Questionnaire on information security and data protection for the processor

Name of the organisation (third party)	Name: .... Address: .... Business number (Crossroads Bank): ....
First name, Surname & e-mail address of the chief information security officer (CISO) (mandatory)	....
First name, Surname & e-mail address of the information security contact person (assistant CISO) (optional)	....
First name, Surname & e-mail address of the data protection officer (DPO) (mandatory)	....
First name, Surname & e-mail address of the local data protection contact person (assistant DPO or representative) (optional)	....
First name, Surname & e-mail address of the person responsible for day-to-day management (CEO, mandatory)	....

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
1	Do you have a formal, up-to-date information security policy approved by the person responsible for day-to-day management?	□ YES □ NO	
2	Do you have a risk assessment for each process/project for information security/data protection which you use for the provision of services?	□ YES □ NO	
3	Within your organisation: • is there a department responsible for information security reporting directly to the person responsible for day-to-day management of the organisation?	□ YES □ NO □ YES □ NO	
4	Do you have an information security plan approved by the person responsible for day-to-day management?	□ YES □ NO	
5	How many hours are worked by the CISO and his/her team? • CISO • Team How many hours of training on information security have the DPO and his/her team followed? • DPO • Team	1) hours/month 2) hours/month 3) hours/year 4) hours/year	
6	Do you have procedures for the development of new systems or major changes to existing systems so that the project leader can take account of the security requirements described in the minimum security standards?	YES NO N/A □ □ □	
7	Do you take appropriate measures so that the professional, confidential and sensitive data stored on mobile media are accessible only to authorised persons?	□ YES □ NO	
8	Do you take appropriate measures, depending on the access medium, for the information security of the access from outside your organisation to the professional, confidential and sensitive data?	□ YES □ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
9	Do you have teleworking facilities arranged in such a way that at the teleworking location (at home, in a satellite office or in another location) no information is stored on external appliances without encryption and that possible threats from the teleworking location do not reach the IT infrastructure?	☐ YES ☐ NO	
10	Do you call the attention of each staff member each year to information security and data protection and do you carry out an annual evaluation of compliance with this policy in practice?	☐ YES ☐ NO	
11	Have you secured access by means of a clear access procedure and have you implemented a (logical or physical) access system to prevent any unauthorised access?	☐ YES ☐ NO	
12	Do you have a classification system for personal data for which you are providing the services and do you apply this classification system?	☐ YES ☐ NO	
13	Have you processed the rules, specified in an 'E-mail, online communication and internet use' policy line, in an information security policy?	☐ YES ☐ NO	
14	Have you appointed at least one access manager when you make use of remote access to the healthcare institution?	☐ YES ☐ NO	
15	Have you encouraged your staff to read and apply extra security measures which the care provision imposes (if applicable)?	☐ YES ☐ NO	
16	If you wish to apply 'cryptography': • do you have a formal policy for the use of cryptographic controls? • do you have a formal policy for the use, protection and life of cryptographic keys for the entire lifecycle?	☐ YES ☐ NO ☐ YES ☐ NO	
17	Do you take the necessary measures to limit access to the buildings and premises to authorised persons and do you monitor this access both during and outside working hours?	☐ YES ☐ NO	
18	Do you take the necessary measures to prevent loss, damage, theft or compromise of equipment and interruption of the activities?	☐ YES ☐ NO	
19	In the case of reuse of the information carrier, do you use it again at a data classification level which is at least comparable?	☐ YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a ‘no’ response
20	Do you establish appropriate measures for the erasure of data contractually with the principal?	□ YES □ NO	
21	Do you apply the rules relating to logging of access as stipulated by the principal?	□ YES □ NO	
22	Have rules been laid down for the acquisition, development and maintenance of systems between the various parties concerned?	□ YES □ NO	
23	Do all staff members work with ICT resources for the purposes of the assignment on the basis of minimum authorisation for the performance of their task?	□YES □NO	
24	Have the access security requirements (identification, authentication, authorisation) been defined, documented, validated and communicated? Are these accesses logged?	□ YES □ NO □ YES □ NO	
25	Are the security and data protection risks established contractually between you and any subcontractors?	□ YES □ NO	
26	Do you use a checklist so that the project leader can obtain the assurance that all the information security and data protection policy lines have been evaluated correctly and if necessary implemented during the development phase of the project?	□ YES □ NO	
27	Each time a project is put into production, do you carry out a check that the security and data protection requirements laid down at the beginning of the project were also in fact implemented?	□ YES □ NO	
28	Under the supervision of the project leader, are there separated facilities for development, testing and/or acceptance and production – including the related separation of the responsibilities under the project?	□ YES □ NO	
29	Is each access to personal and confidential data logged in accordance with a logging policy and the applicable laws and regulations?	□YES □NO	
30	Is it included in project specifications how access to and use of systems and applications will be logged to contribute to the detection of divergences with regard to information security and data protection?	□ YES □ NO	

Question	*Place cross (X) in the box corresponding to your answer*	Explain in the case of a ‘no’ response

31	Does the log management at least comply with the following objectives? • The information to be able to determine by whom, when and how access was obtained to which information • The identification of the nature of the information consulted • The clear identification of the person	□ YES □ NO	
32	Have the necessary tools been made available to allow the log data to be operated by the authorised persons?	□ YES □ NO	
33	Do the transactional/functional log data correspond to the storage period corresponding to the data themselves (e.g. 30 years for medical data)?	□ YES □ NO	
34	Are the project deliverables (processed data, documentation (source code, programs, technical documents, etc.) integrated in the back-up management system?	□ YES □ NO	
35	In the course of the project development, have the requirements with regard to continuity of service provision been formalised, in accordance with your expectations?	□ YES □ NO	
36	Have your continuity plan and the related procedures been updated in line with the development of the project, including continuity tests?	□YES □NO	
37	Is a risk analysis carried out at the beginning of the project to define the emergency procedures?	□ YES □ NO	
38	In the course of the project development, are the procedures concerning incident management formalised and validated?	□ YES □ NO	
39	Is the CISO informed of security incidents and the DPO for incidents concerning data protection?	□YES □NO	
40	During the lifecycle of the project, is the documentation (technical, procedures, manuals, etc.) kept up to date?	□ YES □ NO	
41	Is all equipment, including purchased or developed systems added to the inventory of the operational resources?	□YES □NO	
42	Is appropriate cooperation given to audits carried out in the form of the personnel being made available, documentation, log management and other information which is reasonably available?	□ YES □ NO	
43	Are requirements concerning information security and data protection documented to mitigate risks concerning access to information tools?	□ YES □ NO	
45	Are all relevant requirements concerning information security and privacy drawn up and agreed between you and third parties/suppliers (who read, process, store, communicate information of the organisation or supply ICT infrastructure components and ICT services	□YES □ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
46	Are the services provided to you by third parties/suppliers monitored, evaluated and audited?	□ YES □ NO	
47	Are the changes in the provision of services to you by the third party/supplier managed, including keeping records of existing policy lines, procedures/measures for information security and data protection?	□ YES □ NO	
48	Do you have a 'Cloud computing' policy line when you call on cloud services?	□ YES □ NO	
49	When you wish to process professional, confidential or sensitive data in a cloud, do you satisfy the minimum contractual guarantees?	□ YES □ NO	
50	Do you have procedures for establishment and management of incidents relating to information security or data protection with the related responsibilities and have you made these procedures known in-house?	□ YES □ NO	
51	Do you have an agreement with all staff members that each staff member (permanent or temporary, in-house or external) is required to report unauthorised access, use, alteration, disclosure, loss or destruction of information and information systems?	□ YES □ NO	
52	Are the incidents and weaknesses of information security or data protection relating to information and information systems made known to the principal so that you and the principal can take appropriate corrective measures in good time?	□ YES □ NO	
53	Does the supplier have a procedure to communicate/report incidents concerning information security/data protection in-house as quickly as possible?	□ YES □ NO	
54	In the case of information security or data protection incidents, is the evidence collected correctly in accordance with statutory and regulatory requirements?	□ YES □NO	
55	Is each information security or data protection incident formally validated so that procedures and control measures can be improved and are the lessons drawn from an incident communicated to your management for validation and approval of further actions?	□ YES □NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
56	Do you have a continuity plan for all critical processes and essential information systems?	□ YES □ NO	

57	Are information security and data protection an integral part of your continuity management?	□ YES □ NO	
58	Do you have your own continuity plan? Is this plan tested and adapted regularly with the necessary communication to your management for validation and approval?	□ YES □ NO □ YES □ NO	
59	Do you carry out a conformity audit periodically with regard to the situation concerning information security and data protection?	□ YES □ NO	
60	Do you have a formal disciplinary process for employees who have breached information security and data protection?	□ YES □ NO	
61	Do you regularly collate all information to map the risks in connection with conformity with the GDPR and do you take the necessary actions as a result of a high ‘residual’ risk of non-conformity?	□ YES □ NO	
62	Do you have an up-to-date central register of the controller or of the processor and do you have formal accountability for non-implementation of control measures focusing on compliance with the European Regulation for the specific processing?	□ YES □ NO	

Date and signature of the CISO or data management officer (DPO) of the organisation (third party) (optional)	.... Date Signature
Date and signature of the person responsible for the day-to-day management of the organisation (third party) **(mandatory)**	.... Date Signature

******* END OF THIS DOCUMENT *******