METAMORPHOSIS
Foundation for Internet and Society

Recommendations for the draft National ICT Strategy 2021-2025 and the accompanying Action Plan related to the right to privacy

(Recommendations are given in the context of the implementation of the Law on Personal Data Protection (Official Gazette of RNM no. 42/20) and the GDPR-General Data Protection Regulation 2016/679)

- In the process of strengthening the IT capacities of the institutions, apart from the IT professionals, a key human resource that needs to be seriously planned is the Personal Data Protection Officer. **The role of the Personal Data Protection Officer** is elevated to a higher level where expertise and independence come first. To ensure efficiency in the fulfillment of the obligations, the institutions are obliged to ensure that the Personal Data Protection Officer is adequately and timely involved in all issues related to personal data protection and support them in performing the tasks, providing them with all necessary resources and access to personal data and processing operations.
- When defining the infrastructure of the central secure data center, especially in the part of downloading all applications of all ministries, agencies, institutions, universities and hospitals, it should be borne in mind that many of the existing applications do not have the principles of personal data Every institution that has an application through which personal data are processed should analyze it, evaluate it and obligatorily harmonize its functionalities with the Law on Personal Data Protection before submitting it to the data center at all. Non-compliant collections of personal data, applications and other e-tools can only further weaken the system of security and protection of personal data, and thus jeopardize the security of the central data center itself.
- There is an essential difference between the e-services of the institutions which are an alternative way of obtaining the service (and not an additional service that the citizens could not otherwise receive) and those services that are only available to the citizens electronically (and the citizens could not otherwise receive). This is a key issue that must be taken into account in centralizing the delivery of e-services. For services that are only accessible to citizens electronically, the principles of “only once” and channel selection will have to be revised and their application re-evaluated.
- The adoption of a communication strategy and the planning of promotional activities must not be forced before it is previously checked whether the existing e-services are supported by Privacy Policies, whether all the principles for protection of privacy in the provision of e-service are respected and whether the institutions have defined ways and channels through which citizens can request the exercise of their right to privacy.
- The government should ensure that the work of each ministry, body, institution and public enterprise that offers e-services is harmonized with the Law on Personal Data Protection. This is especially significant because the principle of Security by design refers

EU with YOU
The project is co-funded by the European Union

ICEDA
Increasing Civic Engagement in the Digital Agenda

to new services, tools, applications, and not to the existing ones that are expected to be redefined following the principles of the Law on Personal Data Protection.

- The government should ensure that every institution offering e-services respects the principles of "legality, fairness and transparency"; "limitation of objectives"; "minimum data volume"; "accuracy"; "limitation of the storage period"; "integrity and confidentiality" and "accountability".
- In the context of establishing a Center for Safer Internet for Children, the Government should support the transposition process of **Directive (EU) 2016/680 of the European Parliament and the Council for the Protection of Individuals about the processing of personal data by the competent authorities to prevent, investigate, detect or prosecute criminal offences or for carrying out criminal sanctions and for the free movement of this data** which ensures the use of technological means by the police which are not invasive to privacy. This directive is the second key regulation, in addition to the General Data Protection Regulation (GDPR) in the field of personal data protection which should be part of the national legislation.
- When creating new e-services or tools, especially for services for the provision of which there is no legally prescribed procedure (such as, for example, StopKorona, vaccination.mk, MOJ DDV), the Government should support the institutions in the process of conducting analysis and privacy impact assessment as a mandatory first step before deciding to create the e-service or tool itself.
- The relationship between the Government and other entities should be clearly defined and it should be known which entity at any time appears in the role of a personal data processor, the user of personal data or a third party. This relationship must be regulated by special agreements between the institutions, which refer exclusively to the provision of measures for personal data protection.
- The Government should adopt a methodology for detection, reporting and remediation of security incidents related to breaches of personal data security of citizens when using e-services or tools. In doing so, re-access to the data subject to the incident should be provided without exception.
- The Agency for **Personal Data Protection Agency (PDPA)** should be actively involved in the implementation of the ICT strategy. Apart from being a resource center of knowledge and practices, PDPA will have to give its opinion, approval and guidance in several activities, so their involvement is essential to ensure a process that will support the implementation of the Law on Personal Data Protection in every aspect.