Internetivabaduse hindamise näitajad ehk indikaatorid

Indicators	Evaluation	Comments
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.		