data. CER was formulated before genetic testing had become a live issue, and DPD does not treat it as a distinct issue; ILOC, however, does contain a special provision (s.6.12) to the effect that genetic screening should be prohibited or limited to cases explicitly authorised by national legalisation.

(ii) The responses from the member states to the Questionnaire reveal a significant diversity of treatment of genetic testing issues in the employment sector. Most of the member states do not treat the issue in a distinct way, but there are some interesting examples of specific provisions concerning genetic data or testing. Thus A has tight data protection controls under its Federal Genetic Engineering Act No 510/1994; Fr limits genetic testing to medical purposes or scientific research purposes under its Law No. 94-564 of 29 July 1994 concerning the donation and use of products of the human body etc., and Ne has particularly tight restrictions under its Medical Examinations Act which came into force on 1 January 1998, and its Moratorium on Genetic Testing.

4 The stage or aspect of the employment relationship.

An obvious and initially attractive employment-specific criterion of the need for data protection regulation, and for the degree of regulation required, consists of distinguishing the stage or aspect of the employment relationship to which the information transactions in question relate. For example, one might conclude that there was a special need for data protection regulation in relation to recruitment for employment, because of the extent to which rights to equality or against various forms of discrimination are so obviously in issue at that stage. One might even validly regard this as a criterion which would help us to keep up with the dynamics of change in patterns of employment and the working of the labour market. For example, one could say that the tendency towards more and more employment on a fixed-term and short-term basis enhances the importance of the recruitment function, and hence heightens the need for data protection in this area. Again, one could say that emerging patterns of continuingly multipartite employment relationships, as described in para. 1.9 above, further extend the recruitment function and corresponding need for data protection, so that we have to include in that concept the recurrent allocation of workers to particular client-employers by employment agencies who are themselves the general or holding employers.

However, if the focus upon recruitment provides a good illustration of the way that we can identify needs for data protection regulation by focusing upon particular stages or aspects of the employment relationship, that does not necessarily mean that we can single out recruitment as an area or aspect requiring regulation to a singular extent. There are many other areas or aspects of the employment relationship where the basic rights, claims, and considerations identified in Stage I of the analysis are just as much at stake, and where the use made of personal data is just as crucial to the vindication of those rights, claims, and considerations. The termination of employment is an obvious case in point. So also, we suggest, are various incentive and control systems operating during the continuance of employment, such as appraisal, performance-related pay, and promotion systems, where the acquisition and use of personal information is of the essence of the systems concerned.

Hence, although it is therefore useful to analyse information transactions according to the stage or aspect of the employment relationship to which they relate, it should not be thought that this is a method of ruling some stage of employment out of the need for data protection regulation, or even for according them low priority. In fact, like many of the criteria we are discussing, it is more inclusionary than exclusionary in its nature, or at least in its effect; that is to say, it is better at telling us where needs for regulation arise, and are pressing, than at confining and concentrating the scope and task of data protection regulation. We shall return to the implications of that in Stage III of our analysis. Suffice it for the moment to emphasise that, although this criterion seems to focus special attention upon recruitment, it also, on further reflection, draws our attention in different senses to needs for data protection during the continuation of employment relationships as well as upon their termination. So we need to look still further for more selective criteria.

5 Method of acquisition or assembly of personal information.

Analysis according to the methods of acquisition or assembly of personal information offers another good way of identifying areas requiring data protection regulation in the employment sector. It is helpful to list types of data transaction in the employment sector which seem particularly to threaten rights to privacy and private life, or rights to health, safety and welfare at work, according to the methods of gathering and marshalling information - thus, as different forms or ways of testing or monitoring workers or job-seekers. So, we can list as such various kinds of physical testing or searching, psychometric testing and probably now genetic testing, and various kinds of monitoring such as by video or closed-circuit television (CCTV), or by interception and recording of communication by voice, telephone, fax machine or computer.

We can, then, make up lists of methods of testing and monitoring which intuitively seem to us to threaten workers' rights to private life or, by occasioning extreme mental stress, their rights to the protection of their health, safety, and welfare at work. However, if this criterion is to be really useful, we have to try to identify the shared characteristics which make these types of data transaction problematical in that sense. One may make some progress in that respect by using notions such as that of surveillance to capture what we find difficult about these kinds of testing and monitoring, but we probably need to probe more deeply than that. If we do so, there seem to be two main sets of negative characteristics involved. The first has to do with omnipresence and intrusiveness. The second is concerned with lack of transparency or predictability to the data subject.

We should note that these two sets of characteristics bear in rather complex ways upon particular forms of testing or monitoring. We might regard workers as being denied their privacy or basic sense of autonomy and well-being because, for instance, they sense that their every action is being recorded by a camera or computer, their every personal characteristic detected by some process of physical or mental testing. On the other hand, we may, rather differently, perceive that the detriment to them comes from their uncertainty when and in what respects, and how closely, their actions and characteristics are being monitored. In this sense, psychometric tests, for instance, or processes of sampling of their e-mails may present themselves as very non-transparent and unpredictable to the workers who are subject to them. So we have to accept that the level of need for regulation of any particular such method of acquiring and assembling personal information will depend on a complex assessment of its characteristics.

Nevertheless, despite that complexity, we can still regard this as a useful criterion. In particular, we can regard it as one which is dynamically related to the development of the use of information technology in the practice of employment relationships, and as therefore able to help identify new employment-specific data protection issues as they emerge. On the other hand, analysis of that kind, precisely because of its dynamic relationship it the development of information technology, has to be keenly attuned to the way in which employers' interests in

efficiency and competitiveness, and wider public interests in the safety and welfare of citizens at large, are also linked to the development of information technology. Testing and monitoring seem to offer to employers, and to society at large, assurances of *objectivity and rigour* while at the same time they seem to encroach upon the interests and claims of workers. In order to get to the heart of that set of analytical difficulties, we need a final set of criteria, of an even more employment-specific kind.

(i) One of the most useful features of ILOC is that it offers important ways forward in the development of a systematic yet adaptable approach to issues of testing and monitoring in the employment context. This contribution is located particularly in ILOC ss. 6.10 to 6.14. Of these provisions, 6.10 is perhaps over-prescriptive compared with the situation in the Member States in declaring simply that polygraphs, truth-verification or any other similar testing procedure should not be used. 6.11 and 6.13 take a less definitive approach to personality tests and to drug-testing. Most significant and potentially helpful is 6.14, which represents a major advance in the recognition of the importance of the set of issues about *monitoring*, especially 6.14(2) on *secret monitoring* and 6.14(3) on *continuous monitoring* - which, according to ILOCCom at p.36 "has proved to be a cause of constant anxiety *which can lead to both physical illness and psychological distress"* (emphasis added).

(ii) That supranational formulation could provide a framework for understanding and building upon various interesting developments towards controls upon monitoring, especially secret monitoring, in member states - for example, A has requirements of works council consent under its Co-determination Statute, Fr has requirements for information to and consultation of works councils under Art 28 of the Law of 31 December 1992, in Ge the introduction and use of technical devices for the purpose of monitoring the conduct or work performance of employees is a matter in which the works council has a say under the Employee Representation Act, in Ne the Data Protection Authority has a Code of Conduct which deals with the registering, monitoring and recording of employees' telephone calls and places tight restrictions on telephone tapping. We could see these developments as gradually evolving a set of notions about *objectivity and transparency* in relation to the testing and monitoring of job-seekers and workers.

6 The changing roles of personal data use in the management of employment relationships.

The final mode of analysis or criterion which we advance here, as one of the ways of identifying needs for data protection regulation in the employment sector, has to do with the different and changing roles assigned to the acquisition and use of personal information about workers in the management of employment relationships. This is essentially an identification of the way in which the use of personal information about workers is coming to play an ever more significant set of roles in the management of employment relationships, and hence implicating

the basic rights, claims, and interests identified at Stage I at an ever deeper level. This is, in a sense, the iceberg of which the visible tip is the problem of "automated decision-making" which we considered earlier. Essentially, there seems to be a general dynamic towards the broadening of the roles of personal information use from the relatively limited traditional roles of selection and discipline into a new set of functions which have to do with the motivation, incentivisation and acculturation of workers, and the control of their behaviour. The increasing centrality of *appraisal systems* of all kinds is a central, though not the only, illustration of this phenomenon.

This set of dynamics in the management of work relationships is deeply bound up with changes in the nature of work and of perceptions of work. When we use the terminology of the "information society", we identify a state of affairs in which the work or productive functioning of enterprises and polities increasingly consists of , or is perceived as dependent upon, information transactions, and the work of individuals increasingly consists of communication rather than of physical production in a more traditional sense. Obviously there has always been a significant section of the workforce engaged in communicative activity, and equally obviously another substantial section of the workforce remains at least partly engaged in the activity of physical production, but the trend is nevertheless a strong one. Moreover, that trend is accompanied and reinforced by the ever-increasing technification of human communication, not only in its manner, as where e-mails replace letters, but also in its substance, as where it consists of information, perceived of as technical facts or "data", rather than of thoughts or opinions. In that environment, we should expect that the nature of work becomes in one sense more personalised - as witnessed by the premium now attached to communication skills - and yet at the same time more technological - as witnessed by the equal premium attached to computing skills.

Accompanying those changes, we find, and should expect to continue to find, a corresponding shift of emphasis in the management of work relationships, so that it tends to be transformed from the management of work as a process of physically based production to the management of work as a process based on inter-personal communication. The management of "tele-working" or computer-or telephone-based home working provides a good set of examples. The management of work relationships within such paradigms - it is significant that it is generally now styled "human resource management" - is increasingly envisaged as the management of information transactions, and the acquisition and use of personal data about workers and job-seekers seems correspondingly integral to it.

It thus appears to be the case that these changes in the role of data use in the management of work relationships increases the actual or potential threats to the basic rights and claims of workers which create and identify the need for data protection regulation. At the same time, these changes also mark and express a correspondingly increased identification of employers' interests in efficiency and competitiveness with the advance of personal data use in the management of work relationships. Thus, monitoring or appraisal systems are genuinely seen as essential to effective management of work relationships; most of the threats of this kind to workers' privacy are motivated in that way, rather than by curiosity or paternalism. This motivation does not in a simple sense justify the practices in question; rather, it shows how

central the issues about acquisition and use of personal data are to the whole set of controversies about what employment relationships should consist of, and what represents justice and fairness at work. This observation may be regarded as the end-point of our search for ways of identifying the areas and degrees of requirement for data protection regulation in the employment sector, for it locates that requirement at the very core of modern work relationships and of the way they are managed. This enables us to draw conclusions about the cumulative outcome of the first two stages of our structural analysis.

7 Conclusions to Stage II.

By putting the first two stages of this analysis together, an agenda or task definition for data protection in the employment sector is arrived at, though it emerges in a form different from that which might have been expected at the outset. Going from Stage I to Stage II does not give us a clear list of problem areas requiring regulation, because so many different factors turn out to interact in such complex ways. But it does provide an *open-ended* framework for identifying evolving data protection issues and needs in the area of employment. Equally, going from Stage I to Stage II does not provide clear ways of prioritising areas for particularly tight or intensive data protection regulation. Rather, it reveals how strongly the basic rights, claims, and public policy considerations compete against each other in a wide range of areas, and so gives a sense of the task of data protection regulation in the employment sector as a set of *balancing operations* between competing considerations. This shows how the framework for regulation has to consist of an apparatus for those balancing operations. It will be helpful for that purpose to summarise the results of Stage II of the analysis by drawing an outline map of the area requiring employment data protection regulation.

The area can be defined in *three main ways*, that is:-

(I) by reference to the phase or aspect of the employment relationship;

(II) by reference to the type of data; and

(III) by reference to the kind of data transaction or activity.

The *phases or aspects of the employment relationship* which it is useful to distinguish are:-

(a) recruitment,

(b) monitoring and discipline during employment, and

(c) termination of employment including pension arrangements.

Distinguishing according to *type of data*, we can identify:-

(a) the general category of personal facts about, and evaluations of, workers and job-seekers, and certain important special categories such as:-

(b) medical reports, records and evaluations,

(c) criminal records,

(d) data about origins and affiliations, and

(e) data about family and sex life.

Defining by reference to the *nature of the data transaction or activity*, we can separate out:-

(a) methods of acquisition of data in general;

(b) special methods of acquisition in the nature of searching and testing such as testing for substances, medical and especially genetic testing, and psychological testing;

(c) special methods of acquisition in the nature of mechanical or electronic surveillance;

(d) storing and internal communication of personal data;

(e) use of personal data in appraisal and management of performance, and

(f) transmission of data to public authorities and other third parties to the employment relationship.

The crucial conclusion from Stage II is that the need for regulation and the degree of that need cannot be assessed in any one of those dimensions alone and have to be judged by configuring them together.

C Stage III of the Analysis - Establishing the Appropriate Regulatory Norms

1 Organising principles.

In the first part of this structural analysis, we sought to identify the agenda or task definition for data protection regulation in the employment sector. In this second part of the

analysis, we seek to build on that in order to analyse what a coherent structure of regulatory norms for data protection in the employment sector will consist of. One approach to this regulatory task might be, indeed frequently is, to think of it in terms of *the specialisation of general data protection law.* This means agreeing that we have a valid self-contained body of regulatory norms for data protection generally - that is, for all spheres of data use - and going on to formulate the ways in which that body of norms apply specifically to the employment sector. This is, on the face of it, the obvious way in which to proceed. Most member states have general data protection legislation in place, and the Data Protection Directive provides a general framework at Community level. It seems obvious to think of the task as one of simply refining down those general norms into an employment-specific form.

However, the problem with this approach is that, by itself, it produces results which are not as fully contextual as we could wish them to be. General data protection norms, valuable and essential thought they are, remain rather abstract, ethereal, and detached unless and until they are *located in the legal and practical normative system* within which they are being applied. That means that the regulatory norms for data protection ultimately have to be derived from and tied in with the legal and normative system of the society or state in question, both at the general and constitutional level and at the sectoral level - in our case, therefore, at the level of the employment sector. If the regulatory norms failed to do this, they would have failed fully to reflect the way that the society or state in question deals with the reconciliation of the basic rights, claims and public policy considerations which we identified at Stage I of the analysis.

(i) It is useful to remind ourselves that it is not just in relation to employment that general data protection frameworks depend for their efficacy upon being developed and applied according to the particular needs of the different sectors to which they apply. Thus, the 1981 Council of Europe Convention for the protection of Individuals with regard to Automatic Processing of Personal Data has been the subject of Recommendations not just in the employment sector (CER), but also in relation to scientific research and statistics [29], direct marketing[30], social security purposes[31], and in the police sector[32]. DPD similarly allows for and is starting to benefit from development in particular areas such as that of telecommunications where there is now a Directive on the protection of personal data and privacy in the context of digital telecommunications networks[33].

---

[29] Recommendation No. R (83) 10.

[30] Recommendation No. R (85) 20.

[31] Recommendation No. R (86) 1.

[32] Recommendation No. R (87) 15.

[33] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, *Official Journal N° L 24/1.*

This might suggest a contrary approach. We might decide that the task of devising appropriate regulatory norms for data protection in the employment sector was simply one of *applying the general legal and normative framework for the employment sector* in the society or state in question to the particular issues of acquisition and use of personal information about workers. This approach also has superficial attractions; it offers the prospect of regulatory norms which are by definition derived from the laws, legal and constitutional culture, and policy discourse of the society or state concerned. It seems, in other words, to be strongly *reflexive* of the general legal and societal norms of the state, and of the employment sector, within which the regulation is taking place.

However, that approach would also have serious defects. It would understate the extent to which the acquisition and use of personal information, in relationships such as that of employment represents, in an age of such rapidly developing information technology, a special and distinctive set of problems the proper regulation of which requires its own focus and a genuinely specialised treatment. To disregard that argument would unduly marginalise the analysis we conducted at Stage II, in which we suggested ways of identifying a set of problems which are distinctively data protection issues thought they happen to be located in the employment sector. There is, in other words, an authentic specialism in data protection which offers the possibility of establishing regulatory norms slightly - though far from totally - set aside from the often highly politicised arena in which general constitutional law and general employment law are formed and applied.

So the question, how should we analyse or approach the task of establishing the regulatory norms, becomes the question, can we find an approach which steers a path between those two extremes, capturing the advantages and avoiding the disadvantages of each. It is suggested that this optimal approach can most nearly be arrived at by regarding the regulatory task as an *integrative* one. This means that we want the regulatory norms to operate so as to integrate the discourses of data protection on the one hand and employment law and policy on the other. It is one thing, however, to state this lofty aim, and another to show how it is to be realised in detail. That requires us to look further at the nature of general data protection norms, and consider what it means to integrate them into the general fabric of norms for the employment sector.

It may in fact be easier than it at first appears to use general data protection norms in this integrative way, once we have understood the real potential for doing so. We will tend not to see and grasp this potential if we regard general data protection norms as hard-edged rules. We should rather regard them as *organising principles*, in the sense of principles which serve to organise a norm-making process which produces specific normative solutions to concrete problems in particular sectors and contexts. A good illustration consists of the normative proposition frequently, indeed almost universally, found in general data protection frameworks, namely that the acquisition and use of personal data should be *conditional upon the consent of*

the data subject. If we attempted to treat this as a hard-edged rule for the employment sector, the results would be wholly unsatisfactory. The requirement of consent would seem in some ways too stringent and in other was not stringent enough.

Thus it would seem too stringent in that we would find some situations where there was a great importance in employers being able to acquire and use personal information without the consent of the workers concerned, as presumably in relation to information from third parties about drug or alcohol abuse by coach or train drivers or airline pilots. On the other hand, we might regard it as quite unsatisfactory for the consent of individual workers to be allowed to confer legitimacy upon the acquisition and use of information about their genetic make-up and defects, not least because we might think their consent was likely to be less than fully informed, and perhaps also given as the result of economic pressure. So as a concrete rule for the employment sector, the requirement of consent of the data subject does not appear to be very coherent.

However, that is not how we have to understand the role of general data protection principles in particular sectors such as the employment sector. And, indeed, that is not how we should conceive of their role if we are to arrive at a coherent set of regulatory norms. We shall find that general data protection norms do, on the other hand, provide the best normative starting point for sectoral data protection if they are regarded not as hard-edged rules but rather as *organising principles.* By this we mean that they should be regarded as broad headings under which or within which we can formulate more detailed regulatory norms for the sector in question. So this gives us a set of normative headings under which to organise our data protection regime for the employment sector. That organising process consists, essentially, of devising the best framework of norms to reconcile the basic rights, claims, and interests which are at stake in the employment sector, and doing so in relation to the particular data protection needs of the employment sector. In other words, this is a process for organising into normative form the logic of the first two stages of our analysis, and the general data protection principles are the tools which we use to carry out that process.

So, let us continue with our example of the requirement of consent of the data subject to show how that organising process might work, and how that general data protection principle might be instrumental to the process. As a general data protection principle, it is not a requirement of consent in the ordinary direct normative sense. Instead, it is an organising idea which may provide one of the ways of balancing, for instance, the worker's right to private life with the employer's need for efficiency and competitiveness. If it is to do this, its detailed application has to be tailored to the particular data protection needs of the employment sector. So we might say, for instance, that the consent principle, as applied to genetic testing in the employment sector, would mean that a given workforce could be subjected to genetic testing only after a procedure for obtaining the agreement of that workforce as a whole had been followed, and that thereafter the consent of the individual worker was needed for release of his personal genetic data to other employers, but was not needed for certain use of that data within

the enterprise in question. In the making of norms of that kind, the idea of consent as a general data protection principle does not provide a complete logic of its own, but rather serves as a instrument for organising a larger set of ideas into a concrete normative form.

As that example illustrates, the application of general data protection principles to the employment sector is thus very far from being a straightforward or mechanistic working-out of the general logic of data protection. It is, on the contrary, a dynamic normative process in itself, which has to respond both to technological development and to broader changes in employment law and policy and in the structures and patterns of employment relationships. This norm-making activity should not be understood simply as the production of a static body of normative principles and rules. It is in and of itself a *regulatory process.* As such it is ultimately inseparable from the process of *implementation* of the data protection regime of which it forms the normative backbone.

The discussion in the preceding paragraphs suggests that we should have the following design for the norms of data protection in the employment sector. They should consist both of principles and of rules. The *principles* should be derived from general data protection principles, but should be adapted to the special situation of the employment sector. The *rules* should represent a working-out in greater detail of the employment data protection principles. There are at least two good reasons for making that distinction between principles and rules in this context. The first is that the norms of employment data protection are more likely to form a logical and coherent structure if they are formulated in this hierarchical way. The second reason is that we may well wish to have a level of detailed rule-making where modification in response to changing needs is relatively easy; but we may not wish the whole normative structure to be too readily susceptible to being modified so that it will not seem too vulnerable to ephemeral notions and opinions. This suggests a separation, both at a conceptual level and at a formal and procedural level between employment data protection principles and the detailed rules for data protection in employment. We shall mainly concern ourselves with the content of the principles rather than with that of the detailed rules.

(i) It is important to make it clear that the supranational formulations do not prescribe any single way of differentiating between data protection principles and data protection rules. Thus, when DPDPre, in recital 68, declares that the DPD principles "may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles", it is recognising that there are a number of options as to the manner in which and the level at which those specific rules may be made. Those options include binding legislation, guidelines, and codes of practice. We should interpret in this broad sense the provision of DPD Art 27.1 that "The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors."

We can establish a common basis or framework for those principles by drawing on two main sources. The first of these sources is that of general data protection principles as articulated in the general data protection legislation of many EU members states and in the Data Protection Directive. The second of those sources is that of employment-specific data protection principles as articulated in the few cases where EU member states have employment-specific data protection legislation, and in the Council of Europe Recommendation and the ILO Code of Practice on data protection in the employment sector. As between those various sources, the norms are organised or set out in quite widely differing ways, but there is quite a high degree of underlying convergence of content.

Within that broad convergence, we can distinguish a group of principles which impose *qualitative* controls, and another group of principles which impose *procedural* controls upon the acquisition and use of personal data in relation to employment. *Qualitative controls* are norms which require the activity in question to achieve or comply with qualitative assessments (for example, "this activity shall be conducted in a way which complies with recognised good practice" or "this function shall not be carried out negatively"). *Procedural controls* are those which require the activity in question to be conducted according to certain procedures or processes (for example, "this activity shall be the subject of prior consultation with those affected by it"). The principles imposing *qualitative controls* upon the acquisition and use of personal data in the employment sphere are of *three main types*, namely:-

(1) principles of confidentiality,

(2) principles of proportionality, and

(3) principles of necessity in specially sensitive situations.

The principles imposing *procedural controls* are also of three main types, namely:-

(1) principles requiring notification, access and verification,

(2) principles requiring consent, and

(3) principles requiring information and consultation.

We need to examine each of those principles in somewhat greater detail.

2 Qualitative controls

2.1 The principle of confidentiality.

The principle of *confidentiality* can be expressed, in the employment context, as a norm requiring that in general personal data relating to workers or job-seekers should be regarded and

treated as confidential to them. It is one of the main conceptual starting points for the historical development of data protection, both generally and in the employment sphere. It serves to vindicate the basic claim to privacy and the right to private life, and it is also important to the protection of the health and welfare of workers to the extent that it protects them from extreme forms of stress capable of resulting in mental illness or injury. On the other hand, the detailed rules required to implement the principle have to admit many qualifications to absolute confidentiality, both in the interests of the efficiency and competitiveness of employing enterprises and in order to take account of major public policy considerations such as public health and safety, and the enforcement of the criminal law and of standards of conduct in public life.

(i) The supranational formulations encourage an approach which groups a number of data protection ideas together into a principle of confidentiality, and they also give important leads as to how to expound that principle. Thus DPD Section VIII on Confidentiality and Security of Processing has Art 17 on Confidentiality of processing - processing only on instructions of data controller unless required by law, and Art 18 on Security of processing - in respects such as those of protection of personal data against accidental or unlawful loss, destruction, disclosure or other forms of processing. ILOC section 5.12 articulates the principle that all persons having access to personal data in the employment context should be "bound to a rule of confidentiality", and sections 7 to 10 deal with security, storage, use and communication of personal data in the employment context in greater detail. ILOCCom is particularly useful in showing how, at various points (see especially ILOCCom pp. 38-39, 43 - 44) , those provisions intersect with the provisions of the ILO Recommendation on Occupational Health Services[34] and point to the need for procedures to secure the special confidentiality of the medical data which often needs to be collected by employers in the interests of the users of the products or services of the enterprise in question and of the workers in the enterprise themselves.

2.2 The principle of proportionality.

If the imposition of controls contributing to a principle of confidentiality was an feature of the early development of data protection frameworks, we can see that as this development has continued and has become more mature, it has reached the point where it probably sustains a principle of *proportionality.* At the very least, we can assert that a coherent normative structure of data protection in the employment sector can usefully be organised on that assumption. Such a principle is to the effect that *the acquisition and use of personal data about workers or job-seekers shall take place so that the extent of its encroachment upon their basic rights, interests, and legitimate expectations is no more than is proportional to the need to achieve the purposes for which the acquisition and use of those data are allowed and established as*

[34] ILO Occupational Health Services Recommendation No. 171 of 1985, see especially paras. 14-15.

appropriate. This principle includes and makes use of the idea of *relevance*, which is frequently invoked in data protection frameworks. It is also a way of expressing or building upon the idea of *finality* which is also now often introduced in this context. Proportionality is perhaps a better term to use than finality, to the extent that finality suggests *conclusiveness* to English speakers, to whom it is not always sufficiently clear that finality usually in this context refers to the *fin* or purpose of the activity in question, and not usually to the idea of *putting an end to data processing or storage,* though that is of course important too, and has its place within the notion of proportionality.

(i) DPD generally supports the above formulation of a principle of proportionality, and DPD Art 6 embodies many of the ideas which we are grouping under the heading of proportionality, in particular when it requires Member States to provide that personal data must be (a) processed fairly and lawfully, (b) collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, and (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The application of this set of ideas to the employment sector in particular is further considered in the next paragraphs of text and commentary.

The principle of proportionality, as thus formulated, has the great advantage that, by definition, it brings into play the whole range of basic rights, claims and considerations which are at stake in employment data protection as we identified them in Stage I of this analysis; thus, it widens the horizons beyond privacy to include issues of health safety and welfare at work and of equality and the elimination of discrimination. For these very reasons there is, of course, the corresponding danger that the principle becomes too broad to be useful. This is where it is important to remind ourselves that these are *organising principles* rather than conclusively determinative rules. The principle of proportionality provides a very good way of organising normative regulation; it provides a robust conceptual framework for handling more specific regulatory notions which we frequently encounter in the discussion of employment data protection, but which need to be placed in a hierarchical structure of norms if they are to produce the best results. This is true, for example, of restrictions on *changes in the purpose of use* of personal data. These are frequently proposed or imposed because it is seen as highly problematical to allow employers to use data which have been acquired for the control of the technical processes of production for the purpose of directly controlling the behaviour of workers. We will have a clearer idea of how to apply such restrictions if we see them as specific expressions of an underlying principle of proportionality. It is suggested that the same thing is true in further instances such as that of restrictions on *automated decision-making.*

(i) Most of the "general principles" articulated in ILOC section 5 amount to or contribute to a proportionality principle for employment data protection. Thus we find in particular 5.1 - lawful and fair processing only for reasons directly relevant to the employment of the worker, 5.2 - use only for the purposes for which originally collected, 5.2 - if for other purposes, not in a manner incompatible with original purpose, 5.3 - if collected in

connection with technical or organisational measures, should not be used to control behaviour of workers.

(ii) The employment data protection frameworks of member states are increasingly drawing upon or embodying ideas of proportionality. A few good examples are:- Fr , where Law No 92-1446 of 31 December 1992 added to the Labour Code Article 1220-2 which lays down the principle that individual and collective rights and freedoms may not be made subject to any restriction which is not justified by the nature of the work to be carried out, *or which is disproportionate to its given aim* (emphasis added); Ge, where judicial protection of the constitutionally guaranteed personal rights of employees involves the principle of proportionality, for example in stating that when recruiting staff, employers may ask only questions which are justified for the purpose of assessing an applicant's suitability and qualifications for the job concerned, and It, where Art 9 of the Data Processing Act (No. 675 of 31.12.96) repeats the qualitative requirements of DPD Art 6 as set out in para 5.16A above. The principle of proportionality seems to offer an increasingly effective way of understanding and rationalising developments at member state level.

2.3 The principle of necessity.

We might be inclined to conclude from the foregoing paragraphs that the principles of confidentiality and proportionality provide an adequate and complete basis for the articulation of qualitative controls upon the acquisition and use of personal data in the employment sector. It is, however, the case that the evolution of data protection frameworks, both generally and in this particular sector, has indicated the continuing presence of perceived needs for a specially rigorous set of controls in relation to certain patterns of acquisition and use of personal data. A good example is that of the acquisition and use of personal medical data relating to workers or job-seekers. In recognition of those perceived needs , and the outcomes they have had, we can usefully articulate a principle of *necessity* as a way of organising a certain type of normative regulation which has an important role in a coherent framework for employment-specific data protection.

This principle of necessity may be articulated as a requirement that in situations appropriately identified as specially sensitive ones, the acquisition and use of personal data about workers or job-seekers shall take place only to the extent and in the manner necessary to achieve purposes the pursuit of which is either sanctioned by law or otherwise identified as essential in the general public interest. According to that principle, in specially sensitive situations the general balancing of workers' rights, claims and interests against employers' needs for efficiency and competitiveness is, as it were, replaced by a more rigorous scrutiny to see whether there is a necessity for the activity in questions in terms of legal requirement or vindication of a clearly identified public interest. For this purpose, situations are to be regarded as specially sensitive where the acquisition or use of data, which they involve, are specifically threatening to fundamental rights, civil liberties or claims to equality or against discrimination.

(i) Art 7 of DPD, under the heading of "Criteria for Making Data Processing Legitimate" supports, in general terms, the principle of necessity which is argued for here, by requiring Member States to provide that personal data may be processed only if (a) the data subject has unambiguously consented, or (b) processing *necessary* for the performance of a contract, or (c) *necessary* for compliance with a legal obligation, or (d) *necessary* for the performance of a public interest task, or (e) *necessary* for pursuit of legitimate interests except where those are overridden by the fundamental rights or interests of the data subject. ILOC at various points makes provision for specially sensitive data processing situations in a way which implements the idea of necessity as identified in the above paragraph, for example in its treatment of *secret monitoring* in 6.14(2), and of *continuous monitoring* in 6.14(3); and in 10.1, various categories of necessity are identified as exceptions to the general requirement that personal data should not be communicated to third parties without the worker's explicit consent, that is to say unless the communication is (a) *necessary* to prevent serious and imminent threat to life or health, or (b) *required* or authorised by law, or (c) *necessary* for the conduct of the employment relationship, or (d) *required* for the enforcement of criminal law.

It is obvious that this principle of necessity requires a particularly difficult and potentially controversial allocation of data protection issues to the category of "specially sensitive" ones. In particular, the analysis in Stage II indicates that "special sensitivity" should not be assessed in a one-dimensional way simply according to the type of information which is involved - that is to say, just using categories such as medical data, criminal records, or information about personal origins, affiliations or sexual orientations. Rather, we need to envisage "specially sensitive situations" as *configurations* in which a very strong factor in one dimension *or a combination of factors from different dimensions* produce the characterisation of "special sensitivity". As one kind of example, we might say that secrecy of acquisition will be an aggravating factor, as with telephone tapping. As another example, we should say that the assessment of whether or when to allocate genetic testing to the "specially sensitive category" has to be a complex multi-dimensional one. We now turn our attention to procedural principles, which present a different set of difficulties and challenges.

(i) It is suggested that the necessity principle as developed in the foregoing paragraphs may provide a good way of understanding and building upon the approach of the European Court of Human Rights to employer's interceptions of employee's telephone calls in the *Halford* case[35].

[35] *Halford v United Kingdom* (1997) -see, for a full and useful discussion, Craig, John and Oliver, Hazel, "The Right to Privacy in the Public Workplace: Should the Private Sector be Concerned?

(ii) A principle of necessity like that argued for here has been used in Ne in applying the Code of Conduct on the registering, monitoring and recording of employees' telephone calls, and generally in controlling secret or continuous monitoring of employees by employers, such as continuous monitoring by CCTV.

3 Procedural controls

3.1 The principle of notification, access and verification.

If we look at the evolution of procedural or process controls upon acquisition and use of personal data in the employment sector, the first normative principle which seems to emerge is one which relates to *notification, access and verification.* It is a principle that, in general, workers or job-seekers should be guaranteed, either personally or through appropriate representatives, access to and the opportunity to verify personal information about them which is acquired or used in the context of employment relationships. Although undoubtedly an important part of the apparatus of procedural principles, this requirement imposes controls which are relatively limited in some ways. Firstly, although not formally confined to, it is nevertheless rather heavily focused upon the control of data holding, and does not in its nature readily extend to the whole range of data acquisition and data processing activities. Secondly - and this is a closely associated point - it is rather narrowly concentrated upon securing the accuracy and up-to-dateness of personal data and may not be very apt to control other hazards or negative effects of the acquisition and use of personal data in connection with employment. Thirdly, and still in the same vein, this principle creates controls which are largely individual in character and somewhat lack a collective dimension, both in the sense that it is individual rather than collective concerns which it vindicates, and in the sense that it does not readily permit of collective exercise of the controls which it requires, because of considerations of the confidentiality of personal data *against* collective representatives of the workforce such as trade union officials. These considerations, though by no means entirely negating the importance of this principle, increase the burden which the other procedural principles have to bear in the employment context.

(i) DPD Art 12 confers a right of access upon data subjects by requiring Member States to guarantee the right, in effect, to obtain from the data controller - that is, in the present context, the employer - (a) details of data processing relating to him or her, (b) rectification (or erasure or blocking) of incomplete or inaccurate data, and (c) notification of the rectification to third parties. ILOC section 11 spells out in considerable detail corresponding rights of notification, access and verification for workers. Interestingly, ILOC makes these provisions under the heading of "Individual rights", though it does provide in 11.5 that workers should be entitled to designate a workers' representative or a co-worker of their choice to assist them in the exercise of their right of access.

(ii) The situation in the member states concerning notification, access and verification broadly corresponds to the provisions of DPD and of ILOC as described in the previous

commentary paragraph (5.12A), though the rights are generally not specified as closely as in ILOC. As in those supranational formulations, these rights are generally treated as individual rights, though in Ge there is a provision in the Employee Representation Act (Betriebsverfassunggesetz) similar to that of ILOC 11.5 for the worker exercising the right of access to have a member of the works council present.

3.2 The principle of consent.

The procedural principle which seems on the face of it to be the one most apt to carry that burden is that of *consent.* This is a principle to the effect that, in general, workers or job-seekers should be given, either personally or through appropriate representatives, meaningful opportunities to decide whether to give consent to or withhold consent from the acquisition and use of personal information in ways which relate to them or affect them. This principle seems deeply embedded in the general discourse of data protection, and in many ways offers to transcend the limitations of the access and verification principle in the employment context. However, we have noted in earlier paragraphs (5.7 - 5.8) certain inadequacies to which requirements of the consent of data subjects are themselves in turn subject in relation to the employment sector. There, we saw that doubt might have to be cast sometimes upon the feasibility of making data practices conditional upon the individual consent of workers or job-seekers, and sometimes, on the other hand, on the meaningfulness of their opportunity to withhold consent, at least on an individual basis.

(i) As was shown in para 5.19A above, both DPD and ILOC make requirements of the data subject's consent, in the former case to processing generally and in the latter case to communication to third parties, which are, however, qualified by exceptions defined in terms of necessity. So we could say that in those formulations consent and necessity are alternatives, in the sense that they mutually qualify each other. ILOC section 10.2 has a more rigorous, unqualified, requirement of consent in one situation: it says that a worker's personal data should not be communicated for commercial or marketing purposes without the worker's informed and explicit consent.

It is, nevertheless, for consideration whether and how far the principle of consent is, by contrast with the principle of access and verification for reasons previously given, capable of being validated, as a method of control of data practices, by provision for decisions about consent to be taken by, workforce representatives acting in a collective capacity. In some situations, this will undoubtedly be a realistic possibility, and a valid way of ensuring that the principle of consent will exert a real control over employers' data practices, and will be exercised with reference to a wide range of collective concerns. On the other hand, it is important to acknowledge that the placing of a wide range of requirements of consent into the hands of collective representatives of the workforce would often mean going further down the road towards collective joint regulation of employment relationships than would be normal in

terms of the enterprise management systems, not to mention the employment law systems, which are in force in most of the member states of the EU.

(i) ILOC makes important points about the collective dimension of the principle of consent. Section 12.1 declares that "All negotiations concerning the processing of workers' personal data should be guided and bound by the principles in this code that protect the individual worker's right to know and decide which personal data concerning that worker should be used, under which conditions, and for which purposes.". ILOCCom adds the associated comment (pp. 46-47) that "The protection of workers against risks arising from the processing of their personal data and the ability to defend their interests successfully depend to a decisive extent on collective rights. Both the form and the content of these rights must be adapted to national systems of industrial relations. Where, for instance, institutions such as the works council play a major role in determining conditions of work, their influence on the processing of workers' personal data will, as the experience of France and Germany illustrates, be comparable. Where, on the contrary, conditions of work are more or less exclusively regulated by collective bargaining, the workers' interests in respect of data processing will have to be defended by their trade unions and their representatives at plant level.". In this connection, the particular collective consent model illustrated in the next commentary paragraph is of special interest.

(ii) In most of the member states, requirements of consent are framed in terms of *individual* consent. There are, however, some significant instances where the requirements are for *collective* consent. Thus, in A and in Ge, the Co-determination legislation (respectively the Arbeitsverfassunggesetz and the Betriebsverfasssunggesetz which make similar provisions to each other in this respect) requires the consent of the works council to the introduction of questionnaires, for use either in recruitment or in personnel management, which go beyond general personal details and questions about the job seeker's or worker's technical qualifications for the job in question (known as "qualified questionnaires"). Moreover, in A that legislation also requires the consent of the works council to the introduction of monitoring systems and technical systems for monitoring employees, in so far as these touch upon human dignity, while in Ge the same requirement is also made for the laying-down and application of guidelines for selection of workers in connection with recruitment procedures, transfers, re-structuring and dismissals. These represent significant instances of mandatory co-determination where consent can only be given in the form of a plant-level agreement within the works council - thus, to that extent, it requires a kind of *social dialogue* before certain kinds of monitoring systems can be introduced.

3.2 The principle of information and consultation.

That brings us to the third and last of our procedural principles, that of *information and consultation,* upon which the considerations discussed in the last paragraph may be thought to

bear very differently. This is a principle which we can formulate in the terms that, in general, workers or job-seekers should be informed and consulted, either personally or through appropriate representatives, about the acquisition and use of personal information by employers in ways which relate to them or affect them. We find this principle increasingly sustained by the recent development of data protection frameworks; but this might on the face of it appear to be the least stringent of the procedural principles. However, we could say that the increasing tendency in the discourse of general data protection to favour, among control procedures, those of information and consultation does fit in well with the general development both of human resource management systems and of employment law systems towards preferring those methods of collective representation and involvement in the management of employing enterprises. If the principle of information and consultation is, for those reasons, to emerge as one of the main sources and safeguards of *collective data protection rights* in the employment sector, there is an important task of making those rights, and the safeguards for them, effective. We return to this question later under the general heading of implementation and the particular heading of self-regulation and social dialogue.

(i) ILOC contains important assertions of the principle of information and consultation in a collective form. Section 5.8 declares that workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights. Section 12.2, even more clearly collective in character, is to the effect that "the workers' representatives, where they exist, and in conformity with national law and practice, should be informed and consulted (a) concerning the introduction or modification of automated systems that process workers' personal data; (b) before the introduction of any electronic monitoring of workers' behaviour in the workplace; (c) about the purpose, contents and the manner of administering and interpreting any questionnaires and tests concerning the personal data of workers".

(ii) Within member states, the most significant development of the principle of information and consultation as a collective control has occurred in the context of works councils systems. For example, in Fr Article 28 of the Law of 31 December 1992 provided for the inclusion of a new Art. L 432-2-1 in the Labour Code concerning the powers of works councils as regards the recruitment and individual freedoms of job applicants and employees, which made various provisions for advance information to and consultation with works councils to ensure greater transparency for the works council as regards measures or procedures to aid recruitment, automated processing of employees' personal data and the monitoring of employees' activities. In A and Ge, the Co-determination legislation, in addition to imposing the specific collective consent requirements referred to above, implements quite a strong form of the principle of information and consultation in that it gives works councils the role of *monitoring compliance with legislation affecting employees, including, therefore, data protection legislation.* It should not be assumed, however, that such forms of the principle of information and consultation have to be confined to works council systems. There are instances where the protection of the collective rights and interests of the workforce, and the monitoring of employers' compliance with their obligations to respect those rights and interests, especially in respect of health and safety at work, are entrusted to employee representatives not

necessarily within a works council system, as for example in the UK under the Health and Safety (Consultation with Employees) Regulations 1996. As the health, safety and welfare implications of various forms of personal data collection and use, such as secret or continuous electronic surveillance, become more apparent we can expect arrangements of this kind to form a more significant part of the apparatus for implementation of employment data protection principles.

4 Conclusions to Stage III.

At this third stage of our structural analysis, it has proved possible to identify a set of qualitative data protection principles for the employment sector, and also a set of procedural principles, which between them seem capable of giving concrete normative effect to the observations made in Stage I about the basic rights, claims, interests and public policy considerations which are at stake, and to those made in Stage II about the areas requiring regulation and the degrees of regulation which are required. However, if we speak of "concrete normative effect", it is important to remind ourselves that this normative effect is concrete only to the extent that we have a framework of organising principles within which detailed rules have to be formulated. Moreover, that process of detailed norm-making has to be a continuing and dynamic one which is reflexive of technological change, and of changes in the patterns and the practice of employment relationships. This means that there is a crucial continuity between the process of norm-making which we have just considered. and the process of implementation which we go on to consider in the next and final stage of our four-part analysis.

D Stage IV of the Analysis - The Implementation of Data Protection Norms in the Employment Sector.

The purpose of this final stage of the analysis is to consider what structures have to be created in order to ensure that an adequate and robust system is in place for the implementation of data protection norms in the employment sector. The task of implementation is itself a large and complex one, to an extent which has perhaps not been fully appreciated as data protection frameworks for the employment sector have developed by processes of accretion which have not always been fully systematic. In order to ensure that those frameworks are systematic so far as implementation is concerned, we suggest that it is necessary, firstly, to ensure that the full relevant range of *regulatory functions* is identified and covered, and, secondly, to satisfy ourselves that the full appropriate set of *institutional arrangements* is established and put in place.

There seem to be *three main types of regulatory functions* to be covered, namely,

(1) adjudication of disputes and complaints,

(2) registration and administrative regulation, and

(3) the making and revising of codes of practice.

There seem to be *three main types of institutional arrangement* to be put in place, namely

(1) judicial or quasi-judicial machinery,

(2) the appropriate administrative agency or agencies, and

(3) machinery for self-regulation and social dialogue.

It should be noted that although there are thus three main types both of regulatory functions and of institutional arrangement, there is not a simple direct relationship between each of the functions and each of the institutional arrangements. So we need to examine these categories and the relationships between them rather more fully.

1 Regulatory functions

1.1 Adjudication of disputes and complaints.

So far as the regulatory functions are concerned, it would be fair to say that in the data protection frameworks for the employment sector in the member states, there is a rather varying degree of recognition of the different functions in question. On the whole, it is treated as uncontroversial that there is a function of adjudication of disputes and complaints, for which due

provision has to be made - though there is less agreement about what the nature of that due provision should be.

(i) It is important to note that DPD *both* makes requirements, in Chapter III Articles 22 to 24, for the provision by member states of *judicial remedies, liability and sanctions* for the violation of rights in respect of data processing, *and* in Art 28.4 requires the *supervisory authority* (see further below, paras. 6.4A and 6.7A) to hear "claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data". It is also very important to recognise that in the context of the employment sector, a significant part of the task of adjudication of disputes and complaints may be carried out, and may best be carried out, at least in the first instance, within the institutional arrangements for self-regulation and social dialogue, as to which see further below, para. 6.8.

1.2 Registration and administrative regulation.

Many data protection frameworks in member states provide for the *registration* of data bases containing personal data, especially computerised data bases. But the recognition of the further function of *administrative regulation*, which we suggest should be associated with registration, and of the making and revising of codes of practice, is much more sporadic and less systematic. This state of affairs is perhaps the product of thinking from a significant period of time - quite a recent one - when the issues of data protection were seen, both generally and in relation to the employment sector, as more self-contained and less far-reaching than they are currently regarded as being. There must, in the current context of rapidly-developing information technology and rapidly changing patterns of employment and of management, be serious doubt whether registration of data bases can be regarded as a satisfactory way of giving effect to data protection principles unless it is associated with a capacity for administrative scrutiny or review of the practice of acquisition and use of personal data in the employment sector.

(i) One of the major impacts of DPD is, in Article 28 under the heading of "Supervisory authority", to require member states to provide for various kinds of *administrative regulation*, by one or more public authorities constituting a supervisory authority (as to which see further below), to monitor the application of the national measures adopted to give effect to the Directive. These requirements for administrative regulation go well beyond the function of registration and include requirements for the supervisory authority to be consulted in the drawing up of administrative measures or regulations for data protection (28.2), for it to be endowed with investigative powers and effective powers of intervention (28.3), and for it to make regular public reports on its activities.

1.3 The making and revising of codes of practice.

As we have argued in the previous stage of this analysis, the implementation of data protection cannot satisfactorily be regarded as the application of a static and complete set of norms. So we have to recognise a continuing function of specifying, adapting and modifying the main data protection norms (even the employment-specific ones) if the data protection system in question is to keep up with the demands which will be made upon it - we can think of this in terms of *the function of making and revising codes of practice*.

(i) Another of the major impacts of DPD is, in Article 27 , to identify the importance of the function of the making and revising of codes of practice by requiring the Member States (and the Commission) to "encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, *taking account of the specific features of the various sectors* (Art 27.1, emphasis added). Not only is this making of codes of conduct thus intended to be *sector-specific*, but it is also clearly intended to be, where possible, carried out at the drafting stage by "trade associations and other bodies representing other categories of controllers" (see Art 27.2), and therefore within the institutional arrangements for self-regulation and, in the employment sector, social dialogue, as to which see further below.

2 Institutional arrangements.

2.1 Judicial or quasi-judicial machinery.

There is also a comparable lack of systematisation, in the member states of the EU at large, with respect to the question of what *institutional arrangements* need to be made to carry out those functions effectively. It is, of course, extremely important not to regard diversity in this respect as in itself demonstrating the inadequacy of any one particular set of arrangements. Thus, so far as *machinery of adjudication of disputes and complaints* is concerned, the fact that there is divergence, as to whether the machinery is or should be that of the general court system, or that of tribunals specialised either in data protection or in employment law, does not itself discredit either the specialist or the generalist approach - though it is worth making the point that it is important for the adjudication machinery not to be remote and practically or culturally separated from the other institutional arrangements, given the underlying continuity between their functions.

2.2 The appropriate administrative agency or agencies.

There are points at which the incompleteness of some parts of the machinery of implementation might be regarded as a cause of concern, or at least as an indication of a lack of systematic analysis of what machinery is required for a fully effective implementation of data protection norms in the employment field. Thus, one may doubt whether an *administrative agency*, the role of which was cast simply in terms of keeping a register of computer data bases containing personal data, would have a sufficiently strong commitment to the wider purposes, which data protection frameworks serve, to be able to contribute to keeping the working of the

framework under effective review, still less to be able to take part in the formulation and negotiation of codes of practice. Of course one accepts that there will not always be a willingness to accord a major political role to an administrative agency devoted to data protection, nor, equally, will there always be a willingness to accept such a role; nevertheless, we seem to be moving away from a situation where the role of such an agency can satisfactorily be an entirely narrow and technocratic one.

(i) It was noted above in para 64A that DPD Article 28 requires each member state to constitute one or more public authorities as supervisory authorities to carry out the functions of administrative regulation (and hearing of claims - see above) in the matter of data protection. It should be noted that Art 28.1 requires that "These authorities shall act with complete independence in exercising the functions entrusted to them". In relation to the employment sector, this must be taken to imply independence both from the state and from each of the social partners.

2.3 Machinery for self-regulation and social dialogue.

A further concern is that there is little systematic development of the third kind of institutional arrangements, that is to say arrangements for *self-regulation.* It is suggested that in the employment sector, this should be seen as properly part of the apparatus of regulation, and that it should moreover be understood in terms of the need for some form of *social dialogue* between the social partners, that is to say as a dialogue between employers and representatives of the workforce. This would certainly to present itself as one of the ways of maximising the likelihood that data protection regulation for the employment relationship would be effectively implemented in a way that was responsive to the changing demands of that relationship. It is particularly important that there should be possibilities of social dialogue about that aspect of implementation of data protection which consists of the making and revising of codes of practice.

(i) It was shown above how DPD encourages the entrusting of the development of data protection frameworks at sectoral level to the machinery for self-regulation within the sector in question, especially in the matter of the making and revising of codes of conduct or practice. The supranational formulations of data protection frameworks for the employment sector in particular strongly support that approach in terms of *self-regulation* and, furthermore, they equally strongly support the view that self-regulation in this sector is integrally dependant for its effectiveness upon the processes of *social dialogue.* Thus CER in its Preamble "Recommends that the governments of member states ... promote acceptance *and implementation* of the principles contained in the Recommendation by ensuring its wide circulation *among representative bodies of both employers and employees*" (emphases added). ILOC in its Preface indicates that the non-binding guidance which ILOC is intended to provide should be understood as recommendations to be implemented in part by self-regulation and social dialogue:-"The

code does not replace national laws, regulations, international labour standards or other accepted standards. It can be used in the development of legislation, regulations, *collective agreements, work rules, policies and practical measures at enterprise level* (emphasis added). Such an approach to the institutional arrangements for data protection regulation in the employment sector is entirely in line with the general strategy for the productive development of work relationships which was presented by the European Commission in its Green Paper, *Partnership for a new organisation of work*[36].

3 Conclusions to Stage IV.

Obviously there is a complex task of combing these conclusions about implementation with the conclusions from the three earlier stages of the analysis. There are very many possible permutations between the findings at the different stages, and it would be very unwise to suggest that there was a single valid pattern. But merely to present a structure for systematic thinking about the options has some utility, and in the next part of this study it will be argued that there is a case for action at European Union level to stimulate and maintain systematic development of that kind.

[36] European Commission, *Green Paper - Partnership for a new organisation of work* COM(97) 128 final - see especially paras. 81-86, "The challenge to the social partners".

III The case for action at European Union level.

In this concluding section, it is suggested that the structural analysis of data protection needs and methods in the employment sector has indicated both a *basis and rationale* for action in this field at European Union level, and a set of ideas about the *form* which such action might take. In order to demonstrate this, we shall consider what the successive stages of the structural analysis tell us both about the need for action at EU level, and about the lines along which that action should be designed. The first part of that structural analysis, ie stages I and II, tells us about the basis and rationale, while the second part, ie stages III and IV, tells us about the form which it might take.

So far as the question of the basis and rationale for action at European Union level is concerned, in one sense we might say that we need look no further than the general Data Protection Directive, which in its preamble as well as its substantive provisions indicates the basis for concern with data protection in general, and also recognises that its own logic may necessitate further action in particular sectors such as employment. So there is no lack of basic foundations for further action in this sphere. But in a sense, the first part of our structural analysis takes the matter one stage further than that, both because of what it tells us about the basic rights, claims and interests which are at stake in employment data protection, and because of what it tells us about where the needs for regulation in the employment sector lie.

Thus, if we remind ourselves of the basic rights, claims and interests which are at stake in relation to data protection in the employment sector in particular, we find that they are all ones with which the European Union is seriously concerned - the right to private life by reason of its place in the European Convention on Human Rights, the right to health, safety and welfare at work as a matter of Social Policy, the rights to equality or against discrimination as the results of specific commitments at EU level to combat discrimination, and the interests in efficiency and competitiveness as a matter of employment policy in particular and economic policy in general. So these are all crucial Community interests, as is made especially clear by the approach to them in the Treaty of Amsterdam. Of central importance in that respect is the new Article 13 on Community action to combat discrimination.

Moreover, if we consider the particular and changing needs for regulation which we identified in Stage II of our analysis, we find that they fall within areas of economic and social development in which the European Union as a whole and its organic institutions are significantly involved. Thus, we saw how the evolution of the needs for data protection regulation in the employment sector was a function of the development both of information technology and its role in society, and in the nature and practice of work relationships. These are both sets of development which the institutions of the European Commission are strongly committed to monitoring and to integrating into the processes of formation and implementation of European Union policies - hence the development within the Commission of policy

discourses about the Information Society, and about changing patterns of work as expressed in the Green Paper on *Partnership for a New Organisation of Work* [37].

If the first two stages of our structural analysis thus indicate a basis and rationale for action at European Union level in the field of employment data protection, the second two stages give a preliminary indication of what that action might consist of, to the extent that they seek to establish a systematic framework for the articulation of data protection norms in the employment sector, and for the implementation of those norms. The suggestion is that the structural analysis might be used as a starting point, or a set of benchmarks for, the development of data protection in the employment sector within the Member States. The set of benchmarks might be based on the structural analysis of employment specific data protection, in the sense that it might use the successive stages of that analysis to provide a series of targets against which the employment data protection frameworks of members states could be measured or audited. This would mean that the national data protection frameworks could be assessed according to whether they:-

(1) reflected the full range of basic rights, claims, interests and public policy considerations which were at stake,

(2) addressed the full range of areas requiring regulation in all the relevant dimensions,

(3) gave effect in some shape manner or form to the main normative principles of employment data protection, and

(4) had put in place institutional machinery to fulfil the different implementation functions.

An auditing or assessment of this kind would be in nature different from an imposition of a single model of employment data protection. It would involve a recognition that there are many different ways in which a particular member state might provide a data protection framework for its employment sector which measured up to those benchmarks or met those targets. In fact, it should also involve the further recognition that, because of the rapidly changing context within which an employment data protection framework has to operate, its compliance with those benchmarks or targets is a dynamic process rather than the achievement of a crystallised state of affairs at a given moment. We are concerned with employment data protection frameworks as *processes of regulation* rather than as static enactments.

[37] See above, fn 36.

This means that the assessment or auditing of employment data protection frameworks also has to be a continuing and dynamic process. On the one hand, the assessment should not be looking for compliance with a particular model at a particular moment; the margin of appreciation which is built in to the assessment has to have a time dimension to it. On the other hand, the process of assessment has in itself to be one which is responsive to the changing context, both in terms of developments in information technology and in terms of changes in the world of employment. It will presumably be felt that such a process of assessment has to consist first and foremost of self-assessment by and within Member States. Equally, it is to be hoped that there would be a consensus in favour of a reporting and reviewing process at European Union level. This could be initiated by the identification of tentative benchmarks and targets in the form suggested by the structural analysis which has been conducted in this study.

A further proposal could be for the instituting of an annual report and review by the Commission (not unlike the annual Employment Report, but in this more specific area) which would receive the results of self-assessment by the Member States, and interact with that self-assessment process, firstly by commenting as necessary on the development of employment data protection frameworks at Member State level, and secondly by adapting its own benchmarks and targets in response to changes in the relevant circumstances, which might be revealed by the reporting from the Member States, or in other ways. The instituting of a process of this kind would seem to come within both the letter and the spirit of the general Data Protection Directiv