

**Recommendation CM/Rec(2016)5^[1]
of the Committee of Ministers to member States
on Internet freedom**

*(Adopted by the Committee of Ministers on 13 April 2016
at the 1253rd meeting of the Ministers' Deputies)*

1. The European Convention on Human Rights (ETS No. 5, hereinafter “the Convention”) applies both offline and online. The Council of Europe member States have negative and positive obligations to respect, protect and promote human rights and fundamental freedoms on the Internet.
2. Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection in compliance with the Convention and the International Covenant on Civil and Political Rights. The member States of the Council of Europe should take a proactive approach to implementing the Convention and other Council of Europe standards with regard to the Internet. The understanding of Internet freedom should be a comprehensive one and firmly based on these standards.
3. Internet governance arrangements, whether national, regional or global, must build on this understanding of Internet freedom. States have rights and responsibilities with regard to international Internet-related policy. In the exercise of their sovereign rights, States should, subject to international law, refrain from any action that would directly or indirectly harm persons or entities inside or outside of their jurisdiction. Any national decision or action restricting human rights and fundamental rights on the Internet must comply with international obligations and in particular be based on law. It must be necessary in a democratic society, fully respect the principles of proportionality and guarantee access to remedies and the right to be heard and to appeal with due process safeguards.
4. As part of their obligation to secure to everyone within their jurisdiction the rights and freedoms enshrined in the Convention, States should create an enabling environment for Internet freedom. To this end, it is recommended that States carry out regular evaluations of the Internet freedom environment at the national level, with a view to ensuring that the necessary legal, economic and political conditions are in place for Internet freedom to exist and develop. Such evaluations contribute to a better understanding of the application of the Convention to the Internet in member States and to its better implementation by national authorities.
5. The Convention and other Council of Europe standards provide benchmarks and references for national evaluations of Internet freedom. They can be considered as indicators which guide and enable member States to identify existing or potential challenges to Internet freedom, as an analytical framework to evaluate the implementation of human rights standards on the Internet and as a reference for developing international policy and approaches relating to the Internet.
6. The Council of Europe should play a key role in promoting Internet freedom in Europe and globally. Building on member States' national evaluations, the Council of Europe can observe the evolution of regulatory frameworks and other developments in its member States and provide regular overviews on the challenges to Internet freedom in Europe. This would be a good basis for further development of Council of Europe Internet-related policies.

7. The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, recommends that member States:

- periodically evaluate the level of respect for and implementation of human rights and fundamental freedom standards with regard to the Internet, using the indicators in the appendix to this recommendation, with a view to elaborating national reports, wherever appropriate;
- ensure the participation of all stakeholders from the private sector, civil society, academia and the technical community, in their respective roles, in the evaluation of the state of Internet freedom and preparation of national reports;
- consider sharing, on a voluntary basis, information or national reports on Internet freedom with the Council of Europe;
- be guided by and promote these indicators when participating in international dialogue and international policy making on Internet freedom;
- take appropriate measures to promote the United Nations “Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect, and Remedy’ Framework”.

Appendix to Recommendation CM/Rec(2016)5

Internet freedom indicators

Internet freedom is understood as the exercise and enjoyment on the Internet of human rights and fundamental freedoms and their protection in compliance with the Convention. These Internet freedom indicators focus on the right to freedom of expression, the right to freedom of assembly and association, the right to private life and the right to an effective remedy. They build on the existing and established human rights standards and enforcement mechanisms. A comprehensive approach to Internet freedom considers all indicators as they are intended to provide guidance in conducting a qualitative and objective evaluation of and reporting on Internet freedom in Council of Europe member States. They are not designed to rate the levels of Internet freedom or as a means of comparing countries.

1. An enabling environment for Internet freedom

1.1. The protection of human rights and fundamental freedoms on the Internet is guaranteed in law, in full compliance with the Convention.

1.2. Any State interference with the exercise of human rights and fundamental freedoms on the Internet complies with the Convention.

1.3. Laws and policies relating to the Internet are assessed, at their drafting stage, with regard to the impact that their implementation may have on the exercise of human rights and fundamental freedoms.

1.4. Laws and policies relating to the Internet are developed by State authorities in an inclusive and transparent process which enables the participation of all stakeholders, including the private sector, civil society, academia and the technical community.

1.5. Any State body which has regulatory or other competence over Internet matters carries out its activities free from political or commercial interference, in a transparent manner and protects and promotes Internet freedom.

1.6. The State protects individuals from cybercrime through effective criminal justice or other measures. Where such measures risk interference with the right to private life, the right to freedom of expression or the right to freedom of peaceful assembly and association, they are subject to conditions and safeguards against abuse. These measures comply with Articles 8, 10 and 11 of the Convention. Notably they are prescribed by a law, which is accessible, precise, clear and foreseeable; pursue a legitimate aim; are necessary and proportionate in a democratic society and allow for effective remedies.

1.7. The State formulates policies and takes measures to implement the United Nations “Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect, and Remedy’ Framework”.

1.8. The State provides media and digital literacy programmes for users to foster their ability to make informed decisions and to respect the rights and freedoms of others. It promotes access to and use of educational, cultural, scientific, scholarly and other content.

2. The right to freedom of expression

2.1. Freedom to access the Internet

2.1.1. The Internet is available, accessible and affordable to all groups of the population without any discrimination.

2.1.2. The public has access to the Internet in facilities supported by public administration (Internet access points), educational institutions or private owners (universal community service).

2.1.3. The State takes reasonable measures to ensure access to the Internet to those with low income, in rural or geographically remote areas and those with special needs such as persons with disabilities.

2.1.4. There are no general, nationwide restrictions on access to the Internet except when this is in compliance with Article 10 of the Convention.

2.1.5. The State recognises in law and in practice that disconnecting individuals from the Internet, as a general rule, represents a disproportionate restriction of the right to freedom of expression.

2.1.6. Any restriction of Internet access, including in penitentiary institutions, complies with the conditions of Article 10 of the Convention regarding the legality, legitimacy and proportionality of restrictions on freedom of expression and the positive obligation of the State to protect the right to freedom of expression.

2.1.7. Before restrictive measures to Internet access are applied, a court or independent administrative authority determines that disconnection from the Internet is the least restrictive measure for achieving the legitimate aim. The continuing necessity of the restrictive measure is evaluated by these authorities on a continuing basis. These conditions do not apply to cases of non-payment by users for their Internet services.

2.1.8. When restrictive measures are applied, the person concerned has the right to due process before a court or an independent administrative authority whose decisions are subject to judicial review, in compliance with Article 6 of the Convention.

2.2. Freedom of opinion and the right to receive and impart information

2.2.1. Any measure taken by State authorities or private-sector actors to block or otherwise restrict access to an entire Internet platform (social media, social networks, blogs or any other website) or information and communication technologies (ICT) tools (instant messaging or other applications), or any request by State authorities to carry out such actions complies with the conditions of Article 10 of the Convention regarding the legality, legitimacy and proportionality of restrictions.

2.2.2. Any measure taken by State authorities or private-sector actors to block, filter or remove Internet content, or any request by State authorities to carry out such actions complies with the conditions of Article 10 of the Convention regarding the legality, legitimacy and proportionality of restrictions.

2.2.3. Internet service providers as a general rule treat Internet traffic equally and without discrimination on the basis of sender, receiver, content, application, service or device. Internet traffic management measures are transparent, necessary and proportionate to achieve overriding public interests in compliance with Article 10 of the ECHR.

2.2.4. Internet users or other interested parties have access to a court in compliance with Article 6 of the Convention with regard to any action taken to restrict their access to the Internet or their ability to receive and impart content or information.

2.2.5. The State provides information in a timely and appropriate manner to the public about restrictions it applies to the freedom to receive and impart information, such as indicating websites that have been blocked or from which information was removed, including details of the legal basis, necessity and justification for such restrictions, the court order authorising them and the right to appeal.

2.3. Freedom of the media

2.3.1. The editorial independence of media operating on the Internet is guaranteed in law, policy and practice. They are not subjected to pressure to include or exclude information from their reporting or to follow a particular editorial direction.

2.3.2. Media are not required to obtain permission or a licence from the government or State authorities, beyond business registration, in order to be allowed to operate on the Internet or blog.

2.3.3. Journalists and other media actors using the Internet are not subject to threats or harassment by the State. They do not practise self-censorship because of fear of punishment, harassment or attack.

2.3.4. The confidentiality of journalists' and other media actors' sources is protected in law and respected in practice.

2.3.5. Media websites and websites of new media actors are not affected by cyber-attacks or other action disrupting their functioning (for example, denial of service attacks).

2.3.6. There are prompt and effective investigations of threats and crimes against journalists and new media actors. There is no climate of impunity.

2.4. Legality, legitimacy and proportionality of restrictions

2.4.1. Any restriction of the right to freedom of expression on the Internet is in compliance with the requirements of Article 10 of the Convention, namely it:

- is prescribed by a law, which is accessible, clear, unambiguous and sufficiently precise to enable individuals to regulate their conduct. The law ensures tight control over the scope of the restriction and effective judicial review to prevent any abuse of power. The law indicates with sufficient clarity the scope of discretion conferred on public authorities with regard to the implementation of restrictions and the manner of exercise of this discretion;
- pursues a legitimate aim as exhaustively enumerated in Article 10 of the Convention;
- is necessary in a democratic society and proportionate to the legitimate aim pursued. There is a pressing social need for the restriction, which is implemented on the basis of a decision by a court or an independent administrative body that is subject to judicial review. The decision should be targeted and specific. Also, it should be based on an assessment of the effectiveness of the restriction and risks of over-blocking. This assessment should determine whether the restriction may lead to disproportionate banning of access to Internet content, or to specific types of content, and whether it is the least restrictive means available to achieve the stated legitimate aim.

2.4.2. The State does not impose undue restrictions to freedom of expression on the Internet in its legislation. Defamation laws are specific and narrowly defined as to their scope of application. They do not inhibit public debate or criticism of State bodies and do not impose excessive fines or disproportionate awards of damages or legal costs. Severe sanctions, such as imprisonment, are applied only when the fundamental rights of other people have been seriously impaired such as in cases of incitement to violence or hatred.

2.4.3. Laws addressing hate speech or protecting public order, public morals, minors, national security or official secrecy and data protection laws are not applied in a manner which inhibits public debate. Such laws impose restrictions of freedom of expression only in response to a pressing

matter of public interest, are defined as narrowly as possible to meet the public interest and include proportionate sanctions.

3. The right to freedom of peaceful assembly and association

3.1. Individuals are free to use Internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards.

3.2. Associations are free to use the Internet in order to exercise their right to freedom of expression and to participate in matters of political and public debate.

3.3. Individuals are free to use Internet platforms, such as social media and other ICTs in order to organise themselves for purposes of peaceful assembly.

3.4. State measures applied in the context of the exercise of the right to peaceful assembly which amount to a blocking or restriction of Internet platforms, such as social media and other ICTs, comply with Article 11 of the Convention.

3.5. Any restriction on the exercise of the right to freedom of peaceful assembly and right to freedom of association with regard to the Internet is in compliance with Article 11 of the Convention, namely it:

- is prescribed by a law, which is accessible, clear, unambiguous and sufficiently precise to enable individuals to regulate their conduct;
- pursues a legitimate aim as exhaustively enumerated in Article 11 of the Convention;
- is necessary in a democratic society and proportionate to the legitimate aim pursued. There is a pressing social need for the restriction. There is a fair balance between the exercise of the right to freedom of assembly and freedom of association and the interests of the society as a whole. If a less intrusive measure achieves the same goal, it is applied. The restriction is narrowly construed and applied, and does not encroach on the essence of the right to freedom of assembly and association.

4. The right to private and family life

4.1. Personal data protection

4.1.1. The right to private and family life is guaranteed in compliance with Article 8 of the Convention. Any restriction to this right pursues one of the legitimate aims exhaustively enumerated in Article 8 of the Convention, is necessary in a democratic society and proportionate to the legitimate aim pursued.

4.1.2. The law guarantees that all personal data is protected in compliance with Article 8 of the Convention and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) in States which have ratified it.

4.1.3. Personal data are processed lawfully (with the unambiguous consent of the data subject or on the basis of law) for legitimate purposes and not in excess of such purposes, accurately and securely. These conditions apply also to profiling (personal data automatic processing techniques that collect and use information about an individual in order to identify, analyse or predict his or her personal preferences, behaviour and attitudes).

4.1.4. Individuals are not subjected to a decision significantly affecting them based solely on automated processing of data without having their views taken into account. There are effective processes enabling every individual to obtain, on request, information on the processing of his or her personal data and the reason underlying processing; to object to processing; to obtain, on request, rectification or erasure of the personal data; and to consent to, object to or withdraw consent to personal data processing or profiling. An effective remedy exists for individuals when these rights are not respected. Legal frameworks for personal data protection provide adequate safeguards for access to information and freedom of expression.

4.1.5. The law defines the duties of public and private entities with regard to processing of personal data.

4.1.6. A supervisory authority, which acts with complete independence and impartiality, ensures compliance with data protection legal frameworks.

4.1.7. The State does not prohibit, in law or in practice, anonymity, pseudonymity, confidentiality of private communications or the usage of encryption technologies. Interference with anonymity and confidentiality of communications is subject to the requirements of legality, legitimacy and proportionality of Article 8 of the Convention.

4.2. Surveillance

4.2.1. Surveillance measures taken by public authorities (such as security services) comply with the requirements of Article 8 the Convention and are subject to effective, independent and impartial oversight.

4.2.2. Surveillance measures are carried out in accordance with the law, which is accessible, clear, precise and foreseeable. The law contains safeguards for the exercise of discretion by public authorities and thus defines with sufficient clarity and precision:

- the nature of offences which may give rise to surveillance measures;
- the competent authorities that carry out surveillance measures, the scope of any discretion conferred on such authorities and the manner of its exercise having regard to the legitimate aim of the measure in question;
- the categories of individuals liable to be subjected to surveillance measures;
- time limitations for carrying out surveillance measures;
- the procedures for examining, using and storing data obtained from surveillance measures;

- the precautions to be taken when communicating data acquired through surveillance measures to other parties and the measures applicable during the communication to ensure data security;
- the circumstances for the destruction and erasure of data obtained from surveillance measures;
- the bodies responsible for overseeing surveillance measures.

4.2.3. Surveillance measures pursue a legitimate aim as exhaustively enumerated in Article 8 of the Convention, are necessary in a democratic society and proportionate to the legitimate aim pursued.

4.2.4. Surveillance measures carried out by State authorities either directly or through/in collaboration with private-sector entities are authorised by an independent and impartial tribunal established by law or another State body which is independent from both the authorities carrying out such measures and the executive.

4.2.5. Surveillance measures carried out by State authorities either directly or through/in collaboration with private-sector entities do not involve activities which weaken encryption systems and the integrity of communication infrastructure (for example built-in flaws and backdoors in security, information and communication systems).

4.2.6. Surveillance measures are subject to an effective review assured by a judicial authority or oversight by another State body offering the best guarantees of impartiality and independence from the authorities carrying out surveillance or the executive.

4.2.7. The law guarantees the right of an oversight body to have access to all information which is relevant to the fulfilment of its mandate, regardless of the level of information classification. Access to information by an oversight body extends to all relevant information held by public authorities, including information provided by foreign bodies.

4.2.8. Oversight bodies exercise their powers, including seeking and handling classified information and personal data, professionally and strictly for the purposes for which they are conferred by law while ensuring that the information is protected from being used or disclosed for any purpose that is outside the mandate of such bodies.

4.2.9. Oversight bodies scrutinise, within their competences, the human rights compliance of surveillance measures taken by public authorities, including those taken in co-operation with foreign bodies through the exchange of information or joint operations.

4.2.10. Judicial authorities and oversight bodies have the power to quash and discontinue surveillance measures when such measures are deemed to be unlawful, and the power to require the deletion of any information obtained from the use of such measures.

4.2.11. Public authorities that carry out surveillance measures and their oversight bodies are not exempt from the ambit of freedom of information legislation. Decisions not to provide information are taken on a case-by-case basis, properly justified and subject to the supervision of an independent

information or data protection commissioner. Oversight bodies make informative versions of their periodic and investigation reports available to the public.

5. Remedies

5.1. The State ensures that individuals have access to judicial or administrative procedures that can impartially decide on their claims concerning violations of human rights online, in compliance with Article 6 of the Convention.

5.2. The State provides for the right to effective remedy in compliance with Article 13 of the Convention. This includes effective non-judicial mechanisms, administrative or other means for seeking remedy such as through national human rights institutions. There are no legal, procedural, financial or other practical barriers that individuals encounter in seeking an effective remedy.

5.3. The State, as the primary responsible entity, takes appropriate steps to protect against human rights abuses with regard to the Internet by private-sector actors and to ensure that those affected have access to an effective remedy.

5.4. The State implements policies and measures to encourage all private-sector actors to respect human rights with regard to the Internet throughout their operations, in particular by establishing effective complaint mechanisms to address early and remedy directly grievances of individuals whose human rights and fundamental freedoms on the Internet may be adversely impacted. These mechanisms are legitimate (enabling trust, accountable for the fair conduct of grievance processes), accessible (known by those concerned, without barriers to access), predictable (providing a clear and known procedure with an indicative time frame for each stage, clarity of types of process and outcome available, and means of monitoring implementation), equitable (reasonable access to sources of information, advice and expertise necessary to engage in a complaint process), transparent (keeping parties informed about the progress of a complaint) and compatible with Article 13 of the Convention.

[1] When adopting this recommendation, the Permanent Representative of the Russian Federation indicated that, in accordance with Article 10.2c of the Rules of Procedure for the meetings of the Ministers' Deputies, he reserved the right of his government to comply or not with the recommendation, in so far as it referred to the methodology for its implementation at national level.

