



SEMDOC compilation no 4

Secrecy proposal and access to information

Supplement to: “Key texts on justice and home affairs in the European Union, Volume 1 (1976-1993)”

**Statewatch European Monitoring and Documentation Centre on
justice and home affairs in the European Union (SEMDOC)**

**Statewatch European Monitoring and Documentation Centre on
justice and home affairs in the European Union (SEMDOC)**

SEMDOC compilation no 4

Supplement to: "Key texts on justice and home affairs in the European Union, Volume 1
(1976-1993)"

CONTENTS

1

Proposal for a Council Regulation (EEC) on the security measures applicable to classified information produced or transmitted in connection with European Economic Community or Euratom activities (92/C 72/16) COM(92) 56 final (Submitted by the Commission on 26 February 1992) plus Statewatch article on its withdrawal

2

Public access to the institutions' documents (Communication to the Council, the Parliament and the Economic and Social Committee) (93/C 156/05)

SEMDOC document compilations are a service provided for the purposes of research or private study.
For further information contact:

SEMDOC,
PO Box 1516,
London N16 0EW,
UK

tel: (00 44) (0)208 802 1882 fax: (00 44) (0)208 880 1727
e-mail: office@statewatch.org

ISBN 1 874481 14 8

Printed by Instant Print West One, 12 Heddon Street, London W1R 7LJ

1

Proposal for a Council Regulation (EEC) on the security measures applicable to classified information produced or transmitted in connection with European Economic Community or Euratom activities

Introduction

This proposal, which passed through the Commission as an "A" point, (that is, as an uncontroversial item) was published in February 1992. It was quietly withdrawn in December 1993 after objections in the Legal Affairs Committee of the European Parliament and causing much embarrassment in the second Danish referendum on the Maastricht Treaty.

However, it stands as a record of what some EU governments, as well as elements in the Council's Secretariat would like to see in place.

Proposal for a Council Regulation (EEC) on the security measures applicable to classified information produced or transmitted in connection with European Economic Community or Euratom activities

(92/C 72/16)

COM(92) 56 final

(Submitted by the Commission on 26 February 1992)

THE COUNCIL OF THE EUROPEAN COMMUNITIES,

Having regard to Article 235 of the Treaty establishing the European Economic Community,

Having regard to Article 203 of the Treaty establishing the European Atomic Energy Community,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament,

Whereas the development of the Community will generate increasing flows of information between the Member States and the institutions of the European Communities;

Whereas protection should be afforded to sensitive information whose unauthorized disclosure could be detrimental to the essential interests of the European Communities and of Member States;

Whereas some common classification rules should therefore be laid

down to ensure adequate protection of information at both the production and the transmission stages; whereas the rules should be implemented by the competent administrative and judicial authorities within the framework of existing provisions in Member States and the Community institutions;

Whereas under present Community law it is for each institution and each Member State to determine which information should be classified, with the proviso that the security gradings should be respected by all parties; whereas access to information is one of the fundamental principles of democracy; whereas it is therefore necessary to limit classification of information to the absolute minimum;

Whereas the rules should cover not only physical protection of classified information but also the persons and firms who may have access to it, without prejudice to the status of persons who are exercising an electoral mandate or a government function or who are members of an institution or body established by the Treaties;

Whereas protection of personal data and privacy are covered by separate measures;

Whereas special measures should be laid down for the protection of computerized information to allow for the particular characteristics of electronic techniques;

Whereas any failure to comply with the requirements of this Regulation or of supplementary provisions adopted by the institutions or the Member States will render the offender liable to disciplinary action; whereas provision must be made for other appropriate sanctions to be taken, where necessary, against serious offenders;

Whereas this Regulation will help to further the achievement of Community objectives in general and to protect the interests of the Community institutions and Member States;

Whereas a Commission decision based on Article 95 of the Treaty establishing the European Coal and Steel Community will be adopted to cover ECSC classified information;

Whereas the Treaties do not provide specific powers of action for the establishment of common rules in this field;

Whereas this Regulation is without prejudice to the application of the specific security measures laid down in Council Regulation (Euratom) No 3 (1) on the security gradings and the security measures to be applied to Euratom classified information;

Whereas the provisions of this Regulation do not affect the normal rules of confidentiality which apply to all public servants with regard to information not expressly intended for the public,

HAS ADOPTED THIS REGULATION:

TITLE I

PROTECTION: PRINCIPLES AND GENERAL RULES

Article 1

Scope: subject matter

1. This Regulation establishes security gradings for sensitive information connected with EEC or Euratom activities and the security measures to be applied to such information both inside Member States and institutions and when it is transmitted by one Member State or institution to another.
2. This Regulation also establishes the conditions of access to classified information by public servants and persons or firms under contract.
3. This Regulation does not apply to information covered by Regulation (Euratom) No 3.

Article 2 Supplementary provisions

1. The security measures laid down in this Regulation provide a framework of general principles and coordinated rules.
2. The institutions of the European Communities (hereinafter called "the institutions") and the Member States, may, where necessary, supplement them by rules on matters within their jurisdiction in order to take account of local conditions, provided this does not jeopardize the uniformity of treatment of the information referred to in Article 1 (1).
3. The institutions of the European Communities are the European Parliament, the Council, the Commission and the Court of Justice.
4. For the purposes of this Regulation, the Court of Auditors, the Economic and Social Committee and the European Investment Bank are deemed to be institutions.

Article 3 Classified information

1. For the purposes of this Regulation, "classified information" means all forms of information whose unauthorized disclosure could be detrimental to the essential interests of the European Communities and of the Member States and which therefore must be protected by appropriate security measures.
2. "Information" means any information, whether recorded in writing, orally or optically and whatever the medium used: paper, audio or video tape, transmission networks, technical or physical processes. For the purposes of this Regulation, the concept of classified information must be understood solely by reference to its context.
3. Where information is not contained in a written document, protection of classified information may require special rules taking account of the nature of the medium, in particular for audio and video recordings, microfilm, film or video tapes or computer media.
4. The information referred to in paragraphs 1 and 2 above shall retain its classified status even when it is preparatory or only for temporary use.

Article 4 Classification principles

1. The security grading applicable to an item of information shall be determined by reference to the content of the information in question.
2. Security gradings shall be assigned only where necessary and for the time necessary.
3. Where the information to be protected has a temporary security grading, the date shall be indicated beyond which it can be considered declassified or an equivalent embargo shall be attached.
4. Where a number of items of information are grouped together, the security grading to be applied to the whole shall be at least as high as that of the item of information bearing the highest grading. A collection of information may, however, be given a higher grading than any of its constituent parts.

Article 5 Security gradings

Security gradings for EC classified information shall be as follows:

- (a) EC-TOP SECRET: where unauthorized disclosure might be extremely detrimental to the essential interests of the Communities or of one or more Member States;
- (b) EC-SECRET: where unauthorized disclosure might be seriously detrimental to the essential interests of the Communities or of one or more Member States;
- (c) EC-CONFIDENTIAL where unauthorized disclosure might be detrimental to the essential interests of the Communities or of one or more Member States.

Article 6 Information from outside sources

1. Classified information from any of the institutions or Member States shall retain its original security grading.
2. Information from any other source, whether or not bearing a security grading, shall if necessary be assigned an EC security grading by the

recipient institution or Member State, account being taken of the legitimate interests of the author or the source of the information.

TITLE II

PROCEDURAL PROVISIONS

Article 7 Assignment of security gradings

The assignment of security gradings shall be the responsibility of the institution or Member State in which the document originates.

Each institution and each Member State shall determine the internal procedures for assignment of security gradings, taking account of the criteria laid down in Article 4 and avoiding unnecessary gradings.

Article 8 Declassification of information

1. The institution or Member State which assigned the security grading to an item of information shall be responsible for deciding that the grading is to be lifted or changed and for informing the recipients.
In the case of TOP SECRET or SECRET information such decisions shall be communicated to recipients in writing.
2. Information temporarily classified shall be declassified automatically on the expiry date or as otherwise specified.
3. Information in historical archives is subject to a declassification procedure after 30 years with a view to allowing public access.

Article 9 Scope: persons

1. The security measures laid down in this Regulation shall be observed by all officials or other public servants who, for any reason, have occasion:
 - (a) in an institution, in a committee for which an institution is responsible or in the course of work with the staff of an institution, to have access to classified information produced within the institution or communicated to it;
 - (b) in a Member State, to have access to EC classified information produced in the Member State or communicated to it.
2. Any firm or company, including subcontractors, working for an institution or Member State whose staff may have occasion to read classified information by reason of their work shall be bound by the requirements of this Regulation and shall impose the same obligations on every member of staff concerned. It shall designate a person to be responsible for monitoring the implementation of these measures.

Article 10 Access to classified documents

1. Access to and possession of EC classified information shall be restricted to the persons referred to in Article 9 who, by reason of their duties or of service requirements, need to acquaint themselves with such information or to handle it.
2. To be allowed access to EC-TOP SECRET and EC-SECRET and EC-CONFIDENTIAL information, the persons referred to in paragraph 1 must be given authorisation in accordance with Article 11.
3. Such authorization shall be granted only to persons who have been vetted in accordance with Article 12.
4. Where only occasional access to EC-CONFIDENTIAL information is required, such access may be authorized by way of exception without prior vetting, provided that all necessary precautions are taken.

Article 11 Authorization

1. Authorizations under Article 10 shall be granted by each institution and Member State to persons subject to its authority in accordance with its own arrangements.
2. Authorizations shall terminate when the authorized person leaves the service of the Communities or their contract ends.
3. Authorizations shall be subject to periodical review every five years

at least.

Article 12 Vetting

1. (a) Vetting shall be undertaken at the request of the institution or Member State to whose authority the person to be given authorization in accordance with Article 10 (2) or (3) is subject.

The vetting shall be carried out by the Member State of which the person concerned is a national.

(b) Where the person concerned is not a Community national, the Member State responsible for vetting is the one in which the person is domiciled or usually resident.

(c) Where the person concerned has been resident for a period of time in a Member State other than the one referred to in the previous paragraph, or if the person has ties in another Member State, the Member State in question shall take part in the vetting procedure. The Member State in question shall communicate the results of its enquiries to the Member State responsible for vetting.

2. The vetting procedure shall be governed by the relevant rules and requirements applied in the Member State in question.

3. Institutions and Member States shall cooperate and exchange whatever information is necessary for the proper application of this Article.

In particular, institutions and Member States shall notify each other of anything which may cast doubts on the credentials of the authorized person.

Article 13 Instructions

All persons authorized in accordance with Article 10 shall, at the time of authorization and at regular intervals thereafter, be given appropriate instructions concerning the protection of classified information and methods to be applied. They shall sign a declaration that they have received the instructions and that they undertake to comply with them.

TITLE III

STRUCTURES

Article 14 Responsibility for security

Each institution and Member State shall designate a department to supervise the application of this Regulation and of supplementary measures as provided for in Article 2 and shall inform the other institutions and Member States through the Commission.

Article 15 Coordination between institutions and Member States

1. The institutions and Member States shall set up whatever procedures are necessary for the coherent application of this Regulation.

2. The Commission shall organize the necessary coordination between institutions and between the institutions and the Member States.

3. The Commission shall be assisted in this task by an Advisory Committee on Security composed of representatives of the Member States and chaired by a Commission representative.

4. The committee shall draw up its rules of procedure. Representatives of other institutions may attend its meetings as observers.

5. The committee's remit shall be to examine, on the initiative of its chairman or at the request of an institution or Member State, any matter coming within the scope of this Regulation.

Article 16 Security officers

1. The institutions and Member States shall designate, in each department receiving or handling classified information, officials of appropriate rank (hereinafter called "security officers") to be responsible for the implementation of this Regulation.

2. It shall be the task of security officers to:

(a) keep up to date the list of persons in their departments authorized to

have access to CONFIDENTIAL, SECRET and TOP SECRET information;

(b) give instructions to staff regarding their responsibility for the protection of classified information;

(c) enforce the physical security measures;

(d) supervise the work of the special offices provided for in Article 17.

3. Only persons authorized in accordance with Article 10 to have access to classified information may be security officers.

Article 17 Special offices

1. The institutions and Member States shall use specialized departments (hereinafter called "special offices") for the exchange of EC-TOP SECRET, EC-SECRET, and EC-CONFIDENTIAL information.

2. The special office shall assume responsibility for handling classified information referred to in paragraph 1, in particular registration, reproduction, translation, transmission, storage and destruction.

3. Where necessary for the discharge of their duties, officials assigned to the special offices shall be authorized to have access to classified information in accordance with Article 10.

TITLE IV

PROTECTION OF DOCUMENTS

Article 18 Distinctive marking of classified documents

1. The security grading assigned to classified information in written form shall be shown as follows:

EC-TOP SECRET and EC-SECRET: by a clearly visible stamp on the top and bottom of each page or by some equivalent indication, such as a diagonal band extending across the full page,

EC-CONFIDENTIAL: by a clearly visible stamp on each page or by some equivalent indication, such as a diagonal band extending across the full page.

The stamp shall be in all the official languages of the Community.

2. In the case of temporary classification, the date after which the document may be considered declassified or the equivalent embargo formula shall be added in a suitable place.

3. Each copy of an EC-TOP SECRET or EC-SECRET document shall bear a serial number, by means of which the source, recipient and year can be identified. This serial number shall be repeated on the cover page of each document. The pages shall be numbered.

4. If the security grading of a classified document is changed, the document shall be marked as appropriate for the new grading.

5. References to EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL information, including computerized references, shall be kept to a minimum and under no circumstances must they reveal either the content or the security grading of the information.

Article 19 Preparation, production and reproduction of EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL documents

1. Runs of EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL documents shall be strictly limited to the number of copies required to cover estimated essential needs.

2. Classified information may be reproduced in whole or in part, in whatever form and by whatever means, only under the authority of one of the special offices referred to in Article 17.

The number of copies (e.g. further runs, duplicates or extracts) shall be limited to essential needs not foreseen when the document was originally produced.

Article 20 Registration, distribution and reception of EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL information

All EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL

documents shall be registered in one of the special offices referred to in Article 17; the special office thereby takes delivery of the document and arranges any necessary transmission. The purpose of such registration shall be to make it possible:

- to draw up immediately a list of the persons who have consulted the information or had it in their possession,

- to ascertain at once, after distribution, who is in possession of each copy and of any duplicates.

Article 21 Messengers

With the agreement of the security department concerned, messengers shall be specially designated to carry classified documents, in particular EC-TOP SECRET and EC-SECRET documents.

Article 22 Delivery

1. EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL information shall be dispatched and received by the special offices.
2. The following procedures shall apply for the delivery of classified documents:
 - (a) EC-TOP SECRET and EC-SECRET:
by authorized messenger, or by diplomatic bag or by insured mail, with advice of delivery;
 - (b) EC-CONFIDENTIAL:
by messenger, internal mail or registered post, with advice of delivery;
 - (c) whatever the means of delivery, the envelope shall bear no distinctive marking on the outside.

Article 23 Diplomatic bag

The delivery of classified documents by diplomatic bag shall be governed by appropriate rules which afford adequate protection.

Article 24 Removal of classified documents from buildings

1. Classified documents shall be kept at all times in a secure location.
2. Classified documents may only be taken away where absolutely necessary and shall remain at all times in the personal custody of the person who removes them.

Classified documents should not be left in locations where they cannot remain under surveillance at all times.

TITLE V

DESTRUCTION

Article 25 Destruction of classified documents

1. Outdated and surplus copies of classified documents shall be destroyed under the responsibility of the appropriate authorities.

The destruction of EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL documents shall be carried out using a shredder or another approved method of destruction.
2. The destruction of EC-TOP SECRET and EC-SECRET documents shall be witnessed, recorded in a report and noted in the register of the special office in question.
3. At least one copy shall be kept in the archives with adequate protection.

TITLE VI

PROTECTION OF OTHER INFORMATION MATERIAL AND MEDIA

Article 26 Other information material

Information material and media other than those referred to in Titles IV and V shall be protected in accordance with the principles laid down in these two titles.

TITLE VII

TRANSMISSION BY TELECOMMUNICATIONS

Article 27 Transmission of classified documents by telecommunications

1. EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL information shall not be sent by telegram, radio, telephone, telex, telefax or any other electronic means unless it is enciphered using a system the security department regards as safe.
2. Notwithstanding paragraph 1, EC-CONFIDENTIAL information may in cases of emergency and absolute necessity be sent by such means without being enciphered, provided that authorization is obtained from the competent authority of the institution or the Member State and the Cipher Office is informed.
3. EC-CONFIDENTIAL information which has been sent without being enciphered may never subsequently be sent in enciphered form.
4. The provisions of this Article shall apply in conjunction with the rules and directives on the security of computerized information laid down in Article 32.

TITLE VIII

PHYSICAL PROTECTION

Article 28 Buildings

1. Buildings or parts of buildings housing classified documents shall be accessible only to persons authorized to enter them. They shall be suitably protected by providing, where necessary, permanent surveillance or installing an alarm system.
2. Visitors shall not be left unaccompanied in places where classified documents are kept.

Article 29 Security furniture

EC-TOP SECRET, EC-SECRET and EC-CONFIDENTIAL documents shall be kept in cupboards or other storage units approved by the security office as being sufficiently sturdy and having a safe locking mechanism.

Article 30 Protection of combination-lock settings and security keys

1. The setting of combination locks shall be changed at the time of delivery, every time staff having knowledge of the setting is changed, whenever the setting has or appears to have been compromised and, at all events, every 12 months at least.
2. The term "security keys" shall mean all keys to furniture used to house classified documents.
3. Holders of security keys and the departments responsible shall take whatever measures are necessary to safeguard security keys, in particular, to prevent unauthorized persons from having access to them.
4. The loss of a security key or the compromising of a combination-lock setting shall be brought to the immediate attention of the security officer, who shall arrange at once for the lock to be replaced or the setting to be changed.

Article 31 Special provisions for the protection of classified information

If special circumstances prevent the application of any of the provisions of this Regulation or dictate stricter measures, the responsible security officer, after consulting the security department, shall take or cause to be taken appropriate measures to provide a degree of protection equivalent to that provided for in this Regulation.

TITLE IX

PROTECTION OF COMPUTERIZED INFORMATION

Article 32

Security of computerized information

1. Classified information in computerized or electronic form shall be governed by the protective measures laid down in this Regulation. The processing of such information (for example, its storage or transmission) using equipment such as computers, networks and terminals shall be subject to security measures specially devised for these techniques.

2. Each Member State and institution shall adopt special rules for the security of computerized information. These rules shall comprise general measures supplemented by specific measures based on an analysis of the risks.

3. These measures shall in particular:

(a) define responsibilities for:

- authorizing access,
- applying the authorization procedure (ie: permitting access),
- checking effective access against authorizations granted;

(b) ensure reliable identification and authentication of users;

(c) set the technical security criteria for operating systems, networks and software on the basis of recognized standards;

(d) determine rules for the management of computer configurations and in particular rules for the certification of the criteria provided for in (c).

4. The measures shall also include common rules and technical options as regards:

(a) the enciphering and authentication of data and the management of keys;

(b) the precautions to be taken for the elimination of electromagnetic radiation by reference to the Tempest standard (or a European equivalent to be defined).

TITLE X

FINAL PROVISIONS

Article 33

Procedure in the event of infringement of this Regulation

1. Any person employed by an institution who in the course of his duties has access to classified information shall be informed by the security department or the security officers that failure to comply with the requirements of this Regulation renders him liable to disciplinary action.

2. Any person who finds, or has reason to believe, that classified information has gone astray or been compromised or that an infringement of this Regulation or of security measures has been committed shall immediately inform the security officer, who will at once inform his superior.

3. If there is a suggestion that EC-TOP SECRET, EC-SECRET or EC-CONFIDENTIAL information has come to the knowledge of an unauthorized person, the security department shall be informed immediately so that it can assess the situation.

4. If the suspected breach within the meaning of paragraph 3 is confirmed, the security department shall take appropriate steps with the responsible officials concerned in order to limit the damage caused to a minimum and to prevent any recurrence.

5. If a serious infringement committed in an institution or a Member State concerns information originating in another institution or Member State, that institution or Member State shall be advised.

Article 34

Penalties

Member States and institutions shall take appropriate action to penalize failure to comply with the requirements of this Regulation.

Article 35

Treaties or agreements with Member States and regulations

1. These provisions shall be without prejudice to the obligations of the Community and/or the Member States in this field arising out of treaties or agreements concluded with third countries, international organisations or a national of a third country.

2. This Regulation shall be without prejudice to Regulation (Euratom) No 3 implementing Article 24 of the Treaty establishing the European Atomic Energy Community.

Article 36

Entry into force

This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Communities.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

EC to drop secrecy law

Statewatch bulletin, vol 3 no 1, January-February 1993

The European Commission is to drop its proposal to introduce a UK-style secrecy law in the EC (reported in May by Statewatch, see vol 2 nos 3 & 4). This emerged after the Edinburgh EC Summit in December when 21 proposals were listed as being amended, withdrawn or being considered for withdrawal under the "subsidiarity" clause. The secrecy law was listed as one the Commission would consider withdrawing, Statewatch understands that it is now to be dropped.

The proposal called for the classification of documents whose disclosure would be "detrimental to the essential interests of the Community and member state", security gradings and sanctions against disclosure. The Commission put forward the proposal in February 1992. In May the International Federation of Journalists in Brussels, the European Federation of Trade Unions and Article 19 expressed their opposition to the proposal. In the European Parliament (EP) the rapporteur in its Legal Affairs Committee on the proposal, Alex Falconer MEP, opposed the measure.

The Committee sent a letter to the Commission asking why it had been sent to the parliament under the "consultation" rather than the "co-operation" procedure (the latter allow the parliament two chances to comment, the former just one). Officials from the Commission defended the proposal at the meeting of the EP's Civil Liberties and Internal Affairs Committee in September. However, the Civil Liberties Committee rapporteur on the issue, Mr Jarzembowski MEP, called for substantial amendments or the withdrawal of the proposal.

Although it would have been consulted over the original proposal the UK government later came out against it because it was not sure whether this was "the best means of implementing such procedures". This suggested that they would favour an inter-governmental agreement between the 12 EC states rather than a formal directive from the Commission on which the EP has to be involved.

The proposal has been withdrawn under the heading of "subsidiarity" (meaning matters best left to member states rather than the Commission) which suggests it may surface again, though not during the Danish Presidency because they opposed the measure.

2

Public Access to the institutions' documents (Communication to the Council, the Parliament and the Economic and Social Committee) (93/C 156/05)

Introduction

This report from the Commission preceded the introduction of: 1) the Code of conduct concerning public access to Council and Commission documents (6.12.93) (known as the "Code") and 2) Council decision on public access to Council documents (20.12.93) (known as the "Decision"). Both of which are still in force - the latter has had minor amendments including the introduction of charges for supplying documents.

Public access to the institutions' documents (Communication to the Council, the Parliament and the Economic and Social Committee) (93/C 156/05)

INTRODUCTION

During the adoption of the Treaty on European Union at Maastricht on 15 December 1991, a declaration was made on improved public access to information. The text of the declaration is the following:

"the Conference considers that transparency of the decision-making process strengthens the democratic nature of the institutions and the public's confidence in the administration. The Conference accordingly recommends that the Commission submit to the Council no later than 1993 a report on measures designed to improve public access to the information available to the institutions."

The European Council at Birmingham subsequently declared that the Community must demonstrate to its citizens the benefits of the Community and the Maastricht Treaty and that the Council, Commission and Parliament must do more to make this clear. Moreover, in Birmingham the Commission was asked to complete by early 1993 its work on improving public access to the information available to the Community institutions.

The Edinburgh European Council continued the work for a more open and transparent Community. Specific measures were adopted to start the process of opening up the work of the Council. Before Edinburgh the Commission had already taken a package of measures to increase transparency.

This package included producing the annual work programme in October, to allow for wider debate including in national parliaments; wider consultation before making proposals, including the use of Green Papers; making Commission documents more rapidly available to the public in all Community languages; and attaching higher priority to the consolidation and codification of legal texts. The Commission has taken these initiatives whilst being aware that it has already a commendable history of an open door policy, especially in comparison with existing practices in national administrations. Traditionally it has been open to input from the public. This stems from the belief that such a process is fundamental for the development of sound and workable policies.

The Edinburgh European Council welcomed these measures taken by the Commission. At the same occasion the European Council reconfirmed its invitation made at Birmingham for the Commission to complete by early next year its work resulting from the declaration in the Maastricht Treaty on improving access to information.

RESPONSE

The Commission views this declaration as an important element of the Community's policy on transparency of the institutions. Improved access to information will be a means of bringing the public closer to the Community institutions and of stimulating a more informed and involved debate on Community policy matters. It will also be a means of increasing the public's confidence in the Community.

In order to implement the Maastricht declaration the Commission has undertaken a comparative survey on existing access to information policies in the Member States and in some third countries. The results of this survey are summarised in the Annex as requested in Maastricht.

The fact finding survey has shown the different experiences of improved access to information. Access to information consists of two main elements.

Firstly it encompasses a series of measures taken by the public authorities themselves aimed at informing the general public of their actions. In this respect the Commission has noted that from the time the Community was established both Community institutions and Member States have taken numerous initiatives in this field to inform the public and to make them more aware of Community policies.

Secondly, access to information also consists of making information available upon request from a member of the public. Some countries have developed a relatively long tradition in this respect, which has evolved over the years. This policy is based on the principle that access is granted while at the same time protection is given to public and private interests, and the proper functioning of the public authority concerned is preserved.

The public is granted access to specific types of information in some countries, while in other cases these were combined with general access rules. Directive 90/313/EEC on access to environmental information is an example of a Community initiative on access to a specific area of information.

FURTHER STEPS

Taking account of the comparative survey on the situation in different Member States and third countries there is a strong case for developing further the access to documents at Community level.

The Commission therefore is prepared to take further steps in order to establish a framework for granting general access to documents. This will entail some adjustments of the Commission's working practices but the Commission considers that general access is a particularly important instrument to bring the Community closer to its citizens.

The Commission feels that the principle of access to information held should be shared by the other institutions and Member States. It invites the other institutions to cooperate in the development of such an approach which should contain at least the fundamental principles and a minimum set of requirements. As a first step, this could take the form of an interinstitutional agreement. Special attention should be given to the specific role of each institution within the existing interinstitutional framework.

In order to contribute to this common approach, the Commission, for its part, suggests that work be based on the following principles which it intends to elaborate upon further:

- access to information is granted to documents, the precise definition of which will be established,
- access to such documents will be provided subsequent to a sufficiently

- precise request from the public,
- there shall be no obligation on the person making the request to justify the reasons for wanting the document,
 - a reply to a request for information should be given as soon as possible.

A request for a document may be refused in order to safeguard:

- personal privacy,
- industrial and financial confidentiality,
- public security including international relations and monetary stability,
- information passed to the institutions in confidence.

Should a request meet with a refusal, then the institution must reply in writing giving the reasons for the decision.

The Commission will use the time remaining before the European Council to be held at Copenhagen by the end of June to prepare a further outline of the general access to documents policy. It intends to submit this to the other institutions in the context of a second communication on transparency which will focus on a general framework and specific actions to improve the Community's transparency.

ANNEX

PUBLIC ACCESS TO INFORMATION

(Comparative survey)

1. HISTORICAL OVERVIEW

Public administrations in many countries have in the past often tended to carry out their work within a framework of secrecy laws designed to protect major public interests (e.g. defence, foreign affairs, etc.). Security regulations were thus established to ensure that information not destined for public release remained protected.

Furthermore, legislation protecting the citizens themselves with regard to such issues as health and fiscal matters traditionally has been quite important.

A dual track rationale for restricting information on public administration can therefore be seen: to protect both public and private interests.

The traditional way in which a government administration informs the public of its decisions is through some form of official publication (journal, gazette, etc.). The public is also kept informed through the accountability of ministers to parliament, through the oversight of such external bodies as the court of auditors and law courts, through public access to plenary meetings of parliament and its various select committees and, finally, through a statutory right of petition.

Turning point

During the course of the 1960s there was a growing belief that such a relationship between government and those it governs should be supplemented with a more open approach. This belief arose from a desire for a stronger form of democracy, i.e., a more democratic form of government. It was felt that the public's business, in particular the way its affairs are administered, should be conducted more publicly. Another driving force was the fact that whilst administrations were being entrusted with more and more tasks parliamentary control appeared to be less effective.

It was also assumed that a more open approach stimulates an informed debate on public policy issues and also opens up the possibility of improving control over the workings of the administration.

Policies adopted

A number of Member States and third countries therefore gradually adopted a series of measures designed to open up and improve public administration.

These national measures included mechanisms to increase the public participation in the administrative decision-making process. The

measures vary from an obligation to pre-consult the public (through, for example, the issuing of Green and White Papers), the right to call for a public hearing and the granting of a right to the public to propose legislation which the relevant public authority would then be obliged to adopt or to consider.

The measures also included the reinforcement of provisions dealing with improved explanation and justification of decisions to the public; the improved publication of final decisions and increased opportunities for appeal against administrative decisions. In certain cases, new ways of appeal were created, such as the establishment of an ombudsman.

Finally, a number of countries also adopted the principle whereby information held by public authorities is generally open to the public unless such access has been explicitly exempted for a limited number of specified reasons.

2. ACCESS TO INFORMATION - A COMPARATIVE SURVEY

2.1. General

Three trends can be identified which relate to the strengthening of access to information held by public authorities:

- access to consult administrative files was given to those members of the public who are a party in a lawsuit. The consultation of such files stems from the general right of defence. In several instances this form of access is granted regardless of whether or not the member of the public is involved in a judicial (appeal) procedure. This development led to the establishment of a number of specific access rules for each subject of information,

- access for the individual concerned to consult files containing personal data. These could be files held by the public sector concerning such things as appointments and nominations. It could also comprise access to files held by the private sector (insurance companies, for example). This has resulted in a number of specific access rules for each subject of information,

- general access to information held by public authorities (regardless of whether or not the individual/company concerned has a specific interest or is involved in a lawsuit). This has led to a number of general access to information laws.

The fact-finding carried out indicates that, following the developments described above, however, the situation in individual countries varies. Only access to a specific kind of information was granted to the public in some countries while general access rules came into force in other countries. In a third group of countries both types of rules were established.

Active and passive information supply

The survey has shown that there are essentially two ways in which more access to information can be achieved. Firstly, there is the general (legal) obligation upon government departments actively to make all appropriate information (e.g. circulars, policy statements, departmental organigrams, etc.) available to the public at their own initiative.

Secondly, there is the more passive (legal) requirement for government departments to make information available upon request by a member of the public. This includes access to information which forms the basis of governmental decisions such as reports, studies, minutes, notes, circulars, instructions, opinions, forecasts, invoices, registers, indexes and other sorts of information which are held in written, computerized or audiovisual form.

Focus

The comparative survey focused on rules dealing with access to information available upon request (passive information supply), as laid down in general access to information legislation. It does not deal with specific access laws to a particular kind of information nor with active information supply by public authorities. The first of these issues has been extensively examined in the framework of another study, at the

request of the Commission (Publaw 1, 1991). In the light of this study, the Commission has made certain proposals in this area (see below).

2.2. Member States and third countries

Inside the Community, Denmark, France, Greece and the Netherlands have statutes establishing general public rights of access to government information. In Belgium, draft proposals on establishing the right of access to information are currently under discussion at federal and regional level. As is also the case in many other countries, Portugal, Spain and the Netherlands have constitutional provisions regarding a general right of access to information without, however, Portugal and Spain having yet implemented specific legislation.

Outside the Community, statutes granting access to information in the United States, Canada, Norway and Sweden have been studied. In the case of the latter country, a right of access to information has been established for over two hundred years.

All of these statutes (see Annex II) have one thing in common: they provide the public with a right of access to information upon request (albeit with certain exemptions from compulsory disclosure in order to protect public and private interests).

3. Main features

Aim of the legislation

The introduction of specific legislation dealing with the public's right of access to information is considered to be a vital element in the proper functioning of a free society as it further extends democracy within the administrative process. The right of access to information is consequently viewed as a fundamental civil right. It deals with the relations between an administration and the citizens it serves (third generation of human rights). In this regard the Council of Europe adopted a recommendation on a right of access to information held by public authorities. It invited the Member States to introduce a systematic right of access to such information.

A number of other benefits are cited in support of the introduction of access to information legislation. These include providing a system of checks and balances with which to oversee and control the workings of public bodies: improving management and ensuring a better allocation of resources, encouraging citizens to participate willingly in the workings of government and stimulating an informed debate on, as well as interest in, public policy.

The subject of the information requested

The statutes examined in the survey grant, in principle, public access to any kind of information held by a public authority which is contained in existing documents. The term 'document' is defined broadly to include not only traditional formats such as written papers and photographs but also more modern information carriers (e.g. microfilms, computer discs, magnetic, video and audio tapes). It is also taken as a basic principle that a request for information will only be granted provided it does not necessitate the creation of information that does not exist (e.g. compiling and summarizing data from a number of separate sources).

In the case of automatic data processing, however, this principle is sometimes difficult to maintain. To take the case of Sweden as an example, the rule has been established that a certain selection or merging of data should be regarded as an existing document if the selection or merging can be produced by routine measures.

Which authorities are obliged to grant access?

The public authorities bound by the access to information legislation differ from one country to another depending on the form of government. Broadly speaking, in federal systems, federal authorities (including the independent regulatory agencies) are the object of access legislation. Moreover, often State (as opposed to federal) legislation exists which provides access to information held by State authorities. In Belgium, for example, initiatives are taken at both federal and regional

levels to provide access to information.

In other governmental systems it is often the case that all public authorities (including the agencies) are governed by legislation concerning access to information.

Some statutes also include specific provisions with regard to the right of access to information and opinions originating from independent advisory bodies i.e. bodies to advise one or more public authorities on a particular subject.

Who may make a request for information?

Most of the general access laws studied contain provisions whereby any person, regardless of his or her nationality, has the right to exercise access to information. In virtually all cases the individual making the request for information is under no obligation to give a reason for his or her request.

How is information made available to the public?

There are essentially four ways in which an individual can obtain the information: either by requesting a full copy, a summary, an extract or an opportunity to examine the document in person. In deciding which of these alternatives it should choose, the public authority concerned must bear in mind the preferences expressed by the individual making the request.

Exemptions from the right of access to information

The study has shown that grounds for exemption from access to information legislation vary considerably from country to country. In certain cases exemption is compulsory, it is sometimes optional and in other instances it can be either one or the other.

Regulations in all the countries examined contain exemptions. These can be divided into two main categories:

- exemptions with regard to the protection of general public interest. Information shall not be disclosed if it damages international relations, the security of the State, national security and defence matters, economic and financial interests, the investigation of criminal offences and the prosecution of offenders, inspection activities,

- exemptions with regard to the protection of personal privacy. In this respect, data specifically related to a person is not disclosed to third persons if this would cause disproportionate harm to the privacy of the person concerned.

In some countries internal documents containing personal opinions on policy are also exempt from the legislation.

Time limits within which the public can expect to receive a reply

These range from 10 days to two months. In some cases the authorities simply commit themselves "to reply as soon as possible". Most acts provide an opportunity for the time limit to be extended in exceptional circumstances and for a varying number of working days.

Charges for making information available to the public

In the great majority of cases, copies of requested documents are provided at cost price. However, personnel costs are not included in the calculation of this figure.

Appeal procedures in the event of a request for information being refused

In all the cases studied there exists the possibility of an appeal to an independent body, such as an administrative court, a council of State, an ombudsman or an information commissioner.

Quantitative analysis

It has proved difficult to find material with which to quantify the use to

which these regulations have been put. There do not appear to be any central registers for the filing of requests received. However, in some of the literature consulted, it is indicated that access to government information is used more by individuals or companies who have economic rather than purely civil interests.

Should a request for information be refused or not answered within a given time period under the French system, the individual making the request can turn to the Commission d'accès aux documents administratifs (CADA) for an 'avis'. There has been a steady increase in the number of "avis" issued: from 470 in 1979/80 to 2,098 in 1989. The 10,000th "avis" was given out in 1989.

In Canada, 48,493 people exercised their right to request government records during the period 1983 to 1991. In that same period, 31% of all requested information was disclosed, 37% was disclosed in part and 8% was dealt with in an informal way. In total, 4% was not disclosed while 20% of the requests could not be processed. The most frequently used exemptions were third party information and personal information. The total cost of operations was 39.5 million dollars, being 817 dollars per request. The total fees collected were 586,961 being slightly more than 12 dollars per request. During the period 1990 to 1991 54% of all requests made under the Access to Information Act came from the business sector and 28% from individuals. In Australia, some 25,000 freedom of information requests were made in 1990/91.

2.4. Community institutions

Present situation

The EEC Treaty contains a number of rules relating to administrative transparency which are related to this subject. These include rules governing the non-disclosure of information of a kind covered by the duty of professional secrecy (Article 214 EEC); the non-disclosure by Member States of information which is considered to be contrary to its essential security interests (Article 223 EEC); the obligation to publish legal acts of the Community (Article 191 EEC); the obligation to state the reasons upon which such legal acts are based (Article 190 EEC); the establishment of rules under which the Commission is obliged to give interested parties the opportunity to express their views on, for example, cases falling under Community regulations on competition rules applying to undertakings (Articles 85/90 EEC) and the obligatory annual publication of a General Report on the activities of the European Communities (Article 18 of the Merger Treaty).

Many of the relevant provisions of the EEC Treaty have been implemented through detailed legislation in, for example, the Staff Regulations for officials of the European Communities; Council Regulation No 3 (Euratom) implementing Article 24 of the EEC Treaty establishing the European Atomic Energy Community (1); Council Regulation of 1 February 1983 concerning the opening to the public of the historical archives of the Community and Euratom which foresees access to the archives after a period of 30 years (2); Commission's decision of 7 July 1986 on classified (3) documents and the security measures applicable to such documents which, for example, implies that sensitive commercial information made available in the context of competition policy will obtain the appropriate security classification, and also contains rules on classification and declassification of documents and handling of information received from Member States; and the Council Regulation of 11 June 1990 on data subject to statistical confidentiality addressed to the Statistical Office of the European Communities (4). This applies to the transmission to the Statistical Office of data which falls within the national statistical institutes' field of competence and is covered by statistical confidentiality. Moreover, a number of internal regulations have been established dealing with the internal functioning of each institution.

Over the years, relevant case-law has been established on this issue by the Court of justice (see, for example, the February 1988 case of Zwartveld versus the Commission, as reported on 13 July 1990).

At Community level, no general legislation exists with specific regard to access of information although the Commission has established certain explicit rules which do allow for it in the field of competition policy (see 12th yearly report on competition, 1982, pp. 42 to 43). A

company involved on a proceeding is allowed to have access to the file on a particular case. However, any such access is limited by the Commission's obligation to refrain from discussing business secrets to third companies and the need to preserve the confidential nature of the Commission's internal and/or working documents.

Furthermore the content of Article 47 of the Treaty establishing the European Coal and Steel Community should be noted as it indicates that the Commission must not disclose information of the kind covered by the obligation of professional secrecy.

In 1990 the Council of Ministers adopted Directive 90/313/EEC to allow the possibility of access for any legal or natural person throughout the Community to information held by public authorities relating to the environment (5). In certain specified cases this information may be refused. This Directive came into force on 1 January 1993.

The rules apply to environmental information held by the competent authorities of the Member States. It does not apply to environmental information held by the European institutions. However, the Commission indicated, in the explanatory memorandum accompanying the proposed Directive, that it would take initiatives with the object of applying the principle of access to information (with regard to the environment) to the Community bodies (6).

The Commission has recently proposed specific rules for personal data protection and the free circulation of data (1). This proposal is aimed at facilitating the free movement of data in the Community while ensuring a high level of protection for the individual with regard to the processing of personal data. It includes provisions for an individual's right of access to his or her own personal data. It also lists exhaustively the exceptions with regard to personal data contained in public sector files in order to safeguard such interests as national security, defence, criminal proceedings, etc. The draft Directive was accompanied by a Commission declaration on the application of the data protection principles to personal data held by the Commission and other Community institutions. Work is under way to implement these principles.

OVERVIEW OF GENERAL ACCESS LAWS

Introduction

By "general access laws" this survey refers to such rules as provide a general access to administrative documents. This means access which is neither restricted to a particular area nor demanding a special involvement of the person seeking the information. There are other types of rules on access which are restricted to certain persons or may demand that a person state a legal or at least a legitimate interest. These rules deal for example with company registers, population registers, and credit risk information. Such access rules exist in most of the Member States.

The situation on general access both in the Community and in certain other countries is as follows:

Belgium

Several draft proposals granting general access to information are under discussion at different levels of government.

Denmark

Act No 572 of 19 December 1985 "on access to public administration files".

France

Loi No 78-753 du 17 juillet 1978: Titre premier: "de la liberté d'accès aux documents administratifs" and Loi No 79-587 du 11 juillet 1979 "relative a la motivation des actes administratifs et a l'amélioration des relations entre l'administration et le public".

Germany

There is no general access to information law in Germany. The regulation closest to such a law is the Administrative Procedure Act. However, access to information exists in specific areas, mainly to public registers.

Greece

Law No 1599/1986, "on the relationship between State and citizen, the establishment of a new type of identification card and other provisions", Article 16.

Ireland

There exists no general access legislation, however, in specific areas access to information exists.

Italy

There is no general access to information law in Italy. The regulation closest to such a law is the Access to Administrative Documents Law of 7 August 1990 (No 241). Access is possible for those who have a legal interest.

Luxembourg

There is no general access to information law. Access to administrative documents is regulated in the context of non-contentious administrative procedure.

The Netherlands

Act of 31 October 1991, Stbl. 703 "on public access to government information".

Portugal

Constitutional provision regarding a general right of access to information. Moreover, in specific areas access to information exists.

Spain

Constitutional provision regarding a general right of access to information. Moreover, in specific areas access to information exists.

United Kingdom

No legislation exists on a general right of access to information.

Canada

"Access to Information Act" of 1983.

Norway

Act No 69 of 19 June 1970 concerning public access to documents in the public administration as subsequently amended by Act No 47 of 11 June 1982 and Act No 86 of 17 December 1982.

Sweden

1976 Freedom of the Press Act, Chapter 2, "on the public nature of official documents".

United States of America

Freedom of Information Act of 1982 (5 USC Section 552), as part of the Public Information, Agency Rules, Opinions, Orders, Records and Proceedings (5 USC Section 551 to 559).

FOOTNOTES

- (1) OJ No 17, 6. 10. 1958, p. 406/58.
- (2) OJ No L 43, 15. 2. 1983, p. 1.
- (3) SEC(86) 1132 final.
- (4) OJ No L 151, 15. 6. 1990, p. 1.
- (5) OJ No L 158, 23. 6. 1990, p. 56.
- (6) COM(88) 484 final.