



Ministry of Digital Policy, Telecommunications and Media

Contribution to the questionnaire sent by the United Nations Human Rights

Commissioner's office regarding the right to privacy in the digital age

Each democratic society should function in a social environment that indisputably protects people's right for privacy covering many aspects of their daily lives and allowing them their unobstructed personal development. The rise of the information age has set new standards on the ways we relate to each other, we define ourselves and we perform our duties in the offline as well as the online world. The interaction in the digital environment leads to the development of new behaviors governing our personal, professional and commercial relationships. Providing personal data becomes an integral part of these interactions although the safeguards for their appropriate use are often in absence.

The vast array of opportunities and threats raised by the digital age are intrinsically linked to the automation "principle", the rise of the artificial intelligence and the dominance of "smart engines" that replace partly the human intervention at different stages of the production and communication processes. New possibilities emerge due to exceeding time and place limits as well as challenges related mainly to the limited control users have over their personal data which circulate the electronic environment. In this context, a redefinition of human's rights is needed (being enriched by the "digital" aspect) while we need to explore the ways in which new technologies can provide the remedies in situations that they seem to originate. In accordance to the international conventions and guidelines on human rights, States should remain vigilant to react properly with legislative initiatives and other updated policies in order to offer adequate protection to individuals against these risks.

Greece's legislative framework

In Greece, the basic legislative text governing the protection of personal data is Law 2472/1997 which has incorporated the 95/46/EU Directive. By the same Act, the Hellenic independent Authority for Communication Security and Privacy (ADAE) was established in 2003 and remains until today in full operation. The digital parameter is inserted in legislation more emphatically in 2001, when Article 9A was added in the revised Greek Constitution stipulating that each individual has the right to be protected from the collection, processing and (unauthorized) use of his personal data, especially by **electronic means**. Laws 3741/2006, 3783/2009, 3917/2011

enriched further the protective framework regulating more specifically the sector of electronic communications, including telecommunications. Moreover, our domestic legislative system follows the recent developments at the European level concerning the implementation of the new General Data Protection Regulation as well as the e-Privacy Directive.

Encryption and anonymity

Encryption constitutes a preferable technical method which can transform the data in such a way that an unauthorized user would not be able to access, read or interpret the processed data. The Hellenic independent Authority for Communication Security and Privacy (ADAE) has issued regulation 165/2011 for the assurance of confidentiality in Electronic Communications. The Regulation creates an obligation for the providers of electronic communications networks and services to develop and implement a Security Policy for the Assurance of Communications Confidentiality with the use of algorithms and encryption systems. Sometimes though it is essential to overcome other challenges that relate mainly to cases where encryption methods are used from malicious users for illegal purposes and criminal offences are committed. Despite these possible “side effects”, the implementation of such methods should not be discouraged as they are of great value for the solid protection of the personal data of users. For these reasons, competent authorities should be alert to exploit the potentials offered by the encryption methodology as well as to recognize and address cases of negative encryption’ use.

Children and other vulnerable groups

Children represent a major target group for providers who realize the ongoing and wider participation of minors in the world of electronic communications. The creation of children-tailored spaces, based mainly on the safety principle, remains inadequate to address all the challenges that arise as far as it concerns the circulation of their personal data and the limited control over them. In this context, the importance of *digital literacy* grows even stronger as minors (together with adults and prominently vulnerable groups) need to be empowered with relevant guidance in order to be extremely cautious when it comes to share personal information in the virtual world. Moreover, the legislative framework must be stricter in these cases by acknowledging that children and vulnerable groups (such as disabled persons) require intensified protection when processing their personal data. Relevant measures could possibly include stronger limitations on the collection and use of children’s communications data, a possible prohibition for websites specifically targeted towards children to use controversial marketing techniques, as well as focused protection from software that is developed for children.

Ministry of Digital Policy, Telecommunications and Media: Strategy and targeted actions

The Ministry of Digital Policy, Telecommunications and Media, through the competent authority of Secretariat General for Digital Policy, remains in close collaboration with other ministries and regulatory authorities (such as the ADAE) in order to ensure the immediate transposition of the GDPR in the Greek legislation. In this context and in order to protect the public sector specifically, a strategic plan was drafted involving the development of an integrated security system as well as the creation of a platform that will adopt all technical, procedural and organizational measures required for the protection of the information systems.

The Secretariat General for Digital Policy, within its spheres of competence:

- Promotes educational and communication actions for the empowerment of the staff operating and supporting public systems and infrastructures of high-importance
- Aims at the wider development of the digital skills of the public and the creation of a solid digital culture for the citizens by encouraging partnerships between public and private organisations
- Has created a strategic plan for innovation, research and development actions concerning security issues through the promotion of partnerships between the public and the private sector aiming at the cooperation and mutual exchange of expertise at European and international level, among decision-making bodies. The primary objective is the ongoing improvement and protection against cyber-attacks, with a special emphasis on the protection of public infrastructures.

Finally, it is worth to note that in order to solidify an integrated approach towards the protection of human rights in the digital environment, the Greek Ministry of Digital Policy, Telecommunication and Media signed on March 30th 2018 a Memorandum of Cooperation with the Greek Ministry of Justice, Transparency and Human Rights. The basic aim of this project lies in the promotion of the use all available digital tools for positive actions in the field of human 'rights protection and the pursuance of justice.