Bureau of the Steering Committee on Media and Information Society

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

22/10/2014 **CDMSI-BU(2014)004**

Report of the 6th meeting (24-25 September 2014)

(Strasbourg, Agora Building, Room G02)

1. & 2. Opening of the meeting – Adoption of the agenda

The CDMSI Chair Ms Maja Rakovic (Serbia) opened the meeting. The Bureau adopted the agenda of its meeting in view of the preparation of the CDMSI meeting which will take place from 18 to 21 November 2014. The annotated agenda appears in Appendix 1. The list of participants appears in Appendix 2.

3. Information by the Chair and the Secretariat

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

The Bureau was informed by the Secretariat on and took note of the following information on:

- a working session which will be held on 16 October 2014 in Metz in the context of the "Assises du journalisme", together with representatives of NGO's which are potential partners of the Council of Europe on the Safety of Journalists "platform project". The purpose of the working session is to have a discussion on the concrete conditions of such a partnership;

- the Seminar and inter-regional dialogue on the protection of journalists which will take place on the 3rd of November 2014 (Appendix 3). All Bureau members as well as MSI-JO members who are also CDMSI members will be invited to the Seminar;

- the agenda of Mr Thorbjørn Jagland, Secretary General of the Council of Europe for his second term in office which was presented to the Committee of Ministers at the 1206bis meeting of the Ministers' Deputies (16 September 2014). The Bureau noted that emphasis was put on freedom of expression issues, including free media, safety of journalists, social media and Internet governance. The Secretary General expects to present early next year a comparative study on the laws and practice in respect of filtering, blocking and taking down of illegal content on the Internet in all member states. The Secretary General mentioned also his proposal to the Committee of Ministers for a mechanism on protection of the safety of journalists to be placed within the Directorate of Policy Planning; the latter will have a revised mandate;

- the revised UNESCO Concept Note on a Research project proposal on the safety of journalists as potential indicator of rule of law, democracy and development. The Bureau expressed the interest in strengthening cooperation with UNESCO;

- an UN Inter-Agency meeting organised by UNESCO and hosted by the Council of Europe on 4 November 2014 in Strasbourg on safety of journalists and the issue of impunity;

- the defamation study which will be updated substantially and will be ready to be published at the beginning of 2015. Its appendix which compiles the national legislations is planned to be designed as an online tool providing for regular updating. CDMSI members will be invited to participate;

- the announcement by Mr Nils Muižnieks, the Council of Europe's Human Rights Commissioner, announced at the 1207th meeting of the Ministers' Deputies on 17 September 2014 that he will publish an Issue Paper on rule of law on the Internet. The Secretariat will transmit this paper to the CDMSI as soon as it is published.

3.2. Human rights of Internet users

The CDMSI Bureau was informed about activities planned by the Secretariat with regard to the implementation of Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to Human Rights of Internet Users.

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

The Bureau examined a proposal by the Secretariat regarding questions addressed to CDMSI members on the implementation of the Committee of Ministers guidelines on eradicating impunity for serious human rights violations (30 March 2011), putting these guidelines into the specific context of safety of journalists. The Bureau edited the questions and decided to submit them to CDMSI (Appendix 4). The Bureau recalled that the CDMIS agreed on a proposal by the Secretariat for the format of follow-up of the implementation of Council of Europe adopted standards in member states and that it had decided that the first theme will be "Safety of journalists" to be discussed at its next meeting in November 2014. To facilitate this discussion and its preparation, the Bureau suggest to invite CDMSI members who are also members of the MSI-JO expert committee to actively contribute to the preparation of this item and the plenary discussion.

5. Media

Standard setting activities

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

The Bureau reiterated its support for the outline structure of the draft Recommendation on the protection of journalism and safety of journalists proposed by MSI-JO. Noting that the MSI-JO will have its second meeting on 6 and 7 October 2014, the Bureau stressed that the preliminary draft recommendation should be sent to the CDMSI as soon as possible after the MSI-JO meeting. The preliminary draft recommendation will be discussed during the CDMSI plenary meeting in November 2014.

Being mindful of the limited MSI-JO mandate, the Bureau encouraged the MSI-JO to contribute to the CDMSI's future work on the topic of "professional and ethical journalism". The Bureau underlined the necessity to plan committee of experts meetings, to the extent possible, prior to those of the Bureau and expressed a wish to invite the Chair of the MSI-JO to the CDMSI plenary in November 2014.

The Bureau took note of the information provided by the Secretariat about the state of play of contributions regarding the collection of good practices in member states on initiatives aiming at strengthening the safety of journalists and invited the Secretariat to re-launch the call for contributions.

5.2 Hate speech

The Bureau endorsed a proposal by the Secretariat to invite the Council of Europe Coordinator of the No Hate Speech Campaign together with a young activist to the November CDMSI plenary to give first-hand information.

5.3 Gender equality and the media

The Bureau took note of the information that Bissera Zankova will participate to the 40th EPRA meeting, which will take place in Tbilisi, Georgia, from 8 to 10 October 2014, to present the Recommendation and discuss its implementation.

The Bureau also took note of the information on the draft Toolkit for the implementation of the Recommendation. It expressed interest in forming a working group on gender equality and media. Emir Povlakic (Bosnia and Herzegovina), Bissera Zankova (Bulgaria) and Christina Lamprou (Greece) volunteered to be part of it. The Bureau decided to submit this suggestion to the CDMSI in the next plenary meeting in November 2014.

5.4 Transparency of media ownership

The Secretariat informed the Bureau about discussions which are expected to take place in the Parliamentary Assembly's Committee on Culture, Science, Education and Media on 1 October 2014 where an expert Report on the topic of increasing transparency of media ownership will be presented and discussed. The expert Report will be made available to the CDMSI after the meeting of the Parliamentary Assembly. The Bureau decided to invite the CDMSI at its next meeting to create an informal working group on the issue of transparency of media ownership.

5.5 Public service media

The Bureau proposes that discussions on this topic continue during the upcoming meetings of the CDMSI.

6. Information Society and Internet Governance

Standard setting activities

6.1 Network Neutrality

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

The Bureau recalled the revision process of the draft Recommendation since the last meeting of the CDMSI (23 to 26 May 2014). This process included transmission of the draft to the CDMSI via E-mail for approval ad-referendum on two occasions, namely on 2

June 2014 (immediately after the CDMSI meeting) and on 5 September 2014, including comments received. The Bureau took note of the comments submitted by delegations which appear in Appendix 5.

The Bureau agreed on a revised version of the draft recommendation which takes into account the comments submitted in the most suitable way to preserve the balance and the human rights nature of the text (Appendix 6). Given the extensive discussions on the text and consultations held so far with member states, the Bureau emphasised the need to progress at the upcoming CDMSI meeting (18-21 November 2014), notably in view of its terms of reference and of the considerable amount of time already invested into the finalisation of this very important document. Therefore the Bureau strongly encourages the CDMSI to approve the draft recommendation at its next meeting and transmit it to the Committee of Ministers for adoption without any further delay.

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

The Secretariat informed the Bureau about the last meeting of the MSI-INT (3-4 July 2014) and the progress of work in this committee. The Bureau welcomed the progress and results achieved in the MSI-INT and took note of the fact that an additional meeting will be held on 23 and 24 October 2014. The Bureau discussed the MSI-INT proposal for a draft recommendation on CM/Rec(2014)____ of the Committee of Ministers to member states on free transboundary flow of information on the Internet. It welcomed the text, proposed certain amendments and agreed to submit revised draft to the CDMSI for discussion with the view of its finalisation during the plenary meeting in November (Appendix 7).

In respect of the draft recommendation on Internet Freedom, the Secretariat informed the Bureau about preliminary elements developed by the MSI-INT rapporteur on this expected result and related discussion at the MSI-INT (document MSI-INT(2014)07, date 16 June 2014). The Bureau was also informed about an informal meeting which was held on the margins of the IGF (2-5 September 2014, Istanbul) between the MSI-INT Chair and other members of the MSI-INT in IGF attendance. The idea of using the preliminary elements to develop Internet freedom indicators was discussed at this informal meeting and it will be further considered at an additional MSI-INT meeting to be held on 23 and 24 October. The Bureau took note of this information, expressed support for the indicator approach notably in view of the Secretary General's new agenda to work on implementation of legislation and indexes and asked the MSI-INT to prepare preliminary draft recommendation on Internet Freedom for discussion during the CDMSI meeting in November 2014.

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

The Secretariat informed the Bureau of progress on the implementation of the Internet Governance Strategy 2012-2015 and that a report will be submitted to the CDMSI for its consideration at the next plenary meeting to be held in November 2014.

The Bureau welcomed discussion elements for the Internet governance strategy 2016-2019 and decided to invite the CDMSI to comment on these elements which should be sent to the Secretariat at the latest by 27 October 2014 as a basis for plenary discussion.

The Bureau underlined importance of the follow up of the implementation of the current strategy.

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)

The Bureau took note of the information provided by the Secretariat on the participation of the Secretariat in EuroDIG 2014 and in the Internet Governance Forum 2014, where the work of the Council of Europe on safety of journalists, the Internet guide to the rights of internet users and network neutrality were presented.

6.5 ICANN

The Bureau took note of the Council of Europe expert report, prepared by Dr Monika Zalnieriute, Researcher at the Department of Law European University Institute Italy and Thomas Schneider, Deputy Chair of the Council of Europe's Steering Committee on Media and the Information Society (CDMSI): ICANN's procedures and policies in the light of human rights, fundamental rights and democratic values.

6.6 Other activities

The Bureau took note of the information provided by the Secretariat on the NetMundial meeting. It also took note of information on the World Summit on Information Society +10 Review process carried out by the United Nations. The Bureau expressed the view that the Internet Governance Strategy should take into account the elements discussed during these meetings.

Mr Thomas Schneider informed the meeting about the UNESCO conference "Connecting the dots: multi-stakeholders conference on UNESCO's Internet study on access, free expression, privacy and ethics" which will be held in Paris on 3-4 March 2015.

7. Cooperation activities

The Bureau took note of information on accomplished and ongoing projects in the field of media and freedom of information and ongoing and planned activities in the field of Internet governance, as it appears in the documents prepared by the Secretariat.

8. Data Protection

The Bureau took note of the information provided by the Secretariat of the T-PD on the revision of the Recommendation on the processing of personal data in the context of employment. The draft Recommendation (document T-PD(2014)08) is the result of the work carried out over several years by the T-PD. The draft was approved by the T-PD at its last plenary meeting (2-4 June 2014) and transmitted to the CDMSI, inviting it's written comments on the draft text prior to the Bureau meeting (one delegation expressed general support). The T-PD being a convention committee, the draft legal instruments it prepares have to be sent to the Committee of Ministers via a Steering Committee, which is since 2012 the CDMSI (see terms of reference). It was recalled that this Convention Committee is composed of representatives of 45 member states of the Council of Europe out of the 47 (San Marino and Turkey are not Party to Convention 108), a representative of the first non-European country which acceded to Convention 108 (Uruguay) and several state observers and non-state actors observers. The specialised nature of the expertise of the Committee and its work was underlined and it was acknowledged that, while the draft Recommendation has a different format and language than CDMSI instruments, the CDMSI could decide to endorse the text and submit it to the Committee of Ministers in the T-PD format.

The Bureau proposed to recommend that the CDMSI examines the text under its own field of expertise during the next plenary meeting in November, which will be attended by the Chair of the T-PD, with a view to submitting it for adoption to the Committee of Ministers.

An update on the modernisation of Convention 108 was provided (the third and last meeting of the Ad Hoc Committee on Data Protection is scheduled for 1-3 December 2014) as well as information on the other topics tackled by the T-PD (notably data processing in a police context, medical data and big data).

9. Information about work of other organisations and other Council of Europe bodies

9.1 Participation of CDMSI in events and meetings

The Bureau took note of information provided by its members and the Secretariat.

9.2 Parliamentary Assembly of the Council of Europe (PACE)

The Bureau recalled that the CDMSI provided comments in relation to Committee of Ministers' replies to the Parliamentary Assembly with regard to the latter's Recommendation 2036 (2014) on the "Revision of the European Convention on Transfrontier Television" and Recommendation 2041(2014) on Improving user protection and security in cyberspace. The Secretariat informed the Bureau that the Committee of Ministers adopted its reply on Recommendation 2036 (2014) on 19 September 2014 (CM/AS(2014)Rec2036 final, date 19 September 2014) which took into account the CDMSI comments. The reply to Recommendation 2041(2014) will be considered by the Committee of Ministers' rapporteur group GR-J on 7 October.

10. Budget and administrative matters

The Bureau took note of the information provided by Jan Kleijssen, Director of the Information Society and Action against the Crime Directorate, on two administrative decisions: the appointment of Mr Jan Malinowski as Executive Secretary to the Pompidou Group and the appointment of Mr Patrick Penninckx as Head of the Department of Information Society, which will enter into force on 1 December 2014; and the integration of the Internet Governance Unit into the Media Division, to enter into force on 1 October 2014. The Bureau also took note of the information on new staff members in the Secretariat, notably the recruitment of Ms Giovanna Langella acting as temporary principal administrative assistant in the absence of Anne Boyer-Donnard.

11. Priorities of CDMSI work and working methods

The Bureau took note of an information document provided by the Secretariat on CDMSI priorities and decided to submit it to the next CDMSI plenary meeting. The Bureau suggested that rapporteurs are sought or small internal working groups be created among CDMSI members. Referring to the information document on CDMSI priorities, the Bureau decided to invite the CDMSI to create informal working groups on the following topics: professional and ethical journalism; media pluralism and transparency of media ownership; gender equality dimension in the media coverage of electoral campaigns. The Bureau underlined that this working method appears to be necessary to fulfill the CDMSI terms of reference.

Furthermore, the Bureau invites the CDMSI to consider possible informal working groups on surveillance issues, public service media and hate speech.

12. Other questions

12.1 Co-operation with observers

The Bureau had a discussion on the CDMSI's role in relation to admission of observers in the Committee. It recalled the relevant provisions, specifically section III/ C of Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods. The Bureau also recalled the general criteria that the CDMSI has used in the past in relation to observer status requests, namely the applicant's broad experience in the area of competence of the CDMSI or other subordinate bodies concerned, the ability to make an effective and high quality contribution to the relevant bodies' activities and the applicant's representativeness at European level.

12.2 Application for observer status by Internet Watch Foundation

In respect of the application for observer status by Internet Watch Foundation, the Bureau took note of some additional information provided by the applicant with regard to the Foundation's international engagement and representativeness. On this basis, the Bureau agreed to express its support for this application and to recommend to the CDMSI to approve, at its next meeting (18-21 November 2014), the admission of the Internet Watch Foundation as an observer.

12.3 Application for observer status by Press Club Prague

In respect of the application by the Press Club of Prague, the Bureau took note that the applicant was invited to provide additional information with regard to the criterion of European representativeness. The Bureau was informed about the response of the applicant and of the fact that the Bureau member Ms Bissera Zankova had tried to collect information about the applicant. Given that the applicant has not provided sufficient information with regard to its European representativeness, the Bureau agreed that it will not recommend to CDMSI admission of the Press Club of Prague as an observer to the CDMSI.

13.Draft Agenda of the 7th CDMSI meeting (18-21 November 2014)

The Bureau decided to adopt the draft preliminary agenda of the 7th CDMSI meeting.

Appendix 1 **Annotated Agenda**[1]

1. Opening of the meeting

2. Adoption of the agenda

Notes and expected action	Adopt the agenda in view of the preparation of the 7th meeting of CDMSI (18-21 November 2014); discuss plenary meeting preparation.

3. Information by the Chair and the Secretariat

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

SG/Inf(2014)2	Setting up of a Freedom of Expression Platform to promote the protection of journalism and safety of journalists - Proposals by the Secretary General to the Committee of Ministers
Report	Round Table on Safety of Journalists – From commitment to action, 19 May 2014 – Strasbourg
SG(2014)1-FINAL	Report by the Secretary General of the Council of Europe 'State of Democracy, Human Rights and Rule of Law in Europe'
	Information on 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
	Commissioner for Human Rights issue paper on the Rule of Law on the Internet and in the wider digital world (subject to publication, foreseen for September)
	UNESCO Concept Note: Research project on the safety of journalists as potential indicator of rule of law, democracy and development.
Notes and expected action	Take note of information provided by the Secretariat on these Council of Europe initiatives and activities. Consider possible follow-up discussions in the CDMSI.

3.2. Human rights of Internet users

CM/Rec(2014)6	Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users
Notes and expected action	Take note of information provided by the Secretariat with regard to follow-up activities.

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

[1] As it appears in document CDMSI-BU(2014)OJ2, date 23/09/2014.

CDMSI(2014)006	Implementation of adopted standards
CDMSI (2014)012	List of CM standards related to safety of journalists
Notes and expected action	Discuss preparation of the new format (workshops) of the new item "Follow up of the implementation of CoE adopted standards in MS" agreed during the last CDMSI meeting (theme: safety of journalists on the basis of the information provided by the Secretariat.

5. Media

Standard setting activities

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

Terms of Reference	Terms of reference of the MSI-JO
MSI-JO(2014)01	Agenda of the 2nd meeting of the MSI-JO (6-7 October 2014)
MSI-JO(2014)03	Report of the 1st meeting of the MSI-JO
MSI-JO (2014)04	Proposal for collection of good practices, information document
	MSI-JO outline structure for draft recommendation on protection of journalism and safety of journalists
Notes and expected action	Take note of the information provided by the Secretariat and discuss elements for a draft recommendation on protection of journalism and safety of journalists and other media actors with a view to discussing the first draft of the recommendation at the next CDMSI plenary meeting in November (following the next MSI-JO meeting in October).

5.2 Hate speech

Campaign	No Hate Speech campaign
DDCP-YD/CHS (2014)2rev	Hate speech draft strategic objectives
	Presentation to CDMSI by young activist and Ms Bridget O'Loughlin, Campaign Co-ordinator of the No Hate Speech Movement.
Notes and expected action	Take note of the information provided by the Secretariat and discuss possible follow-up.

5.3 Gender equality and the media

CM/Rec(2013)01	Recommendation of the Committee of Ministers to member States on gender equality and media
CDMSI (2014)013	Implementation of the Committee of Ministers recommendation CM (2013)1 gender equality and media: Terms of reference toolkit implementation
CM(2013)136final	Gender Equality Strategy 2014-2017
Report	UNESCO Global Forum on Media & Gender – Report by Margaret Gallagher
	Gender Equality and the Media at national level - Compilation of good practices in member States
Notes and expected action	Take note of the information provided by the Secretariat and discuss possible follow up.

5.4 Transparency of media ownership

Resolution 2	Belgrade Resolution on Preserving the essential role of media in the digital age
CM Rec No.R(94)13	CM Recommendation No. R(94)13 on measures to promote media transparency
CM Dec (2007)	CM Declaration (2007) on protecting the role of the media in democracy in the context of media concentration
PACE motion of 30/01/2013	PACE motion of 30/01/2013 on "Increasing transparency of media ownership"
10 recommendations	Ten recommendations on transparency of media ownership, paper by Access Info
Conference programme	Conference on transparency of media ownership – Brussels, 24 September 2013
Presentation	Presentation by Fiona Harrisson (Access Info)
Agenda	Regional Conference Transparency in Media Ownership and Preventing Media Concentration, 25-26 September 2014, Skopje
	Digital Agenda for Europe (*New meeting*)- Exchange of best practices on transparency of media ownership, Brussels, 3 October 2014
Notes and expected action	Discuss possible follow up action.

5.5. Public service media

Resolution 2	Declaration of the Committee of Ministers on Public Service Media Governance

	Recommendation CM/Rec(2012)1 of the Committee of Ministers to member States on public service media governance Belgrade Resolution on Preserving the essential role of media in the digital age
Notes and expected action	Consider possible follow-up action or discussions in the CDMSI with regard to public service media matters.

6. Information Society and Internet Governance

Standard setting activities

6.1. Network Neutrality

CDMSI(2014)005Rev7	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
CDMSI(2014)Misc2 rev	Compilation of comments by CDMSI members.
Notes and expected action	Consideration of a revised version of the draft recommendation in light of comments by CDMSI members.

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

MSI-INT(2014)10	Report of the 2nd meeting of the MSI-INT (3-4 July 2014)
MSI-INT(2014)06rev2	Draft recommendation CM/Rec(2014)___ of the Committee of Ministers to member states on free transboundary flow of information on the Internet
MSI-INT(2014)07	Preliminary elements for a draft recommendation on Internet Freedom
Resolution 1	Belgrade Resolution on Internet Freedom
Notes and expected action	Take note of the information provided by the Secretariat on the progress of MSI-INT work. Discuss Draft recommendation CM/Rec(2014)___ of the Committee of Ministers to member states on free transboundary flow of information on the Internet with a view to its submission to the CDMSI plenary meeting in November for finalisation. Discuss preliminary elements for a draft recommendation on Internet freedom.

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

Internet Governance Strategy	Synthesis and follow-up chart to the Council of Europe Internet Governance Strategy 2012-2015 – verbal up-date by the Secretariat
CDMSI(2014)Misc4	Discussion elements for Internet Governance Strategy (2016-2019
CDMSI(2014)Misc3	Comments received on Council of Europe expert report on ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values
Notes and expected action	Take note of the information provided by the Secretariat on the state of implementation of the CoE Internet Governance Strategy 2012-2015. Take note of and discuss proposals by member states for the new Council of Europe 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)

EuroDIG programme	EuroDIG 2014
Messages	EuroDIG Messages from Berlin
IGF programme paper	*IGF 2014*
Notes and expected action	Take note of information provided by Committee members who participated in EuroDIG and IGF and of information from the Secretariat. Consider possible follow-up.

6.5 ICANN

DGI(2014)12	Council of Europe Expert Report: ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values
	Overview of comments by CDMSI members
Notes and expected action	Take note of information provided by the Secretariat. Take note and discuss comments by CDMSI members. Consider possible follow-up.

6.6 Other activities

NETmundial Multistakeholder Statement	NETmundial: Global multi-stakeholder meeting on the future of Internet governance (São Paulo, 23-24 April 2014)
WSIS + 10 Open Consultation Process	World Summit on Information Society (WSIS) +10 Review Process
GCIC	Global Commission on Internet Governance
	Contacts and cooperation with other international organisations
Notes and expected action	Take note of information provided by the Secretariat and consider possible follow-up discussion in the CDMSI. Discuss Council of Europe contribution to the WSIS +10 Review Process.

7. Cooperation activities

MEDIA.COOP(2014)04	On-going and planned activities in the fields of media
	On-going and planned activities in the field of Internet governance
Notes and expected action	Take note of on-going and planned activities. Consider possible CDMSI proposals.

8. Data protection

Standard setting activities

T-PD (2014) WP rev	Work programme of the T-PD for 2014-2015
T-PD(2014)RAP31Abr_rev	Abridged Report of the 31st Plenary meeting of the T-PD (2-4 June 2014)
T-PD(2014)08	T-PD Draft Recommendation on the processing of personal data in the context of employment (Presentation by T-PD Chair to CDMSI plenary)
ToR CAHDATA	Terms of reference of the ad hoc Committee on data protection (CAHDATA)
CAHDATA(2014)3	Working document – Convention 108 with Additional Protocol and Modernisation proposals
CAHDATA (2014)RAP02Abr	Abridged Report of the 2nd meeting (28-30 April 2014)
Notes and expected action	Take note of the state of play and information provided by the Secretariat. Examine the draft recommendation with a view to approval by CDMSI at its next meeting.

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

9.1 Participation of CDMSI in events and meetings

Agenda	New Media Literacy Leonardo da Vinci project – Seminar (Bratislava, 29-30 May 2014)
Agenda	Conference on "Orbital Slots and Spectrum Use in an Era of Interference" organised by the French Institute for International Relations (IFRI), Brussels, 9 October 2014
Notes and expected action	Take note of the information provided by Bureau members.

9.2 Parliamentary Assembly of the Council of Europe (PACE)

CDMSI(2014)009rev	CDMSI comments on PACE Recommendation 2041(2014) Improving user protection and security in the cyberspace List of documents under preparation in the PACE Committee on culture Science, Education and Media
CM/AS(2014)Rec2036	Reply adopted by the Committee of Ministers to "Revision of the European Convention on Transfrontier Television" Parliamentary Assembly Recommendation 2034 (2014)
Notes and expected action	Take note of comments finalised by the CDMSI via E-mail and information provided by the Secretariat with regard to PACE activities and initiatives of relevance to the work of the CDMSI.

10. Budget and administrative matters

11. Priorities of CDMSI work and working methods

Belgrade Political declaration and resolutions	Council of Europe Conference of Ministers responsible for Media and Information Society – Freedom of Expression and Democracy in the Digital Age – Opportunities, Rights, Responsibilities. Adopted Political Declaration and Resolutions
CM(2013)162	Council of Europe Conference of Ministers responsible for Media and Information Society (Belgrade, 7-8 November 2013) – Report of the Secretary General
CM decisions	Council of Europe Conference of Ministers responsible for Media and Information Society (Belgrade, 7-8 November 2013) – Decisions of the Committee of Ministers
CDMSI(2014)011	Priorities of CDMSI, information document
Notes and expected action	Discuss priorities for the work plan of the CDMSI on the basis of an information document prepared by the Secretariat. Discuss possible

	themes for hearings at the next CDMSI meeting.

12. Other questions

12.1 Co-operation with observers

CM/Res(2011)24	Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods.
Notes and expected action	Discuss co-operation with observers and application procedures for observer status in light of Resolution CM/Res(2011)24.

12.2 Application for observer status by Internet Watch Foundation

Application letter	Application letter
Memo IWF	Memorandum of Association of Internet Watch Foundation
Service Level Agreement Association ACPO/IWF	Service level agreement
Annual report 2013	IWF annual report
Human Rights Audit (2014)	2014 Audit
Notes and expected action	Discuss and recommend decision by the CDMSI on the application for observer status by Internet Watch Foundation.

12.3 Application for observer status by Press Club Prague

Application letter	Application letter
Notes and expected action	Discuss and recommend decision by the CDMSI on the application for observer status by Press Club Prague.

13. Draft agenda of the 7th CDMSI meeting (18-21 November 2014)

CDMSI(2014)OJ2	*Draft preliminary agenda of the 7th CDMSI meeting*

GENERAL REFERENCE DOCUMENTS

Terms of reference	CDMSI terms of reference 2012-2013
Terms of Reference	CDMSI terms of reference 2014-2015
CM/Res(2011)24	Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods
CM/Res(2011)7	Resolution CM/Res(2011)7 on Council of Europe conferences of specialised ministers
CDMSI(2014)001 Rev	List and timetable of meetings relevant to the CDMSI in 2014
Political declaration and resolutions	Council of Europe Conference of Ministers responsible for Media and Information Society – Freedom of Expression and Democracy in the Digital Age – Opportunities, Rights, Responsibilities. Adopted Political Declaration and Resolutions
CM(2013)162	Council of Europe Conference of Ministers responsible for Media and Information Society (Belgrade, 7-8 November 2013) – Report of the Secretary General
CM Decisions	Council of Europe Conference of Ministers responsible for Media and Information Society (Belgrade, 7-8 November 2013) – Decisions of the Committee of Ministers

RECENT MEETING REPORTS

CDMSI-BU(2014)002	Report of the 5th meeting of the Bureau of the CDMSI (19-20 March 2014)
CDMSI-(2014)008	Report of the 6th meeting of the CDMSI (20-23 May 2014)

Appendix 2 LIST OF PARTICIPANTS

6th MEETING OF THE BUREAU OF THE STEERING COMMITTEE ON MEDIA AND INFORMATION SOCIETY (CDMSI-BU), 24-25 September 2014

(Strasbourg, Council of Europe, Agora Building, Room G02)
(Gender distribution of the 6 Bureau members attending the meeting: 3 women (50%), 3 men (50%)

Ms Maja Rakovic (Chair/ Présidente), Counsellor, Ministry of Foreign Affairs, Serbia /Serbie

Mr Thomas Schneider, (Vice-Chair / Vice-président) International Affairs, Federal Office of Communication, Federal Department for the Environment, Transport, Energy and Communication, Switzerland/Suisse

Mr Mark Carvell, Media Team, Department for Culture, Media and Sport, United Kingdom /Royaume- Uni

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

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

Mr Emir Povlakic, Head of Division for Licensing, Digitalization and Coordination in Broadcasting, Communications Regulatory, Bosnia and Herzegovina/Bosnie-Herzegovine

Ms Bissera Zankova, Media Expert / Consultant, Ministry of Transport, IT and Communications, Bulgaria/Bulgarie

SECRETARIAT

Mr Jan Kleijssen, Director of the Information Society and Action against the Crime Directorate, Directorate General of Human Rights and Rule of Law (DG I)
Mr Jan Malinowski, Head of Information Society Department, DG I
Ms Silvia Grundmann, Secretary of the CDMSI, Head of Media Division, DGI
Ms Onur Andreotti, Administrator, Media Division, DG I
Ms Elvana Thaçi, Administrator, Media Division, DG I
Mr Lee Hibbard, Administrator, Internet Governance Unit, DG I
Ms Loreta Vioiu, Administrator, Internet Governance Unit, DG I
Mr Luca Belli, Programme Assistant, Internet Governance Unit, DGI
Ms Sophie Kwasny, Administrator, Data Protection Unit, DG I
Ms Giovanna Langella, Principal Administrative Assistant, Media Division, DG I

Appendix 3 Agenda of Seminar and inter-regional dialogue on the protection of journalists (Strasbourg 3 November 2014)

Seminar and Inter-regional Dialogue on the protection of journalists

Towards an effective framework of protection for the work of journalists and an end to impunity

http://www.inter-justice.org/

Organised by
Council of Europe
UNESCO
Centre for Freedom of the Media (CFOM), University of Sheffield
European Lawyer's Union / Union des Avocats Européens (ELU/UAE)

In cooperation with
Region of Alsace
City Council of Strasbourg
Inter-American Commission on Human Rights
African Commission on Human and Peoples' Rights
Media Legal Defence Initiative
Open Society Foundations

European Court of Human Rights, Strasbourg (PRESS ROOM)
Monday 3 November 2014
8.30 -18.00

The Organisers thank Open Society Foundations for supporting this event

United Nations Educational, Scientific and Cultural Organization

CENTRE FOR FREEDOM OF THE MEDIA CFOM

U A E

Union des avocats européens

DRAFT AGENDA (24.09.2014)

8.30-9.00 **REGISTRATION**

9.00 **OPENING REMARKS**

- Guido Raimondi, Vice-President of the European Court of Human Rights
- Nils Muižnieks, Commissioner for Human Rights, Council of Europe
- Philippe Boillat, Director-General, Directorate-General Human Rights and Rule of Law, Council of Europe
- Getachew Engida, UNESCO Deputy Director-General

9.30 – 11.00 **PANEL I. International and Regional Frameworks of protection: examining the evidence**

Moderator: William Horsley, International Director, Centre for Freedom of the Media, University of Sheffield

- The framework of legal protection for journalists at universal level
  Jane Connors, Director, Research and Right to Development Division, OHCHR
- Legal protections and protection mechanisms at regional level among the Organisation of American States
  Ona Flores, senior Attorney, Special Rapporteur for Freedom of Expression, Inter-American Commission on Human Rights, Organization of American States, United States
- The framework of legal protection at regional level: the case of the African Commission on Human and People's Rights
  Faith Pansy Tlakula, Special Rapporteur for Freedom of Expression and Access to Information, African Commission on Human and Peoples' Rights ***(tbc)***
- The protection of journalists in international criminal law
  James Stewart, deputy prosecutor, International Criminal Court (ICC)
- Panel discussion and interventions

11.00 – 11.20 ***Break***

11.20 – 12.30 **PANEL II. Protections for the rights of journalists exercising their public interest function: shortcomings, gaps and advances. *Perspectives of human rights lawyers, media and civil society***

Moderator: Grégory Thuan dit Dieudonné, European Lawyers Union

- Journalists and justice in conflict and in non-conflict zones
  Matthieu Mabin, senior reporter for France 24 TV
- Journalists' defenders: a lawyer's perspective
  Karinna Moskalenko, Director, International Protection Centre
- National protection programs: the Colombian model
  Maria Teresa Ronderos, Head of Open Society Foundations Program on Independent Journalism
- Treaty law as a 'living instrument': levelling up and enforcing the protections
  Barbora Bukovska, Article 19
- Panel discussion and interventions

12:30 – 14.30 ***LUNCH at the Council of Europe*** ***(details TBC)***

14.30 – 15.50 **PANEL III. Judicial and national cooperation to improve standards of protection, prevention and prosecution in cases relating to journalists and freedom of expression**

Moderator: Peter Noorlander, Chief Executive Officer, Media Legal Defence Initiative

- National jurisdictions and issues related to adherence to international norms: a global Overview
  Michael O'Flaherty, Est Professor in Human Rights Law, National University of Ireland Galway, former Vice-Chairperson of the UN Human Rights Committee
- Case studies and lessons drawn from the African experience
  Maureen Kondowe, Vice-President of the Pan African Lawyers Union (PALU)
- The role of special prosecutors and emergency protection mechanisms in Latin America

Eduardo Bertoni, Palermo University School of Law (Argentina) and former special rapporteur for Freedom of Expression of the Inter-American Commission of Human Rights at the Organization of American States

- Panel discussion and interventions

15.50 – 16.10 ***Break***

16.10 - 17.15 **PANEL IV. Agendas for an Inter-Regional Dialogue to strengthen protections and eradicate impunity**

Moderator: Prof. Dirk Voorhoof, University of Ghent

- Strategic litigation and interim measures in cases related to the protection of journalists in the Americas: Prevention, Protection and Prosecution

Catalina Botero, Special Rapporteur for Freedom of Expression, OAS (to 2014)

- International perspectives on Interim measures and positive obligations in the case law of regional human rights courts: the case of the European Court of Human Rights

Lawrence Early, Jurisconsult, Registry of the European Court of Human Rights

The case for a regional protection framework in Asia

Prof. Harry Roque, University of the Philippines, Manila

- Panel discussion and interventions

17.15 – 17.45 **Inter-regional dialogue: necessities, goals and expectations**

Moderator: David Kaye, UN Special Rapporteur on Freedom of Expression

- Manuel Ventura Robles, Judge at the Inter-American Court of Human Rights
- Sophia Akuffo, President of the African Court of Human and Peoples Rights ***(tbc)***
- Ayşe Işıl Karakaş, Judge at the European Court of Human Rights

17.45-17.55 **Rapporteurs' conclusions**

Dr. Tarlach McGonagle, Senior researcher, Institute for Information Law (IViR), Faculty of Law, University of Amsterdam

17.55-18.00 **Closing remarks:**

Jan Kleijssen, Director, Information Society and Action against Crime Directorate, Directorate General Human Rights and Rule of Law, Council of Europe

18.00 **End of Seminar**

19.00 – 21.00 **Drinks and Buffet dinner at Strasbourg City Hall**

Contact persons

CENTRE FOR FREEDOM OF THE MEDIA (CFOM)
William Horsley, william@inter-justice.org

COUNCIL OF EUROPE
Onur Andreotti, onur.andreotti@coe.int
Elisabeth Maetz, Assistant, elisabeth.maetz@coe.int

UNESCO
Ming Kuok Lim, mk.lim@unesco.org
Sylvie Coudray, s.coudray@unesco.org;

EUROPEAN LAWYERS' UNION
Gregory Thuan dit Dieudonné, gthuan@hincker-associes.com
Valeria Reva, Assistant, vreva@hincker-associes.com

* * *

Appendix 4 : Questions for CDMSI members (CDMSI(2014)Misc6)

Questions for CDMSI members on the implementation of the guidelines of the CM on eradicating impunity for serious human rights violations, in the context of safety of journalists (30 March 2011)

I. Have the guidelines of the CM on eradicating impunity for serious human rights violations been translated into the national language, have they been widely disseminated in particular among all authorities responsible for the fight against impunity?

II. Which are the existing mechanisms to ensure investigation and prosecution of attacks against journalists and other media actors?

III. The members are invited to provide information on the execution of ECtHR judgements related to safety of journalists and the issue of impunity, if there are such judgements v. their country. In case of difficulties in the execution of such ECtHR judgements, the members may wish to specify what are the main obstacles (i.e. legislation, practice, other) for the execution and what measures have been taken to overcome these.

IV. Are there any non-judicial mechanisms, such as parliamentary or other public inquiries, ombudspersons, independent commissions, as useful complementary procedures to the domestic judicial remedies guaranteed under the ECtHR, specifically dealing with threats and crimes targeting journalists and other media actors?

Appendix 5 Addendum to compilation of comments on the draft recommendation on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (Addendum to CDMSI(2014)Misc2rev 2 - 29 September 2014)

This document compiles all comments sent to the Secretariat by CDMSI delegations on the Draft Recommendation on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (contained in document CDMSI(2014)005Rev7) during the period of time from 5 September to 19 September 2014.

FRANCE
19/10/2014

We thank you for the opportunity to comment on this new version of the text. Thank you for the work that has been done. We find the text convenient with the exception of two small points of formulation explained in the attachment.
In any case we regret that this recommendation on network neutrality does not cover the neutrality of the value chain (as service platforms and applications)
Paragraph 1.2., 1st line, suggestion to delete the word equally and related comment " the concept of equality is very strict and impossible to put in place in practice (data packets take different paths, only the point of departure and the point of arrival are in common).The principle of non-discrimination is sufficient to attain the objective that is pursued".
Paragraph 5.1, last line, suggestion to add before the phrase "Internet speeds" the words "an estimation of".

GERMANY
21/09/2014

"I am sorry to inform you that due to the ongoing process of national decision finding the German Government neither has a final position on the substance of the draft nor on its proceeding. We would like to withdraw our comments that were made at an earlier stage of the draft."

THE RUSSIAN FEDERATION
19/10/2014

"Dear CDMSI members,
I have studied the remastered Draft recommendation on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (CDMSI (2014) 005Rev7 dated by August 19 of 2014 and appreciating the work done by the Secretariat and Bureau Members have to state with some regret that the fundamental ideas of the Russian position described at the last CDMSI meeting and the last June 20 Statement were not taken into account , the suggestions to balance the document were ignored. In this situation I have only to inform all of you that I can not give my approval for the Draft."

THE UNITED KINGDOM
19/10/2014
"Following further consultations with policy leads on net neutrality in the UK administration, the UK hereby requests an extension of the period for receiving comments on this important CM text until the start of the next Committee meeting in November. By that time we in UK will have had Ministerial clearance which necessarily also takes into account the progress and outcome of the current negotiations in Brussels. I hope therefore that CDMSI colleagues can agree to this extension of the period for comments."

Appendix 6 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 different legitimate purposes such as to preserve the integrity and security of the network. 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 Convention), 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.

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 Convention 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. Recalling the relevant Council of Europe standard-setting instruments[2] and with a view 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;

* As contained in document CDMSI(2014)005Rev7, date 19 August 2014

[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.

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

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 Convention, 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, 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.

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 to:

- give effect to a court order;

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

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

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

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.

3.4. In order to enable end-users to receive, press, radio and audiovisual media services of their choice through the Internet, 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 the right private life and personal data protection.

4.2. The use of techniques for the purpose of Internet traffic management, which are capable of assessing the content of communications, is an interference with the right to private life. Therefore, such use must be fully in line with Article 8 of the Convention, 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 7 Draft Recommendation CM/Rec(2014)___of the Committee of Ministers to member States on free transboundary flow of information on the Internet*

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 rights and freedoms set out in the European Convention on Human Rights (hereinafter the ECHR) and in the Universal Declaration on Human 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.

The right to freedom of assembly and association, as guaranteed by Article 11 of the ECHR, is similarly 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.

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 by such interferences.

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.

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 illegitimately interfere with access to information in other states or negatively impact the transboundary Internet traffic. States

* As contained in document MSI-INT (2014)06 Rev3, date 24 September 2014

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.

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, 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 actions and omissions within their territory pursue the legitimate aims set out in 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.

- [Evaluation] Regulatory or other measures that are capable of having such an impact must be evaluated 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 flows 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 must 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, support and participate as appropriate in 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 also should 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(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 8

Strasbourg, 15 April 2014 T-PD(2013)05rev_en

THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

(T-PD)

Draft Recommendation on the protection of personal data used for employment purposes

ANNEXE8 (T-PD(2013)05rev_en)

INDEX

ANNEXE8 (T-PD(2013)05rev_en)

DRAFT RECOMMENDATION CM/REC(2013)… OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE PROTECTION OF PERSONAL DATA USED FOR EMPLOYMENT PURPOSES.

(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 there are other interests (individual or collective, private or public) to be borne in mind when articulating principles for the employment;

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 domestic law to which the public authority or body is subject, in order to reconcile access to such official documents with the right to the protection of personal data pursuant to this 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 it continues 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 present recommendation and its Appendix, which replace the above-mentioned Recommendation (89)2, are reflected in the application of domestic legislation on data protection to the employment sector, as well as in other branches of the law bearing on the use of personal data for employment purposes,

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

- promote acceptance and implementation of the principles contained in the Appendix of this 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 taken into account in the design, deployment 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 this recommendation apply to any processing of personal data for employment purposes in both public and private sectors.

1.2. Unless domestic law provides otherwise, the principles of this 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.

1BIS. DEFINITIONS

For the purposes of this 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, interconnection, 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 search of personal data; where no automated processing is used, data processing means the operations carried out within a structured set established according to any criteria which allow to search for personal data ;

- 'Controller' means the natural or legal person, public authority, service, agency or any other body which alone or jointly with others has the decision-making power with respect to data processing;

- 'Processor' means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller;

- 'Recipient' means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

- 'sensitive data' covers genetic data, personal data concerning offences, criminal convictions and related security measures, biometric data uniquely identifying a person, as well as personal data for the information they reveal relating to racial origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life;

- 'Information systems' means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic 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' concern the relations between employers and employees which relate to recruitment and end of employees' labour affiliation, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as planning and organisation of work. 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 who has an employment relationship with an employee or a prospective employee and has the legal responsibility for the undertaking and/or establishment;

- 'Employee' or 'prospective employee' means any person concerned engaged by an employer under an employment relationship.

2. 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 free development of employees' personality and to foster possibilities of individual and social relationship on the workplace.

3. Application of data processing principles

[3.1. Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned and should anonymise data where relevant in line with additional conditions and safeguards set out in domestic law, or pseudonymise data where anonymisation is not possible.]

3.2. 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 employees' fundamental rights and freedoms of the data subjects.

4. Collection of data

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

4.2. Personal data collected for employment purposes should be relevant and not excessive, having regard to the nature of the employment as well as the legitimate needs of the employer in connection with its activities and where relevant, in line with additional conditions and safeguards set out in domestic law.

4.3. Employers should not have access to personal data that the employee shares with others where these data are not necessary for the assessment of the employ's ability to carry out his/ her duties.

4.4. Employers should take appropriate measures to ensure that, in particular for online data publicly available, only relevant, accurate and up-to-date data are processed, thus avoiding data to be used in a different context for which they were originally disclosed.

4.5. Health data may only be collected for the purposes set out in principle 9.2 of this Recommendation.

[5. Storage of data

5.1. 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. Such data should be relevant, adequate, accurate and necessary.

5.2. When evaluation data are stored relating to the performance or potential of employees, such data should only be based on 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. Employer should adopt data protection policies, rules and/or other instruments on internal use of personal data.

6.3. Where data are to be processed for employment purposes other than the purpose for which they were originally collected, the employer should take adequate measures to avoid misuse of the data in a different context and inform the employee.

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. Where substantive changes in the processing occur, the persons concerned should be informed.

7. Communication of data to employee's representatives, including the use of information systems and technologies

7.1. In accordance with domestic law and practice, or the terms of collective agreements, personal data may be communicated to employees' representatives, but only to the extent that such data are necessary to allow those representatives to properly represent the interests of the employees concerned or if such data are necessary for the fulfilment 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.

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 employer's legal obligations or in accordance with other provisions of domestic law.

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

a. where in line with additional conditions and safeguards set out in domestic law, the communication is necessary for employment purpose, the purposes are not incompatible with the purposes for which the data was originally collected and the employees concerned or their representatives, as the case may be, are informed of this; or

b. with the express consent of the individual employee; or

c. if the communication is provided for by domestic law.

8.3. The communication of personal data among a group of companies is lawful only if it is necessary for the purpose of discharging legal obligations or collective agreements and where additional conditions and safeguards are provided for by domestic law. The consent of the employee may also be required in appropriate cases as additional safeguard.

8.4. With regard to the public sector, for the provisions governing the disclosure of personal data to ensure government and other public authority/ body transparency and/or to monitor the correct use of public resources and funds should provide appropriate safeguards for individuals' right to privacy and protection of personal data.

9. Processing of sensitive data

9.1 The processing of sensitive data referred to in Principle 1bis of this Recommendation is only permitted in particular cases, where it is indispensable for the specific employment recruitment or to fulfil legal obligations related to the employment contract of employment. The processing is also conditional on the applicable law providing additional appropriate safeguards, complementing those set out in Convention 108 and in this Recommendation. Appropriate safeguards shall aim 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 is possible under conditions provided in Principle 18 of this Recommendation.

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

a. to determine his or her suitability for the present or future employment;

b. to fulfil the requirements of preventive medicine;

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

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

e. to allow social benefits to be granted; or

f. to satisfy judicial procedures.

The processing of genetic data, to determine for instance the professional suitability of employees or job applicants, is prohibited even with the consent of the person concerned.
Processing of genetic data may exceptionally be provided if it is provided by domestic law and subject to appropriate safeguards, in particular to avoid any serious prejudice to the health of the data subject or third parties.

9.3. Health data and - where their processing is lawful - genetic data should only be collected from the employee concerned except if otherwise determined by law, with appropriate safeguards.

9.4. Health data covered by the obligation of medical confidentiality should only be accessible to and processed by personnel who are bound by medical confidentiality or 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 employee's health; or
c. be necessary to prevent risks to others.

Where such data are communicated to the employer, this processing should be performed by a person duly authorised, such as personnel entitled with administration, 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.

9.5. Health data covered by medical confidentiality and - where their processing is lawful - genetic data, where appropriate should be stored separately from other categories of personal data held by the employer. Technical and organisational security measures should be taken to prevent persons outside the authorised medical service having access to the data.

9.6. The employee's right of access to his or her health data and genetic data should not be restricted unless access to such data could cause serious harm to the employee. Any such restriction must be in accordance with domestic law. The data may thus be communicated to the employee through a medical practitioner of his or her choice.

9.7. In any circumstances health data related to third parties will not be processed unless full unambiguous informed consent is given, such collection is authorised by a data protection supervisory authority, or the collection is mandatory according to domestic law.

10. Transparency of processing

10.1. Employees should be able to obtain information concerning their personal data held by the employer. This information can be provided directly or via their representative.

Except in relation to employees' name and habitual residence or establishment, employers should provide employees with the following information:

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

In this context, a particularly clear and complete description must be provided of the type 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 by Part II of this recommendation.

10.2 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. Employees 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. Employees should be entitled to have personal data rectified or erased, if they are inaccurate and/or if the data have been processed contrary to the law or the principles set out in this recommendation. They should also be entitled to object at any time to the processing of personal data concerning him/her 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 directly corrected by the employee, purely subjective assessments should be open to challenge in the manner laid down in domestic law.

11.4. Employees should not be subject to a decision significantly affecting him or her, based solely on an automatic 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/her.

11.6. Derogations to the rights referred to in paragraph 10, 11.1, 11.3 and 11.4 are permitted when they are provided for by law and constitute 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, the exercise of these rights may, in the case of an internal investigation conducted by the employer, be deferred until the closing of the investigation if the exercise of those rights would undermine/threaten 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, updated as appropriate. Such measures should be designed to ensure the security and confidentiality of personal data stored 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 Employers shall ensure adequate data security when using ICTs for the processing of employees' personal data for employment purposes.

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

13. Preservation of data

13.1. Personal data should not be retained by an employer for a period longer than is justified by the purposes outlined in Principle 1.3 or is required by the interests of a present or former employee.

13.2. Personal data submitted in furtherance of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made.

Where such data are stored with a view to a further job opportunity, the person concerned should be informed in due time and his or her data should be deleted if requested by the person.

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 fulfilment of the purpose.

13.3 Personal data processed for the purpose of an internal investigation carried out by an employer 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 up to the time at which they are deleted.

Part II - Particular forms of processing

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

14.1 The introduction and use of ICTs for monitoring employees should be done with respect of the principles of legitimacy, relevance and proportionality, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards. Employers should strike a fair balance, between the employees' right to respect for private life and the employer's interest in the protection of his property rights.

14.2. The use of such systems for the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted where it leads to the deliberate and systematic surveillance of a specific employee, or a specific group of employees. Exceptions may be considered, with due safeguards, when monitoring is not the main purpose pursued by the employer but is just an indirect consequence of a surveillance needed to protect production, health, safety or work organisations. The use of video surveillance for monitoring occurrences at locations that are part of the most personal area of life of an employee is not permitted.

14.3 In the event of dispute or legal proceedings, employees should be able to obtain copies of the recording made.

15. Internal reporting mechanism

Where employers are obliged by law or internal rules to implement internal reporting mechanisms, such as hotlines, employers should secure 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, law or judicial order.

Where applicable, employers should enable anonymous reporting. However, 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 domestic law infringements.

16. Use of Internet and e-mails in the workplace

16.1 The employer should avoid unjustifiable and unreasonable interferences with employee's 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 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 electronic messages.

16.2 In particular, in respect of the possible 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, providing first for non-individual random checks on data which are anonymous or in some way aggregated.

16.3 Access to professional emails of employees who have been informed in advance of the existence of that possibility can only occur [in accordance with the law and] where necessary for security or other lawful reason. In case of absent employees, the employer should take the necessary measures and foresee the appropriate procedures aimed at enabling, access to professional emails only when such access is of professional necessity. Further access must be undertaken in the least intrusive way possible and only after having informed the employees concerned.

16.4 In any case, the content, sending and receiving of private emails at work shall not be monitored.

16.5 When an employee leaves the organisation, the employer should take the necessary organisational and technical measures to automatically deactivate the employee's account upon his or her departure. If the employer needs to recover the contents of the employee's account for the efficient running of the company, he shall do so before the departure of the employee and when feasible, at his or her presence.

17. Equipment revealing employees' whereabouts

17.1 While devices revealing the location of employees can be used in the interests of the employees (for instance to enable the determination of an occupational injury), their use shall not lead to a permanent or excessive monitoring of employees. Given the potential to violate the rights and freedoms of persons presented by the use of these devices, employers should

ensure all necessary safeguards for the employee's right to privacy and protection of personal data, including the additional safeguards provided for in principle 21. Employers shall in particular pay special attention to the purpose for which such devices are used. Notably, monitoring should not be the main purpose, but only an indirect consequence of action needed to protect production, safety or work organisations.

17.2 When an employee, following his or her employer's instructions or with the knowledge and approval of the latter, uses professional devices outside the company or institution premises, enabling the employer to acquire knowledge of the employee's location, the collection and further processing of that personal data must be exclusively limited to the strict verification of the fulfilment of professional duties or organisational aspects.

17.3 Employers shall apply appropriate internal procedures relating to the processing of these data and shall notify it to the persons concerned in advance.

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 the employer, 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 shall be subject to the requirements of strict security and proportionality. The employee should be in control of the processing of his/ her biometric data.

19. Psychological tests, analysis and similar procedures

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

19.2 These tests, analysis and similar procedures should not take place without the employees or job applicants consent, and domestic law should provide appropriate safeguards, including the additional safeguards provided for in principle 21. The employee's consent should be free, informed and without any financial or other compensation foreseen. The employee or job applicant should be informed in advance of the use that will be made of the results of these tests, analyses or similar procedures and, subsequently, the content thereof.

20. Other processing posing specific risks to employees' rights

20.1 Employer or where applicable processors, should carry out a risk analysis of the potential impact of the intended data processing on the employee's 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 information or consultation procedure referred to in principle 14 reveals such risks.

21. Additional safeguards

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

- Inform the employees before the use of any surveillance/ monitoring system. The information provided should be kept up to date and should be undertaken taking into account principle 10 of the 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;

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

- 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;

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