MSI-NET(2016)05rev4

Draft Recommendation CM/Rec(2017)xxx of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries

FINAL DRAFT AS OF 19 SEPTEMBER 2017

Preamble

1. In line with the jurisprudence of the European Court of Human Rights (hereinafter "the Court"), Council of Europe member states have the obligation to secure to everyone within their jurisdiction the rights and freedoms contained in the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, hereinafter "the Convention"), both offline and online. Access to the internet is a precondition for the exercise of Convention rights and freedoms on the Internet.

2. By enhancing the public's ability to seek, receive and impart information without interference and regardless of frontiers, the internet plays a particularly important role with respect to the right to freedom of expression. It also enables the exercise of other rights protected by the Convention and its Protocols, such as the right to freedom of assembly and association, the right to education, access to knowledge and culture, as well as participation in public and political debate and in democratic governance.

3. The protection of privacy and personal data is a foundation for the enjoyment and exercise of most of the rights and freedoms guaranteed in the Convention. However, the internet has facilitated an increase of privacy-related risks and infringements and has spurred the spread of certain forms of harassment, hatred and incitement to violence, in particular on the basis of gender, race and religion, which remain under-reported and rarely remedied or prosecuted. Moreover, the rise of the internet and related technological developments have triggered substantial challenges for the maintenance of public order and national security, for crime prevention and law enforcement, as well as for the protection of the rights of others, including intellectual property rights**.**

4. A wide, diverse and rapidly evolving range of actors, commonly referred to as internet intermediaries, facilitate interactions between natural and legal persons on the internet by offering and performing a variety of functions and services. Some connect users to the internet, enable the processing of information and data, or host web-based services, including for user-generated content. Others aggregate information and enable searches, and give access to, host and index content and services designed and/or operated by third parties. Some facilitate the sale of goods and services, including audio-visual services, and enable other commercial transactions, including payments.

5. Intermediaries may carry out several functions in parallel. They may also moderate and rank content, including through automated processing of personal data, and may thereby exert forms of control which influence users' access to information online in ways comparable to media, or they may perform other functions that resemble those of publishers. Intermediary services may also be offered by traditional media, for instance, when space for user-generated content is offered on their platforms. The regulatory framework governing the intermediary function is without prejudice to the frameworks that are applicable to the other functions offered by the same entity.

6. The rule of law is a prerequisite for the protection and promotion of the exercise of human rights and for pluralistic and participatory democracy. Member states have the negative obligation to refrain from violating the right to freedom of expression and other human rights in the digital environment. They also have a positive obligation to protect human rights and to create an enabling and safe environment for everyone to participate in the public debate and to express their opinions and ideas without fear, including those that offend, shock, or disturb the state or any sector of the population. This positive obligation to ensure the exercise and enjoyment of rights and freedoms includes, due to the horizontal effects of human rights, the protection of individuals from actions of private parties by ensuring compliance with relevant legal and regulatory frameworks. It is further indispensable that due process guarantees are in place and access to effective remedies is facilitated vis-à-vis both states and intermediaries with respect to the services in question.

7. It is further essential to support initiatives promoting media and information literacy skills for accessing and managing the digital space. Such efforts should be implemented through various means, including formal and non-formal education, with a view to promoting the effective and equal enjoyment of the rights enshrined in the Convention by everyone without discrimination of any kind. Given the particularly high number of young and child users of the internet, the importance of empowering, protecting, and supporting children in their safe access to rights in the digital environment must be acknowledged throughout. To this end, sustained engagement is required to enhance skills among children, parents and educators on how to deal with an information and communications environment that provides access to degrading content of a sexual or violent nature which might be harmful.

8. The regulatory framework governing the services provided by or through intermediaries is diverse, multi-layered and continuously evolving. States are confronted with the complex challenge of regulating an environment in which private actors fulfil a crucial role in providing services with significant public service value. The task of regulation is further complicated by the global nature of the internet networks and services, by the diversity of intermediaries, by the volume of internet communication, and by the speed at which it is produced and processed. Owing to the fact that intermediaries operate or are used across many countries, including in a cloud-computing context, their actions may further have effects under several, sometimes conflicting, laws of different jurisdictions.

9. Internet intermediaries also develop their own rules, usually in form of terms of service or community standards that often contain content restriction policies. Moreover, intermediaries collect, generate, retain and process a wealth of information and data from and about users. These activities may interfere with, among other rights, the users' rights to privacy and freedom of expression. Effective reporting and complaints

mechanisms may be lacking, be insufficiently transparent and efficient, or be provided only through automated processes.

10. In line with the UN Guiding Principles on Business and Human Rights and the Protect, Respect and Remedy Framework, intermediaries should respect the human rights of their users and affected parties in all their actions. This includes the responsibility to act in compliance with applicable laws and regulatory frameworks. Owing to the multi-functionality of intermediaries, their corresponding duties and responsibilities and their protection under law, must be determined with respect to the specific services and functions that are performed.

11. A variety of network effects and mergers have led to the existence of fewer, larger entities that dominate the market in a manner that may jeopardise the opportunities for smaller intermediaries or start-ups and places them in positions of influence or even control of principal modes of public communication. The power of such intermediaries as protagonists of online expression makes it imperative to clarify their role and impact on human rights as well as their corresponding duties and responsibilities.

12. Against this background and in order to provide guidance to all relevant actors who are faced with the complex task of protecting and respecting human rights in the digital environment, the Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, recommends that member states:

- implement the Guidelines included in this recommendation when developing and implementing legislative frameworks relating to internet intermediaries in line with their obligations under the Convention, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, hereinafter "Convention 108"), the Convention on Cybercrime (ETS No. 185, "the Budapest Convention"), the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (ETS No. 201, "the Lanzarote Convention"), and the Convention on Preventing and Combating Violence against Women and Domestic Violence (ETS No. 210, "the Istanbul Convention) and promote them in international and regional forums that deal with the roles and responsibilities of internet intermediaries;

- take all necessary measures to ensure that internet intermediaries fulfill their responsibilities to respect human rights in line with the UN Guiding Principles on Business and Human Rights and the Recommendation CM/Rec (2016)3 of the Committee of Ministers to member states on human rights and business;

- in implementing the Guidelines, take due account of Committee of Ministers Recommendation 2016/5 on internet freedom; Recommendation 2016/1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality; Recommendation 2015/6 on the free, trans-boundary flow of information on the internet; Recommendation 2014/6 on a Guide to human rights for internet users; Recommendation 2013/1 on gender equality and media; Recommendation 2012/3 on the protection of human rights with respect to search engines; Recommendation 2012/4 on the protection of human rights with respect to social networking services; Recommendation 2011/7 on a new notion of media; Recommendation 2010/13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling; Recommendation 2007/16 on measures to promote the public service value of the internet; the 2017 Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data; the 2008 Guidelines for the cooperation between law enforcement and internet

service providers against cybercrime, and the Human Rights guidelines for internet service providers, developed in 2008 by the Council of Europe in co-operation with the European Internet Service Providers Association which, as far as the responsibilities of internet service providers are concerned, are reinforced by this Recommendation.

- engage in a regular, inclusive and transparent dialogue with all relevant stakeholders, including from the private sector, public service media, civil society, education establishments and academia, with a view to sharing and discussing information and promoting the responsible use of emerging technological developments related to internet intermediaries that impact the exercise and enjoyment of human rights and related legal and policy issues;

- encourage and promote the implementation of effective age and gender-sensitive media and information literacy programmes to enable adults, young people and children to enjoy the benefits and minimise the exposure to risks of the online communications environment, in cooperation with all relevant stakeholders, including from the private sector, public service media, civil society, education establishments and academia.

Guidelines on the protection and promotion of human rights and fundamental freedoms with regard to internet intermediaries

1 – Duties and obligations of states

1.1 Legality

1.1.1. Any request, demand or other action by public authorities addressed to internet intermediaries that interferes with human rights and fundamental freedoms must be prescribed by law and must constitute a necessary and proportionate measure in a democratic society. All powers of public authorities in relation to internet intermediaries must be prescribed by law and exercised within the limits conferred by law. States should not use informal means to circumvent the guarantees offered by formal legal proceedings.

1.1.2. Laws, regulations and policies applicable to internet intermediaries, regardless of their objective or scope of application, including commercial and non-commercial activities, shall effectively safeguard human rights and fundamental freedoms, and shall maintain adequate guarantees against arbitrary application in practice.

1.1.3. States shall not seek to absolve themselves from their ultimate obligation to protect human rights and fundamental freedoms in the digital environment. All regulatory frameworks, including self- or co-regulatory approaches, must include effective oversight mechanisms to comply with that obligation and must be accompanied by appropriate legal redress opportunities.

1.1.4. The process of enacting legislation or regulations applicable to internet intermediaries should be transparent and inclusive. States should regularly consult with all relevant stakeholders with a view to ensuring that an appropriate balance is struck between the public interest, the interests of the users and affected parties, and the interest of the intermediary. Before adopting legislation or regulations, states should conduct human rights impact assessments to understand potential negative impacts on human rights in order to prevent or mitigate these.

1.1.5. States shall ensure that legislation, regulation, and policies related to internet intermediaries are interpreted, applied and enforced without discrimination, also taking into account multiple and intersecting forms of discrimination. The prohibition of discrimination may in some instances require special measures to address specific needs or correct existing inequalities. States should further take into account the substantial differences in size, function and organisational structure of intermediaries when developing, interpreting and applying the legislative framework in order to prevent possible discriminatory effects.

1.1.6. States should ensure that legislation, regulation and policies relating to internet intermediaries are effectively implementable and enforceable and that they do not unduly restrict the operation and free flow of trans-border communication.

1.2. Legal certainty and transparency

1.2.1. Any legislation applicable to internet intermediaries and to their relations with states and users must be accessible and predictable. All laws should be clear and sufficiently precise to enable intermediaries, users and affected parties to regulate their conduct. The laws should create a safe and enabling online environment for private communications and public debate and should comply with relevant international standards.

1.2.2. Any legislation must include clear limits to the powers, discretionary or non-discretionary, granted to public authorities in relation to internet intermediaries, particularly when exercised by the executive branch and specifically by law enforcement. The law must indicate the scope of such discretion to protect against arbitrary application.

1.2.3. States should make publicly available, in a timely and regular manner, comprehensive information on the number, nature and legal basis of restrictions of human rights, such as regarding content restrictions or disclosure of personal data, that they have applied in a certain period through requests addressed to intermediaries, including those based on international mutual legal assistance treaties, and on actions taken as a result of those requests. States should require intermediaries to disclose clear (easily accessible and machine-readable) and meaningful information about interferences with the exercise of rights and freedoms in the digital environment, whether based on court or administrative orders, private complainants' requests, or enforcement of their own content restriction policies.

1.2.4. With a view to avoiding legal uncertainty and conflicts of laws, states should commit to cooperating with each other and with all relevant stakeholders in cases where different laws apply, and should support the development of common approaches and jurisdictional principles, including through appropriate non-state forums.

1.3. Safeguards for freedom of expression

1.3.1. Any request, demand or other action by public authorities addressed to internet intermediaries to restrict access (including blocking or removal of content), or any other measure that interferes with the right to freedom of expression, must be prescribed by law, pursue one of the legitimate aims foreseen in Article 10 of the Convention, be necessary in a democratic society and proportionate to the aim pursued. State authorities must carefully evaluate possible, including unintended, impacts of any restrictions before and after applying them, while seeking to apply the least intrusive measure necessary to meet the policy objective.

1.3.2. State authorities should obtain an order by a judicial authority or other independent administrative authority whose decisions are subject to judicial review when demanding intermediaries to restrict access to content. All exceptions must also be clearly prescribed by law, pursue one of the legitimate aims foreseen in Article 10, be necessary in a democratic society and proportionate to the aim pursued.

1.3.3. When internet intermediaries restrict access to third-party content, state authorities should ensure that intermediaries provide effective redress mechanisms and adhere to due process guarantees. When intermediaries remove content based on their own terms of service, state authorities should not consider this as a form of control that makes them liable for the third-party content they give access to.

1.3.4. State authorities should consider the adoption of appropriate legislation to prevent strategic lawsuits against public participation (SLAPP) or abusive and vexatious litigation against users, content providers and intermediaries which is intended to curtail the right to freedom of expression.

1.3.5. State authorities should not directly or indirectly impose a general obligation on intermediaries to monitor content which they merely give access to, or which they transmit or store, be it by automated means or not. When addressing any request to internet intermediaries or promoting, alone or with other states or international organisations, co-regulatory approaches by internet intermediaries, state authorities should avoid any action that may lead to general content monitoring. They should further consider that any content monitoring performed through automated means is unable to assess context properly. All co-regulatory approaches must comply with rule of law and transparency safeguards.

1.3.6. The imposition of disproportionate sanctions on intermediaries for non-compliance with regulatory frameworks is likely to lead to restriction of lawful content. It therefore has a chilling effect for the right to freedom of expression. In addition, content monitoring risks interfering with user's enjoyment of their right to privacy.

1.3.7. States should ensure in law and in practice that intermediaries are not held liable for third-party content, to which they merely give access to or which they transmit or store. State authorities may hold intermediaries co-responsible with respect to content that they store, if they do not act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature, including through notice-based procedures. State authorities should ensure that notice-based procedures are not designed in a manner that incentivises the take-down of legal content, such as through inappropriately short timeframes. Notices should contain sufficient information for intermediaries to act upon. Notices submitted by states should be based on their own assessment of the illegality of the notified content. Content restrictions should allow notice of such restriction as early as possible to the content producer/issuer, unless this interferes with ongoing law enforcement activities. Information should also be made available to users seeking access to the content, in accordance with applicable data protection laws.

1.3.8. In order to ensure that content identical to that which has previously been determined to be illegal by a judicial authority or other independent administrative authority whose decisions are subject to judicial review, is effectively prevented from being accessed, states should co-operate closely with intermediaries to secure the restriction of such content in line with the principles of legality, necessity and proportionality. Such restrictions should not prevent the legitimate use of identical or similar content in other contexts.

1.3.9. In cases where the function of intermediaries consists of producing or managing content available on their platforms or where intermediaries perform curatorial or editorial-like functions, including through operation of algorithms, state authorities should apply an approach that is graduated and differentiated, in line with Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media. States should determine corresponding levels of protection as well as duties and responsibilities according to the role that intermediaries play in content production and dissemination processes, while paying due attention to their obligation to protect and promote pluralism and diversity in the online distribution of content.

1.3.10. When determining the applicable duties and responsibilities of intermediaries who are engaged in curatorial or editorial-like functions, including the production and dissemination of content, states should encourage appropriate self-regulatory or the development of co-regulatory mechanisms, taking due account of the extent that their action may negatively affect pluralism and diversity of online content, as well as the ability of the intermediary to provide services of public value, such as platforms for public discourse and democratic debate, as protected by Article 10 of the Convention.

1.4. Safeguards for privacy and data protection

1.4.1. Any demand or request by state authorities addressed to internet intermediaries to access, collect or intercept personal data of their users, including for criminal justice purposes, or any other measure which interferes with the right to privacy, must be prescribed by law, must pursue one of the legitimate aims foreseen in Article 8 of the Convention and Article 9 of Convention 108, and must be used only when it is necessary and proportionate in a democratic society to the aim pursued. The protection of the right to privacy and data protection extends to devices used to access the internet or store data.

1.4.2. State authorities should ensure that their legal frameworks and the ensuing policies and practices of intermediaries uphold the principles of data processing (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage time limitations, and data security, including integrity and confidentiality,) and guarantee the rights of the data subject in full compliance with Convention 108, providing also for the oversight of an independent authority within the meaning of Article 1 of the Additional Protocol concerning Supervisory Authorities and Trans-border Data Flows.

1.4.3. State authorities should protect the right to confidentiality of all private communications facilitated by internet intermediaries, extending to the content of the communication as well as metadata, and should ensure that appropriate levels of data protection and respect for privacy are also guaranteed in situations of trans-border data flows.

1.4.4. Surveillance measures undertaken by states, whether in co-operation with internet intermediaries or not, must be targeted, precisely defined, and must comply with Article 8 of the Convention as well as Article 9 of Convention 108. They must in particular be mandated by law, necessary in a democratic society and proportionate to the aim pursued, and they must include sufficient oversight, procedural safeguards and redress mechanisms. All surveillance must

be authorised by a judicial authority or other independent administrative authority whose decisions are subject to judicial review.

1.4.5. State authorities should ensure that appropriate complementary safeguards, such as explicit consent of the data subject, apply to the automatic processing of special categories of data as defined in Article 6 of Convention 108.

1.5. Access to an effective remedy

1.5.1. States should guarantee accessible and effective judicial and non-judicial procedures that ensure the impartial review of all claims of violations of Convention rights in the digital environment, such as the right to privacy, right to freedom of expression, or the right not to be discriminated against, in compliance with Article 6 of the Convention.

1.5.2. States should guarantee an effective remedy for all violations of human rights and fundamental freedoms by internet intermediaries, in compliance with Article 13 of the Convention. They should further ensure that intermediaries provide access to prompt, transparent and effective reviews of user or affected party grievances and alleged terms of service violations, and provide for effective remedies. These may include various forms, such as restoration of content, apology, rectification and damages. Judicial review must remain available, when internal and alternative dispute settlement mechanisms prove insufficient or where the affected parties opt for judicial redress or appeal.

1.5.3. States should proactively seek to reduce all legal, practical or other relevant barriers that could lead to a denial of access to an effective remedy for grievances of users, affected parties and internet intermediaries.

1.5.4. States should support age- and gender-sensitive media and information literacy promotion activities to ensure that all users are effectively made aware of their rights and freedoms, in particular regarding their right to access to an effective remedy vis-à-vis both state authorities and internet intermediaries. The promotion of media and information literacy should encompass education about the rights of all stakeholders, including other users and affected parties.

2 - Responsibilities of internet intermediaries with regard to human rights and fundamental freedoms

2.1. Respect for human rights and fundamental freedoms

2.1.1. Internet intermediaries should in all their actions respect the internationally recognised human rights and fundamental freedoms of their users and of other parties who are affected by their activities. This responsibility, in line with the UN Guiding Principles on Business and Human Rights, exists independently of the states' ability or willingness to fulfil their own human rights obligations.

2.1.2. The responsibility of intermediaries to respect human rights and to employ adequate measures applies regardless of their size, sector, operational context, ownership structure, or nature. The scale and complexity of the means through which intermediaries meet their responsibilities may vary, however, taking into account the severity of the possible human rights impact of the services provided by the intermediary. The higher the impact and the potential damage to the objects of legal protection and the higher the value of the services for the exercise of human rights, the greater the precautions that the intermediary must employ when developing and applying policies, community standards, and codes of ethics aiming, notably, at the prevention of the spread of abusive language and imagery, of hatred and of incitement to violence.

2.1.3. Any interference by intermediaries with the free and open flow of information and data should be based on clear and transparent policies and must be limited to specific legitimate purposes, such as to restrict access to content that has been determined as unlawful by a judicial authority or other independent administrative authority whose decisions are subject to judicial review, or in accordance with their own content restriction policies or codes of ethics.

2.1.4 Internet intermediaries should carry out regular due diligence assessments of their compliance with the responsibility to respect human rights and fundamental freedoms and with their applicable duties. To this end, they should conduct assessments of the direct and indirect human rights impacts of their current and possible future policies, products and services on users and affected parties, and ensure appropriate follow-up to these assessments by acting upon the findings, and monitoring and evaluating the effectiveness of identified responses. Intermediaries should conduct these assessments as openly as possible and encourage active user engagement. In all their actions they should be mindful of the public service value of the services they deliver and should seek to avoid and mitigate any adverse effects on the effective exercise of rights by their users or affected parties.

2.1.5. Internet intermediaries should seek to provide their products and services without discrimination. They should seek to ensure that their actions do not have direct or indirect discriminatory effects or harmful impacts on their users or other parties affected by their actions, including on those who have special needs or disabilities or may face structural inequalities in their access to human rights. Intermediaries should further take reasonable and proportionate measures to ensure that their terms of service agreements, community standards and codes of ethics are applied and enforced consistently and in compliance with applicable due process safeguards. The prohibition of

discrimination may under certain circumstances require that intermediaries make special provisions for certain users or groups of users in order to correct existing inequalities.

2.2. Transparency and accountability

2.2.1. Internet intermediaries should ensure that all terms of service agreements and policies specifying the rights of users and all other standards and practices for content moderation and the processing and disclosure of user data are publicly available in clear, plain language and accessible formats. When operating globally, intermediaries should translate such documents into the languages that their users and affected parties understand. Users should be notified in advance of all changes in relevant policies regarding their terms of service and operating conditions as applicable and without delay, and in formats that they can easily access and understand, including explanatory guides.

2.2.2. The process of developing and applying terms of service agreements, community standards and content restriction policies should be transparent, accountable and inclusive. Intermediaries should seek to collaborate and negotiate with consumer associations, human rights advocates, and other organisations representing the interests of users and affected parties, as well as with data protection authorities before adopting and modifying their policies. Intermediaries should seek to empower their users to engage in processes of evaluating, reviewing and revising, where appropriate, intermediaries' policies and practices.

2.2.3. Internet intermediaries should clearly and transparently provide meaningful public information about the operation of automated data processing techniques in the performance of their functions, including the operation of algorithms that facilitate searches based on user profiling or the distribution of algorithmically selected and personalised content, such as news. This should include information on which data is being processed, which criteria are used, and for what purpose the processing takes place.

2.2.4. Intermediaries should regularly publish transparency reports that provide clear (easily accessible and machine-readable) and meaningful information about all interference and all requests for such interference with the free and open flow of information and ideas and related to requests for data access and preservation, whether based on court orders, international mutual legal assistance treaties, private complainant's requests or enforcement of their own content restriction policies.

2.3. Content moderation

2.3.1. Internet intermediaries should respect the rights of users to receive and impart information, opinions and ideas. They should not on a general basis monitor content to which they merely give access, or which they transmit or store, as a result of a state order or request. Any measures taken to restrict access (including blocking or removal of content) as a result of a state order or request must be necessary and be implemented through the least restrictive means, following a careful assessment of their effectiveness and proportionality to the legitimate aim pursued.

2.3.2. When restricting access to content in line with their own content restriction policies, intermediaries should do so in a transparent and non-discriminatory manner. All content restrictions must be performed by the least restrictive technical means and must be only as broad and maintained for as long as strictly necessary to avoid the collateral restriction or removal of legal content.

2.3.3. Any restriction of content must be limited in scope to the precise remit of the order or request and should be accompanied with information to the public, explaining which content has been restricted and on what legal basis. Notice should also be given to the user and, as appropriate, other affected parties, including information on procedural safeguards, opportunities for adversarial procedures for both parties as appropriate, and available redress mechanisms.

2.3.4. All staff of intermediaries who are engaged in content moderation should be given adequate initial and on-going training on the applicable laws, international human rights standards, their relationship with the intermediaries' terms of service and their internal standards, as well as on the action to be taken in case of conflict. Such training may be provided internally or externally, including through intermediary associations, and should in its scope correspond to the importance of the intermediaries' role and the impact that their actions may have on the ability of users to exercise their freedom of expression. Staff should further be provided with appropriate working conditions. This includes the allocation of sufficient time for deciding on the legality of content and opportunities to seek professional support and qualified legal advice where necessary.

2.3.5. Given that automated means of content identification used to prevent the reappearance of specific items of previously restricted content have limited ability to assess context, intermediaries should carefully assess the human rights impact of automated content management, and should ensure human review where appropriate. They should take into account the risk of over- and under-blocking as a result of inexact algorithmic systems, and the effect this may have on the services that they provide for public debate. Restrictions of access to identical content should not prevent the legitimate use of such content in other contexts.

2.3.6. In cases where content is restricted by intermediaries in line with their own content restriction policies because it contains an indication of a serious crime under international law, restriction must be accompanied by adequate measures to ensure that evidence is retained for effective criminal law investigations. If intermediaries have specific knowledge of such restricted content, they should report this to a law enforcement authority without undue delay.

2.4. Use of personal data

2.4.1. Intermediaries should not disclose personal data unless required by law or requested to do so by a judicial authority or other independent administrative authority whose decisions are subject to judicial review that has determined that the disclosure is consistent with applicable laws and standards, necessary in a democratic society and proportionate to the legitimate aim pursued.

2.4.2. Internet intermediaries should limit the processing of personal data from users to what is necessary in the context of a clearly defined purpose, which is explicitly communicated to all users in a proactive manner. The processing,

including collection, retention, aggregation, linking or sharing of personal data must be based on the free, specific, informed and unambiguous consent of the user, with respect to a specific purpose, or on another legitimate basis laid down by law, as prescribed by Convention 108. Complementary safeguards, such as explicit consent, should be applied to the automatic processing of special categories of data, as defined in Article 6 of Convention 108.

2.4.3. Intermediaries should minimise the processing of personal data in light of the purposes for which they are processed. 'Privacy by default' and 'privacy by design' principles should be applied at all stages with a view to prevent or minimise the risk of interference with the rights and fundamental freedoms of users. User data should only be aggregated and migrated across multiple devices or services following the free, specific, informed and unambiguous consent of users. Users should have the option of using a service without agreeing to such combining of their data.

2.4.4. Users have the right to access their personal data and to obtain correction of it, and they should be informed about it in clear and plain language. They should further be informed clearly about the conditions under which they may exercise the right to data erasure, to object to the processing of data, and to withdraw consent provided for the processing of personal data, following which all processing based on the consent of the user should be terminated.

2.4.5. Intermediaries should act in line with applicable legal conditions and safeguards regardless of where the collection of data has occurred and including with respect to trans-border data flows.

2.4.6. Any tracking and profiling of users by intermediaries should be fully transparent towards users. In order to protect their users' identity, internet intermediaries should not employ profiling and digital tracking techniques that infringe on the user's exercise of human rights. Intermediaries should seek to protect their users from tracking and profiling by third parties. Adequately trained staff should oversee all matters related to the disclosure of user data to third parties in line with the intermediaries' responsibilities and duties under international personal data protection and privacy standards. A person subjected to a decision that is taken on the basis of profiling or affected by legal consequences stemming from that decision, should be able to object to that decision.

2.5. Access to an effective remedy

2.5.1. Internet intermediaries should make available – online and offline – effective remedies and dispute resolution systems that provide prompt and direct redress in cases of user, content provider and affected party grievances. While the complaint mechanisms and their procedural implementation may vary with the size, impact and role of the internet intermediary, all remedies must allow for an impartial and independent review of the alleged violation. These should - depending on the violation in question - include inquiry, explanation, reply, correction, apology, reinstatement, reconnection and compensation.

2.5.2. Complaint mechanisms, including notice-based procedures, should comply with due process safeguards and should be accessible, equitable, rights-compatible, affordable and transparent. They should further include in-built safeguards to avoid conflicts of interest when the company is directly administering the mechanism, for example, by involving oversight structures. Complaints

mechanisms should be handled without unwarranted delays and should not negatively impact the opportunities for complainants to seek recourse through national, including judicial, review mechanisms.

2.5.3. Intermediaries should ensure that all users and other parties affected by their actions have full and easy access to transparent information in clear and easily understandable language about applicable complaints mechanisms, the various stages of the procedure, indicative time frames, and expected outcomes.

2.5.4. Intermediaries should not include in their terms of service waivers of rights or hindrances to the effective access to remedies, such as mandatory jurisdiction outside of a user's country of residence or non-derogable arbitration clauses.

2.5.5. Intermediaries should seek to provide access to alternative review mechanisms that can facilitate the resolution of disputes that may arise between users. Intermediaries should not, however, make alternative dispute mechanisms obligatory as the only means of dispute resolution.

2.5.6. Intermediaries should engage in dialogue with consumer associations, human rights advocates and other organisations representing the interests of users and affected parties, as well as with data protection authorities, to ensure that their complaint mechanisms are designed, implemented, and evaluated through participatory processes. They should further regularly analyse the frequency, patterns and causes of complaints received in order to learn lessons for improving their policies, procedures and practices and for preventing future grievances.

2.5.7. Intermediaries should engage in and promote targeted age- and gender-sensitive efforts to promote the awareness of all users of their rights and freedoms in the digital environment, both vis-à-vis states and intermediaries, including in particular information about applicable complaints mechanisms and procedures. The promotion of media and information literacy should encompass education about the rights of all stakeholders, including other users and affected parties.