



107 Three Hot Topics in 90 Minutes

James Bellerjeau
General Counsel & Secretary
Mettler-Toledo International Inc.

Wolter Wefers Bettink
Partner
Houthoff Buruma

Michel P. Cloes
European Counsel
Dana Law Department Europe

Jyoti Pakrasi
Rechtsanwalt
Cisco-Linksys

Faculty Biographies

James Bellerjeau

James Bellerjeau is general counsel and secretary of Mettler-Toledo International Inc., headquartered in Greifensee, Switzerland. Mettler-Toledo is the world's largest manufacturer and marketer of weighing instruments for use in laboratory, industrial and food retailing applications.

Prior to joining Mettler-Toledo, Mr. Bellerjeau worked at the law firms Cleary, Gottlieb, Steen & Hamilton in Frankfurt, Germany, and Fried, Frank, Harris, Shriver & Jacobson in New York City. His practice included securities, structured finance, mergers & acquisitions, and corporate law.

Mr. Bellerjeau is member of the board of directors of the European chapter of ACC, as well as a country representative for that organization. He also serves on the legal committee of the Swiss American Chamber of Commerce.

Mr. Bellerjeau received a B.A. from Clark University, a M.A. in Business Administration from Rensselaer Polytechnic Institute, and a Juris Doctor from Albany Law School.

Wolter Wefers Bettink

Partner
Houthoff Buruma

Michel P. Cloes

Michel Cloes is the Paris-based European counsel for Dana Corporation in Toledo, Ohio. Dana is a \$10 billion automotive parts supplier and listed on the NYSE.

Mr. Cloes has a wide range of legal management experience in Europe, India, and Asia Pacific. Prior to joining Dana, he was European and Asia counsel for Denver-based Gates Corporation. Prior to that, he was in private practice in Los Angeles where he also worked for EuroDisneyland Corporation. He started his career in the United States.

Mr. Cloes is a member of the California Bar and the Los Angeles County Bar Associations. He is a former member of the Brussels Bar where he worked in the area of EU competition law for Liedekerke Wolters, Waelbroeck & Kirkpatrick. He is the founding president of ACC Europe. He is a member of the ACC Board of Directors. Mr. Cloes is co-author of European Union Business Law, West Publishing 1995. He is a frequent speaker on EU-US corporate compliance and corporate social responsibility issues, as well on law department management.

He holds a J.D. from the Faculty of Law at Liège State University, Belgium and a LLM from the University of San Diego School of Law.

Jyoti Pakrasi
Rechtsanwalt
Cisco-Linksys

ATTORNEY-CLIENT PRIVILEGE PROTECTION/EROSION

ACC continues to work with the ABA Task Force on Attorney Client Privilege, but is concerned that this group continues to meet to discuss the issues without much action resulting. We are moving forward with a few of our projects planned in this area and will hope to coordinate with the ABA, but we feel we can't wait for them to make decisions any longer. Accordingly, the Advocacy Committee will be presented with a "red-lined" version of the Thompson Memorandum that we have developed with our counsel on this issue, and if the Committee approves it, we will take the redline to the Justice Department leadership first, and then the membership and the media after we've had their comments.

Additionally, we are about to conduct a second survey on privilege issues that asks more detailed questions than our first highly publicized survey in this area. This survey has been requested by the US Sentencing Commission at their hearings in November at which they requested us to collect more information with the promise that such might lead to their reform of the offensive language in the Sentencing Guidelines' commentary that we have protested since its proposal and adoption last year.

The US Sentencing Commission recently informed us that our testimony in November of 2005 has had its intended impact. They intend to introduce amendments for comment (comments will be accepted for 60 days) that will amend the guidelines commentary to exclude the offensive language offering prosecutors the "authority" to request privilege waivers of corporations that wish to be deemed "cooperative" under the Guidelines' process. This is a huge victory for us, and one we hope will survive the comment process and be proposed to Congress by the Commission around April or May of this year. The momentum at that point will be swinging in our direction.

ABC Company

Guideline

Use of E-Mail and the Internet

valid for:

ABC Company Employees

from:

February 2006

1. Introduction

ABC Company makes available to its employees access to e-mail and the Internet to facilitate communication among its employees, customers and other parties in connection with company business. These technologies assist employees in the performance of their jobs in obtaining and exchanging work-related information. At the same time, Internet and e-mail use can create certain risks that may subject both individuals and the company to financial loss, and may damage ABC Company's reputation.

2. Purpose and Scope

The following rules have been established to help ensure responsible and productive Internet and e-mail use within ABC Company. This policy applies to all ABC Company employees. The General Managers of each business unit shall take steps to ensure compliance with local law and with this guideline.

3. General Guidelines

The e-mail system, computers, computer files and software furnished to employees are ABC Company property intended for business use. Access to the Internet through company-provided equipment shall be used to fulfill business needs. Users may only keep messages in one company e-mail account and mailbox.

Limited or occasional private use of e-mail and the Internet is permitted. As a general rule, however, any such private use should not be made during business hours and should not interfere with the performance of work duties as determined by ABC Company in its discretion. No private e-mail accounts may be created on the company's e-mail system.

3.1 E-Mail Messages May Be Business Records

Messages created by ABC Company employees may be business records with potential legal implications. Employees should not send messages to unauthorized third parties or persons without a legitimate business purpose that contain content or attachments that are company or customer confidential.

Employees cannot assume that e-mail messages will remain confidential, regardless of whether sent inside or outside the company. Even when a message is deleted, it may still be possible to retrieve and read that message. Because of confidentiality concerns, employees should not set automatic forwarding of their e-mail to an address outside the ABC Company system (for example, while traveling or on vacation).

ABC Company

3.2 E-Mails May Only Be Kept in On-Line Folders

E-mails may only be kept in the main Outlook Mailbox folders (Inbox, Deleted Items, and Sent Items) as well as in custom folders that each user may create as subfolders underneath their main Outlook Mailbox folders. The use of public folders is discussed in Section 3.4 below. E-mails may not be saved in any off-line methods, including in personal folders, to your hard drive, on removable media, or otherwise. "Personal folders" are custom folders you create anywhere other than under the main Outlook Mailbox folders.

Attachments should be kept together with the related e-mail message whenever possible.

3.3 Employees Should Proactively Manage Their Messages

The e-mail system will limit the age of e-mails in the main Outlook Mailbox folders to no more than 60 days. Experience shows that the large majority of matters can be addressed within this time period.

In certain cases, it may be necessary or appropriate to preserve a message for longer periods to comply with local law, document retention policies, or otherwise consistent with prudent business practices. Such messages may be printed out and maintained in hard copy. Messages may also be maintained electronically in custom folders underneath the Inbox or in other on-line archive systems the company may make available. Messages moved to custom folders under your Inbox will not be subject to the 60 day restriction.

The e-mail system will also limit the overall size of the Mailbox. For this reason, employees should only retain messages that are clearly required to be kept for a business purpose. Experience suggests that only a small percentage of all messages need and are appropriate to be archived for longer periods.

Please note that you must keep all messages and other documents relating to anticipated or ongoing lawsuits, and when you have been advised to do so by counsel. You should move such messages to custom folders to prevent inadvertent deletion.

3.4 Public Folders

"Public folders," are on-line folders that are shared among more than one user. The owners of existing public folders should manage the messages in these folders similar to how they manage their own Mailbox. Creating a new public folder will require prior approval of the relevant IT manager and unit general manager.

4. Instant Messaging

Instant messaging is not permitted. Exceptions may be made only by the Head of Information Systems and CEO. If an exception is granted, instant messaging may only be done using company-provided software. In any event, because of security concerns, instant messaging should never be done with parties outside the company.

ABC Company

5. Content Guidelines; Do's and Don'ts

E-mail messages and other documents created by employees are a reflection of the core values, policies and ethics of ABC Company. All employees should therefore exercise appropriate judgment in creating documents, and should ensure they are consistent with our code of conduct.

Corporate documents and data that is composed, transmitted, accessed, or received via the Internet or e-mail must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include jokes, gossip, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law. Keep in mind that messages you send may be forwarded to unknown third parties.

Before creating a document, including e-mail messages, carefully consider what information you need to communicate, why you are communicating it in the form you are, and how others may misinterpret or take out of context what you have written. As a general rule, you should use the same care in drafting messages as if you were going to send a letter by regular mail.

Do's and don'ts

1. Consider what is the most appropriate means of communication, which may be a writing, a phone call or a meeting.
2. If a writing is necessary, make sure your document is factual and accurate.
3. Deal with inappropriate statements sent to you by others, for example by clarifying what is meant, correcting inaccuracies, taking follow-up actions, and so on.
4. Avoid irony, sarcasm or exaggeration. Humor is often misunderstood when communicated electronically.
5. Assume that if a statement can be misconstrued or taken out of context, it will be.
6. Don't comment about legal liability, or ongoing or potential litigation. Avoid speculations or statements beyond your field of professional expertise.
7. Avoid overly broad distribution; send only to persons who have a need to know.
8. Assume your document will be read by an adversary in litigation.
9. Be aware the company will have access to your messages. Would you still be comfortable if your message became public?

6. Respect Copyright, Trademark and Patent Ownership

The unauthorized use, installation, copying or distribution of copyrighted, trademarked or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it or has not gotten authorization for its use, it should not be put on the Internet. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.

ABC Company

7. Monitoring and Access

Use of the e-mail system, and access to the Internet through company-provided equipment is not private. Access to any Internet site may be blocked at ABC Company's sole discretion. Subject to compliance with local law, ABC Company reserves the right to monitor any Internet or e-mail use made using company equipment, including circumstances where there are grounds to suspect misuse or noncompliance with this guideline, as determined by ABC Company in its sole discretion.

ABC Company may also monitor compliance with this guideline by randomly inspecting e-mails and Internet log files. The decisions about access to Internet and e-mail records will be made at the discretion of the general manager. In appropriate circumstances, access to and review of these records will be made under supervision of the Internal Audit function or other persons independent of line management.

Abuse of the Internet access and e-mail facilities provided by ABC Company in violation of law or company policies will result in disciplinary action, up to and including termination of employment according to the country-specific legal requirements.

Distribution:	All general managers of the ABC Company Group	February 2006
Author:	General Counsel	
Replaces:	Prior versions	Chief Executive Officer



**Three Hot Topics in 90 Minutes –
Data Retention & E-Mail Policies**

James T. Bellerjeau
(Mettler-Toledo)

ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam
Marriott Hotel



Agenda

- Why is E-Mail So Important?
- Policy Alternatives
- Behavioral Challenges
- Technical Challenges
- Sample Policies

ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam Marriott Hotel



E-mails are now the first thing asked for: “where the good stuff is”

- Formal litigation requests are just one possible way your e-mails may be requested, and perhaps not the most likely way
- Other reasons you may want or need to produce e-mails:
 - Audit Committee investigation
 - Whistleblower complaint
 - Regulatory request
 - Tax audit, etc.
- If you haven't had to deal with a significant e-mail production ... you will



E-Mail Presents two key risks: 1st Content

- E-mails are informal, written carelessly
 - Almost anything can be taken out of context
 - Newspaper headline is much more damaging than evidence at trial
- Microsoft antitrust case
 - AOL executive e-mail: “Gates delivered a characteristically blunt query: “How much do we need to pay you to screw Netscape?”
 - Microsoft lawyer: e-mails are “snippets taken out of context”
- Merck – Vioxx
 - Headline: “Vioxx E-mails Suggest Early Knowledge”
 - Merck lawyer: e-mails were “taken out of context”







E-Mail Presents two key risks: 2nd Cost

- Employees keep a lot of e-mails by default
 - Easier to just keep everything than actively managing messages
- Cost of e-mail production can be very high
 - Restoring e-mail backup tapes
 - Searching hard drives for off-line data
 - “De-duplicating” multiple copies
 - Converting e-mails into a searchable database
- Cost of searching e-mails is also tremendous
 - Even innocuous messages take time to review



Policy Alternatives

-  Keep everything – unworkable
-  Delete everything – impractical
-  Filter out “sensitive” e-mails - impossible
-  **Teach responsible e-mail use**
 - Accept that we will continue to use e-mail
 - Raise awareness of risks & shift responsibility to users

Goal is to address risks without killing productivity
Challenges are both behavioral and technical



Raise Awareness of E-Mail Risks

- Improper e-mails put both the employee and the company at risk
 - Embarrassing publicity, civil or criminal action, regulatory sanctions, disciplinary actions
- Problems come up in seemingly harmless areas
 - Chevron paid \$2.2 million to female employees to settle a sexual harassment lawsuit stemming from inappropriate e-mail, including one entitled “25 Reasons Why Beer is Better Than Women”
- Risks come in many forms – E-mails
 - are easily misunderstood, are not always the best means of communication
 - allow the inappropriate dissemination of sensitive information
 - should never be considered private



Focus on Document Creation – Do’s and Don’ts

- 📁 Consider what is the most appropriate means of communication
 - If a writing is necessary, make sure your document is factual and accurate
- 📄 Deal with inappropriate statements sent to you by others, for example by clarifying what is meant, correcting inaccuracies, taking follow-up actions, etc.
- 🗨️ Avoid irony, sarcasm or exaggeration. Humor is often misunderstood
- 🗨️ Assume that if a statement can be misconstrued or taken out of context, it will be



Focus on Document Creation – Do's and Don'ts

- ⌚ Avoid speculations or statements beyond your field of professional expertise
- ✉ Avoid overly broad distribution; send only to persons who have a need to know
- ⚖ Assume your document will be read by an adversary in litigation
- 🔒 Be aware the company will have access to your messages. Would you still be comfortable if your message became public?



Are Messages Accessible?

- Know where your content is
 - On-line on company server
 - "Personal" folders on user hard drive
 - Public / shared folders
 - Removable media / backup tapes
 - CRM systems and other databases
 - Instant Messaging logs
- Bring off-line (inaccessible) content on-line
 - Prohibit personal folders or storage on removable media
 - Give incentives to bring content on-line: company archive with more sophisticated searching, automatically enforced retention periods, etc.



How to Use Age & Size Limits

- **Age Limits** reinforce the need to regularly manage messages
 - Most matters are addressed within 2 weeks; survey of global multinationals shows limits range from 20 to 180 days
 - Because accumulation is in order messages, consider a more generous current period to provide greater flexibility: 60 days
- **Size Limits** make users focus on which messages must be kept
 - Average size limit for all US companies: 110 MB
 - Average message size (w/attachments): 40 KB
 - Corresponding # of messages: 2,750
- Need to have an approach for documents, large attachments
 - Separate document management system? Need for limited exceptions?



Are Your Messages Easily Searchable?

Type of Data / Database

Litigation database
 Professional, searchable archive
 Mail environment (e.g. Outlook)
 Personal folders
 Individual message files
 Backup tapes ⁽¹⁾
 Removable media

Location of Data

Company / Third party
 Storage area network
 Company server
 User hard drive
 User hard drive
 Tape
 CD-Rom, etc.

⁽¹⁾ Consider also time and cost to restore and de-duplicate, and ability to include in otherwise searchable database

- You should be able to conduct sophisticated searches in-house
 - Can you search in attachments, embedded messages?
 - Can you search by user, keyword, with indexing, etc.?



Sample E-Mail Policy (see handout)

- ☞ Computers and e-mail system are company property
- ☞ Address expectations of privacy, and private use of systems
- ☞ Content guidelines on creating messages, do's and don'ts
- ☞ Messages must be accessible on company systems
- ☞ Users should manage messages – age and size limits
 - ☞ Specify broadly messages that should be retained, and how
- ☞ Instant messaging
- ☞ Company monitoring and access to user accounts



Backup Policy – Know Where Your Tapes Are

- ☞ Separate e-mail backups from other server data that may need to be retained longer
- ☞ Reduce the number of e-mail servers as much as possible
- ☞ Create daily backup of e-mail data
- ☞ Keep 10 daily backups, then rotate oldest tape
 - Do not retain older tapes unless required in connection with litigation
- ☞ Periodic confirmation from IT managers



Cisco's Contract Management System

Jyoti Pakrasi
Cisco Systems - Linksys

ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam
Marriott Hotel



Agenda

- Internal vs. commercial solution ?
- Audit / SOX requirements
- An integral part of an e-Commerce environment
- Cisco's Contract Management System
- Benefits

ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam Marriott Hotel



Internal vs. Commercial Solution ?

- What are my requirements ?
 - National vs. international business
 - Highly customized vs. standard contracts
 - Dynamic vs. static environment
 - Highly regulated industry ?
 - Need for Chinese walls ?
 - Standalone or integrated in IT environment ?



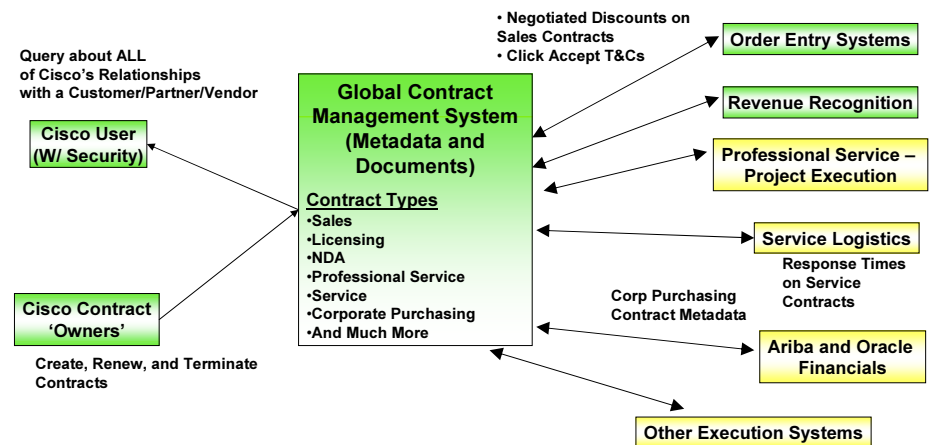
Internal vs. Commercial Solution ?

- Potential constraints
 - Budget availability
 - Know-how, expertise
 - Existing IT-tools
- Return on Investment analysis
 - including Total Cost of Ownership of both options

Audit / SOX requirements

- Do we have a contract with a certain Customer ?
- What are the terms?
- When does it expire?
- What is the Customer entitled to?
- What are Cisco's obligations?
- Where is the paper?

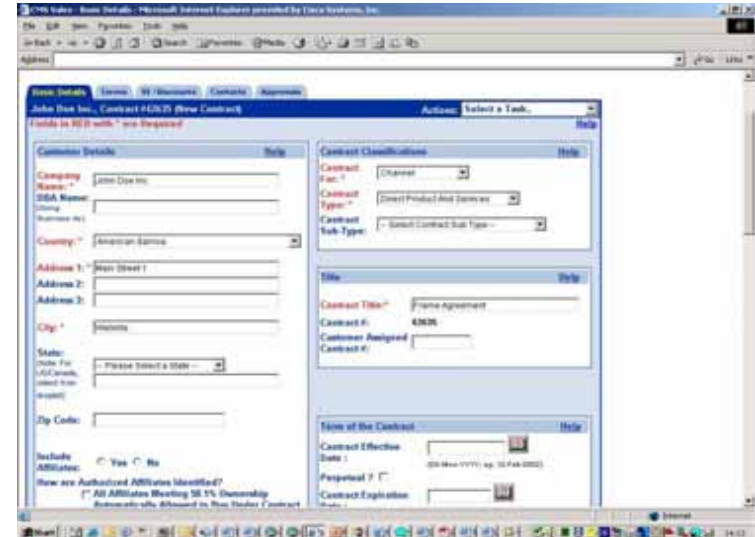
Global Contract Management System = eCommerce Enabler





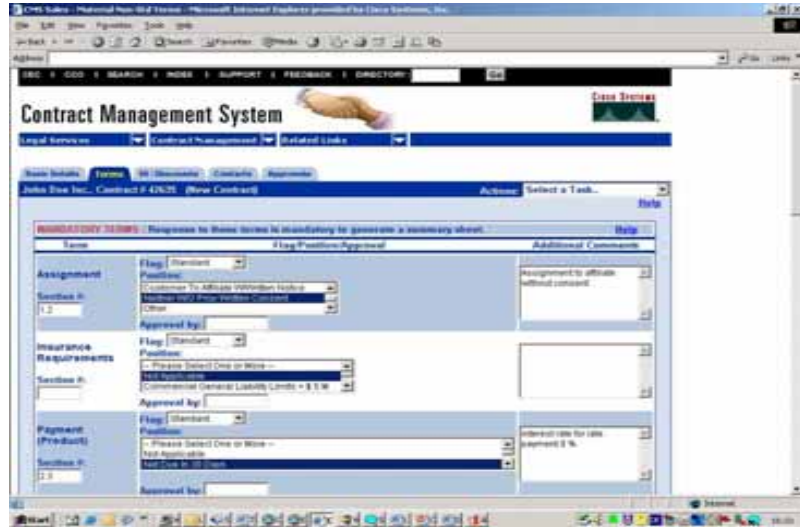
ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam Marriott Hotel



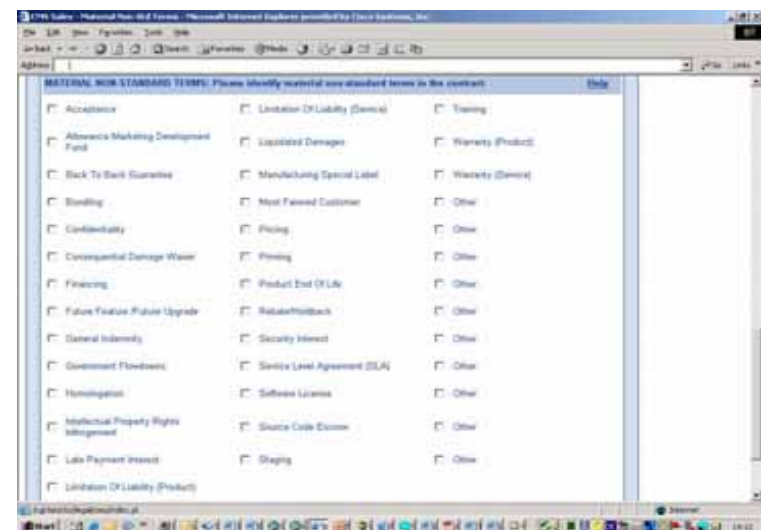
ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam Marriott Hotel



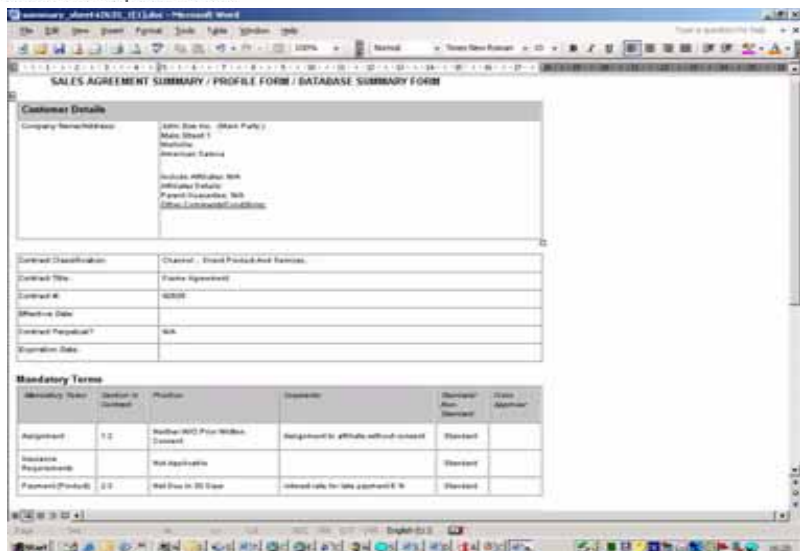
ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam Marriott Hotel



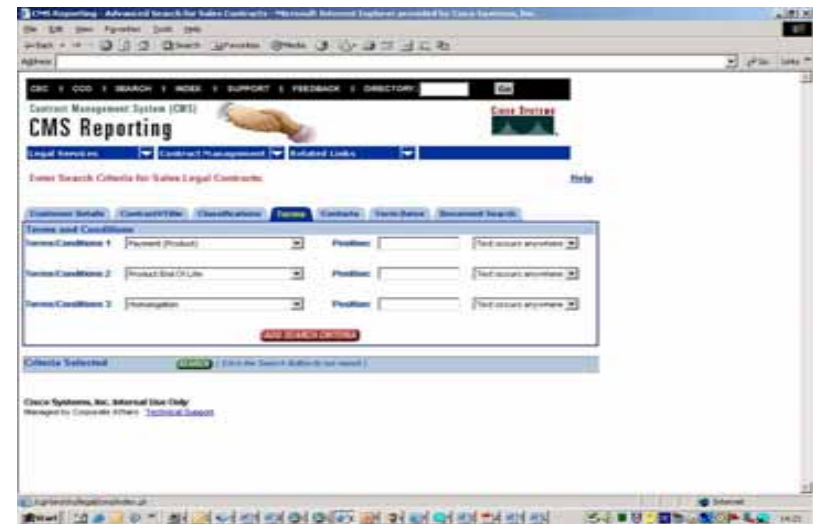
ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam Marriott Hotel



ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam Marriott Hotel



ACC Europe 2006 Corporate Counsel University

February 12-14, Amsterdam Marriott Hotel



Workload

- Automatically for click-accept contracts
- Approx. 15 min for standard contract
- About 45 min for heavily negotiated contracts



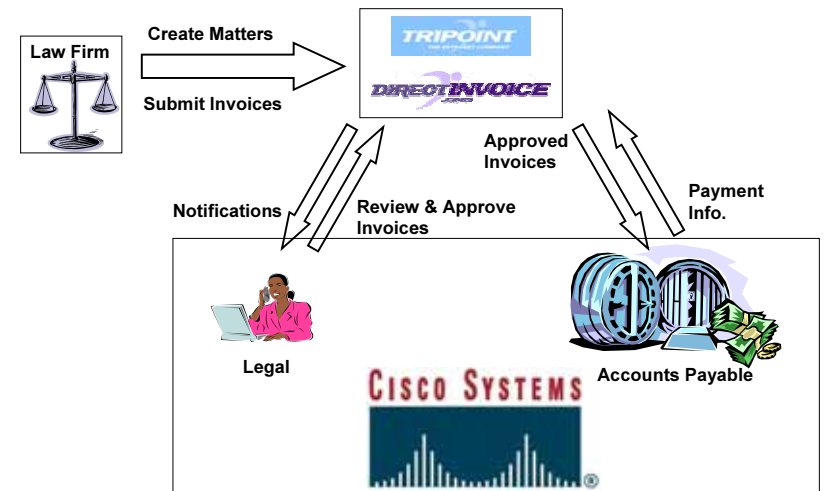
Benefits

- Automate workflow
- Self-service access to data/documents
- Structured information about contract enables eCommerce
- Estimate **\$300 savings per contract during lifecycle** (40,000+ contracts)

Benefits of proprietary solution

- Customized to user needs
- Seamless integration in e-commerce environment
- In-house expertise allows quick updates, no external support costs
- Various IT-tools launched in Law Dept. later rolled out to other departments

A commercial solution



Hot Topic: Privilege

ACC has a number of online resources related to the subject of privilege. Look for these and other documents online at www.acca.com.

Attorney/Client Privilege survey:

<http://www.acca.com/Surveys/attyclient.pdf>

Legal Professional Privilege: the Issues for Multinational Businesses with Operations in Europe:

<http://www.acca.com/protected/article/attyclient/multinationalbuss.pdf>

ACC Docket article on the EU Commission issues in 2002-3

<http://www.acca.com/protected/pubs/docket/ji02/hostility1.php>

PowerPoint presentation:

http://www.acca.com/chapters/program/gcca/trap_unwary.pdf

Article on privilege issues:

<http://www.acca.com/protected/pubs/docket/sept05/wither.pdf>

Listing of Attorney/Client Privilege articles on general:

<http://www.acca.com/advocacy/attyclient/articles.php>

05/EN
WP108

**Working Document Establishing a Model Checklist Application for Approval of
Binding Corporate Rules**

Adopted on April 14th, 2005

The participation of data protection authorities in the approval of binding corporate rules is entirely voluntary¹. The decision to participate can be made on a case by case basis. No data protection authority would be obliged to participate in any procedures aimed at approval of binding corporate rules. The participation of authorities that do not have the power to authorise international data transfers would be understood as reporting favourably, where appropriate, to the national authority in charge of granting authorisations for international data transfers.

The elements described in this document are no doubt very important but are not carved in stone and the Article 29 Working Party may revisit this document in the future in the light of experience. Companies are invited to use this check-list when submitting BCRs for the consideration of national data protection authorities. Companies should also bear in mind that their proposals may require supplementation to comply with the relevant requirements of the national legal systems concerned, in particular as regards those means being proposed to guarantee that data subjects can exercise their rights under the BCRs.

Those issues not covered by the model check-list will be discussed and dealt with by those authorities concerned as a part of normal consultations during the co-operation procedure. The checklist is intended to encompass all the requirements of the Article 29 Working Party number 74² ("WP 74") and concentrates on the matters that a DPA needs to consider in the assessment of adequacy as laid down by the Article 29 Working Party in WP 74.

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission. Justice, Freedom and Security Directorate-General.
Website: www.europa.eu.int/comm/privacy

¹ References to data protection authorities should be understood as including data protection authorities of EU and EEA countries.

² Working Document Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. Adopted on June 3, 2003.

1. **What is this checklist for?**

2. This checklist is designed to assist a group of companies when it applies for approval of its binding corporate rules and in particular to help demonstrate how the group complies with WP74³.

3. **Which data protection authority should you apply to?**

3.1. If the ultimate parent or operational headquarters of your group is a company incorporated in a member state of the EU, you should apply to the data protection authority of that member state.

3.2. If it is not clear where the ultimate parent or operational headquarters of your group is situated, or if it is situated outside the EU, you should apply to the most appropriate data protection authority in accordance with the criteria set out below.

3.3. When applying you need to explain in detail why the data protection authority you have applied to is the most appropriate data protection authority. Factors that are taken into account to determine whether you have applied to the most appropriate data protection authority include:

- 3.3.1. the location of the group's European headquarters.
- 3.3.2. the location of the company within the group with delegated data protection responsibilities⁴;
- 3.3.3. the location of the company which is best placed (in terms of management function, administrative burden etc) to deal with the application and to enforce the binding corporate rules in the group;
- 3.3.4. the place where most decisions in terms of the purposes and the means of the processing are taken; and
- 3.3.5. the member states within the EU from which most transfers outside the EEA will take place.

3.4. Priority will be given to factor 331.

3.5. These are not formal criteria. The data protection authority to which you send your application will exercise its discretion in deciding whether it is in fact the most appropriate data protection authority and, in any event, the data protection authorities among themselves may decide to allocate the application to a data protection authority other than the one to which you applied.

³ WP74 sets out the requirements for binding corporate rules.

⁴ As provided for in the working document number 74, if the headquarters of the corporate group were not in the EU/EEA, the corporate group should appoint a European member with delegated data protection responsibilities in charge of ensuring that any foreign member of the corporate group adjust their processing activities to the undertakings contained in the corporate group, interface with the leading authority where appropriate and pay compensation in case of damages resulting from the violation of the binding corporate rules by any member of the corporate group.

4. **What information is required for your application?**

4.1. You will need to supply:

4.1.1. A separate document containing:

4.1.1.1. contact details of the responsible person within your organisation to whom queries may be addressed; and

4.1.1.2. all the relevant information to justify the choice of data protection authority including the basic structure of your group and the nature and structure of the processing activities in the EU/EEA with particular attention to the place/s where decisions are made, the location of affiliates in the EU, the means and purposes of the processing, the places from which the transfers to third countries are being made and the third countries to which those data are transferred (this is needed so that the 'entry point data protection authority' can circulate it to the data protection authorities concerned);

4.1.2. A background paper summarising how the required elements of WP74 (as set out below) have been satisfied (this will help the data protection authorities to identify the relevant sections of the documents you are providing);

4.1.3. All relevant documents that comprise the 'binding corporate rules' to be adopted by your organisation (e.g. any policies, codes, notices, procedures and contracts that may be relevant to the application). As well as a general statement of principles, the data protection authorities need to see how personal data is actually handled within your group;

4.1.4. It is important to note that whilst a data protection authority will have duties under its national law not to disclose information received from a data controller as part of the authorisation process without lawful authority, some data protection authorities are also subject to freedom of information legislation. Accordingly, if any documentation submitted in support of your application for authorisation of your binding corporate rules is commercially sensitive, please mark the appropriate documents appropriately. However, the decision on whether to disclose the information will be taken by each data protection authority involved in accordance with national freedom of information legislation. Also, the information that is necessary for the other involved data protection authorities to assess the binding corporate rules will have to be circulated.

5. **Evidence that the measures are legally binding:**

5.1. The rules must be binding both –

5.1.1. within the organisation and;

5.1.2. externally for the benefit of individuals.

5.2. There are a number of ways in which this requirement may be met and how this is done will depend upon the structure and size of your organisation and the

procedures adopted with regard to other regulatory requirements to which your organisation may be subject. It will also depend upon the national laws in the Member States in which your organisation is located.

5.3. **Binding within the organisation**

5.4. **How are the rules binding between the component parts of the organisation?**

5.5. You must ensure compliance with the binding corporate rules by other members of the group. This is particularly important where there is no 'head office' or where the head office is outside the EEA. How this is achieved will depend upon the structure of your organisation but will also be subject to the national laws of the Member States in which your organisation is located.

5.6. The following are suggestions as to how a set of corporate rules may be binding on an organisation but there may be other ways more suited to your proposed arrangements:

5.6.1. Binding corporate or contractual rules that you can enforce against the other members of the group;

5.6.2. Unilateral declarations or undertakings made or given by the parent company which are binding on the other members of the group;

5.6.3. Incorporation of other regulatory measures, for example, obligations contained in statutory codes within a defined legal framework; or

5.6.4. Incorporation of the rules within the general business principles of an organisation backed by appropriate policies, audits and sanctions.

5.7. All of the above suggestions may have a different effect in different member states. For example, simple unilateral declarations are not regarded as binding in some member states. You would, therefore, need to take local advice if you intended to rely on such declarations.

Please explain how the rules are binding upon the members of the group.

5.8. **How are the rules made binding on employees?**

5.9. Employees must be bound by the rules. This might be achieved by way of specific obligations contained in a contract of employment and by linking observance of the rules with disciplinary procedures for example. In addition, there should be adequate training programmes and senior staff commitment, and the title of the person ultimately responsible within the organisation for compliance should be included in your application.

Please explain how the rules are binding upon employees within your organisation and the sanctions for failure to comply with the rules.

5.10. **How are the rules made binding on subcontractors handling the data?**

5.11. You need to show how your binding corporate rules are made binding on subcontractors. Please provide evidence of the type of contractual clauses that you impose on subcontractors and explain how those contracts deal with the consequences of non-compliance.

Please specify how the rules are binding upon subcontractors and the sanctions for failure to comply with the rules.

5.12. **How are the rules binding externally for the benefit of individuals?**

5.13. Individuals covered by the scope of the binding corporate rules must be able to enforce compliance with the rules both via the data protection authorities and the courts.

5.14. Individuals must be able to commence claims within the jurisdiction of:

5.14.1. the member of the group at the origin of the transfer or,

5.14.2. the EU headquarters or the European member of the group with delegated data protection responsibilities.

5.15. Your application will need to show the practical steps a data subject can take to obtain a remedy from your organisation, including a complaint handling process.

5.16. For example, if your headquarters and the lead authority are in Belgium and one of your group companies in Italy breaches your corporate rules, it should be clear to the data subject that he or she can make a claim against the infringing company in Italy and/or the headquarters in Belgium.

5.17. Your application should contain confirmation that the European headquarters of the organisation, or that part of the organisation with delegated data protection responsibilities in the EU, has sufficient assets or has made appropriate arrangements to enable payment of compensation for any damages resulting from the breach, by any part of the organisation, of the binding corporate rules.

5.18. In your application please identify which part of the organisation is responsible for handling claims, and how the individual can access the complaints handling process.

5.19. Your application will need to make clear that the burden of proof with regard to an alleged breach of the rules will rest with the member of the group at the origin of the transfer or the European headquarters or that part of the organisation with delegated data protection responsibilities, regardless of where the claim originates.

5.20. Your application should acknowledge that a data subject will have the rights afforded under Directive 95/46/EC.

- 5.21. Your application should also include confirmation that you will cooperate with the data protection authorities with regard to any decisions made by the supervisory authority and abide by the advice of the data protection authority with regard to interpretation of WP 74.

Please specify how the rules are binding externally

6. Verification of compliance

- 6.1. WP74 states that the binding corporate rules adopted by an organisation must provide for the use of either internal auditors, external auditors or a combination of both.
- 6.2. The data protection audit programme and audit plan need to be clearly set out either in a document containing your data protection standards or in other internal procedure documents and audits provided to a data protection authority upon request. The authority will need to be satisfied that the audit programme adequately covers all aspects of the binding corporate rules including methods of ensuring that corrective actions have taken place. The audit plan should allow for the supervisory authority to have the power to carry out a data protection audit if required.
- 6.3. Data protection authorities neither need nor want to see anything in your audit results that does not relate to data protection. The authorities are not concerned with corporate governance, except to the extent that it affects data protection compliance. Equally, the authorities are not interested in seeing commercially sensitive information. The information provided should be limited to that which is required to satisfy WP 74. However, it is appreciated that issues relating to data protection compliance may be included in reports containing other information and it will sometimes not be possible to separate those elements relating to data protection from other unrelated information.
- 6.4. Please summarise your audit arrangements for data protection matters and the way in which audit reports are handled internally within your organisation (i.e. information as to the recipients of the report and their position within the structure of the organisation).

Please give details of your data protection audit programme and audit plan.

7. Description of processing and flows of information

- 7.1. The binding corporate rules should identify the following:
- 7.1.1. the nature of the data, i.e. whether the binding corporate rules relate to only one type of data, for example, human resource data, or, if the rules relate to more than one type of data, how this is addressed in the binding corporate rules. In any event, there should be sufficient detail included in the application to enable a supervisory authority to assess whether the

safeguards put in place address adequately the nature of the processing being undertaken;

- 7.1.2. the purposes for which the data are processed;
- 7.1.3. the extent of the transfers within the group that are covered by the rules. We need to have details of:
- 7.1.3.1 any group members in the EU from which personal data may be transferred; and
- 7.1.3.2 any group members outside the EEA to which personal data may be transferred.

- 7.2. You also need to show whether the binding corporate rules apply only to transfers from the EU only or whether all transfers between members of the group are covered. The data protection authorities need to understand on what basis onward transfers (ie transfers of data from group members outside the EEA to third parties) take place.

Please describe the nature of the data, the purposes for which they are processed and the extent of the transfers within the group.

8. Data protection safeguards

- 8.1. The rules must contain a clear description of the standard of data protection safeguards applied to the data consistent with Directive 95/46/EC and must set out how these requirements are met within your organisation.
- 8.2. In particular, the binding corporate rules must address the following:
- 8.2.1. transparency and fairness to data subjects;
- 8.2.2. purpose limitation;
- 8.2.3. ensuring data quality;
- 8.2.4. security;
- 8.2.5. individual rights of access, rectification and objection to processing;
- 8.2.6. restrictions on onward transfer out of the multinational company covered by the rules (although this may be possible under other arrangements facilitating transfers).

Please provide a summary of how this has been addressed in the binding corporate rules adopted by your organisation with supporting documentation e.g. relevant policies.

9. Mechanism for reporting and recording changes

9.1. There must be a system in place for informing other parts of the organisation and the data protection authority of any changes to the rules in line with paragraph 4.2 of WP74. The data protection authorities will only need to see changes that significantly affect data protection compliance. Administrative changes, for example, do not need to be notified unless they impact on the operation of the binding corporate rules. Your lead authority will inform you of any specific requirements to report to or update any data protection authorities.

Please describe the mechanism that your organisation will use to report changes.

Done in Brussels, on April 14, 2005

For the Working Party
The Chairman
Peter Schaar

IMPORTANT LEGAL NOTICE - The information on this site is subject to a [disclaimer](#) and a [copyright notice](#).

JUDGMENT OF THE COURT

6 November 2003 (1)

(Directive 95/46/EC - Scope - Publication of personal data on the internet - Place of publication - Definition of transfer of personal data to third countries - Freedom of expression - Compatibility with Directive 95/46 of greater protection for personal data under the national legislation of a Member State)

In Case C-101/01,

REFERENCE to the Court under Article 234 EC by the Göta hovrätt (Sweden) for a preliminary ruling in the criminal proceedings before that court against

Bodil Lindqvist,

on, inter alia, the interpretation of 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 (OJ 1995 L 281, p. 31),

THE COURT,

composed of: P. Jann, President of the First Chamber, acting for the President, C.W.A. Timmermans, C. Gulmann, J.N. Cunha Rodrigues and A. Rosas (Presidents of Chambers), D.A.O. Edward (Rapporteur), J.-P. Puisseochet, F. Macken and S. von Bahr, Judges,

Advocate General: A. Tizzano,

Registrar: H. von Holstein, Deputy Registrar,

after considering the written observations submitted on behalf of:

- Mrs Lindqvist, by S. Larsson, advokat,
- the Swedish Government, by A. Kruse, acting as Agent,
- the Netherlands Government, by H.G. Sevenster, acting as Agent,
- the United Kingdom Government, by G. Amodeo, acting as Agent, assisted by J. Stratford, barrister,
- the Commission of the European Communities, by L. Ström and X. Lewis, acting as Agents,

having regard to the Report for the Hearing,

after hearing the oral observations of Mrs Lindqvist, represented by S. Larsson, of the Swedish Government, represented by A. Kruse and B. Hernqvist, acting as Agents, of the Netherlands Government, represented by J. van Bakel, acting as Agent, of the United Kingdom Government, represented by J. Stratford, of the Commission, represented by L. Ström and C. Docksey, acting as Agent, and of the EFTA Surveillance Authority, represented by D. Sif Tynes, acting as Agent, at the hearing on 30 April 2002,

after hearing the Opinion of the Advocate General at the sitting on 19 September 2002,

gives the following

Judgment

By order of 23 February 2001, received at the Court on 1 March 2001, the Göta hovrätt (Göta Court of Appeal) referred to the Court for a preliminary ruling under Article 234 EC seven questions concerning inter alia the interpretation of 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 (OJ 1995 L 281, p. 31).

Those questions were raised in criminal proceedings before that court against Mrs Lindqvist, who was charged with breach of the Swedish legislation on the protection of personal data for publishing on her internet site personal data on a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church.

Legal background

Community legislation

Directive 95/46 is intended, according to the terms of Article 1(1), to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.

Article 3 of Directive 95/46 provides, regarding the scope of the directive:

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to 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 areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 8 of Directive 95/46, entitled The processing of special categories of data, provides:

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is

necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9 of Directive 95/46, entitled Processing of personal data and freedom of expression, provides:

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

Article 13 of Directive 95/46, entitled Exemptions and restrictions, provides that Member States may adopt measures restricting the scope of some of the obligations imposed by the directive on the controller of the data, inter alia as regards information given to the persons concerned, where such a restriction is necessary to safeguard, for example, national security, defence, public security, an important economic or financial interest of a Member State or of the European Union, or the investigation and prosecution of criminal offences or of breaches of ethics for regulated professions.

Article 25 of Directive 95/46, which is part of Chapter IV entitled Transfer of personal data to third countries, reads as follows:

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third

country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

At the time of the adoption of Directive 95/46, the Kingdom of Sweden made the following statement on the subject of Article 9, which was entered in the Council minutes (document No 4649/95 of the Council, of 2 February 1995):

The Kingdom of Sweden considers that artistic and literary expression refers to the means of expression rather than to the contents of the communication or its quality.

The European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950 (the ECHR), provides, in Article 8, for a right to respect for private and family life and, in Article 10, contains provisions concerning freedom of expression.

The national legislation

Directive 95/46 was implemented in Swedish law by the Personuppgiftslag (SFS 1998:204) (Swedish law on personal data, the PUL).

The main proceedings and the questions referred

In addition to her job as a maintenance worker, Mrs Lindqvist worked as a catechist in the parish of Aiseda (Sweden). She followed a data processing course on which she had inter alia to set up a home page on the internet. At the end of 1998, Mrs Lindqvist set up internet pages at home on her personal computer in order to allow parishioners preparing for their confirmation to obtain information they might need. At her request, the administrator of the Swedish Church's website set up a link between those pages and that site.

The pages in question contained information about Mrs Lindqvist and 18 colleagues in the parish, sometimes including their full names and in other cases only their first names. Mrs Lindqvist also described, in a mildly humorous manner, the jobs held by her colleagues and their hobbies. In many cases family circumstances and telephone numbers and other matters were mentioned. She also stated that one colleague had injured her foot and was on half-time on medical grounds.

Mrs Lindqvist had not informed her colleagues of the existence of those pages or obtained their consent, nor did she notify the Datainspektionen (supervisory authority for the protection of electronically transmitted data) of her activity. She removed the pages in question as soon as she became aware that they were not appreciated by some of her colleagues.

The public prosecutor brought a prosecution against Mrs Lindqvist charging her with breach of the PUL on the grounds that she had:

- processed personal data by automatic means without giving prior written notification to the Datainspektionen (Paragraph 36 of the PUL);

- processed sensitive personal data (injured foot and half-time on medical grounds) without authorisation (Paragraph 13 of the PUL);

- transferred processed personal data to a third country without authorisation (Paragraph 33 of the PUL).

Mrs Lindqvist accepted the facts but disputed that she was guilty of an offence. Mrs Lindqvist was fined by the Eksjö tingsrätt (District Court) (Sweden) and appealed against that sentence to the referring court.

The amount of the fine was SEK 4 000, which was arrived at by multiplying the sum of SEK 100, representing Mrs Lindqvist's financial position, by a factor of 40, reflecting the severity of the offence. Mrs Lindqvist was also sentenced to pay SEK 300 to a Swedish fund to assist victims of crimes.

As it had doubts as to the interpretation of the Community law applicable in this area, *inter alia* Directive 95/46, the Göta hovrätt decided to stay proceedings and refer the following questions to the Court for a preliminary ruling:

(1) Is the mention of a person - by name or with name and telephone number - on an internet home page an action which falls within the scope of [Directive 95/46]? Does it constitute the processing of personal data wholly or partly by automatic means to list on a self-made internet home page a number of persons with comments and statements about their jobs and hobbies etc.?

(2) If the answer to the first question is no, can the act of setting up on an internet home page separate pages for about 15 people with links between the pages which make it possible to search by first name be considered to constitute the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system within the meaning of Article 3(1)?

If the answer to either of those questions is yes, the hovrätt also asks the following questions:

(3) Can the act of loading information of the type described about work colleagues onto a private home page which is none the less accessible to anyone who knows its address be regarded as outside the scope of [Directive 95/46] on the ground that it is covered by one of the exceptions in Article 3(2)?

(4) Is information on a home page stating that a named colleague has injured her foot and is on half-time on medical grounds personal data concerning health which, according to Article 8(1), may not be processed?

(5) [Directive 95/46] prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden - with the result that personal data become accessible to people in third countries - does that constitute a transfer of data to a third country within the meaning of the directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?

(6) Can the provisions of [Directive 95/46], in a case such as the above, be regarded as bringing about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the EU and are enshrined in *inter alia* Article 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms?

Finally, the hovrätt asks the following question:

(7) Can a Member State, as regards the issues raised in the above questions, provide more extensive protection for personal data or give it a wider scope than the directive, even if none of the circumstances described in Article 13 exists?

The first question

By its first question, the referring court asks whether the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46.

Observations submitted to the Court

Mrs Lindqvist submits that it is unreasonable to take the view that the mere mention by name of a person or of personal data in a document contained on an internet page constitutes automatic processing of data. On the other hand, reference to such data in a keyword in the meta tags of an internet page, which makes it possible to create an index and find that page using a search engine, might constitute such processing.

The Swedish Government submits that the term the processing of personal data wholly or partly by automatic means in Article 3(1) of Directive 95/46, covers all processing in computer format, in other words, in binary format. Consequently, as soon as personal data are processed by computer, whether using a word processing programme or in order to put them on an internet page, they have been the subject of processing within the meaning of Directive 95/46.

The Netherlands Government submits that personal data are loaded onto an internet page using a computer and a server, which are essential elements of automation, so that it must be considered that such data are subject to automatic processing.

The Commission submits that Directive 95/46 applies to all processing of personal data referred to in Article 3 thereof, regardless of the technical means used. Accordingly, making personal data available on the internet constitutes processing wholly or partly by automatic means, provided that there are no technical limitations which restrict the processing to a purely manual operation. Thus, by its very nature, an internet page falls within the scope of Directive 95/46.

Reply of the Court

The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies.

According to the definition in Article 2(b) of Directive 95/46, the term processing of such data used in Article 3(1) covers any operation or set of operations which is performed upon personal data, whether or not by automatic means. That provision gives several examples of such operations, including disclosure by transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing.

It remains to be determined whether such processing is wholly or partly by automatic means. In that connection, placing information on an internet page entails, under current technical and computer procedures, the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet. Such operations are performed, at least in part, automatically.

The answer to the first question must therefore be that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46.

The second question

As the first question has been answered in the affirmative, there is no need to reply to the second question, which arises only in the event that the first question is answered in the negative.

The third question

By its third question, the national court essentially seeks to know whether processing of personal data such as that described in the first question is covered by one of the exceptions in Article 3(2) of Directive 95/46.

Observations submitted to the Court

Mrs Lindqvist submits that private individuals who make use of their freedom of expression to

create internet pages in the course of a non-profit-making or leisure activity are not carrying out an economic activity and are thus not subject to Community law. If the Court were to hold otherwise, the question of the validity of Directive 95/46 would arise, as, in adopting it, the Community legislature would have exceeded the powers conferred on it by Article 100a of the EC Treaty (now, after amendment, Article 95 EC). The approximation of laws, which concerns the establishment and functioning of the common market, cannot serve as a legal basis for Community measures regulating the right of private individuals to freedom of expression on the internet.

The Swedish Government submits that, when Directive 95/46 was implemented in national law, the Swedish legislature took the view that processing of personal data by a natural person which consisted in publishing those data to an indeterminate number of people, for example through the internet, could not be described as a purely personal or household activity within the meaning of the second indent of Article 3(2) of Directive 95/46. However, that Government does not rule out that the exception provided for in the first indent of that paragraph might cover cases in which a natural person publishes personal data on an internet page solely in the exercise of his freedom of expression and without any connection with a professional or commercial activity.

According to the Netherlands Government, automatic processing of data such as that at issue in the main proceedings does not fall within any of the exceptions in Article 3(2) of Directive 95/46. As regards the exception in the second indent of that paragraph in particular, it observes that the creator of an internet page brings the data placed on it to the knowledge of a generally indeterminate group of people.

The Commission submits that an internet page such as that at issue in the main proceedings cannot be considered to fall outside the scope of Directive 95/46 by virtue of Article 3(2) thereof, but constitutes, given the purpose of the internet page at issue in the main proceedings, an artistic and literary creation within the meaning of Article 9 of that Directive.

It takes the view that the first indent of Article 3(2) of Directive 95/46 lends itself to two different interpretations. The first consists in limiting the scope of that provision to the areas cited as examples, in other words, to activities which essentially fall within what are generally called the second and third pillars. The other interpretation consists in excluding from the scope of Directive 95/46 the exercise of any activity which is not covered by Community law.

The Commission argues that Community law is not limited to economic activities connected with the four fundamental freedoms. Referring to the legal basis of Directive 95/46, to its objective, to Article 6 EU, to the Charter of fundamental rights of the European Union proclaimed in Nice on 18 December 2000 (OJ 2000 C 364, p. 1), and to the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, it concludes that that directive is intended to regulate the free movement of personal data in the exercise not only of an economic activity, but also of social activity in the course of the integration and functioning of the common market.

It adds that to exclude generally from the scope of Directive 95/46 internet pages which contain no element of commerce or of provision of services might entail serious problems of demarcation. A large number of internet pages containing personal data intended to disparage certain persons with a particular end in view might then be excluded from the scope of that directive.

Reply of the Court

Article 3(2) of Directive 95/46 provides for two exceptions to its scope.

The first exception concerns the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any case 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 areas of criminal law.

As the activities of Mrs Lindqvist which are at issue in the main proceedings are essentially not economic but charitable and religious, it is necessary to consider whether they constitute the processing of personal data in the course of an activity which falls outside the scope of Community law within the meaning of the first indent of Article 3(2) of Directive 95/46.

40. The Court has held, on the subject of Directive 95/46, which is based on Article 100a of the Treaty, that recourse to that legal basis does not presuppose the existence of an actual link with free movement between Member States in every situation referred to by the measure founded on that basis (see Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989, paragraph 41, and the case-law cited therein).
41. A contrary interpretation could make the limits of the field of application of the directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations (*Österreichischer Rundfunk and Others*, cited above, paragraph 42).
42. Against that background, it would not be appropriate to interpret the expression activity which falls outside the scope of Community law as having a scope which would require it to be determined in each individual case whether the specific activity at issue directly affected freedom of movement between Member States.
43. The activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 (in other words, the activities provided for by Titles V and VI of the Treaty on European Union and processing operations concerning public security, defence, State security and activities in areas of criminal law) are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals.
44. It must therefore be considered that the activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 are intended to define the scope of the exception provided for there, with the result that that exception applies only to the activities which are expressly listed there or which can be classified in the same category (*ejusdem generis*).
45. Charitable or religious activities such as those carried out by Mrs Lindqvist cannot be considered equivalent to the activities listed in the first indent of Article 3(2) of Directive 95/46 and are thus not covered by that exception.
46. As regards the exception provided for in the second indent of Article 3(2) of Directive 95/46, the 12th recital in the preamble to that directive, which concerns that exception, cites, as examples of the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses.
47. That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.
48. The answer to the third question must therefore be that processing of personal data such as that described in the reply to the first question is not covered by any of the exceptions in Article 3(2) of Directive 95/46.

The fourth question

49. By its fourth question, the referring court seeks to know whether reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.
50. In the light of the purpose of the directive, the expression data concerning health used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual.
51. The answer to the fourth question must therefore be that reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.

The fifth question

[/curia.eu.int/jurisp/cgi-bin/gettext.pl?where=&lang=en&num=79968893C190101...](http://curia.eu.int/jurisp/cgi-bin/gettext.pl?where=&lang=en&num=79968893C190101...) 27-1-2006

By its fifth question the referring court seeks essentially to know whether there is any transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person (the hosting provider) who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country. The referring court also asks whether the reply to that question would be the same if no one from the third country had in fact accessed the data or if the server where the page was stored was physically in a third country.

Observations submitted to the Court

The Commission and the Swedish Government consider that the loading, using a computer, of personal data onto an internet page, so that they become accessible to nationals of third countries, constitutes a transfer of data to third countries within the meaning of Directive 95/46. The answer would be the same if no one from the third country had in fact accessed the data or if the server where it was stored was physically in a third country.

The Netherlands Government points out that the term transfer is not defined by Directive 95/46. It takes the view, first, that that term must be understood to refer to the act of intentionally transferring personal data from the territory of a Member State to a third country and, second, that no distinction can be made between the different ways in which data are made accessible to third parties. It concludes that loading personal data onto an internet page using a computer cannot be considered to be a transfer of personal data to a third country within the meaning of Article 25 of Directive 95/46.

The United Kingdom Government submits that Article 25 of Directive 95/46 concerns the transfer of data to third countries and not their accessibility from third countries. The term transfer connotes the transmission of personal data from one place and person to another place and person. It is only in the event of such a transfer that Article 25 of Directive 95/46 requires Member States to ensure an adequate level of protection of personal data in a third country.

Reply of the Court

Directive 95/46 does not define the expression transfer to a third country in Article 25 or any other provision, including Article 2.

In order to determine whether loading personal data onto an internet page constitutes a transfer of those data to a third country within the meaning of Article 25 of Directive 95/46 merely because it makes them accessible to people in a third country, it is necessary to take account both of the technical nature of the operations thus carried out and of the purpose and structure of Chapter IV of that directive where Article 25 appears.

Information on the internet can be consulted by an indefinite number of people living in many places at almost any time. The ubiquitous nature of that information is a result inter alia of the fact that the technical means used in connection with the internet are relatively simple and becoming less and less expensive.

Under the procedures for use of the internet available to individuals like Mrs Lindqvist during the 1990s, the author of a page intended for publication on the internet transmits the data making up that page to his hosting provider. That provider manages the computer infrastructure needed to store those data and connect the server hosting the site to the internet. That allows the subsequent transmission of those data to anyone who connects to the internet and seeks access to it. The computers which constitute that infrastructure may be located, and indeed often are located, in one or more countries other than that where the hosting provider is established, without its clients being aware or being in a position to be aware of it.

It appears from the court file that, in order to obtain the information appearing on the internet pages on which Mrs Lindqvist had included information about her colleagues, an internet user would not only have to connect to the internet but also personally carry out the necessary actions to consult those pages. In other words, Mrs Lindqvist's internet pages did not contain the technical means to send that information automatically to people who did not intentionally seek access to those pages.

It follows that, in circumstances such as those in the case in the main proceedings, personal data which appear on the computer of a person in a third country, coming from a person who has loaded them onto an internet site, were not directly transferred between those two people but through the computer infrastructure of the hosting provider where the page is stored.

It is in that light that it must be examined whether the Community legislature intended, for the purposes of the application of Chapter IV of Directive 95/46, to include within the expression transfer [of data] to a third country within the meaning of Article 25 of that directive activities such as those carried out by Mrs Lindqvist. It must be stressed that the fifth question asked by the referring court concerns only those activities and not those carried out by the hosting providers.

Chapter IV of Directive 95/46, in which Article 25 appears, sets up a special regime, with specific rules, intended to allow the Member States to monitor transfers of personal data to third countries. That Chapter sets up a complementary regime to the general regime set up by Chapter II of that directive concerning the lawfulness of processing of personal data.

The objective of Chapter IV is defined in the 56th to 60th recitals in the preamble to Directive 95/46, which state inter alia that, although the protection of individuals guaranteed in the Community by that Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection, the adequacy of such protection must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations. Where a third country does not ensure an adequate level of protection the transfer of personal data to that country must be prohibited.

For its part, Article 25 of Directive 95/46 imposes a series of obligations on Member States and on the Commission for the purposes of monitoring transfers of personal data to third countries in the light of the level of protection afforded to such data in each of those countries.

In particular, Article 25(4) of Directive 95/46 provides that, where the Commission finds that a third country does not ensure an adequate level of protection, Member States are to take the measures necessary to prevent any transfer of personal data to the third country in question.

Chapter IV of Directive 95/46 contains no provision concerning use of the internet. In particular, it does not lay down criteria for deciding whether operations carried out by hosting providers should be deemed to occur in the place of establishment of the service or at its business address or in the place where the computer or computers constituting the service's infrastructure are located.

Given, first, the state of development of the internet at the time Directive 95/46 was drawn up and, second, the absence, in Chapter IV, of criteria applicable to use of the internet, one cannot presume that the Community legislature intended the expression transfer [of data] to a third country to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them.

If Article 25 of Directive 95/46 were interpreted to mean that there is transfer [of data] to a third country every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.

Accordingly, it must be concluded that Article 25 of Directive 95/46 is to be interpreted as meaning that operations such as those carried out by Mrs Lindqvist do not as such constitute a transfer [of data] to a third country. It is thus unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country.

The reply to the fifth question must therefore be that there is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.

The sixth question

By its sixth question the referring court seeks to know whether the provisions of Directive 95/46, in a case such as that in the main proceedings, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined in inter alia Article 10 of the ECHR.

Observations submitted to the Court

Citing inter alia Case C-274/99 P *Connolly v Commission* [2001] ECR I-1611, Mrs Lindqvist submits that Directive 95/46 and the PUL, in so far as they lay down requirements of prior consent and prior notification of a supervisory authority and a principle of prohibiting processing of personal data of a sensitive nature, are contrary to the general principle of freedom of expression enshrined in Community law. More particularly, she argues that the definition of processing of personal data wholly or partly by automatic means does not fulfil the criteria of predictability and accuracy.

She argues further that merely mentioning a natural person by name, revealing their telephone details and working conditions and giving information about their state of health and hobbies, information which is in the public domain, well-known or trivial, does not constitute a significant breach of the right to respect for private life. Mrs Lindqvist considers that, in any event, the constraints imposed by Directive 95/46 are disproportionate to the objective of protecting the reputation and private life of others.

The Swedish Government considers that Directive 95/46 allows the interests at stake to be weighed against each other and freedom of expression and protection of private life to be thereby safeguarded. It adds that only the national court can assess, in the light of the facts of each individual case, whether the restriction on the exercise of the right to freedom of expression entailed by the application of the rules on the protection of the rights of others is proportionate.

The Netherlands Government points out that both freedom of expression and the right to respect for private life are among the general principles of law for which the Court ensures respect and that the ECHR does not establish any hierarchy between the various fundamental rights. It therefore considers that the national court must endeavour to balance the various fundamental rights at issue by taking account of the circumstances of the individual case.

The United Kingdom Government points out that its proposed reply to the fifth question, set out in paragraph 55 of this judgment, is wholly in accordance with fundamental rights and avoids any disproportionate restriction on freedom of expression. It adds that it is difficult to justify an interpretation which would mean that the publication of personal data in a particular form, that is to say, on an internet page, is subject to far greater restrictions than those applicable to publication in other forms, such as on paper.

The Commission also submits that Directive 95/46 does not entail any restriction contrary to the general principle of freedom of expression or other rights and freedoms applicable in the European Union corresponding inter alia to the right provided for in Article 10 of the ECHR.

Reply of the Court

According to the seventh recital in the preamble to Directive 95/46, the establishment and functioning of the common market are liable to be seriously affected by differences in national rules applicable to the processing of personal data. According to the third recital of that directive the harmonisation of those national rules must seek to ensure not only the free flow of such data between Member States but also the safeguarding of the fundamental rights of individuals. Those objectives may of course be inconsistent with one another.

On the one hand, the economic and social integration resulting from the establishment and functioning of the internal market will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States, whether businesses or public authorities of the Member States. Those so involved will, to a certain extent, need to have access to personal data to perform their transactions or carry out their tasks within the area without internal frontiers which the internal market constitutes.

On the other hand, those affected by the processing of personal data understandably require those data to be effectively protected.

The mechanisms allowing those different rights and interests to be balanced are contained, first, in Directive 95/46 itself, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided for. Second, they result from the adoption, by the Member States, of national provisions implementing that directive and their application by the national authorities.

As regards Directive 95/46 itself, its provisions are necessarily relatively general since it has to be applied to a large number of very different situations. Contrary to Mrs Lindqvist's contentions, the directive quite properly includes rules with a degree of flexibility and, in many instances, leaves to the Member States the task of deciding the details or choosing between options.

It is true that, in many respects, the Member States have a margin for manoeuvre in implementing Directive 95/46. However, there is nothing to suggest that the regime it provides for lacks predictability or that its provisions are, as such, contrary to the general principles of Community law and, in particular, to the fundamental rights protected by the Community legal order.

Thus, it is, rather, at the stage of the application at national level of the legislation implementing Directive 95/46 in individual cases that a balance must be found between the rights and interests involved.

In that context, fundamental rights have a particular importance, as demonstrated by the case in the main proceedings, in which, in essence, Mrs Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site.

Consequently, it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality.

Whilst it is true that the protection of private life requires the application of effective sanctions against people processing personal data in ways inconsistent with Directive 95/46, such sanctions must always respect the principle of proportionality. That is so *a fortiori* since the scope of Directive 95/46 is very wide and the obligations of those who process personal data are many and significant.

It is for the referring court to take account, in accordance with the principle of proportionality, of all the circumstances of the case before it, in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed.

The answer to the sixth question must therefore be that the provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the ECHR. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order.

The seventh question

By its seventh question, the referring court essentially seeks to know whether it is permissible for the Member States to provide for greater protection for personal data or a wider scope than are required under Directive 95/46.

Observations submitted to the Court

The Swedish Government states that Directive 95/46 is not confined to fixing minimum conditions for the protection of personal data. Member States are obliged, in the course of implementing that

directive, to attain the level of protection dictated by it and are not empowered to provide for greater or less protection. However, account must be taken of the discretion which the Member States have in implementing the directive to lay down in their domestic law the general conditions for the lawfulness of the processing of personal data.

The Netherlands Government submits that Directive 95/46 does not preclude Member States from providing for greater protection in certain areas. It is clear, for example, from Article 10, Article 11 (1), subparagraph (a) of the first paragraph of Article 14, Article 17(3), Article 18(5) and Article 19 (1) of that directive that the Member States may make provision for wider protection. Moreover, the Member States are free to apply the principles of Directive 95/46 also to activities which do not fall within its scope.

The Commission submits that Directive 95/46 is based on Article 100a of the Treaty and that, if a Member State wishes to maintain or introduce legislation which derogates from such a harmonising directive, it is obliged to notify the Commission pursuant to Article 95(4) or 95(5) EC. The Commission therefore submits that a Member State cannot make provision for more extensive protection for personal data or a wider scope than are required under the directive.

Reply of the Court

Directive 95/46 is intended, as appears from the eighth recital in the preamble thereto, to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. The tenth recital adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.

The harmonisation of those national laws is therefore not limited to minimal harmonisation but amounts to harmonisation which is generally complete. It is upon that view that Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate.

It is true that Directive 95/46 allows the Member States a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations as a large number of its provisions demonstrate. However, such possibilities must be made use of in the manner provided for by Directive 95/46 and in accordance with its objective of maintaining a balance between the free movement of personal data and the protection of private life.

On the other hand, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof, provided that no other provision of Community law precludes it.

In the light of those considerations, the answer to the seventh question must be that measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it.

Costs

The costs incurred by the Swedish, Netherlands and United Kingdom Governments and by the Commission and the EFTA Surveillance Authority, which have submitted observations to the Court, are not recoverable. Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the national court, the decision on costs is a matter for that court.

On those grounds,

THE COURT,

in answer to the questions referred to it by the Göta hovrätt by order of 23 February 2001, hereby rules:

1. The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of 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.

2. Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46.

3. Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.

4. There is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.

5. The provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined inter alia in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order.

6. Measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it.

Jann
Timmermans
Gulmann

Cunha Rodrigues
Rosas
Edward

Puissochet
Macken
von Bahr

Delivered in open court in Luxembourg on 6 November 2003.

R. Grass

V. Skouris

Registrar

President

1: Language of the case: Swedish.