REPUBLIC OF ESTONIA
MINISTRY OF ECONOMIC AFFAIRS
AND COMMUNICATIONS

GUIDELINES

FOR IMPLEMENTING THE REGULATION *PRINCIPLES FOR MANAGING SERVICES AND GOVERNING INFORMATION*

Version 1.0

27 June 2017

Introduction

On 25 May 2017 the Government of the Republic passed Regulation No. 88 *Principles for Managing Services and Governing Information*, prepared by the Ministry of Economic Affairs and Communications. The Regulation was published in the *Riigi Teataja* on 31 May 2017 and it entered into force on 3 June 2017.

It is provided in the Regulation that its provisions shall be specified in guidelines. The objective of issuing these guidelines is to ensure that authorities would interpret the Regulation in a uniform manner and would be provided advice for implementing the provisions of the Regulation. For this purpose, the provisions are supplemented by concise explanations and examples. The guidelines will be updated as necessary.

Chapter 1 GENERAL PROVISIONS			
§ 1.	**Scope of regulation and application**	**Explanations, examples**	**Application**
§ 1 (1)	(1) This Regulation establishes, as the principles for managing services and governing information, the requirements for: 1) management and development of services; 2) information governance.		
§ 1 (2)	(2) This Regulation shall apply to governmental authorities (hereinafter *authorities*) in its entirety.	The rules of authorisation of the Regulation are subsection 27 (3) of the Government of the Republic Act and subsection 6 (2) of the Archives Act. Based on the rule of authorisation of the Government of the Republic Act, the Government of the Republic issues regulations for the management of the organisation, operations and work of governmental authorities. The principles provided in the rule of authorisation of the Archives Act – see subsection 1 (3).	
§ 1 (3)	(3) The provisions of Chapter 4 and subsections 18 (6) to (10) of this Regulation, being the principles provided for in subsection 6 (2) of the Archives Act, shall apply to all the authorities and persons performing public law functions.	The provisions apply to state and local government authorities and other persons performing public law functions, including persons in private law. Also the explanations for sections 2 and 3 will be taken into account. Although the requirements for management of services are compulsory only for governmental authorities, adherence to the principles set out in Chapter 3 is recommended also to other persons performing public law functions.	
§ 1 (4)	(4) An authority shall direct the state authorities administered by it towards adhering to the Regulation in its entirety.	The requirements for managing services are not compulsory for the authorities administered by governmental authorities, but the services of the area of government of a ministry are to be developed as a whole. Governmental authorities can support the application of the Regulation by the authorities administered by them through briefing, training and joint projects.	
§ 1 (5)	(5) The Regulation shall not be applied to	The cultural specifics of the states and their capability for	

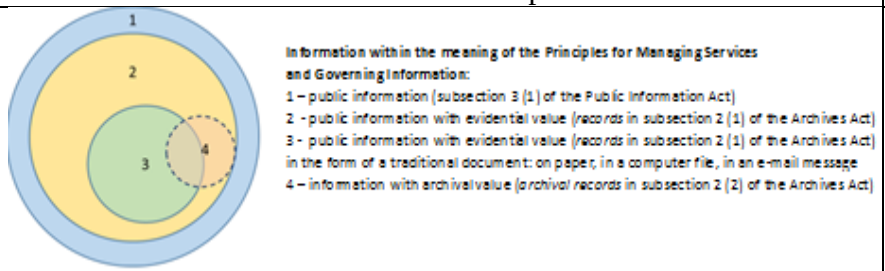
	document exchange with foreign states.	document and data exchange must be considered in document exchange with foreign states. If possible, partners should still be directed towards using the solutions supporting the development of Estonia's services and information governance (solutions created for data exchange, the *X-Road*, electronic documents, etc.). Estonia's digital signature can be used in document exchange with EU Member States since 1 July 2017.	
§ 2.	**Services**		
§ 2 (1)	(1) Within the meaning of this Regulation, services are direct public services and support services.	All provisions that refer generally to "services". The reference includes support services.	
§ 2 (2)	(2) Direct public services are the services provided by an authority to a natural person or a legal person in private law (hereinafter *person*) in accordance with the latter's will, including presumed will, via a service contact in any communication channel (hereinafter *channel*), enabling the person to perform an obligation deriving from law or exercise a right deriving from law.	Direct public services **<u>are not</u>** the so-called genuine public services, such as: 1) provision of vocational education; 2) protection of forests; 3) collection of public revenues. Direct public services **<u>are</u>** the services that involve interaction between a person and an authority, such as: 1) application for admission to a vocational educational institution; 2) submission of forest notification; 3) filing of tax returns. Direct public services **<u>comprise</u>** not only the application/notice/report etc., but also the processing of such document by an authority. Direct public services **<u>are also,</u>** for example: 1) state supervision services directed to a specific persons and provided either at the request of a person (e.g. inspection of recreational craft) or on the initiative of the authority (e.g. supervision of animal health); 2) services to persons for providing information or assistance. Direct public services are always provided to individual persons and **<u>are</u>** therefore **<u>not</u>** for example:	

		1) organisation of state supervision (e.g. preventive action to prevent offences, collection and analysis of data, determination of the district or scope of supervision, planning of activities, including direct supervision contacts). **Service contact** is the approach of a person to an authority or the approach to a person by an authority, including via a website or any other electronic channel. **Communication channels** are either electronic or physical. Direct public services can always be provided by electronic means, but in some cases it is reasonable to provide them also by physical means. **Electronic channels** are, for example: 1) electronic self-service; 2) information gateway eesti.ee; 3) website/portal; 4) smartphone application; 5) digital television; 6) e-mail; 7) telephone; 8) fax; 9) text message. **Physical channels** are, for example: 1) post; 2) counter services in an office; 3) services provided at the customer's place (at home, at a company's premises). If direct public services are **well organised,** there is little bureaucracy.	
§ 2 (3)	(3) Proactive services are the direct public services provided by an authority on its own initiative in accordance with the presumed will of persons and based on the data in the	Under proactive services, information systems analyse the facts and data collected into databases in order to ascertain when a person will have the right to a benefit or advantage, or an obligation. When the right or obligation arises, the information	

	databases belonging to the state information system. Proactive services are provided automatically or with the consent of a person.	system provides the service automatically or asks for the consent of the person (offers them the service). Proactive services are, for example: 1) a child's health insurance upon the child's birth; registration of a child in the practice list of the mother's family physician upon the child's birth – provided automatically; 2) one-click tax return – the person confirms acceptance of a prepared tax return; 3) benefit to a pensioner residing alone – the benefit is granted automatically on the basis of registered data, the person is notified about his or her right to receive the benefit and the person is entitled to waive such right; 4) notification of the right to old-age pension – a person is notified about the right to the pension at least 6 months in advance (as some of the data necessary for granting the pension may be missing from the state information system but may be included in different documents held by the person).	
§ 2 (4)	(4) Event services are the direct public services provided jointly by several authorities so that a person would be able to perform all the obligations and exercise all the rights conferred on the person due to an event or situation. An event service compiles several services (hereinafter *component service*) related to the same event into a single service for the user.	An event service must seem like a single seamless service to its user, and must be convenient to use. Services may be compiled into an event service based on: 1) a life event of a person (birth of a child, building a house, etc.); 2) a business event of an entrepreneur (starting a business, winding up business activities, etc.). At least some of the component services of an event service are proactive. A person may use also only a part of the component services of an event service. For example, a person may waive some services offered upon the birth of a child, or may draw up design documentation for a house, but decide not to build it. Event service are, for example: 1) hiring of an employee – the employer submits information about hiring an employee to the Tax and Customs Board, and the	

		information is automatically forwarded to the Health Insurance Fund (health insurance), Estonian Unemployment Insurance Fund (unemployment insurance) and Labour Inspectorate (the fact of employment), and the employer does not have to contact any of these authorities separately. The target group of this service is the employers, but one of the interest groups is the employees who are provided with various rights. In 2017, an analysis for the development of two event services begins: 1) complex service for family events (except the birth of a child) – under the management of the Ministry of the Interior; 2) complex service based on the birth of a child – under the management of the Estonian National Social Insurance Board. The analysis will focus on the proactive provision of both state benefits as well as local government benefits as a joint service, so that a family would be ensured with necessary information and with the opportunity to receive all the necessary benefits quickly and conveniently.	
§ 2 (5)	(5) Support services are provided by an authority to its own officials or employees or to the officials or employees of another authority. Support services support the performance of the functions of an authority.	Support services are, for example: - accounting; - human resource work; - document management; - organisation of procurement; - IT support; - etc. See also § 7 of the Civil Service Act. Support services provided to another authority may include also counselling in a specific field (guidelines/guidance, training and briefing, participation in projects, etc.), administrative supervision, portal service, etc. See also subsection 8 (1). Every support service affects directly or indirectly the quality of public services.	

§ 2 (6)	(6) Within the meaning of this Regulation, processes are the organised sets of activities aimed at the performance of the principal function of an authority or at the provision of a service.	The principal functions of an authority derive from the statutes of the authority or from other legislation. One or several direct public services and/or support services may be provided upon performance of a principal function (including support services to another authority). Every service has its own process for providing the service. Joint services of authorities – see subsections 7 (7) and (9).	
§ 3.	**Information governance**		
§ 3 (1)	(1) Information governance is the activity that supports the achievement of the objectives of an authority and the public sector through management, sharing and exchange of information in all information systems and databases. The subactivities of information governance are data governance, document management, content governance in the intranet and extranet, and organisation of access to and protection of information.	Information governance **is not** a synonym for document management, data governance, internal communication or any other separable activity. Information governance comprises the entire information of the authority in all information systems and storage facilities, all the information assets. Data governance comprises the management of data in relational databases, geographical information systems and other information systems. Document management – see subsection 3 (3). Content governance in the intranet and extranet aggregates information from different information systems and other sources and presents it in a user-friendly manner. Organisation of access to and protection of information comprises the access for officials and employees, as well as access for the public, and protection of personal data and other data.	
§ 3 (2)	(2) Information means the information specified in subsection 3 (1) of the Public Information Act and in subsections 2 (1) and (2) of the Archives Act which is recorded in any manner and on any medium.	Information is a comprehensive concept that comprises all information and information assets. Information may appear in whatever form (data, working papers, official documents, publications, social media messages, etc.), it may or may not have evidential value, and it may have very different retention periods. An authority has to determine, as a result of an analysis, which part of information has evidential value, i.e. which part of information is the information specified in subsection 2 (1) of the Archives Act as *records*. Records comprise traditional documents,	

		information in databases, and any other information needed by an authority to evidence facts or activities within a specified period of time. The information specified in subsection 2 (2) of the Archives Act as *archival records* are records with evidential value to which archival value has been granted by a public archives, and which must not be destroyed. Archival records are needed for evidencing facts or activities, and for understanding the functioning and processes of our contemporary society in the distant future. Archival records are to be transferred to public archives.	
§ 3 (3)	(3) Within the meaning of this Regulation, document management as a subactivity of information governance means traditional records management which forms a part of arrangement of information and which organises the management, processing, exchange of and access to information specified in subsections 2 (1) and (2) of the Archives Act if such information is recorded on paper, in a computer file or an e-mail message.	 In this Regulation, document management refers to traditional records management which is usually organised by the so-called electronic document and records management systems (EDRMS). The information specified in subsections 2 (1) and (2) of the Archives Act and recorded on paper, in a computer file or in an e-mail message **refers** to records and archival records on certain media – the so-called official documents which have evidential value and can be destroyed only under a destruction instrument or will be preserved permanently. In the drawing, these documents are in circle no. 3. This **does not refer** to the so-called working papers (e-mails with very short-term relevance, versions of a planned document, etc.) which can be destroyed also by the user. An authority is to determine which working papers have	

		evidentiary value and are to be treated as documents. The term *computer file* has been used in the common meaning: a computer file is managed as a separate unit and processed as a whole, it has a name and extension, and it can be in text, image, sound or other format. Arrangement of information – see § 12.	
Chapter 2 **RESPONSIBILITY FOR MANAGEMENT AND DEVELOPMENT OF SERVICES**			
§ 4.	**Responsibility for management and quality of services**		
§ 4 (1)	(1) An authority shall determine the posts or positions held by the persons who shall ensure: 1) management and quality of the direct public services; 2) management and quality of the processes; 3) information governance and quality thereof; 4) every subactivity of information governance and quality thereof of the authority.	The clauses of this subsection refer to the areas related to the management of services. It refers to the responsibility for the so-called big picture. For example: although every process has a person responsible for it, there still has to be someone holding it all together over all the processes. Responsibility must be personal. In this subsection, there is a list of roles. Depending on the authority, one person may perform several roles, especially at smaller authorities. For example, the same person may be responsible for processes and information governance or for processes and direct public services. The person responsible for an area must have the competence, powers and resources to manage the area.	To be determined no later than by 1 October 2017.
§ 4 (2)	(2) The persons holding the posts or positions set out in subsection (1) above shall cooperate in order to ensure the homogeneous quality of the services of the authority.	Cooperation must be continuous. Various requirements, the experience of different parties and new opportunities must be taken into account in a process or service development. Every person responsible for an area has knowledge about the area, and such knowledge has to be shared. The "owners" of services, processes and channels and external parties must also be involved in the cooperation.	
§ 4 (3)	(3) An authority shall determine, with regard	The responsible person or the "owner" has to be determined for	To be determined

	to every service and every channel of providing direct public services, a structural unit or a post or position that shall be responsible for the development, management and quality of such service or channel.	every support service and every direct public service. The "owner" of a channel is responsible for the channel as a whole – for example, for a service bureau, helpline or electronic self-service environment. The same channel can be used for providing different public services.	no later than by 1 October 2017
§ 5.	**Coordination of development of services across authorities**		
§ 5 (1)	(1) The authorities coordinating development of services across authorities (hereinafter *coordinators*) shall be: 1) the Ministry of Economic Affairs and Communications in management of direct public services, including upon determination, sharing and exchange of the information necessary for providing such services; 2) the Data Protection Inspectorate in organising access to and protection of information; 3) the Estonian Information System Authority in implementation of the requirements for the architecture of the state information system and for the key components of the state information system.	Under existing legislation, coordinators have the task to ensure development or compliance with requirements across the whole public sector.	
§ 5 (2)	(2) A coordinator shall perform the following functions: 1) plan the main directions of development and the activities supporting development; 2) issue guidelines and recommendations; 3) monitor the implementation of planned activities and application of guidelines;	Clause 4). The guidelines of the coordinators and materials of council meetings have to be made available, and presentations are to be made at seminars, training and information events. A joint information day of coordinators should be held regularly (e.g. once a year) for different council members and other officials and employees engaged in the service management. (see also clause 5)).	

	4) manage communication; 5) cooperate with other coordinators; 6) engage other parties as necessary.	Clause 5). The cooperation among coordinators entails at least keeping one another informed about the planned activities and guidelines, and coordinating them as necessary. The representative of another coordinator may also be engaged in the work of the council, joint guidelines may be issued, and presentations can be made at information events.	
§ 5 (3)	(3) The integrated development of the services within the area of government of a ministry shall be organised by the secretary general of the ministry or by a person authorised by the secretary general, based on the functions of the area of government and the goals set in the relevant strategic development documents.	The person responsible for the development of services within the whole area of government must have the respective requisite powers. It can be a secretary general, deputy secretary general, development manager or a person holding another office. Strategic development documents are the general principles of policy (adopted by the Riigikogu), the sectoral development plan, and the development plan and programmes for the area of government.	
§ 5 (4)	(4) A council shall operate with the coordinator in order to support the performance of the functions set out in clauses 1), 2) and 3) of subsection (2), consisting of representatives appointed by ministries and by the Government Office, and as necessary, other persons appointed by the coordinator. The composition and work procedure of the council shall be approved by a directive of the coordinator. The materials of the council meetings shall be published on the website of the coordinator and, as necessary, in another manner.	Several ministries may appoint a joint representative to the council. A ministry may appoint also an official or employee of its subordinate authorities as its representative. The websites of the coordinators: Ministry of Economic Affairs and Communications (direct public services): https://www.mkm.ee/en/objectives-activities/information-society/information-society-services Ministry of Economic Affairs and Communications (document management): https://www.mkm.ee/en/objectives-activities/information-society/records-management-information-governance Estonian Data Protection Inspectorate: http://www.aki.ee/en Estonian Information System Authority: https://www.ria.ee/en/	The records management council formed under subsection 54^2 (1^1) of Regulation of the Government of the Republic, *Uniform Principles for Records Management Procedures*, will continue operating as a council supporting the development of document management and

			transition to information governance until this is no longer necessary.
§ 5 (5)	(5) A member of the council shall inform the relevant officials and employees of the authority such member represents and of the authorities within the area of government of such authority about the activities of the council, and shall engage said persons in the formation of his or her positions and proposals.	A council member must be competent and authoritative in the respective area, and must ensure that necessary information reaches all appropriate persons through him or her. The council facilitates the so-called pyramidal coordination – decisions, guidelines and other significant information move downward from the top (from the coordinator to the council, from the council to all the authorities). Feedback, problems of the practitioners, examples of best practices, etc. move upwards from the bottom.	
§ 5 (6)	(6) An authority shall take into consideration the guidelines and recommendations of the coordinator and shall direct the authorities administered by it towards adhering to the same.	Guidelines and recommendations serve two different objectives: 1) to give tips to authorities on how to implement legislation or better organise their work, or 2) to ensure minimum interoperability of information systems and uniform operation of authorities where differences would have negative impact on the exchange of information, statistics and analyses, and costs of the public sector. Coordinators may issue joint guidelines, including together with other competent authorities (see subsection 10 (1)).	
Chapter 3 MANAGEMENT OF SERVICES			
§ 6.	**General requirements**		
§ 6	The management of the services by an authority shall ensure: 1) creation of measurable or perceptible value for every target group and interest group of services; 2) discontinuance or rearrangement of	The list sets out general objectives to be achieved by management of services. Clauses 1) and 2): defining the target groups and interest groups and the value created for them – see clause 7 (2) 3). Clause 3): As some direct public services ensure the performance of obligations of a person (reports, notices, and tax returns), a	

	services that do not create value; 3) satisfaction of the users of services and optimum administrative burden of persons; 4) optimum extent of documentation of the performance of the functions and provision of services by the authority; 5) cooperation with other authorities and parties, contributing to the efficiency of the public sector as a whole and to consideration of the needs of persons in the development of direct public services; 6) continuity of the provision of services and cooperation upon termination of the service or employment relationship of an official or employee, modification of the work procedures of the authority and during the suspension of an official's right to exercise official authority or during temporary absence of an employee.	certain degree of administrative burden may be necessary. However, the burden cannot be unreasonably heavy. Clause 4): The optimum extent means that the documentation must not come into a means to its own end, and therefore its extent must be based on the actual needs – for evidencing or other. Clause 5): The public sector must get rid of the so-called "silos" and become more efficient and client-friendly as a whole. For example, instead of asking a client to provide a certificate obtained from another authority, the data in the certificate should be exchanged with other authorities. Clause 6): The provision of services and cooperation must not discontinue when an official or employee is absent from work or leaves work, or in case of any modifications in the work procedures of the authority.	
§ 7.	**Management and development of services**		
§ 7 (1)	(1) An authority shall have an overview of the services provided in the course or as a result of performing its principal functions. The overview shall be prepared in the manner enabling easy updating thereof.	The principal functions of an authority derive from its statutes and other legislation. The performance of the principal functions may involve direct public services and/or support services. The services provided in the course or as a result of a process are to be determined. The overview can be created using process charts prepared by using freeware or other software, including additional information presented as text, also service cards or other descriptions that are managed by the owners of processes or services and that can be compiled into a whole without duplication. If services are modified, the descriptions must also be updated as necessary.	A comprehensive overview must be created no later than by 1 July 2018.

§ 7 (2)	(2) If there is no overview covering a single or several principal functions as specified in subsection (1) or if it is out of date, an authority shall determine: 1) the services provided in the course or as a result of performing its principal function; 2) the significance of every service, considering the value created by the provision of the service; 3) the target group and interest groups of every significant service, and the value created to them by the provision of the service; 4) the legislation regulating the significant services and the processes of providing these services; 5) the processes of providing significant services; 6) the information created in the course of the processes of providing significant services in the manner set out in subsections 12 (3) and (4); 7) the channels for providing direct public services.	An authority is free to choose the form of the overview and the persons who are to manage any changes to the overview. The overview cannot remain the mere knowledge of the official who has prepared it. Clause 1). A process may involve direct public services and/or support services. The services provided in the course or as a result of a process are to be determined. Clause 2). The significance of a service is primarily determined by the value created by it to the users and the society. The significance may be affected also by other factors, such as the number of users, frequency of use, the cost of the service or satisfaction of the users. An authority determines the significance of a service on its own, and it may change in time. Clause 3). The target group of a direct public service may be, for example, the recipient of a specific benefit or support whose life quality is improved by the service. Direct supervision services, however, have a narrower target group (the person subject to supervision) as well as a broader interest group (other persons in whose interest supervision is exercised). Saving of time, and also obtaining more specific information when needed, as well as the sense of justice and the experience of proper servicing are important to the target group. Even more significant value is created for the interest group, whether it consists of buyers, taxpayers or the entire population. The value created for the interest group is better genuine public services and adherence to social agreements. Determination of interest groups is important also for other services, not only with regard to supervision services. Good management of support services may create value added directly for the recipient of direct public services (a matter is settled quickly and with high quality), but the value is also created for the officials/employees (who can quickly make correct	

		decisions, do not have to perform unnecessary acts or manual work or do the same thing over and over again, etc.) and for the authority and the state as a whole (increase of efficiency, cost saving). Clause 4). The process of providing a service may be affected by legislation or the work procedures of the authority itself. The authority must know the legislation that provides for the requirements for the service and the service process. Clause 6). See subsection 12 (3) and 12 (4). Clause 7). See subsection 2 (2).	
§ 7 (3)	(3) As necessary, an authority shall apply the provisions of clauses (2) 3) to 6) to other services.	Upon transition to service-based management, an authority can start from more significant services, and while learning from its own experience, include gradually other services. In particular, a service must be analysed when its users are not satisfied with the service, if the provision of the service is too expensive for the authority, or if the service has to be made electronic.	
§ 7 (4)	(4) An authority shall assess, at least once a year, the quality of the significant services and of the processes of providing such services.	Services must be developed continuously, not on a project basis. Quality assessment is a prerequisite for planning the activities and budget of an authority. Therefore, significant services must be assessed at least once a year. The actual outcome of any changes made will turn out in the course of the assessment. The quality of direct public services can be assessed using the guidelines of the Ministry of Economic Affairs and Communications – see subsection 8 (4).	
§ 7 (5)	(5) Carrying out the assessment, an authority shall ascertain organisational, legal and technological factors inhibiting the development of the services. The authority shall determine the needs for modification and development, the priorities thereof and the value created upon implementation	An authority has to determine whether the development of a service is inhibited by unreasonable organisation of work or whether the legislation regulating it is outdated or whether the IT solutions must be changed.	

	thereof.		
§ 7 (6)	(6) An authority shall plan and implement activities based on the priorities, minimising the effect of the factors that inhibit development.	In order to remove any obstacles, an authority may change its work procedures, the manner of collection or processing of information, upgrade technological solutions or initiate amendments to legislation (amendments to legislation can also be initiated by submitting a proposal to a competent authority).	
§ 7 (7)	(7) Authorities may manage and provide a service jointly in order to ensure the better quality of the service. Regarding the service to be provided jointly, the authorities shall agree upon: 1) the authority that shall be responsible for its development, management and quality; 2) the process of providing the service; 3) the term of providing the service; 4) as necessary, amendment of the legislation regulating the provision of the service; 5) the technical solution and use thereof; 6) the resources of the responsible authority and other authorities, needed for providing the service; 7) the details of elaboration or development and of provision of the service.	Direct public services (e.g. helpline service) or support services (e.g. document registration service) can be provided jointly. Event services as jointly provided services – see subsection 7 (9).	
§ 7 (8)	(8) If the information needed for the provision of a direct public service exists in the databases of the state information system, the authority shall devise a proactive service, where appropriate, in cooperation with the authorities administering the databases.	Proactive services – see subsection 2 (3). Initiation of the exchange of information with other authorities requires agreements, and in case of personal data, also a legal basis. It may become necessary to amend legislation and change the work procedures of authorities. Initiation of data exchange requires IT developments. Also, external parties must be involved, especially the representatives of the target group. The expectations of service	

		users and the value created must be ascertained upon the creation and development of every direct public service. The determination of the expectations of the target group and the value created is especially important upon elaboration of proactive services.	
§ 7 (9)	(9) The planning or development of an event service may be initiated by the coordinator or by an authority providing at least one direct public service related to the event. In addition to the provisions of subsection (7) above, the authorities shall agree upon the terms for providing component services.	Event services – see subsection 2 (4). It is important to note that the coordinator may also initiate an event service. Event services are at least partially proactive. The creation of any proactive service requires cooperation and agreements among different authorities in order to exchange data, and often also amendments to legislation. While creating event services, the owner and details of an event service must also be jointly agreed upon, just like in the case of other joint services. Agreements regarding jointly provided services – see subsection 7 (7). An event service process is supposedly shorter than the sum of all the terms of the previously provided services. Therefore also the terms of the component services must be agreed upon, while planning the respective amendments to legislation as necessary.	
§ 7 (10)	(10) If an authority administers an information system where another authority provides or uses a service, the authority administering the information system shall be responsible for the technical solution and for its functioning and development. The administrator of the information system and the authorities using the information system shall agree upon: 1) the potential of the information system, use and modification thereof; 2) the division of responsibility for the process and service quality.	One of the problems of centralised information systems has earlier been that the processes were "forced" on the users and do not take into account the users' needs and their other processes. This has created surplus or duplicating activities. It has also been problematic if the information system enables one to work better but the process should be developed by a user who does not take up the opportunities created. In both cases, the question has been who is responsible for the quality of the processes and the service – irrespective of whether it is a direct public service or a support service. Whereas the core of the problem differs depending on the information system, it is provided for that the authority administering the information system shall agree upon responsibility with the authorities using the information system. It is closely connected with the establishment of the rights and obligations of the chief and authorised processor specified in the	

		Personal Data Protection Act and Public Information Act. The administrator of the information system is responsible for the technical solution.	
§ 7 (11)	(11) The administrator of the information system set out in subsection (10) shall ensure the facilities for analysis and reporting for the authority using the information system in order to support the authority upon the assessment of the quality of the service provided by it and upon making other management decisions.	The facilities for analysis and reporting must be included in every information system. If the information system is administered by one authority but used by several others, the administrator cannot be guided only by its own needs for analysis and reporting. Every authority using the system must be able to use the information entered by it for making decisions. Initially it is acceptable if the accessibility of information is ensured by means of *ad hoc* database queries. For future developments, the needs for reporting and queries must be carefully considered already in the planning phase.	
§ 8.	**List of services**		
§ 8 (1)	(1) An authority shall have an up-to-date list of its own direct public services and of the support services provided to other authorities, containing at least significant services.	The support services provided to other authorities do not refer to those support services that are provided by the IT authority of a ministry only to the ministry and to the authorities in its area of government. The support services provided to other authorities comprise more areas of government than that of one ministry. Support services – see subsection 2 (5). Determination of the significance of a service – see clause 7 (2) 2).	To be prepared (at least) with regard to all significant services no later than by 1 July 2018.
§ 8 (2)	(2) To draw up a list or adjust an existing list of services, an authority shall use the guidelines, uniform form for describing and machine readable description language devised by the coordinator.	An authority can describe services in a central catalogue of governmental authorities or use a tool created for its own use, while adapting it in accordance with the guidelines. The lists of different authorities can be aggregated only in case they have been prepared in a uniform manner. It also requires the descriptions to be both human readable as well as machine readable. For this reason, descriptions should be based on the guidelines of the Ministry of Economic Affairs and Communications.	The guidelines are to be prepared no later than by 1 January 2018.
§ 8 (3)	(3) An authority shall publish the list of services in the central catalogue of the	As the list of services is, in addition to being human readable, also machine readable, it can be reflected in other electronic	To be published no later than by 1 July

	services of governmental authorities administered by the coordinator, and where possible, also on its own website.	environments as a whole or in part. If the lists are drawn up in a uniform manner, no manual work needs to be done for publication.	2018. See also clause 4).
§ 8 (4)	(4) The list of services shall include the quality indicators for the significant direct public services, which shall be calculated taking into account the guidelines devised by the coordinator. An authority shall submit the quality indicators for every calendar year.	The quality of different direct public services can be compared only if the quality indicators have been calculated on the basis of uniform methodology. Different types of services may have different quality indicators. The guidelines will be prepared in cooperation with the Ministry of Finance and council of services. An authority will have to submit the quality indicators not later than for the year 2018 if the guidelines are completed in 2017, or not later than for the year 2019 if the guidelines will be completed in 2018. The data are to be submitted at the end of a year or at the beginning of the following year.	The guidelines are to be prepared no later than by 1 January 2018. The quality indicators are to be presented for the first time no later than for the year following the issue of the guidelines.
§ 9.	**Provision of direct public services**		
§ 9 (1)	(1) An authority shall ensure that the information necessary for using a direct public service is easy to find. The information shall be provided to the target group of the service in an appropriate manner and volume. If the information is published in the Estonian information gateway eesti.ee (hereinafter *eesti.ee gateway*), the authority shall take into consideration the requirements set out in the Public Information Act and legislation established on the basis thereof regarding publication of information in eesti.ee gateway.	The reference is to the information that a person needs before using a public service, including information about the channels of providing the service (e.g. self-service environment in the web, helpline, service bureau), contents of the service, contact details and official hours for obtaining additional information or advice, and everything else that is needed. It is important that the user should not have to search for information for a long time, but would find it intuitively and quickly. The specifics of the target group should be considered – for example that the users of the service are mainly older people or that the user group has got specialised vocabulary. This provision applies also to the information, supplementary texts, notices and error messages given to a user in the course of using an electronic service. As to the services provided in an electronic environment, the accessibility standards (e.g. the international WCAG standard) and legislation (e.g. EU Directive on the accessibility of the websites and mobile applications of	

		public sector bodies, which must be transposed in the Member States in September 2018[1]) have to be taken into account. Publication of information in eesti.ee gateway – see subsection 13 (12).	
§ 9 (2)	(2) An authority shall not request a person to submit again the data that are required for providing a direct public service but are already in the database of the authority, or are included, as basic data, in any other database belonging to the state information system. A person shall have an opportunity to inform the datasource about a change in the previously submitted data.	This requirement is to be applied at least upon provision of significant services – see subsection 9 (7). Subsection § 43^6 (2) of the Public Information Act: if the data needed by an authority already exist in another database as basic data, the data of such other database are to be taken as a basis. This requirement does not apply to the data needed for identification purposes (personal identification code, registry code, etc.), as without these data, a person cannot be connected with the data necessary for providing a service. This requirement can be met in a different way – for example, by supporting a person with a pre-filled application form or by verifying by automated queries that the prerequisites for receiving the service have been met. Informing a datasource about a change in the data submitted earlier – see also subsection 9 (3). It covers also submission of contact details, which differ from the ones submitted before, for exchange of data in relation to the given proceeding.	No later than from 1 July 2019.
§ 9 (3)	(3) An authority shall not require a person to check and confirm the correctness of the data created or processed by authorities, but the person shall have an opportunity to inform the datasource about inaccurate or misleading data and require correction of such data.	This requirement is to be applied at least upon provision of significant services – see subsection 9 (7). The requirement is in compliance with clause 6 7) and subsection 21 (1) of the Personal Data Protection Act. A person is liable only for the correctness of the data submitted by him or her. An authority is liable for the quality of the information created and entered by it. The datasource of an authority can be the person himself or herself, the authority providing a service and its data media (as to	Not later than from 1 July 2019.

[1] Directive (EU) 2016/2102 of the European Parliament and of the Council on the accessibility of the websites and mobile applications of public sector bodies: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=OJ:L:2016:327:TOC

		basic data in the database of the authority providing the service) or another authority (as to the basic data taken from the database of the other authority). The legislation regulating the management of databases stipulate also who is the person submitting the data in connection with every type of data. If a person informs the authority providing the service about any changes or errors in the basic data of the database of another authority, it is important to ensure that such notice would reach such other authority. Otherwise the authority providing the service corrects the error in its database, but the error remains uncorrected at the other authority and elsewhere. At the same time, it has to be taken into account who has the right to give notice of changes in the basic data or of an error to the other authority – whether the persons themselves, or also the authority providing the service.	
§ 9 (4)	(4) The rights of the users of a direct public service to carry out acts in the web environment may differ based on the manner of authentication of the person.	The requirement is to be applied at least upon provision of significant services – see subsection 9 (7). It means that certain acts can be carried out only if secure means of authentication, i.e. Estonia's eID (e.g. ID card and mobile ID) is used, while in case of some acts also a lower level of authentication can be accepted (e.g. username and password). The more personal the data used in the service are or the greater the impact of the service, the securer the means of authentication must be. If a service has users from other EU Member States, all electronic IDs of such other states of which the states have notified the European Commission and which are on the same or on a higher level, are to be accepted in the same service under the eIDAS Regulation[2].	The part concerning electronic identification of the eIDAS Regulation will be applied from 18.09.2018, the Electronic Identification and Trust Services for Electronic Transactions Act entered into force on 26.10.2016.
§ 9 (5)	(5) An authority shall inform the user of a	The term of providing a service is often set out in the legislation	

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC: http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1498054625100&uri=CELEX:32014R0910

	direct public service about the term of providing the service and about the course of the service. The authority shall ensure the provision of the service within the term.	regulating the provision of the service. However, a person may not be aware of the term, and must therefore be informed about it. If the setting of the term is to be decided by the authority, it must set the term in such manner that the authority will surely be able to provide the service within the term. The authority may and even must try to provide the service before the end of the term, but must not do it later. Extending a term is not a good practice, especially if the reason derives from the work procedures of the authority. If the term is extended in the cases permitted by legislation, the user must be informed in good time about the future extension of the term as well as the reasons for it. While informing about the course of the service, it must be known which information the user needs about the service in order to avoid overburdening the user with excessive information (e.g. regarding the movement of an application inside the authority).	
§ 9 (6)	(6) An authority shall enable the user of a direct public service to receive advice and assistance in the course of using the service, provide feedback and make proposals on the service.	Receipt of advice and assistance and provision of feedback must be a clearly understandable and accessible opportunity. Providing users with the information about where and when they can get advice and assistance – see subsection 9 (1). Feedback is collected from the direct users of service and preferably directly after the use of the service. To obtain feedback on electronic services, for example the recommendation index has been used. Feedback from daily users should be asked at reasonable intervals not to overburden the users.	
§ 9 (7)	(7) The requirements set out in subsections (2) to (4) shall be applied at least to the provision of significant direct public services.	Determination of the significance of direct public services – see clause 7 (2) 2).	
§ 10.	**Establishment of additional requirements for management and provision of direct public services**		

§ 10 (1)	(1) A coordinator or any other competent authority may issue guidelines to specify the requirements provided for in this Chapter. The coordinators and competent authorities may issue joint guidelines.	In addition to coordinators, there are also other competent authorities that may also issue guidelines affecting the development of services – for example the National Archives, Ministry of Justice, etc. Joint guidelines facilitate the work of the managers and providers of servicers, as they aggregate different views and are not in conflict with one another.	
§ 10 (2)	(2) If it is necessary to agree on a uniform response to a single case of application of legislation or guidelines, the council operating on the basis of subsection 5 (4) shall make a decision on the proposal of the coordinator.	It may appear upon application of legislation or a guideline that the same requirement may be applied in several possible manners. In such case the council operating with the coordinator can agree on the choice of the manner of application. The council members are practitioners who intermediate the problems of their own authority as well as the problems of the divisions to the coordinator. A decision of the council is to be made on the proposal of the coordinator and it may be reflected in the subsequent version of the coordinator's guidelines.	
§ 10 (3)	(3) The detailed arrangement of the provision of the direct public services by an authority shall be provided for in the instruments and guidelines regulating the internal work procedures of the authority. The authority shall keep the instruments and guidelines up to date and shall support the conformity to the provided requirements by IT tools.	The work procedures have to be supported by IT tools – breaking rules must be as difficult as possible, or even impossible. It need not mean new IT solutions – the existing opportunities must be examined. Instruments and guidelines must be updated by 1 July 2018, but they may enter into force on 1 January 2019.	An authority has to bring the instruments and guidelines into conformity with the requirements of the Regulation no later than by 1 July 2018.
Chapter 4 INFORMATION GOVERNANCE			
§ 11.	**General requirements**		
§ 11	The information governance of an authority shall ensure: 1) the quality and availability of	Clause 1). The quality of information is supported, for example, by decreasing the number of documents and increasing the usage and exchange of data, as well as ensuring the quality of data.	

	information; 2) the management of risks and reduction of costs related to the storage, exchange and use of information; 3) continuity of information governance upon termination of the service or employment relationship of an official or employee, modification of the work procedures of the authority and during the suspension of an official's right to exercise official authority or during temporary absence of an employee.	Clause 2). Risks are managed, for example, by appropriate management and protection of data with high evidential value as well as adherence to the rules by the support of ICT tools. Among other things, costs are reduced by discontinuation of the collection of unnecessary information and reduction of duplication and paper documents. Clause 3). It must not happen that information cannot be found or managed for the reason that an official or employee is temporarily absent from work or has left work, or if the work procedures of the authority are being modified. In order to ensure the continuity of information governance, an authority has to establish rules for the transfer of activities, information and responsibility. Regulation must involve stipulation for the granting and terminating the rights of access to databases and information systems.	
§ 12.	**Arrangement of information**		
§ 12 (1)	(1) An authority shall have an overview of the information created upon performance of its principal functions, sources and storage facilities for such information. The overview shall be prepared in the course of analysing the processes and in the manner enabling easy updating thereof.	Process analysis – see subsections 7 (1) and (2). Authorities may manage an overview on their entire information in any manner. Information with evidential value, i.e. records, must be recorded in classification scheme provided for in the archival rules. The part of the list of records regarding the functions and series has mainly been used as a classification scheme.	A comprehensive overview is to be prepared not later than by 1 July 2018.
§ 12 (2)	(2) If there is no overview covering a single or several principal functions as specified in subsection (1) above or if it is out of date, the authority shall prepare the overview in the manner specified in subsections (3) and (4).	The already existing materials can be used to decide on the integrity of an overview. For example, one can use process charts that indicate the receipt of applications or data, adoption of decisions, etc., and the facilities where they are stored. Also the existing classification schemes and lists of records, and the overviews prepared upon the implementation of the *System of Security Measures for Information Systems* can be used. Additional information can be found in work environments or working papers managed by the process owner or information governor. Users can be interviewed as necessary.	Not later than by 1 July 2018.

		A missing overview is to be created if: - there is an overview of the processes, but not all information generated in the course of a process has been mapped; - the authority uses several different information systems, but the list of records and the classification scheme do not reflect the whole information with evidential value that is generated there (the information systems / databases are shown as single units); - authorities are merged, established or restructured; - a new principal function is assigned to the authority.	
§ 12 (3)	(3) To obtain an overview of the information created upon performance of the principal function, the authority shall determine: 1) the information that is needed for providing the services related to the performance of the principal function, based on the conditions provided for by legislation; 2) the additional information that is created or obtained upon performance of the principal function or provision of services; 3) the information sources; 4) the formats and storage facilities where information is stored; 5) the information retention periods and the conditions for accessing the information; 6) the users of information.	The existing situation (*as is)* has to be ascertained: Clause 1). The statutory requirements for information, including which data is needed to decide whether a person has the right to the service or whether they have performed or have to perform an obligation; whether documents or data need to be submitted, etc. Clause 2). In process charts or other descriptions – in which stage the information required by legislation (e.g. an application) and other information (e.g. specifying correspondence) is created. Clause 3). Whether the information set out in clauses 1) and 2) is obtained: (1) from the authority's own or another authority's information system, (2) from the authority's own or another authority's document, (3) from the person and in which manners (all manners). Clause 4). Where the information is stored, e.g.: (1) as data in the information system, (2) as a document in the information system / EDRMS, (3) on paper, (4) in the mailbox of an official/employee, (5) on the hard drive in a folder of an official/employee, (6) in a social media account, (7) … (etc.). All storage facilities for the same information. Clause 5). (1) Whether or not a retention period has been established with regard to information, (2) whether the information is public or for internal use, and if it is for internal use then which official/employee of the authority may have access to it.	

		Clause 6). Whether the information has to be issued to other authorities as evidence, forwarded to other structural units, etc.	
§ 12 (4)	(4) An authority shall analyse the use and necessity of information, ascertain the duplication of the same information in different formats and storage facilities, determine the missing retention periods and access conditions, specify the information referred to in subsection 2 (1) of the Archives Act, and classify it in accordance with the classification scheme set out in the regulation established under § 13 of the Archives Act (hereinafter the *archival rules*).	The existing situation has to be analysed – see subsection 12 (3). The problems to be resolved must be ascertained: duplication, collection of unnecessary information, missing retention periods, shortcomings in the distribution of information, obsolete statutory requirements, etc. It helps planning the activities set out in subsections (5) and (6) in order to achieve the desired situation (*to be).* If no retention periods or access conditions have been established for information, they must be established considering also the statutory requirements. A retention period is established through assessing the value of information in time – during which period of time the information will be needed. Also the needs of other authorities and persons have to be considered. Information with evidential value, i.e. records are to be identified by an analysis of the retention periods, and if it is not reflected in the classification scheme, the classification scheme must be amended. NB! The persons compiling the archives are to coordinate a new or amended classification scheme with the National Archives. The persons compiling the archives – see subsection 13 (1). Retention periods must be established for all information. The tasks of deciding on the retention periods of the information with no evidential value and destruction of it upon the expiry of a term may be assigned to the official/employee who creates or receives such information. Information with no evidential value is important only for a short while: preliminary drafts of documents and interim versions of plans, exchanged e-mails regarding current daily work matters, etc. Access conditions must be determined with a view to the authority's internal as well as external users. The requirements of	

		the Public Information Act are to be taken into account in an analysis of disclosure of information (including reuse) – see e.g. sections 3^1 and 4 of the Public Information Act.	
§ 12 (5)	(5) An authority shall discontinue collecting unnecessary information and reduce duplication of necessary information. Upon reduction of the duplication of information, an authority shall prefer the information stored as data to the information stored on paper, in computer files or e-mail messages. The reproduction of the information stored as data within the retention period shall be ensured by IT tools.	The fact that information is unnecessary may appear, for example: (1) while comparing the data requested in an application with the statutory requirements and the actual need, (2) while determining the users of the information (no usage). The reuse of data, i.e. the information that has better machine processability is, as a rule, much easier than the reuse of traditional documents. If the information created in an information system can be reproduced in unchanged form during the entire retention period, there is no need to duplicate it into a traditional document. If data are overwritten before the expiry of the term, and the information cannot be reproduced, it is reasonable to store the information as a document.	
§ 12 (6)	(6) In addition to other information, an authority shall organise the storing, sharing and usage of the knowledge and experience gained in the course of the work of its officials and employees. The authority shall set the rules for documenting work meetings and the significant knowledge gained at information events, trainings and assignments abroad, and for sharing information.	An authority has to determine the information that is needed by various parties in their work in order to avoid duplicated and contradicting activities due to information blockage. It refers to transfer of significant information to an authority when an official or employee leaves work. The storage and distribution of such information must not become into a means to its own end. The rules of an authority must be based on the actual needs.	
§ 13.	**Management of information and organising access to information**		
§ 13 (1)	(1) An authority shall ensure the preservation, usability and protection of information until it is transferred to the public archives or destroyed. An authority shall preserve and transfer information set out in subsections 2 (1) and (2) of the	The information set out in subsections 2 (1) and (2) of the Archives Act, i.e. records and archival records – see subsection 3 (2). Records may be destroyed only if there is an appraisal decision of the National Archives to this end. If the National Archives has decided that the authority is the	

	Archives Act and destroy the information set out in subsection 2 (1) of the Archives Act on the basis of the archival rules, taking into consideration the guidelines of the National Archives.	person compiling the archives (i.e. information with archival value or archival records may be created in the course of the activities of the authority), the information cannot be destroyed before an appraisal decision is made and before it is determined which part of the authority's information are archival records. Archival records must be transferred to the public archives and must not be destroyed.	
§ 13 (2)	(2) An authority shall ensure that the administration system for the state information system (hereinafter the *RIHA*) shall contain up-to-date and correct data specifying the information systems administered or used by it as a chief processor of information, and that the description shall conform to the established requirements.	This requirement is in compliance with the provisions of subsection 43^7 (1) of the Public Information Act and the so-called RIHA Regulation established under the Public Information Act. The requirement applies to all information systems – a database is a part of every information system. At the state level it must be known at any moment of time which information systems are being used, and in case of standard solutions, also the extent of their use. The RIHA requirements may differ for different systems. The describing of basic data supports the creation of the X-Road data exchange services, while the data of EDRMSs and other standard solutions is uniform for different authorities. If an authority uses a standard solution, the authority is the chief processor of the information created by it, and the authority has to register the use of a standard solution.	
§ 13 (3)	(3) Information can be entered in an information system, used or otherwise processed by a person who has appropriate rights and who has been identified. The processing of information shall be described and auditable and it shall ensure the quality of information.	It refers to the employees of an authority as well as to persons in private law. Identification can be based on different authentication methods, and thus the user's rights in an information system may vary. Different levels of authentication methods – see subsection § 9 (4). The rules determining the creation, use and other ways of information processing have to be described; metadata and log entries can be used for auditing purposes. The quality of information can be ensured, e.g., by using automated data quality assessment measures, by reducing manual	

		entering of data, by deciding which data should be verified by "four eyes" while entering the data, etc..	
§ 13 (4)	(4) If an authority administers an information system where other authorities process information, the administrator shall be responsible for the preservation, usability and protection of information, for the transfer of information to the public archives or for its destruction, and for granting access to the information.	It cuts down duplicating activities of authorities upon registration of a document, disclosure of information, etc. However, an authority using an information system must still have an overview which records and archival records are stored in such system. It has to be reflected also in the classification scheme of the authority. The authority also has to appoint the officials and employees who are entitled to create, use and view the data. The authority is also responsible for the correctness of the data entered by it.	
§ 13 (5)	(5) An authority shall grant access to information and manage the protection of personal data and other information on the basis of the Public Information Act and legislation regulating data protection, taking into consideration the guidelines of the coordinator.	It is reasonable that one person is responsible for the disclosure of information and arrangement of access to information at an authority, and that such person is directly subordinated to such level that allows the person to perform the tasks assigned to him or her. Such person should also be a data protection officer within the meaning of the General Data Protection Regulation[3]. Protection of information must be arranged considering the Personal Data Protection Act as well as other legislation, e.g. the Regulation *System of Security Measures for Information Systems*, and for governmental authorities also the Regulation *Information Security Management System.* The General Data Protection Regulation will apply from 25 May 2018. The Estonian Data Protection Inspectorate may issue guidelines to implement the Public Information Act and Personal Data Protection Act.	
§ 13 (6)	(6) The administrator of an information system referred to in subsection (4) shall	Ensuring the facilities for analysis and reporting – see subsection 7 (11).	

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

	ensure the facilities for analysis and reporting for the authority using the information system in order to support the authority upon use of the information created by it and upon making management decisions.		
§ 13 (7)	(7) If an authority houses information with a person in private law, or authorises a person in private law to perform an administrative duty, an agreement shall specify the following terms and conditions with regard to the public information created in the course of such housing or performance of an administrative duty: 1) arrangement of the storage, usability and protection thereof and access thereto; 2) arrangement of its transfer to the authority upon termination of the agreement or upon winding up the activities of the person in private law.	This requirement applies also to the use of EDRMS and other standard products if information is housed in a server of the company administering the standard product or of another company.	
§ 13 (8)	(8) Upon the development of a new information system, an authority shall determine the retention periods for the data in the information system and other information managed in the information system.	The information on the relations and retention periods of data is to be stored (in documentation, in the code, etc.), and for records, it must be in compliance with the information classification scheme. The retention periods of technical and other auxiliary data and the documents administered in the information system should also be known. Information must not be overwritten, changed or deleted before the expiry of the retention period. Archival records must be transferred to the public archives – see subsection 13 (1).	
§ 13 (9)	(9) Before transfer of information from an existing information system to a new information system, the authority shall	This requirement should be especially observed when replacing these information systems which were created before the entry into force of the Regulation.	

	review the retention periods for the information. The information with an expired retention period and information not needed by the authorities using the new information system shall not be transferred. Retention periods shall be determined for the transferable information.	Replacement of an information system always involves an analysis of data in order to ensure the transfer of data from the old system to the new one. In each subsequent updating of a system, it will become more and more difficult to understand the meaning of the data that were already outdated and unnecessary at the time of their previous transfers. The retention of outdated information affects also the quality of open data and protection of personal data. Such information is to be destroyed instead of transferring it to a new system. The prerequisite is an appraisal decision of the National Archives that permits destruction – see subsection 13 (1). Archival records that are outdated for an authority must be transferred to the National Archives.	
§ 13 (10)	(10) Upon the development of a new or an existing information system, technological and organisational conditions shall be created to enable a person to get an overview of the data concerning him or her, which are processed in the information system, and to whom and when his or her personal data have been transferred from the system, and where possible, also who and when have used his or her personal data.	This requirement is connected with subsection 19 (1) of the Personal Data Protection Act and with measure 5.3.1.2 of the *Digital Agenda 2020 for Estonia*. The creation of organisational conditions means responding to the inquiries of persons. Technological conditions mean that an overview can be automatically generated on the basis of the information system data. This requirement is to be taken into account upon creation and development of information systems. For example, the data monitor that is being developed by the Information System Authority can be used to give an overview of the use of personal data in the information system.	
§ 13 (11)	(11) An authority shall publish on its website user-friendly information regarding: 1) the processing of personal data by the authority; 2) the access to the information provided for re-use by the authority, and the fee charged for the re-use of the information.	An interested person has to receive an overview regarding the processing of personal data as set out in clause 28 (1) 31^1) of the Public Information Act. An interested person has to receive an overview regarding reusable information, indicating what type of information it is, where it can be accessed and what the fee for the reuse is. It covers information on the provisions of subsections 14 (2^1), 25 (4) to (6), clause 28 (1) 31^2) and subsection 32^1 (1) of the Public Information Act.	

		User-friendly publication of information – see subsection 9 (1).	
§ 13 (12)	(12) An authority shall publish information describing its field of activity and direct public services in eesti.ee gateway in accordance with the requirements for publication of information in eesti.ee gateway provided for in the Public Information Act and legislation established on the basis thereof.	The eesti.ee gateway aggregates the information of authorities to better support persons in use of services. This necessitates special requirements for disclosure of information in the eesti.ee gateway. The special requirements are provided for in section 32^1 of the Public Information Act and in the Regulation of the Republic of Estonia *Requirements and Procedure for the Management of eesti.ee Gateway, Making Information Available, Development and Use of Information*.	
§ 14.	**Sharing and exchange of information**		
§ 14 (1)	(1) An authority shall find out the needs of different user groups for the information, manner and volume of presentation of the information, and shall take into consideration the needs of users in the development of processes and services.	To make right decisions quickly, the necessary information must be easily and quickly findable and be presented in the form and quantity that suits the given group of users. For example, about a direct public service, completely different information may be needed by the user of the service, employee of the service bureau, the person making the administrative decision, the service owner and the head of the authority.	
§ 14 (2)	(2) Authorities shall cooperate to share information and use it for the provision of services.	For example, it is not sufficient if an authority plans to ask the data necessary to its information system from the system of another authority – also the authority issuing the data must be aware of such plan in good time, as it has to plan its own resources for it (time and finance). It covers also the description of own information systems in the RIHA – see subsection 13 (2).	
§ 14 (3)	(3) The exchange of the information set out in subsections 2 (1) and (2) of the Archives Act which has been recorded on paper, in a computer file or an e-mail message (in this Regulation hereinafter the *document*) shall be replaced, where possible, for exchange of the data contained in the documents or for granting access to information.	See also subsection 12 (5). Access to the data that were previously exchanged in documents, or to other information (e.g. to a large document) can be enabled: by (1) a single inquiry, (2) granting relevant rights in an information system or portal, or (3) enabling access on a public web site (if the information is public).	

§ 14 (4)	(4) Authorities shall exchange documents between themselves electronically, unless they have to transfer: 1) a document which is not usable by the recipient in electronic form due to the format of the document or quality of presentation; 2) a paper document or file created before the entry into force of the Regulation or received, the digitation whereof is not expedient due to its volume or for an exceptional reason.	For example, it may be more sensible to forward on paper planning documents or bulky paper documents and files created before the entry into force of the Regulation.	
§ 14 (5)	(5) Constitutional institutions, governmental authorities and local authorities, and where possible, other authorities shall exchange documents between themselves electronically via the inter-authority document exchange centre (hereinafter the *DEC*) of the data exchange layer for information systems (hereinafter the *X-Road*). A document sent shall include metadata describing the document, which correspond to the list of metadata for document exchange, registered with the RIHA.	DEC is a secure document transmission method which facilitates the registration of documents, as documents are captured in EDRMS automatically, together with the standardised and machine-readable metadata which describe the document. Presently the data specifications of the metadata for document exchange (the so-called *DEC container*) are registered in the XML assets' subregister of the RIHA. All the senders and recipients of documents must use the same container to ensure smooth exchange of documents. The data description of DEC container is one of the guidelines for document management, and its files are published in the RIHA. The currently valid version must be used. Documents can be sent also to the official mailbox of a person via the DEC – see subsection 15 (2).	
§ 14 (6)	(6) The administration of the DEC shall be organised and the uninterrupted operation of the DEC shall be ensured by the Information System Authority. If the DEC is replaced for an alternative X-Road document exchange solution, the respective solution shall be devised and its implementation shall be	The Information System Authority has created the new exchange protocol DHX, as well as a standardised software component that facilitates transition to the new protocol. The Information System Authority will implement the solutions necessary for the transition also in the official mailbox service of persons. The implementation of the new exchange protocol is coordinated by the Information System Authority: it will coordinate the	

	organised by the Information System Authority. The resources required for ensuring the continuity of document exchange shall be provided for by the Ministry of Economic Affairs and Communications.	transition plan with authorities, monitor the application of the new protocol, handle the problems, counsel authorities and, as necessary, make changes to the developed solutions.	
§ 15.	**Sending of information via official e-mail address of person**		
§ 15 (1)	(1) If the addressee of the information set out in subsections 2 (1) or (2) of the Archives Act which is sent out from an authority is a person who has activated his or her official e-mail address in eesti.ee gateway and has not provided any other contact details for communication related to the given proceeding, the authority shall send a message regarding communication of the information to the official e-mail address of the person. The message shall include a reference to the web environment where the person can read the information after authentication and authorisation. The authority shall ensure that the web environment contains information regarding the time when the person examined the communicated information.	Information which is sent out refers to both documents as well as the so-called official information in other forms. An official e-mail address is personal identification code@eesti.ee and registry code@eesti.ee. To use it, a person has to forward the address to one or several personal or corporate e-mail addresses (in the near future, also to the mobile phone, etc.). The official e-mail address is for communicating with the public sector authorities, and a person can use it only if they agree with it. A person can submit other contact details for exchange of information in relation to a single proceeding (including post address). A person may withdraw their consent while discontinuing the forwarding of their official e-mail address. A notice sent to a person regarding communication of information does not contain sensitive information, and therefore such notice or the information sent need not be encrypted. Security is ensured by the fact that a person examines the received information in an electronic environment where they have authenticated and authorised themselves. The same environment is used for storing the information about the time when the person read the information sent to them. Information can be sent to a person in the form of a document or in any other form but it must be understandable to the person and usable, and it must not change later.	Not later than from 1 January 2019.
§ 15 (2)	(2) If an authority lacks a secure web	To the person's official mailbox, documents are sent through the	Not later than from

	environment for communication of the information referred to in subsection (1) above, the authority shall send a document via eesti.ee gateway's infrastructure service for official documents (hereinafter the *person's official mailbox*). The information stating that a document is sent to the person's official mailbox is sent to the person from eesti.ee gateway. Eesti.ee gateway shall provide the authority with information on the time when the document reached the person's official mailbox and when the person opened, downloaded or forwarded the document.	DEC. See also subsection 14 (5).	1 January 2019.
§ 15 (3)	(3) In addition to the information referred to in subsections (1) and (2), an authority may send a reminder or any other awareness raising message to the official e-mail address of a person, if it derives from the performance of a public law function imposed on the authority. An authority shall not send any information that is not related to the performance of a public law function, especially advertising, to the official e-mail address of a person.	To receive messages, a person may use the service of a reminder calendar of eesti.ee where the person can choose the types of messages that are of interest to them. Messages must not contain personal data or any other sensitive information – for communication of such information, see subsection 15 (1) and 15 (2) A person's official e-mail address cannot be used for sending information such as event advertising.	
§ 15 (4)	(4) Constitutional institutions, governmental authorities and local government authorities, and where possible, other authorities shall send information in the manner described in subsections (1) to (3).	See subsection 14 (5).	
§ 15 (5)	(5) The functioning of the activation of official e-mail addresses shall be ensured		

	and the administration and development of a person's official mailbox shall be organised by the Information System Authority. The resources required for it shall be provided for by the Ministry of Economic Affairs and Communications.		
§ 16.	**Organisation of document management**		
§ 16 (1)	(1) Document management and organisation of access thereto shall be governed by the requirements provided for in section 13, taking account of the specifications set out in this section.		
§ 16 (2)	(2) The sharing and exchanging of documents, and sending documents via a person's official e-mail address shall be governed by the requirements provided for in sections 14 and 15 above, taking account of the specifications set out in this section.		
§ 16 (3)	(3) An authority shall create, coordinate and process documents electronically. If it is necessary to issue a document on paper, the authority may issue a copy of the electronic document.	A document register is to be maintained in digital form – see subsection 11 (1) of the Public Information Act. A document register forms a part of EDRMS. Even though it is not recommended, working papers (drafts of documents, supplementary materials, etc.) can be created and used also on paper. However, if the draft of a document reaches the coordination stage, and if it may later be necessary to evidence the approval given or comments made in the course of coordination, the EDRMS will ensure the evidence. If a document must be sent on paper, an electronically created document can be signed or approved digitally in the EDRMS instead of signing it on paper, and then a paper copy can be sent out. If necessary, a certification notation can be added to the copy. In such case, the document creation process will be uniform both	

		for paper documents and digital documents up to the very end, and there will be no need to store any copies of the sent documents on paper.	
§ 16 (4)	(4) A document created by an authority shall have the mandatory elements, and in addition, also the elements inherent in the type of document. The mandatory elements are: 1) issuer of the document; 2) date; 3) contents; 4) signatory or approver of the contents or a notation regarding the automatic approval by the authority.	The elements of a document are within the document or are inseparably connected with the document. Examples of elements inherent in document types: (1) addressee, identifier of the document sent, original identifier of the document received, title (document type "letter"), (2) title of the instrument, preamble, part, section (document type "Act") Clause 1): In the public sector, the main issuer of a document is an authority, but also a body operating with the authority (working group, council, etc.). Clause 4): The element consists of several subelements (e.g. name, official title, structural unit and, as necessary, a text describing the method of signing or approval). The approver of the content is the person who is responsible for the contents of the document if the document is without a signature – see subsection 16 (7). A notice of the automatic approval of an authority is entered in the document if the document has been prepared automatically in the authority's information system.	
§ 16 (5)	(5) The composition of the elements of a document created by an authority shall be based on the data description of the respective document type if it is registered with the RIHA. Documents of the respective type and their web forms shall be prepared on the basis of the data description.	The data description of the document type consists of several parts: human-readable and machine-readable description of the document's elements and type-specific metadata together with the examples of the document, including displays. Presently data descriptions are registered in the XML assets' subregister of the RIHA. Data descriptions of different types of legislation are registered, including the data descriptions of single instruments (resolution, order, decree, precept).	
§ 16 (6)	(6) The text of a document created by an authority shall be unambiguously understandable and as concise as possible, and shall conform to the Estonian Literary	Estonian Literary Standard – see § 4 of the Language Act.	

	Standard.		
§ 16 (7)	(7) A document may be unsigned unless the requirement for a signature derives from legislation, provided that the authenticity, reliability and integrity of the document are ensured.	If a document is created and sent in a secure environment (e.g. web environment requiring a strong authentication instrument), the requirement for a signature is often surplus. A secure environment for sending a document may be, for example, EDRMS –> DEC (–> a person's official mailbox). See also subsections 13 (3), 14 (5), 15 (1) and 15 (2).	
§ 16 (8)	(8) An authority shall digitise a paper document received unless: 1) the document is not usable in a digitised form; 2) it is not expedient to digitise the document due to its volume or for an exceptional reason.	A digitised document is easier to find, to send and to electronically process. The quality of a digitised copy has to be checked before registration. See also subsection 14 (4), 14 (5) and 16 (3).	
§ 16 (9)	(9) An authority may return a digitised paper document to the person providing it or to the sender, or destroy it, if the transfer of information to an electronic medium took place in accordance with the procedure provided by archival rules and unless the requirement for preservation of the original derives from legislation.	It is reasonable to return, for example, a document that is handed over personally at a customers' service point, but also a diploma, certificate, statement or other document on paper that the person may need. At the same time, an original may also be retained on paper. An authority has to determine the practice to be used in each case. The originals which may have to be verified by handwriting assessment by experts or the preservation of which is required by legislation, must not be destroyed.	
§ 16 (10)	(10) An authority shall store the documents with a retention period of over 10 years and, where possible, also other electronic documents in an archival format. Where needed, the authority shall also retain a version in another format.	This requirement applies also to archival records. Archival formats are listed in annex 1 to the archival rules. Versions in another format may be necessary, for example, upon preparation of draft legislation or the subsequent versions of guidelines or other documents.	
§ 16 (11)	(11) A document shall be retained together with the metadata describing the document, its relationships and history of management. The metadata of a document shall conform	The uniformity of principal metadata facilitates the exchange of documents, transfer of documents from one EDRMS to another one and transfer of documents from an authority to digital archives. The document management metadata list is one of the	

	to the document management metadata list registered with the RIHA, and with the data description of the document type.	document management guidelines, and its files are published in the RIHA. The currently valid version must be used.	
§ 16 (12)	(12) While establishing a restriction on access to a document, an authority shall take account of the classifier of the bases of the restriction on access registered with the RIHA.	The classifier of the bases of the restriction on access must be applied in EDMRS and may be applied also in other information systems where appropriate. The classifier is one of the document management guidelines and its files, including the explanatory memorandum, are published in the RIHAs. The currently valid version must be used.	
§ 16 (13)	(13) An authority shall publish an electronic text document and a digitised copy of the paper document without any restrictions on access in PDF format or in any other human-readable format independent of application software via the document register.	Documents in PDF format can be read by different devices and software. PDF (A) is also an archival format. Other equivalent formats are allowed too. This requirement does not apply to the previously created documents which have already been published in other formats in the document register.	Not later than from 1 July 2018.
§ 16 (14)	(14) A state authority may transfer the electronic documents with a retention period of over 10 years which do not have archival value to the National Archives for storage. The National Archives shall ensure that the authority that transferred the documents shall have access to the documents. The expenses related to the transfer and storage of the documents shall be covered by the authority transferring the documents on the basis of expense standards established by the minister responsible for the area of archives.		
§ 17.	**Establishment of additional requirements for information governance**		
§ 17 (1)	(1) A coordinator or another competent authority may issue guidelines to specify the provisions of this Chapter. The coordinators	See subsection 10 (1).	The document management guidelines issued

	and competent authorities may issue joint guidelines.		under subsection 54^2 (1) of Regulation of the Government of the Republic, *Uniform Principles for Records Management Procedures*, have to be observed until the guidelines are updated or repealed. The guidelines are to be updated or repealed no later than by 1 January 2018.
§ 17 (2)	(2) If it is necessary to agree on a uniform response to a single case of application of legislation or guidelines, the council operating on the basis of subsection 5 (4) shall make a decision on the proposal of the coordinator. If a decision affects the work of local authorities and constitutional institutions, the representatives of these authorities shall be engaged in the preparation of the decision.	See subsection 10 (2). If representatives of local governments and constitutional institutions are engaged, the decision may, subject to an agreement with these authorities, cover also these authorities, or cover only governmental authorities.	
§ 17 (3)	(3) The detailed arrangement of the information governance of an authority shall be provided for in the instruments and guidelines regulating the internal work	See subsection 10 (3).	An authority is to take instruments and guidelines into conformity with

	procedure of the authority. The authority shall keep the instruments and guidelines up to date and support the conformity to the provided requirements by IT tools.		the requirements of the Regulation not later than by 1 July 2018.