List of Documents

	NAME OF THE DOCUMENT	EXPLANATION	+ / -
RULES ON THE PROCESSING OF PERSOAL DATA			
1.	Rules on the processing of personal data	The main document that every institution should have. It contains a set of measures to ensure proper compliance with the General Data Protection Regulation (hereinafter – GDPR).	
RELATIONS WITH DATA CONTROLLERS AND PROCESSORS			
2.	Agreement with the data processor	This is a necessary document if you have any agreements with IT, accountants and the like.	
3.	Agreement with joint data controllers	When two or more data controllers jointly determine the purpose and means of data processing, they are joint data controllers. In such case, the joint controllers must determine, by mutual agreement, their respective responsibilities for the fulfilment of their obligations under GDPR.	
RELATIONS WITH EMPLOYEES			
4.	Notification of personal data processed	The employer must inform employees about the processing of their personal data in concise, transparent, comprehensible manner and simple language.	
5.	Procedure for the use of information and communication technologies and for the monitoring and control of employees in the workplace	The employer must document in detail the procedure for the use of information and communication technologies and the monitoring of employees: which employees are being monitored, in which cases and under what conditions they are monitored. Employees must be informed, by signature or other means of proof, of the procedure, which must be clear and precise in order for the employees to understand the scope to which their personal data is being processed and any possible consequences of such actions.	
6.	Consent to the use of image	If the employee's image is to be made public (e.g. on the company's website), the employer must obtain the employee's consent to the use of the image.	
7.	Consent to the announcement of the date of birth, public birthday congratulations	The date of birth of employee may be announced publicly and (or) the employee is congratulated with birthday only with the employee's prior consent.	
8.	Legitimate interest assessment for employee e-communication tracking	In order to monitor the employee, the employer should usually perform a legitimate interest assessment to ensure that employer's interests outweigh the employee's interests and fundamental rights and freedoms. In this case, monitoring of employee can not be based on the mere consent of employee to be monitored (due to inherent dependence of the employer-employee relationship).	
9.	Data protection impact assessment for employee e-communication monitoring	Data protection impact assessment (hereinafter – DPIA) must be carried out when employee's personal data are processed for the purpose of employee monitoring and control. The DPIA should include a detailed assessment of potential hazards and risk management measures.	

10.	Consent to the storage of the candidate's personal data	Curricula vitae (CV) of job candidates may be kept only with the prior consent of the individual. Otherwise, curricula vitae of unsuccessful candidates must be destroyed immediately at the end of the recruitment process for a particular position.	
WEBSITE			
11.	Privacy policy	Every organization that maintains a website should publish a privacy statement on the website.	
12.	Consent for cookies	If cookies are used on the website, it is necessary to inform all website visitors about them. That is, when website window opens, a message should appear regarding cookies used on the website.	
DATA PROTECTION OFFICER			
13.	Job description of the data protection officer	The data protection officer is mandatory for public authorities or bodies and organizations which core activities consist of data processing operation that require regular and systematic monitoring of data subjects on a large scale or large-scale processing of special categories of data (e.g. personal health information).	
14.	Contract with data protection officer	Data protection officer may also conduct job duties without being employed by the data controller or data processor but rather acting under a service agreement. Therefore, a separate contract with data protection officer is necessary.	
PHONE CONVERSATION RECORDING			
15.	Rules for recording telephone conversations	The rules for recording telephone conversations must be regulated and systemized in a document written by the controller. In case of recording telephone conversations, employees must be informed of the purpose for which the telephone conversations will be recorded, when and which conversations will be recorded, who will listen to them, in which cases, and so on.	
16.	Legitimate interest assessment for recording telephone conversations	In order to record employee conversations with customers and (or) potential customers, a company should conduct a legitimate interest assessment to establish whether its interests outweigh the employee's interests, fundamental rights and freedoms.	
17.	Data protection impact assessment for the recording of telephone conversations	It is compulsory to carry out data protection impact assessment when recording telephone conversations.	
VIDEO SURVEILLANCE			
18.	Rules for video surveillance	The controller must provide the data subject with all information that will ensure fair and transparent processing of the data, taking into account the specific circumstances of the processing of personal data.	
19.	Legitimate interest assessment for video surveillance	Video surveillance is usually carried out based on the condition of lawful processing of personal data – the pursuit of one's legitimate interests. Where this condition is invoked, the legitimate interests of the data controller and data protection impact on the data subject should be assessed. What is more, the existence of a legitimate interest and the need for surveillance should be periodically reassessed (it is recommended once a year, depending on the circumstances).	

20.	Data protection impact assessment for video surveillance	Data protection impact assessment must be carried out when video surveillance is carried out in premises and (or) areas which are not owned by the data controller or on other lawful grounds; in health care, social care, prisons and other institutions where services are provided to vulnerable persons; together with sound recording; processing of personal data of employees for monitoring or control purposes; large-scale processing of personal data where personal data is not obtained from the data subject.	
21.	Informative notice regarding video surveillance	Data subjects should be aware of video surveillance by video cameras. They should be informed in detail about the sites monitored.	
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES			
22.	Binding rules for the company (hereinafter – BCR)	Personal data may be transferred on the basis of a BCR only if the personal data is transferred within a group of companies where part of the companies belonging to the group are located in a third country.	
23.	Standard contract terms	Personal data may be transferred to third countries in accordance with standard data protection terms and conditions.	
BREACHES OF PERSONAL DATA SECURITY AND SECURITY INCIDENTS			
24.	Procedure for responding to personal data security breaches	The procedure shall establish appropriate procedures for detection, reporting and investigation of personal data breaches. In the event that the size and importance of the breach may jeopardize data subject's rights and freedoms, the company must immediately notify the data subject of the personal data breach.	
25.	Data subject notification form	In the event of a personal data breach which may pose a "significant risk to an individual's rights and freedoms", the company must complete data subject notification form in order to inform him (her) of the data breach.	
26.	Supervisory authority notification form	In the event of a personal data breach which needs to be reported to the State Data Protection Inspectorate, the company must complete supervisory authority notification form to inform supervisory authority of the data breach.	
27.	Register of personal data security breaches	The controller must document all personal data breaches, including the facts related to the data breach, its effects and corrective actions taken. On the basis of those document, supervisory authority must be able to verify that the company has complied with all requirements.	
DIRECT MARKETING			
28.	Consent form for the use of direct marketing	Direct marketing may only be carried out with the prior consent of the data subjects, except in the case of exceptions provided by the law.	
29.	Right to object to the sending of direct marketing communications	A person who receives email contact details from his (her) customers when providing services or selling goods may use them to market his (her) goods or services, provided that customers are given clear, free and easily enforceable opportunity to object to or refuse to the use of contact details for direct marketing purposes.	
30.	Legitimate interest assessment for direct marketing	Where an undertaking sends direct marketing communications using an exception provided by the law without having consent of the data subject, it must justify a legitimate interest in sending direct marketing communications. Undertaking should make sure that its legitimate interests do not significantly affect the rights and freedoms of those people to whom direct marketing is addressed.	

OTHER ORGANIZATIONAL DATA SECURITY MEASURES			
31.	Personal data storage policy	This policy should include a process for deciding how long specific types of personal data will be stored and how after the set period it will be safely destroyed.	
32.	IT resource register	The company shall have a register of IT resources (used to process personal data). Proper management of hardware, software and network equipment is essential for the security and integrity of personal data, as it allows to control data processing measures. Resource management must include the registration of IT resources and the network typology (schema) that is used to process personal data.	
33.	Business continuity plan	Undertaking shall establish a general procedure which to be followed in the event of security incident or personal data breach in order to ensure the proper continuity of the processing of personal data by relevant IT systems.	
34.	Activity records	Document that records purposes of the data processing activities performed by the company, the data subjects and recipients, the deadlines for data deletion and other required and relevant information regarding data processing activities.	
35.	Access control policy	The security policy sets out the basic principles of information security and personal data protection. This is the basis for the implementation of all technical and organizational data security measures. Based on this policy, specific technical and organizational measures are described in more detailed policies (e.g. facility management, resource management). The security policy establishes overall security management of the organization's information and it must clearly emphasize and distinguish the protection of personal data.	
DOCUMENTS RECOMMENDED TO HAVE			
36.	Privacy Policy register	This document can be useful if privacy notices are posted in many different places and you want to control them and, if necessary, self-assess when and what changes were made.	
37.	Data protection impact assessment procedure	The document can be used when carrying out data protection impact assessments.	
38.	Legitimate interest assessment procedure	Useful document when carrying out legitimate interest assessment.	
39.	Data controller compliance checklist	The document can be used to verify the data controller's compliance with GDPR requirements.	
40.	Consent withdrawal form	Useful document if data subject wishes to withdraw his (her) consent to the processing of personal data.	
41.	Revocation of parental consent form	Useful document when processing data of persons under the age of 14.	
42.	Procedure for cross border transfers of personal data	Useful document if personal data is transferred outside the European Economic Area (EEA).	

The list is prepared in accordance with the requirements of the General Data Protection Regulation (GDPR) and the recommendations, guidelines and opinion prepared by the State Data Protection Inspectorate, the European Data Protection Board and the Article 29 Data Protection Working Party.