Steering Committee on Media and Information Society

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

21/11/2014

CDMSI(2014)015

7th meeting of Steering Committee on Media and Information Society (CDMSI)

18-21 November 2014
(Strasbourg, Agora Building, Room G03)

Abridged meeting report

The Steering Committee on Media and Information Society (CDMSI) held its 7th meeting from 18 to 21 November 2014, in Strasbourg chaired by Ms Maja Rakovic (Serbia). The CDMSI adopted the agenda as it is set out in Appendix I. The list of participants appears in Appendix II. Gender distribution: 71 attendants, 27 women (38%), 44 men (62%).

Items submitted to the Committee of Ministers for decision

The CDMSI discussed and finalised the following documents:

1. the draft Recommendation CM/Rec__ of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (Appendix III). The CDMSI agreed that in the absence of objections submitted by delegations by 15 December 2014, the draft recommendation will be submitted to the Committee of Ministers for possible adoption.

2. the draft Recommendation CM/Rec__ of the Committee of Ministers to member states on free transboundary flow of information on the Internet (Appendix IV) on the basis of a proposal by the Committee of Experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT). The CDMSI agreed that in the absence of objections submitted by delegations by 15 December 2014, the draft recommendation will be submitted to the Committee of Ministers for possible adoption.[1]

3. the draft Recommendation CM/Rec(2014)__ of the Committee of Ministers to member states on the processing of personal data in the context of employment (Appendix V) proposed

[1] As regards items 1 and 2 and the term "sexual orientation" used in the general principles of both recommendations, in the meeting the Russian Federation stated that the general clause on anti-discrimination already covers this possible ground of discrimination and given the absence of any explicit definition or provision relating to such a group or such persons as separate rights holders under international human rights law; "under international human rights law, this term should not appear in the recommendation."

by the Consultative Committee (TP-D) of Convention ETS No 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data. The CDMSI agreed to submit it to the Committee of Ministers for possible adoption.

Items submitted to the Committee of Ministers for information

4. The CDMSI elected Ms Maja Rakovic (Serbia) as Chairperson for a second term of office expiring on 31 December 2015 and Ms Elfa Ýr Gylfadóttir (Iceland) as Vice Chairperson for a first term of office expiring on 31 December 2015.

5. The CDMSI had an exchange of views on how to promote European values globally, notably in the context of the UN WSIS +10 Review, IGF and ICANN on the basis of the Council of Europe Internet Governance Strategy. In this context, under the existing terms of reference, the CDMSI decided to prepare (a) draft declaration(s) on these issues for possible adoption by the Committee of Ministers.

6. In order to ensure delivery on its Terms of Reference, the CDMSI agreed, on the basis of Resolution CM/Res(2011)24,

i.to create drafting committees on media pluralism and transparency of media ownership; gender equality dimension in the media coverage of election campaigns; professional and ethical journalism and hate speech; public service media; surveillance issues;

ii. the Bureau will make a proposal regarding the scope of work, objectives and timetable of these drafting committees on the basis of information provided by the Secretariat until 15 January 2015.

***

In addition, the CDMSI dealt with the items below:

7. Committee of Experts on protection of journalism and safety of journalists and other media actors (MSI-JO):

i. took note of the information provided by the Secretariat on the progress of work in this committee;

ii. discussed, exchanged views and gave specific guidance regarding a preliminary draft recommendation on protection of journalism and safety of journalists and other media actors and invited comments by CDMSI delegations to be submitted to the Secretariat by 22 December 2014;

iii. asked MSI-JO to prepare a revised draft for the next CDMSI meeting.

8. Committee of Experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT);

i. took note of the information provided by the Chair of the MSI-INT and the Secretariat on the progress of work in this committee;

ii. discussed, exchanged views, gave guidance on the elements for a draft recommendation on Internet freedom and the elements for a report on freedom of assembly, expression and access to content on the Internet, and invited comments by delegations to be submitted to the Secretariat by 22 December 2014;

iii. designated Mr Vlasios Doumpiotis (Greece) as new member in the MSI-INT following the departure of Mr Johan Hallenborg (Sweden) due to his change of functions;

iv. asked MSI-INT to prepare a revised draft on Internet freedom for the next CDMSI meeting.

9. In respect of the implementation of existing standards, the CDMSI:

i. discussed the content of a questionnaire on the implementation of Committee of Ministers' guidelines on eradicating impunity for serious human rights violations in the context of safety of journalists and agreed that the Secretariat should prepare a concrete list of questions by 15 January 2015 on the basis of discussions in the Committee and the list of CM standards related to safety of journalists;

ii. agreed to appoint Ms Malgorzata Pek (Poland) and Ms Christina Lamprou (Greece) as rapporteurs for the preparation of the implementation item on safety of journalists for the next CDMSI meeting. In particular, the rapporteurs will review the questionnaire by 22 January 2015, which will be sent to the Bureau and thereafter to the CDMSI.

10. Internet governance strategy - the CDMSI:

i. took note of the information provided by the Secretariat on and discussed the state of implementation of the Strategy 2012-2015 and agreed that comments by delegations should be sent by 22 December 2014 to the Secretariat;

ii. took note of information provided by the Secretariat and discussed elements for a new strategy 2016-2019 and agreed that comments by delegations should be sent by 22 December 2014 to the Secretariat. A first draft of the strategy 2016-2019 should be discussed at the next meeting of the Bureau of CDMSI.

11. In respect of the Expert Report commissioned by the Council of Europe 'ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values' the CDMSI:

i. received a presentation by the Secretariat and took note that the Governmental Advisory Committee of ICANN has discussed the expert report and has formed the basis for cross-community discussions;

ii. agreed that a drafting committee should be created to prepare a possible Council of Europe declaration based on the report with a view to advancing the further discussions in ICANN on the implementation of the report's recommendations.

12. European Dialogue on Internet Governance (EuroDIG) – the CDMSI:

i. took note of information provided by Bulgaria about EuroDIG 2015 which will take place from 4 to 5 June 2015 in Sofia;

ii. invited members of the Committee to participate and make proposals for workshops. The Bulgarian delegation will co-ordinate contributions.

13. Data protection - the CDMSI took note of information provided by Mr Jean-Philippe Walter, Chair of the TP-D on the:

i. revision of the Recommendation on the processing of personal data in the context of employment;

ii. modernisation of the Convention 108 and the holding of the third and last meeting of the Ad hoc Committee on Data Protection (CAHDATA) scheduled for 1-3 December 2014;

iii. other topics dealt with by T-PD, notably data processing in a police context, medical data and big data.

14. Regarding information about work of other Council of Europe bodies, the CDMSI took note of the Recommendation 364(2014) "The role of regional media as a tool for building participatory democracy" adopted by the Congress of Local and Regional Authorities, discussed and agreed that the Secretariat will draft a reply on the basis of written comments to be provided by delegations by 1 December 2014. The draft reply will be considered by the Bureau and the CDMSI via e-mail.

15. In respect of observer status requests, the CDMSI:

i. agreed to admit the Internet Watch Foundation as an observer;

ii. noting the criteria it has applied in the past, in particular with regard to representativeness at the European level, did not grant at this stage observer status to International Press Club Prague;

iii. took note of the applications for observer status by the Internet Rights and Principles Coalition and the European Media Platform and agreed to invite these two applicants to present their applications at the next meeting of the CDMSI.

16. The CDMSI took note of information provided by the Secretariat and CDMSI members on the following activities, meetings and events:

i. the setting up of a Freedom of Expression Platform to promote the protection of journalism and safety of journalists;

ii. a comparative study on the laws and practices in respect of filtering, blocking and taking down of illegal content on the Internet in all 47 member states, which will be carried out at the initiative of the Secretary General of the Council of Europe;

iii. accomplished and ongoing projects in the fields of media and Internet governance, in particular the implementation of the Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users;

iv. NETMundial: Global multi-stakeholder meeting on the future of Internet governance (Sao Paolo, 23-24 April 2014); World Summit on the Information Society (WSIS) +10 Review Process; Global Commission on Internet Governance;

v. implementation of the recommendation on gender equality and media.

17. The CDMSI took note of the information given by Mr Jan Kleijssen, Director of Information Society and Action against Crime, Directorate General Human Rights and Rule of Law, on developments within the Council of Europe related to the CDMSI's work as well as on administrative arrangements concerning the Secretariat.

18. The CDMSI expressed its deep appreciation for all the contributions which Jan Malinowski made to advancing the work of the committee and in raising awareness on human rights issues in the information society and the relevance of the Council of Europe's expertise in this field on a regional and global level. The committee wished him well in his future work. The committee welcomed Patrick Penninckx as Mr Malinowski's successor.

APPENDIX I

Agenda

1. Opening of the meeting

2. Adoption of the agenda

3. Information by the Chair and the Secretariat

3.1 Council of Europe action to strengthen the protection of freedom of expression

3.2. Human rights of Internet users

4. Follow-up on the implementation of Council of Europe adopted standards in member states regarding the information society

5. Media

Standard setting activities

5.1 Committee of experts on protection of journalism and safety of journalists (MSI-JO)

5.2 Hate speech

5.3 Gender equality and the media

5.4 Transparency of media ownership

6. Information Society and Internet Governance

Standard setting activities

6.1. Network Neutrality

6.2 Committee of Experts on cross-border flow of Internet traffic and Internet freedom (MSI-INT)

6.3 Council of Europe Internet Governance Strategy 2012-2015 and new Internet Governance Strategy 2016-2019

Cooperation and outreach activities

6.4 European Dialogue on Internet Governance (EuroDIG – 12-13 June 2014, Berlin) and Internet Governance Forum (IGF, Istanbul, 2-5 September 2014)

6.5 ICANN

6.6 Other activities

7. Cooperation activities

8. Data protection

Standard setting activities

9. Information about work of other organisations and other CoE bodies

9.1 Participation of CDMSI in events and meetings

9.2 Parliamentary Assembly of the Council of Europe (PACE)

10. Budget and administrative matters

11. Priorities of CDMSI work and working methods

12. Other questions

12.1. Application for observer status by Internet Watch Foundation

12.2 Application for observer status by Press Club Prague

13. Elections of Chair and Vice-Chair

14. Any other business

15. Adoption of the abridged report

General reference documents

Recent meeting reports

APPENDIX II

LIST OF PARTICIPANTS / LISTE DES PARTICIPANTS

Total number of participants : 71
Gender distribution – 44 men (62%) / 27 women (38%)
Parité entre hommes / femmes - 44 hommes (62%) / 27 femmes (38%)

ALBANIA/ALBANIE
Mr Glevin Dervishi
Albanian Ministry of Foreign Affairs

AUSTRIA/AUTRICHE
Mr Matthias Traimer
Federal Chancellery, Head of Department, Media Affairs and Information Society, Federal Chancellery, Constitutional Service

AZERBAIJAN
Ms Jeyran Amiraslanova
Chief Advisor for Public and Political Issues, Office of the President of the Republic of Azerbaijan

BELGIUM/BELGIQUE
Apologised / Excusé

BOSNIA AND HERZEGOVINA/BOSNIE-HERZEGOVINE
Mr Emir Povlakic
Head of Division for Licensing, Digitalization and Coordination in Broadcasting, Communications Regulatory

BULGARIA/BULGARIE
Ms Bissera Zankova, Media Expert / Consultant
Ministry of Transport, IT and Communications

CROATIA/CROATIE
Mr Milan F. Zivkovic
Head Advisor for Communication Policy, Ministry of Culture

Ms Vesna Roller
The Council for Electronic Media

CYPRUS/CHYPRE
Ms Eleonora Gavrielides
Ministry of Interior

CZECH REPUBLIC/REPUBLIQUE TCHEQUE
Apologised / Excusé

DENMARK/DANEMARK
Ms Katja Just Maarbjerg (19th – 21th of November)
Ministry of Culture

ESTONIA/ESTONIE
Mr Indrek Ibrus
Senior specialist of audiovisual affairs, Estonian Ministry of Culture

FINLAND/FINLANDE

Mr Moisander Juuso,
Commercial Secretary, Information Society and ICT, Ministry for Foreign Affairs of Finland

FRANCE
Ms Joanna Chansel
Ministère de la Culture et de la Communication

Mr Plubel Julien
Ministère des Affaires étrangères, Direction de la coopération culturelle, universitaire et de la recherche, Pôle de l'audiovisuel extérieur

GEORGIA/GEORGIE
Ms Irine Bartaia
Deputy Director, Department of International Law, Ministry of Foreign Affairs of Georgia

GERMANY/ALLEMAGNE
Mr Oliver Schenk (18th – 19th November)
Division K 31, International Media Cooperation, Federal Government Commissioner for Culture and the Media

Mr Jan Wiegandt (20-21 November)
VERTRETUNG DES LANDES, RHEINLAND-PFALZ in Brüssel
60, Avenue de Tervueren,
1040 Bruxelles, BELGIQUE

Ms Annick Kuhl
EU Representation of the Free State of Bavaria to the EU

GREECE/GRECE
Ms Christina Lamprou
Head of the Department of Audiovisual Affairs, Directorate of Mass Media - General Secretariat of Information and Communication, Hellenic Republic

HUNGARY/HONGRIE
Mr György Ocskó
International Legal Adviser, National Media and Infocommunications Authority

Mr János Auer
Member of the Media Council of the National Media and Infocommunications Authority

ICELAND/ISLANDE
Ms Elfa Ýr Gylfadóttir
Media Commission, Ministry of Education, Science and Education

IRELAND/IRLANDE
Mr Éanna O'Conghaile
Principal Officer, Broadcasting Policy Division, Department of Communications, Energy & Natural Resources

Mr Richard Browne,
Department of Communications, Energy & Natural Resources

ITALY/ITALIE
Mr Piergluigi Mazzella
Director General, Agency for the right to university education, Professor of Information and Communication, University of Rome

LATVIA/LETTONIE

Mr Andris Mellakauls
Information Space Integration, Ministry of Culture

LITHUANIA/LITUANIE
Ms Vida Česnaitė
Ministry of culture of the Republic of Lithuania, Information Society Development Division, Department advisor

LIECHTENSTEIN
Mr. Claudio Nardi,
Officer for Foreign Affairs

MALTA/ MALTE
Ms. Nancy Caruana,
Ministry for the Economy, investment and Small Business, Office of the Permanent Secretary

MONACO
M. Serge Robillard,
Chef de Division, Direction des Communications Électroniques, Principauté de Monaco

MONTENEGRO
Mr Ranko Vujovic,
Executive Director, UNEM

REPUBLIC OF MOLDOVA
Ms Ana Taban,
Head of Information and Media Outreach Office, Ministry of Foreign Affairs and European Integration

THE NETHERLANDS/PAYS-BAS
Ms Pien van den Eijnden (18^{th}-20^{th} of November)
Legal Adviser, Constitutional Affairs, Ministry of the Interior and Kingdom Relations

NORWAY/NORVEGE
Mr Olav Guntvedt
Assistant Director General, Departement of Media Policy and Copyright, Ministry of Culture

POLAND/POLOGNE
Ms Małgorzata Pek
Deputy Director of Strategy Department, Office of the National Broadcasting Council

Mr Maciej Gron
Director of the Department of Information Society, Ministry of Administration and Digitization

PORTUGAL
Mr Pedro Ruivo
GMCS, Portugal, Cabinet pour les Medias ("Gabinete para os Meios de Comunicação Social")

ROMANIA / ROUMANIE
Ms Delia Mucica,
Ministry of Culture and National Heritage

RUSSIAN FEDERATION / FEDERATION RUSSIE
Mr Alexander Surikov
Deputy Director Department of Information and Press
Ministry of Foreign Affairs

SERBIA/SERBIE
Ms Maja Rakovic,

First Counselor
Serbian Embassy, France

Ms Maja Zaric,
Adviser, Sector for International Relations, EU integration and projects, Ministry of Culture and Information

SLOVENIA/SLOVENIE
Mr Skender Adem
Undersecretary, Ministry of Culture of Republic of Slovenia

SLOVAKIA/SLOVAQUIE
Ms Ivana Maláková,
Head of Unit Media Law and Audiovisual Unit Media, Audiovisual and Copyright Department
Ministry of Cultura of Slovak Republic

SWEDEN
Mr Christoffer Lärkner
Department of Culture

SWITZERLAND
Mr Thomas Schneider
International Affairs, Federal Office of Communication, Federal Department for the environment, transport, energy and communication

M. Frédéric Riehl
Head of International Affairs, Federal Office of Communication, Federal Department for the environment, transport, energy and communication

„Former Yugoslav Republic of Macedonia"/ „Ex république yougoslave de Macédoine"
Ms Vesna Poposka
Head of International PR Department, Government of the Republic of Macedonia, PR Department

TURKEY/TURQUIE
Mr Mehmet Bora Sönmez
Media Expert, Radio and Television Supreme Council of Turkey

Mr Nurullah Öztürk,
Member of the Supreme Council, Radio and Television Supreme Council of the Republic of Turkey

UKRAINE
Ms Olga Herasymiuk,
First Deputy Chair of the National Council of Ukraine for Television and Radio Broadcasting

Ms Larysa Vasylenko
Head of International Relations Division of the National Television and Radio Broadcasting Council

UNITED KINGDOM/ROYAUME-UNI
Mr Mark Carvell
Media Team, Department for Culture, Media and Sport

* * *

OBSERVERS/PARTICIPANTS

BELARUS
Ms Maria Vanshina
Deputy Head of Communication Department, Head of Press Service, Ministry of Foreign Affairs of the Republic of Belarus

BLACK SEA BROADCASTING REGULATORY AUTHORITIES FORUM (BRAF)
Dr Hamit Ersoy
Secretary General

EUROPEAN PLATFORM OF REGULATORY AUTHORITIES (EPRA)
Ms Emmanuelle Machet
Secretary to the EPRA

EUROPEAN AUDIOVISUAL OBSERVATORY/OBSERVATOIRE EUROPEEN DE L'AUDIOVISUEL
Ms. Nikoltchev Susanne,
Executive Director

EUROPEAN ASSOCIATION FOR VIEZERS INTERESTS (EAVI)
Ms Krstina Stoycheva

EUROPEAN UNION/UNION EUROPEENNE
Maciej Tomaszewski (20th – 21st of November)
Policy officer – international, DG Connect, Unit D1, European Commission

EUROPEAN BROADCASTING UNION (EBU) / UNION EUROPEENNE DE RADIO-TELEVISION (UER)
Ms Anne-Catherine Berg,
Legal Adviser, Legal Department

Mr Giacomo Mazzone,
Head of Institutional Relations, Public Affairs & Communciations

EuroISPA
Mr Michael Rotert
Honorary Spokesman

ASSOCIATION OF EUROPEAN JOURNALISTS (AEJ) / MEDIA FREEDOM REPRESENTATIVE
Mr William Horsley (18th – 20th of November)
Media Freedom Representative

EUROPEAN NEWSPAPER PUBLISHERS ASSOCIATION (ENPA) / ASSOCIATION EUROPEENNE DES EDITEURS DE JOURNAUX
Mr Holger Rosedal,
Head of Legal Department

CONFERENCE OF INTERNATIONAL NON-GOVERNMENTAL ORGANISATIONS OF THE COUNCIL OF EUROPE / CONFÉRENCE DES ORGANISATIONS INTERNATIONALES NON GOUVERNEMENTALES DU CONSEIL DE L'EUROPE
Didier Schretter, Member of the Standing Commitee,
Vice-chair Education and Culture Committee

COPEAM
Mrs Alessandra Paradisi

HOLY SEE / SAINT SIEGE
Dr Michael Lukas

Episcopal Press Office

ICANN
Mr Nigel Hickson (20th – 21st)
VP, IGO Engagement

ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE (OSCE)
Dr. Juan (Joan) Barata Mir,
Principal Advisor, Representative on Freedom of Media

PREPOSE FEDERAL A LA PROTECTION DES DONNES ET A LA TRANSPARENCE
M. Jean-Philippe Walter,

MEXICO / MEXIQUE
M. Diego Sandoval Pimentel
Adjoint à l'Observateur Permanent du Mexique auprès du Conseil de l'Europe

PARLIAMENTARY ASSEMBLY OF THE COUNCI OF EUROPE / ASSEMBLEE PARLEMENTAIRE DU CONSEIL DE L'EUROPE
Mr Rüdiger Dossow
Secretary of the Committee on Culture, Science and Education

* * *

INTERPRETERS / INTERPRETES
Ms Sarah Adlington
Ms Gillian Wakenhut
Ms Bettina Ludewig
Mr Jean-Louis Wunsch

* * *

SECRETARIAT

Mr Jan Kleijssen, Director of Information Society and Action against Crime, Directorate General Human Rights and Rule of Law
Mr Jan Malinowski, Head of Information Society Department, Directorate General Human Rights and Rule of Law
Mr Patrick Penninckx, Executive Secretary, Cooperation Group to Combat Drug Abuse and Illicit Trafficking in Drugs, Directorate General of Human Rights and Rule of Law
Ms Silvia Grundmann, Head of Media Division, Directorate General of Human Rights and Rule of Law, Secretary to the Steering Committee on Media and Information Society
Ms Onur Andreotti, Administrator, Media Division, Directorate General Human Rights and Rule of Law
Mr Luca Belli, Administrator, Information Society Unit, Directorate General Human Rights and Rule of Law
Ms Ana Gascón-Marcén, Administrator, Information Society Unit, Directorate General Human Rights and Rule of Law
Mr Lee Hibbard, Administrator, Information Society Unit, Directorate General Human Rights and Rule of Law
Ms Elvana Thaçi, Administrator, Media Division, Directorate General Human Rights and Rule of Law
Ms Loreta Vioiu, Administrator, Information Society Unit, Directorate General Human Rights and Rule of Law

Ms Maria Michaelidou, Programme Advisor, Data Protection Unit, Directorate General Human Rights and Rule of Law

Ms Anne Boyer-Donnard, Principal Administrative Assistant, Media Division, Directorate General Human Rights and Rule of Law
Ms Giovanna Langella, Principal Administrative Assistant, Media Division, Directorate General Human Rights and Rule of Law
Ms Sarah Gregg, Assistant, Information Society Unit, Directorate General Human Rights and Rule of Law
Ms Krystyna Khokhlova, Assistant, Media Division, Directorate General Human Rights and Rule of Law
Ms Julia Whitham, Assistant, Media Division, Directorate General Human Rights and Rule of Law

Mr Naser Bislimi, Trainee, Media Division, Directorate General Human Rights and Rule of Law

APPENDIX III

Draft Recommendation CM/Rec(2014)___of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality

1. In information society, the exercise and enjoyment of the right to freedom of expression, including the right to receive and impart information and ideas as well as their participation in democratic life is increasingly reliant upon accessibility and quality of an Internet connection.

2. Providers of Internet access services have the ability to manage information and data flows (Internet traffic) transiting through the networks that they operate. They may engage in Internet traffic management for specific legitimate purposes such as to preserve the integrity and security of the network. They may also take action to prevent access to, or the dissemination of, unlawful or harmful content, for example through self-regulatory systems in co-operation with public authorities. However, other interferences with Internet traffic may affect the quality of the Internet service delivered to users and may result in blocking, discrimination or prioritisation of specific types of content, applications or services. Moreover, some of the techniques used in this context permit inspection or monitoring of communications, which can undermine users' trust in the Internet.

3. These matters raise concerns in respect of the protection and promotion of the right to private life and the right to freedom of expression, which are guaranteed respectively by articles 8 and 10 of the European Convention on Human Rights (ETS No. 5, hereinafter the ECHR), as well as in the light of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108). In addition, there are implications for access to diverse and pluralistic information and public service media content on the Internet, which are fundamental for democracy and cultural diversity. The right to freedom of expression, including the right to receive and impart information is not an absolute right. However, any restrictions to this right must meet the requirements of Article 10, paragraph 2 of the ECHR.

4. The principle of network neutrality underpins non-discriminatory treatment of Internet traffic and users' access to information and services of their choice. It reinforces the full exercise and enjoyment of the right to freedom of expression since Article 10 of the ECHR applies not only to the content of information but also to the means of its dissemination. Also, the principle of network neutrality supports technological innovation and economic growth.

5. The Committee of Ministers recalls Article 1 of the Statute of the Council of Europe and relevant Council of Europe standard-setting instruments[2]. With a view to protecting and promoting the right to private life and the right to freedom of expression in full compliance with Articles 8 and 10 of the ECHR as well as to promoting the full delivery of the public service value of the Internet, the Committee of Ministers recommends that member states:

- take all the necessary measures, in co-operation with all relevant stakeholders, to safeguard the principle of network neutrality in their policy frameworks having due regard to the guidelines set out in this recommendation;

- promote these guidelines in other international and regional fora that deal with the issue of network neutrality.

[2] Declaration of the Committee of Ministers on protecting the role of the media in democracy in the context of media concentration (31 January 2007); Recommendation Rec(2007)3 on the remit of public service media in the information society; Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet; Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters; Declaration of Committee of Ministers on network neutrality (29 September 2010); Declaration by the Committee of Ministers on Internet governance principles (21 September 2011); Recommendation CM/Rec (2014)6 to member States on a Guide to human rights for Internet users.

Guidelines on network neutrality

1. General principles

1.1. In the exercise of their right to freedom of expression, in compliance with Article 10 of the ECHR, Internet end-users have the right to access and distribute information, applications and services and to use devices of their choice. This right must be enjoyed without discrimination on any ground such as gender, sexual orientation, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.2. Internet traffic should be treated equally, without discrimination, restriction or interference irrespective of the sender, receiver, content, application, service or device. This is understood as the network neutrality principle for the purpose of this recommendation.

1.3. Internet users' freedom of choice should not be restricted by favouring or hindering the transmission of Internet traffic associated with particular content, services, applications or devices or traffic associated with services provided on the basis of exclusive arrangements or tariffs.

1.4. The network neutrality principle should be applied to all services that provide Internet connectivity to Internet users (Internet access services) irrespective of the infrastructure or the network used for Internet connectivity and regardless of the underlying technology used to transmit signals.

2. Traffic management

2.1. Providers of Internet access services should not restrict Internet users' freedom of choice by blocking, slowing down, altering, degrading or discriminating against specific content, applications or services.

2.2. Internet traffic management measures, wherever applicable, should be non-discriminatory, transparent, necessary and proportionate:

in giving effect to a court order or an order of a regulatory authority

- to preserve the integrity and security of the network, services provided via the network and end-users' terminal equipment;

- to prevent the transmission of unsolicited communications for marketing purposes to end-users who have given their prior consent to such restrictive measures;

- to minimise the effects of temporary or exceptional network congestion, provided that equivalent types of traffic are treated equally;

- in fulfilling contractual obligations with an end-user to deliver a guaranteed level of quality of service to that end-user provided that this does not impair the quality of open Internet access and does not constitute a discriminatory or anti-competitive practice.

2.3. Internet traffic management measures should be maintained no longer than strictly necessary and traffic management policies should be subject to periodic review by competent authorities within each member state.

3. Pluralism and diversity of information

3.1. Internet service providers should not discriminate against traffic from other providers of content, applications and services which compete with their own content, applications and services. This requires that traffic management decisions be strictly dissociated from content-related decision-making processes of the operator in the spirit of the 2007 Committee of Ministers Declaration on protecting the role of the media in democracy in the context of media concentration.

3.2. Preferential treatment of traffic on the basis of arrangements between Internet service providers and providers of content, applications and services should not diminish or affect the affordability, performance or quality of users' access to the Internet. Such arrangements should not have a negative impact on users' ability to access and use information, diverse and pluralistic content that is publicly available, applications and services of their choice.

3.3. In managed networks, states may consider imposing reasonable, transparent and proportionate obligations to carry content which meets general interest objectives.

4. Privacy

4.1. Traffic management measures should involve processing of personal data only to the extent that is necessary and proportionate to achieve the purposes set out in the second section and should be in accordance with applicable legislation on the right to private life and personal data protection.

4.2. Some techniques for the purpose of Internet traffic management are capable of assessing the content of communications. The way in which such techniques are used can be an interference with the right to private life. Therefore, such use must be fully in line with Article 8 of the ECHR, be tested against applicable legislation on the right to private life and personal data protection and reviewed by a competent authority within each member state in order to assess compliance with legislation.

5. Transparency

5.1. Internet service providers should provide users with clear, complete and publicly available information with regard to any traffic management practices that they have applied which might affect users' access to and distribution of content, applications or services. Internet users should be enabled to obtain information from Internet service providers about Internet traffic management and Internet speeds.

5.2. Competent authorities within each member state should monitor and report on Internet traffic management practices. Reports should be prepared in an open and transparent manner and made available to the public for free.

6. Accountability

6.1. Internet service providers should put in place appropriate, clear, open and efficient procedures to respond within reasonable time limits to complaints of Internet users alleging breaches of the principles included in the foregoing provisions. Internet users should be enabled to refer the matter to competent authorities within each member state.

6.2. States should ensure in their policy frameworks the accountability of Internet service providers with regard to respect for the principle of network neutrality. Accountability also includes that appropriate mechanisms are in place to respond to network neutrality complaints.

APPENDIX IV

Draft Recommendation CM/Rec(2014)___of the Committee of Ministers to member States on free transboundary flow of information on the Internet

1. The right to freedom of expression, including the right to receive and impart information and ideas without interference and regardless of frontiers constitutes a cornerstone of democratic society and is one of the basic conditions for its sustainability and progress and for the development of every human being. The provisions on rights and freedoms set out in the European Convention on Human Rights (hereinafter the ECHR) and Article 19 of the International Covenant on Civil and Political Rights apply equally online and offline. Article 10 of the ECHR applies not only to the content of information but also to the means of its dissemination or hosting, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.

2. Similarly, the right to freedom of assembly and association, as guaranteed by Article 11 of the ECHR, is also fundamental to democracy. In addition, safeguarding the right to private life as enshrined in Article 8 of the ECHR and ensuring the protection of personal data in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, hereinafter Convention 108) underpins the exercise of the right to freedom of expression and contributes to the free flow of information on the Internet.

3. The unimpeded transboundary flow of information is critical for the full realisation of these rights and freedoms, safeguarding pluralism and diversity of information, the development of culture and innovation and economic growth. National policies or measures, commercial activities or technological practices which interfere, whether deliberately or inadvertently, with Internet traffic or which place restrictions on Internet content or services within one state may have a bearing beyond that state's frontiers on the exercise of the right to freedom of expression and the right to freedom of association. Consequently, the exercise of national sovereignty may be affected.

4. Multiple states may claim jurisdiction over the same information and services on the Internet, which may leave individuals subject to inconsistent or conflicting rules. The variety/diversity of national laws on illegal content and services, as well as the application of competing and conflicting national laws, creates a complex legal environment which can make it difficult for individuals to claim the protection to which they are entitled under Article 10 of the ECHR. Developments in technology, for example content delivery networks and the growth of services that store and process data in remote locations rather than in locations proximate to the information owner or custodian/recipient (cloud services) will also increase complexities.

5. There is a need to promote a common international understanding, to consolidate norms and adhere to best practices on free transboundary flow of information on the Internet while ensuring full compliance with international agreements on the protection of children online, combatting cybercrime, protection of personal data and other relevant agreements. State action in this context should rely on Recommendation CM/Rec(2011)8 of the Committee of Ministers which sets out a commitment of member states to protect and promote the universality, integrity and openness of the Internet. This includes state responsibility to ensure that actions within one state do not interfere with access to information in other states or negatively impact the transboundary Internet traffic. States should also have due regard to other Council of Europe standards which are referenced in the appendix of this recommendation as well as to the value of self-regulation. This contributes to the elaboration of best practices and new models of behaviour that promote the unhampered flow of information, opinion and ideas on the Internet.

6. Therefore, the Committee of Ministers recommends that member states, when developing and implementing Internet-related policies at national level and within the international community:

- promote and protect free transboundary flow of information having due regard to the principles of this recommendation, in particular by ensuring that these principles are reflected in regulatory frameworks or policies and in practice;

- encourage private sector actors, civil society and technical communities to support and promote the implementation of the principles included in this recommendation.

Principles for free transboundary flow of information on the Internet

1. General principles

1.1. States have an obligation to guarantee to everyone within their jurisdiction the right to freedom of expression and the right to freedom of assembly and association, in full compliance with Articles 10 and 11 of the ECHR which apply equally to the Internet. These rights and freedoms must be guaranteed without discrimination on any ground such as gender, sexual orientation, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

1.2. States should protect and promote the global free flow of information on the Internet. They should ensure that interferences with Internet traffic within their territory pursue the legitimate aims set out in Article 10 of the ECHR and other relevant international agreements and do not have an unnecessary or disproportionate impact on the transboundary flow of information.

2. Due diligence principles

States should exercise due diligence when developing, assessing and implementing their national policies with a view to identifying and avoiding interferences with Internet traffic which have an adverse transboundary impact on the free flow of information on the Internet.

- *Assessment* - regulatory or other measures that are capable of having such an impact should be assessed with regard to state responsibility to respect, protect and promote the human rights and fundamental freedoms enshrined in the ECHR.

- *Transparency, foreseeability, accountability* -when developing policy and regulatory frameworks that may impact free flow of information on the Internet states should ensure transparency, including the results of evaluations mentioned above, foreseeability as to their implementation and accountability. In particular, proposed regulatory frameworks should be published with sufficient time and opportunity for public comment.

- *Proportionality and review of measures* - states are obliged to ensure that the blocking of content or services deemed illegal is in compliance with Articles 8, 10 and 11 of the ECHR. In particular, measures adopted by state authorities in order to combat illegal content or activities on the Internet should not result in unnecessary and disproportionate impact beyond the state's borders. States should strive towards measures which are least intrusive and least disruptive and which are carried out through a transparent and accountable process. Measures adopted or promoted by states should be regularly reviewed to determine their practical effectiveness and ongoing necessity and proportionality.

3. Value of self-regulation

States should encourage, facilitate and support as appropriate the development of self-regulatory codes of conduct so that all stakeholders respect the right to freedom of

expression, the right to freedom of assembly and association and the right to private life, with particular regard to the free flow of Internet traffic.

4. Promoting technical best practices

4.1. States should promote multi-stakeholder co-operation in the development and implementation of technical best practices that respect the right to freedom of expression and the right to freedom of association, including evaluations of the necessity of actions and proportionality of measures that may have a transboundary impact on Internet traffic.

4.2. States should ensure that national policies respect the global Internet architecture. This includes adherence to best practices regarding the domain name system.

5. International dialogue and policy

5.1. When national policies and commercial activities interfere with Internet traffic beyond the state's boundaries, the parties concerned may not have standing to raise their grievances within that state. States should ensure that structures and procedures exist for hearing and resolving the grievances of these parties. In this regard, states should engage in international dialogue to progressively develop shared understandings, international standards and norms and to adhere to best practices with regard to applicable law and competent jurisdiction in cases where competing (conflicting) laws apply to freedom of expression and access to information.

5.2. In the context of development of international policy or regulation for the Internet, states should protect and promote Internet connectivity as well as availability and accessibility of diverse and pluralistic information as these impact the free transboundary flow of information on the Internet.

5.3. In relation to services that store or process information in remote locations, states should safeguard the right to personal data protection in accordance with Convention 108 and the right to privacy in compliance with Article 8 of the ECHR. This is important for the full exercise of the rights in Article 10 of the ECHR. Regarding such services, states should also engage in international dialogue to develop shared norms, practices and understandings to address questions about jurisdiction and applicable law.

Appendix

Relevant Council of Europe standards

- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No.201)

- Convention on Cybercrime (ETS No. 185) and Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and Additional Protocol to the Convention for the Protection of

Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181)

- Recommendation CM/Rec(2011)8 of the Committee of Ministers to member states on the protection and promotion of the universality, integrity and openness of the Internet

- Recommendation CM/Rec(2009)5 on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment

- Declaration on protecting the dignity, security and privacy of children on the Internet (20 February 2008)

- Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters

- Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet

- Declaration on network neutrality (29 September 2010)

APPENDIX V

Draft Recommendation CM/Rec(2014)__ of the Committee of Ministers to member states on the processing of personal data in the context of employment

INDEX

DRAFT RECOMMENDATION CM/REC(2014)… OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE PROCESSING OF PERSONAL DATA IN THE CONTEXT OF EMPLOYMENT.

(Adopted by the Committee of Ministers on … 2014 at the … meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity among its members;

Aware of the increasing use of new technologies and means of electronic communication in the relations between employers and employees, and the corresponding advantages thereof;

Believing, however, that the use of data processing methods by employers should be guided by principles designed to minimise any risks that such methods might pose to employees' rights and fundamental freedoms, in particular their right to privacy;

Bearing in mind the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (hereunder referred to as "Convention 108") and of its Additional Protocol regarding Supervisory Authorities and Transborder Data Flows of 8 November 2001, and the desirability of articulating the application to the employment sector;

Recognising also that the interests to be borne in mind when developing principles for the employment sector are individual or collective, private or public;

Considering that personal data in official documents held by a public authority or a public body may be disclosed by the authority or body in accordance with the domestic law to which the public authority or body is subject, thus reconciling access to such official documents with the right to the protection of personal data [in accordance with the principles of the present Recommendation];

Aware of the different traditions which exist in member states with respect to the regulation of different aspects of employer-employee relations, and noting that law is only one of the means to regulate such relations;

Aware of the changes which have occurred internationally in the employment sector and related activities; notably due to the increased use of information and communication technologies (ICTs) and the globalisation of employment and services;

Considering that, in light of such changes Recommendation No. 89 (2) on the protection of personal data used for employment purposes should be revised so that they continue to provide an adequate level of protection for individuals in the employment sector;

Recalling that Article 8 of the European Convention on Human Rights protects the right to private life, including activities of a professional or business nature, as interpreted by the European Court of Human Rights;

Recalling the applicability of the existing principles set out in other relevant Recommendations of the Council of Europe, in particular Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation R(97)5 on the protection of medical data and Recommendation R(92)3 on genetic testing and screening for health care purposes;

Recalling the 'Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance' adopted by the European Committee on Legal Co-operation (CDCJ) of the Council of Europe in May 2003, referred to in Resolution 1604 (2008) of the Parliamentary Assembly of the Council of Europe, which are especially relevant;

Recalling the European Social Charter (CETS No.: 163), as revised on 3 May 1996, and the International Labour Office's 1997 Code of Practice on the Protection of Workers' Personal Data;

Recommends that governments of member States:

- ensure that the principles contained in the Appendix to the present Recommendation, which replaces the above-mentioned Recommendation (89)2, are reflected in the application of domestic legislation on data protection in the employment sector, as well as in other branches of the law which have a bearing on the use of personal data for employment purposes,

- for this purpose, ensure that the present Recommendation and its Appendix are brought to the attention of the authorities established under domestic data protection legislation which are competent to supervise the implementation of such legislation;

- promote acceptance and implementation of the principles contained in the Appendix to the present Recommendation by means of complementary instruments such as, codes of conducts, to ensure that the principles are well known, understood and applied by all employment sector participants, including representative bodies of both employers and employees, and are taken into account in the design and use of ICTs in the employment sector.

Appendix to the Recommendation

Part I – General principles

1. Scope

1.1. The principles set out in the present Recommendation apply to any processing of personal data for employment purposes in both the public and private sectors.

1.2. Unless domestic law provides otherwise, the principles of the present Recommendation also apply to the activities of employment agencies, whether in the public or private sector, which process personal data so as to enable one or more concurrent contracts of employment, including part-time contracts, to be established between individuals concerned and prospective employers, or to help employers discharge their duties relating to those contracts.

2. DEFINITIONS

For the purposes of the present Recommendation:

'Personal data' means any information relating to an identified or identifiable individual ("data subject");

'Data processing' means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, , preservation, alteration, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data; where no automated processing is used, data processing means the operations carried out within a structured set established according to any criteria which allows for the search of personal data;

'Information systems' means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automated processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purpose of their operation, use, protection or maintenance;

'Employment purposes' concerns the relations between employers and employees which relate to recruitment, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, planning and the efficient running of an organisation and termination of the employment relationship. The consequences of the contractual relationship may extend beyond the term of the contract of employment;

'Employer' means any natural or legal person, public authority or agency that has an employment relationship with an employee or is considering such a relationship in respect of a job applicant and has the legal responsibility for the undertaking or establishment;

'Employee' means any natural person concerned engaged by an employer under an employment relationship.

3. Respect for human rights, dignity and fundamental freedoms

Respect for human dignity, privacy and the protection of personal data should be safeguarded in the processing of personal data for employment purposes, notably to allow for the free development of employees' personality as well as for possibilities of individual and social relationship on the workplace.

4. Application of data processing principles

4.1. Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned.

4.2. Employers should develop appropriate measures, to ensure that they respect in practice the principles and obligations relating to data processing for employment purposes. At the request of the supervisory authority, employers should also be able to demonstrate their compliance with such principles and obligations. These measures should be adapted to the volume and nature of the data processed, the type of the activities being undertaken, and should also take into account possible implications on fundamental rights and freedoms of employees.

5. *Collection and storage of data*

5.1. Employers should collect personal data directly from the data subject concerned. When it is necessary and lawful to process data collected from third parties, for example to obtain professional references, the data subject should be duly informed in advance.

5.2. Personal data collected for employment purposes should be relevant and not excessive, bearing in mind the type of the employment as well as the changing information needs of the employer.

5.3. Employers should refrain from requiring or asking an employee or a job applicant access to information that he or she shares with others online, notably through social networking.

5.4. Health data may only be collected for the purposes set out in principle 8.2 of the present Recommendation.

5.5. The storage of personal data for employment purposes is permissible only if the data have been collected in accordance with the requirements outlined in principles 4, 9 and 14 to 20 and only for the time necessary to pursue the legitimate aim of the processing. When evaluation data are stored relating to the performance or potential of an employee, such data should only be processed for the purpose of assessing professional skills.

6. *Internal use of data*

6.1. Personal data collected for employment purposes should only be processed by employers for such purposes.

6.2. Employers should adopt data protection policies, rules and/or other instruments on internal use of personal data in compliance with the principles of the present Recommendation.

6.3. Under exceptional circumstances, where data are to be processed for employment purposes other than the purpose for which they were originally collected, employers should take adequate measures to avoid misuse of the data for this different purpose and inform the employee. Where important decisions affecting the employee are to be taken, based on the processing of that data, the employee should be informed accordingly.

6.4. Without prejudice to principle 8, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principles of proportionality and purpose specification in the subsequent use of the data. Every substantive change in the processing should be communicated to the persons concerned.

7. *Communication of data and use of ICTs for the purpose of employee representation*

7.1. In accordance with domestic law and practice, or the terms of collective agreements, personal data may be communicated to employee's representatives, but only to the extent that such data are necessary to allow them to properly represent his or her interests or if such data are necessary for the fulfillment and supervision of obligations laid down in collective agreements.

7.2. In accordance with domestic law and practice, the use of information systems and technologies for the communication of data to employees' representatives should be subject to appropriate agreements that set out, in advance, transparent rules prescribing their use and safeguards to protect confidential communications, in accordance with principle 10.

8. *External communication of data*

8.1. Personal data collected for employment purposes should only be communicated to public bodies acting in their official functions, and for the purposes of carrying them out, and only within the limits of employers' legal obligations or in accordance with other provisions of domestic law.

8.2. The communication of personal data to public bodies for purposes other than the exercise of their official functions or to parties other than public bodies, including entities in the same group, should only take place:

a. where it is necessary for employment purposes, the purposes are not incompatible with the purposes for which the data was originally collected and the employee concerned or his or her representatives, as the case may be, are informed of this in advance; or

b. with the express, free and informed consent of the employee concerned; or

c. if the communication is provided for by domestic law and in particular for the purpose of discharging legal obligations or in accordance with collective agreements.

8.3. The provisions governing the disclosure of personal data to ensure transparency in the public sector (government and other public authority/ body), including monitoring the correct use of public resources and funds, should provide appropriate safeguards for the employees right to privacy and protection of personal data.

8.4. Employers should take appropriate measures to ensure that, only relevant, accurate and up-to-date data are communicated externally, particularly in relation to data that is posted online and accessible to a wider public.

9. *Processing of sensitive data*

9.1. The processing of sensitive data referred to in Article 6 of Convention 108 is only permitted in particular cases, where it is indispensable for the specific employment recruitment or to fulfill legal obligations related to the employment contract within the limits laid down by domestic law and in accordance with appropriate safeguards, complementing those set out in Convention 108 and in the present Recommendation. Appropriate safeguards should be aimed at preventing the risks that the processing of such sensitive data may present to the interests, rights and fundamental freedoms of the employee concerned, notably a risk of discrimination. Processing of biometric data should be possible under conditions provided in Principle 18 of the present Recommendation.

9.2. In accordance with domestic law, an employee or a job applicant may only be asked questions concerning his or her state of health and/or be medically examined in order to:

a. indicate his or her suitability for present or future employment;

b. fulfill the requirements of preventive medicine;

c. guarantee an appropriate rehabilitation or comply with any other work environment requirements;

d. safeguard the vital interests of the data subject or other employees and individuals;

e. enable social benefits to be granted; or

f. satisfy judicial procedures.

9.3. Genetic data cannot be processed for instance to determine the professional suitability of an employee or a job applicant, even with the consent of the person concerned. The processing of genetic data may only be permitted in exceptional circumstances, for example to avoid any serious prejudice to the health of the data subject or third parties, and only if it is provided for by domestic law and subject to appropriate safeguards.

9.4. Health data and - where their processing is lawful - genetic data should only be collected from the employee where it is provided for by law, and subject to appropriate safeguards.

9.5. Health data covered by the obligation of medical confidentiality should only be accessible to and processed by personnel who are bound by such an obligation or by other rules of professional secrecy or confidentiality. Such data must:

a. relate directly to the ability of the employee concerned to exercise his or her duties; or
b. be necessary in support of measures to protect the health of the employee; or
c. be necessary to prevent risks to others.

Where such data are communicated to employers, this processing should be performed by a person with the relevant authorisation, such as someone in personnel administration or responsible for health and safety at work, and the information should only be communicated if it is indispensable for decision-making by the personnel administration and in accordance with provisions of domestic law.

9.6. Health data covered by the obligation of medical confidentiality and - where their processing is lawful - genetic data, where appropriate should be stored separately from other categories of personal data held by employers. Technical and organisational security measures should be taken to prevent persons who do not belong to the employer's medical service having access to the data.

9.7. Health data related to third parties should not be processed under any circumstances unless full, unambiguous, free and informed consent is given, or such processing is authorised by a data protection supervisory authority, or it is mandatory according to domestic law.

10. *Transparency of processing*

10.1. Information concerning personal data held by employers should be made available either to the employee concerned directly or through the intermediary of his or her representatives or brought to his or her notice through other appropriate means.

10.2. Employers should provide employees with the following information:

- the categories of personal data to be processed and a description of the purposes of the processing,
- the recipients, or categories of recipients of the personal data,
- the means the employees have of exercising the rights set out in principle 11 of the present Recommendation, without prejudice to more favorable ones provided by domestic law or in their legal system,
- any other information necessary to ensure fair and lawful processing.

10.3 In this context, a particularly clear and complete description must be provided of the categories of personal data that can be collected by ICTs, including video-surveillance and their possible use. This principle also applies to the particular forms of processing provided for in Part II of the present Recommendation.

10.4 The information should be provided in an accessible format and kept up to date. In any event, such information should be provided before an employee carries out the activity or

action concerned, and made readily available also through the information systems normally used by the employee.

11. *Right of access, rectification and to object*

11.1. An employee should be able to obtain, upon request, at reasonable intervals and without excessive delay, confirmation of the processing of personal data relating to him or her. The communication should be in an intelligible form, include all information on the origin of the data, as well as any other information that the controller is required to provide to ensure the transparency of processing, notably information provided in principle 10.

11.2. An employee should be entitled to have personal data relating to him or her rectified, blocked or erased, if they are inaccurate and/or if the data have been processed contrary to the law or the principles set out in the present Recommendation. He or she should also be entitled to object at any time to the processing of his or her personal data unless the processing is necessary for employment purposes or otherwise provided by law.

11.3. The right of access should also be guaranteed in respect of evaluation data, including where such data relate to assessments of the performance, productivity or capability of the employee, at least when the assessment process has been completed, without prejudice to the right of defence of employers or third parties involved. Although such data cannot be corrected by the employee, purely subjective assessments should be open to challenge in accordance with domestic law.

11.4. An employee should not be subject to a decision significantly affecting him or her, based solely on an automated processing of data without having his or her views taken into consideration.

11.5. An employee should also be able to obtain, upon request, knowledge of the reasoning underlying the data processing, the results of which are applied to him or her.

11.6. Derogations to the rights referred to in paragraphs 10, 11.1, 11.2, 11.4 and 11.5 may be permitted if provided for by law and are a necessary measure in a democratic society, to protect State security, public safety, important economic and financial interests of the State or the prevention and suppression of criminal offences, the protection of the data subject or the rights and freedoms of others.

11.7. Furthermore, in the case of an internal investigation conducted by an employer, the exercise of the rights referred to in paragraphs 10, 11.1 to 11.5 may be deferred until the closing of the investigation if the exercise of those rights would prejudice the investigation.

11.8. Unless provisions of domestic law provide otherwise, an employee should be entitled to choose and designate a person to assist him or her in the exercise of his or her right of access, rectification and to object or to exercise these rights on his or her behalf.

11.9. Domestic law should provide a remedy where access to data is refused, or requests for rectification or erasure of any of the data is denied.

12. *Security of data*

12.1. Employers, or entities which may process data on their behalf, should implement adequate technical and organisational measures in response to periodic reviews of the organisation's risk assessment and security policies and update them as appropriate. Such measures should be designed to ensure the security and confidentiality of personal data processed for employment purposes against accidental or unauthorised modification, loss or destruction of personal data, as well as against unauthorised access, dissemination or disclosure of such data.

12.2 In accordance with domestic law, employers should ensure adequate data security when using ICTs for any operation of processing of personal data for employment purposes, including their storage.

12.3. The personnel administration, as well as any other person engaged in the processing of the data, should be kept informed of such measures, of the need to respect them and of the need to maintain confidentiality about such measures as well.

13. *Preservation of data*

13.1. Personal data should not be retained by employers for a period longer than is justified by the employment purposes outlined in Principle 2 or is required by the interests of a present or former employee.

13.2. Personal data submitted in support of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the job applicant. Where such data are stored with a view to a further job opportunity, the person concerned should be informed accordingly and the data should be deleted if requested by the person concerned.

13.3 Where it is required to store data submitted for a job application for the purpose of bringing or defending legal actions or any other legitimate purpose, the data should be stored only for the period necessary for the fulfillment of such purpose.

13.4 Personal data processed for the purpose of an internal investigation carried out by employers which has not led to the adoption of negative measures in relation to any employee should be deleted after a reasonable period, without prejudice to the employee's right of access until such deletion.

Part II - Particular forms of processing

14. Use of Internet and electronic communications in the workplace

14.1 Employers should avoid unjustifiable and unreasonable interferences with employees' right to private life. This principle extends to all technical devices and ICTs used by an employee. The persons concerned should be properly and periodically informed, through a clear privacy policy, in accordance with principle 10 of the present Recommendation. The information provided should be kept up to date and should include the purpose of the processing, the preservation or back-up period of traffic data and the archiving of professional electronic communications.

14.2. In particular, in the event of processing of personal data relating to Internet or Intranet pages accessed by the employee, preference should be given to the adoption of preventive measures, such as the use of filters which prevent particular operations, and to the grading of possible monitoring on personal data, giving preference for non-individual random checks on data which are anonymous or in some way aggregated.

14.3. Access by employers to the professional electronic communications of their employees who have been informed in advance of the existence of that possibility can only occur, where necessary, for security or other lawful reason. In case of absent employees, employers should take the necessary measures and foresee the appropriate procedures aimed at enabling access to professional electronic communications only when such access is of professional necessity. Access must be undertaken in the least intrusive way possible and only after having informed the employees concerned.

14.4. The content, sending and receiving of private electronic communications at work should not be monitored under any circumstances.

14.5. On employee's departure from an organisation, employers should take the necessary organisational and technical measures to automatically deactivate the employee's account. If employers need to recover the contents of an employee's account for the efficient running of the organisation, they should do so before his or her departure and when feasible, in his or her presence.

15. *Information systems and technologies for the monitoring of employees, including video surveillance*

15.1. The introduction and use of information systems and technologies for the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted. Where their introduction and use for other legitimate purposes, such as to protect production, health and safety or to ensure the efficient running of an organisation has an indirect consequence the possibility of monitoring employees' activity, it should be subject to the additional safeguards set out in principle 21, in particular the consultation of employees' representatives.

15.2. Information systems and technologies that indirectly monitor employees' activities and behavour should be specifically designed and located so as not to undermine their fundamental rights. The use of video surveillance for monitoring locations that are part of the most personal area of life of employees is not permitted in any situation.

15.3. In the event of dispute or legal proceedings, employees should be able to obtain copies of the recordings made, when appropriate and in accordance with the domestic law. The storage of the recording should be limited in time.

16. Equipment revealing employees' location

16.1. Equipment revealing employees' location should be introduced only if it proves necessary to achieve the legitimate purpose pursued by employers and their use should not lead to a continuous monitoring of an employee. Notably, monitoring should not be the main purpose, but only an indirect consequence of an action needed to protect production, health and safety or to ensure the efficient running of an organisation. Given the potential to violate the rights and freedoms of persons concerned by the use of these devices, employers should ensure all necessary safeguards for the employees' right to privacy and protection of personal data, including the additional safeguards provided for in principle 21. In accordance with principles 4 and 5, employers should pay special attention to the purpose for which such devices are used and to the principles of minimisation and proportionality.

16.2. Employers should apply appropriate internal procedures relating to the processing of these data and should notify the persons concerned in advance in respect of the internal procedures.

17. Internal reporting mechanism

Where employers are obliged by law or internal rules to implement internal reporting mechanisms, such as hotlines, they should secure the protection of personal data of all parties involved. In particular, employers should ensure the confidentiality of the employee who reports on illegal or unethical conduct (e.g. a whistleblower). Personal data of the parties involved should be used solely for the purpose of appropriate internal procedures relating to the report and as required by the law or as may be required for subsequent judicial proceedings.

Under exceptional circumstances, employers may enable anonymous reporting. Internal investigations should not be carried out on the sole basis of an anonymous report, except where it is duly circumstantiated and relates to serious infringements of domestic law.

18. Biometric data

18.1. The collection and further processing of biometric data should only be undertaken when it is necessary to protect the legitimate interests of employers, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards, including the additional safeguards provided for in principle 21.

18.2. The processing of biometric data should be based on scientifically recognised methods and should be subject to the requirements of strict security and proportionality.

19. Psychological tests, analysis and similar procedures

19.1. Recourse to psychological tests, analysis and similar procedures performed by specialised professionals, subject to medical confidentiality, that are designed to assess the character or personality of an employee or a job applicant should only be allowed if legitimate and necessary for the type of activity performed in the job and if domestic law provides appropriate safeguards.

19.2. The employee or the job applicant should be informed in advance of the use that will be made of the results of these tests, analysis or similar procedures and, subsequently, the content thereof. Principles 11.1 and 11.2 apply accordingly.

20. Other processing posing specific risks to employees' rights

20.1. Employers, or where applicable processors, should carry out a risk analysis of the potential impact of any intended data processing on the employees' rights and fundamental freedoms and design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights and fundamental freedoms.

20.2. Unless domestic law or practice provides other appropriate safeguards, the agreement of employees' representatives should be sought before the introduction or adaptation of ICTs where the analysis reveals such risks.

21. *Additional safeguards*

For all particular forms of processing, set out in Part II of the present Recommendation, employers should ensure that appropriate measures are taken to secure, in particular, the respect of the following safeguards:

a. Inform the employees before the introduction of information systems and technologies enabling the monitoring of their activities. The information provided should be kept up to date and should be undertaken taking into account principle 10 of the present Recommendation. The information should include the purpose of the operation, the preservation or back-up period, as well as the existence or not of the rights of access and rectification and how those rights may be exercised;

b. Take appropriate internal procedures relating to the processing of that data and notify employees in advance;

c. Before any monitoring can occur, or in circumstances where such monitoring may change, employees' representatives should be consulted in accordance with domestic law or

practice. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, the agreement of employees' representatives should be sought;

d. Consult, in accordance with domestic law, the national supervisory authority on the processing of personal data.