The same rights that people have offline must also be protected online, including the right to privacy, as the Human Rights Council and the General Assembly have repeatedly affirmed.

In its recent consensual resolution on the right to privacy in the digital age (A/HRC/42/15) the Human Rights Council has outlined some aspects concerning emerging digital technologies and human rights: The rapid pace of technological development enables individuals all over the world to use information and communications technology. However, it also enhances the capacity of Governments, business enterprises and individuals to undertake surveillance, interception, hacking and data collection, which may violate or abuse human rights, in particular the right to privacy, and is therefore an issue of increasing concern.

Despite its positive effects, the use of artificial intelligence that requires the processing of large amounts of data, often related to personal data, including on an individual’s behaviour, social relationships, private preferences and identity, can pose serious risks to the right to privacy, in particular when employed for identification, tracking, profiling, facial recognition, behavioural prediction or the scoring of individuals. Without adequate safeguards the use of artificial intelligence may pose the risk of reinforcing discrimination, including structural inequalities. On 8 April 2019, the EU High-Level Expert Group on AI presented Ethics Guidelines for Trustworthy Artificial Intelligence. EU Commission President-designate Ursula von der Leyen announced to put forward legislation for a coordinated European approach on the human and ethical implications of artificial intelligence. International human rights law needs to be applied in the design, development, deployment, evaluation and regulation of new technologies, and is must be ensured that these technologies are subject to adequate safeguards and oversight.

In the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association.

States must ensure a safe, secure and high-quality data infrastructure and develop human-centred auditing mechanisms, as well as redress mechanisms. Individuals whose rights may have been violated or abused must have access to an effective remedy, including reparation and guarantees of non-repetition. States should develop or maintain legislation, preventive measures and remedies addressing damage caused by the processing, use, sale or multiple resale or other corporate sharing of personal data without the individual’s free, explicit and informed consent and

take appropriate measures to ensure that digital or biometric identity programmes are designed, implemented and operated with appropriate legal and technical safeguards in place and in full compliance with international human rights law.

Business enterprises should meet their responsibility to respect human rights in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, including the right to privacy in the digital age. They should ensure that individuals have access to their data, and the possibility to amend, correct, update and delete the data, in particular if the data are incorrect or inaccurate, or if the data were obtained illegally. Business enterprises should put in place adequate safeguards seeking to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services, including where necessary through contractual clauses, and promptly inform relevant domestic, regional or international oversight bodies of abuses or violations when misuse of their products and services is detected.

**Concerning the specific questions for states we would like to add the following information:**

In your country, which government agency has an initiative in the decision-making of new and emerging digital technologies policies?

„The German Federal Government established a Data Ethics Commission. The Data Ethics Commission intends to offer answers to key questions related to the use of algorithms, artificial intelligence and the handling of data. Its mandate is to develop ethical guidelines based on scientific and technical expertise to protect individuals, maintain social cohesion and preserve and promote prosperity in the information age. On 23 October 2019, the Commission will submit its report on ethical guidelines for data policy and the use of algorithms, artificial intelligence and digital innovations to the Federal Government. It will also make recommendations for action.“

Does your country have a special agency that exclusively deals with the issues of new and emerging digital technologies? (for example: The Disruption Council in Denmark, The Presidential 4th Industrial Revolution Committee in Korea) If so, how much does the agency take the human rights issues into account in its agenda?

„Following our coalition agreement, the Federal Government decided in August 2018 to establish an Agency for Innovation in Cyber Security The past years have shown that there is a gap in Germany in terms of support and funding for risky digital and technological innovation in cyber security. Closing this gap is in Germany’s fundamental interest. This is why the Federal Ministry of Defense and  the Federal Ministry of the Interior, Building and Community decided to fund and support ambitious and promising basic research and technological innovation projects in cyber security as well as selected key technologies.

The core task of the agency will be to create meaningful networks with existing and future public institutions but also with academia and the private sector to safeguard the internal and external security of Germany A high level of technological ambition coupled with a healthy willingness to take risks is to drive innovation in a way and at a speed so far unheard of in Germany and Europe.

In addition, in 2017 the Central Office for Information Technology in the Security Sector (ZITiS) was set up to strengthen the capabilities of the German security authorities in a transparent, secure and efficient way.

As an authority dedicated solely to research and development, the purpose of ZITiS isto provide technical support to the Federal Criminal Police Office, the Federal Police and the Federal Office for the Protection of the Constitution.

The Federal Government also decided to set up an Agency to Promote Breakthrough Innovations (Agentur für Sprunginnovation), and that the Research and Economic Affairs Ministries would have the lead responsibility for this. This new Agency is to support innovations involving radically new technologies offering great potential to transform the market in the form of new products, services and value chains.