T - TECHNICAL AND ORGANIZATIONAL MEASURES CHECKS & CONTROLS (TOM)

The following criteria aim at addressing technology and organization measures set in place to secure the processed personal data. "Suggested Means of Verification", including referred documents, shall be assessed against the criteria until sufficient evidences are collected to determine

Ref ID	Applicant	Specific / Generic	Level	TITLE	CRITERIA applicable to the Target of Evaluation (prescriptive clauses)	Suggested Means of Verification
T.1			**A**	**Core Security Requirements** The Applicant must set in place adequate measures to secure personal data and to ensure their		
T.1.1				**Data Access Restriction**		
T.1.1.1	CP	G	A	Access rights minimization (least privilege)	A) Access rights shall be limited and delivered on a need basis in conformity with the "Least privilege" principle.	Access rights registry and rules. Inspection.
T.1.1.2	CP	G	A	Access rights registry updates	A) There shall be a procedure or a mechanism in place to systematically adapt the access rights in case an employee leaves the company or changes activity within the company.	Procedures and mechanisms. Inspection and sample test analysis. Interview of the DPOs and employees.
T.1.1.3	CP	G	A	Password policy	A) There shall be a password policy in place that specifies a minimum length, complexity requirements, and renewal frequency for the passwords. AND B) Where applicable, the password policy to access stored data shall be compliant with the national laws and regulations.	Documentation review. Inspection and demonstration. Testing the access control mechanism.
T.1.1.4	CP	G	A	Physical access restriction	A) Access to the rooms where personal data are stored on servers shall be restricted and protected by effective access control mechanisms.	Inspection of physical access controls and physical access rules.
T.1.1.5	CP	G	A	Bring Your Own Device restriction policy	A) The Applicant shall have a written policy in place that: a.1) restricts the use of personal mobile devices; a.2) (AND) is known by the employees who have access to the servers.	Policy. Inspection. Interview of employees.
T.1.1.6	CP	G	B	Automated session logout	A) The access to the stored personal data shall be protected by an automated session log out mechanism.	Inspection and demonstration. Testing the access control mechanism.
T.1.1.7	CP	S	B	Multi-factor authentication	A) Access to stored data by the employees and agents of the Applicant shall require multi-factor authentication.	Inspection and demonstration. Testing the access control mechanism.
T.1.2				**Data Encryption**		
T.1.2.1	CP	G	A	Encrypted communication over public networks	A) The Applicant shall have rules, policies or mechanisms in place to ensure that remote access to personal data is encrypted when passing through public networks (such as the Internet).	Documentation review. Website inspection. Sample tests. Data flow analysis and verifications. Interview of the CISO.
T.1.2.2	CP	G	B	Backups encryption	A) The backup files shall be encrypted.	Inspection and demonstration. Sample analysis.
T.1.2.3	CP	G	B	User Log data encryption	A) The logs of data subject access, including Internet website logs, shall be encrypted.	Inspection and demonstration. Sample analysis.

T.1.2.4	CP	S	B	Data at rest encryption	A) The stored personal data shall be encrypted.	Inspection and demonstration. Sample analysis.
T.1.3				**Other Security Measures**		
T.1.3.1	CP	G	A	Backup recovery test	A) A Procedure shall be in place to perform a data recovery test at least once a year. AND B) The last backup recovery test shall be less than 12 months old. AND C) Where recovery tests identify issues to be addressed, the Applicant shall have taken action on the identified issues.	Backup recovery test report. Interview of the CISO.
T.1.3.2	CP	G	A	Regular server updates	A) There shall be a procedure, configuration or a mechanism in place to ensure that the servers are patched on a regular basis and any time there is a critical security patch required. AND B) The servers shall be effectively updated and patched as needed on a regular basis.	Rules and procedures. Test reports. Inspection and sample test analysis. Interview of the DPOs and employees.
T.1.3.3	CP	G	B	Denial of Service mitigation	IF the personal data are intended to be accessed online by the Data Subjects, THEN: A) Measures shall be in place to mitigate the risk of Denial of Service attacks.	Denial of Service mitigation
T.1.3.4	CP	G	B	Fire and flood protection	A) Protection measures shall be set in place to protect the servers where the personal data are stored against: a.1) fire; a.2) (AND) flood.	Inspection of fire and flood protection measures.
T.1.3.5	CP	G	B	Firewalling with least privilege port policy	A) A firewall shall be in place and configured to protect remotely accessible servers that store personal data. AND B) The firewall configuration shall block all ports that are not needed.	Firewalling configuration. Tests. Interview of the CISO.
T.1.3.6	CP	G	B	Updated antivirus	A) A security solution, containing at least an antivirus application, shall be deployed to protect the servers and terminal devices under the control of the Applicant that are used for the processing in the Target of Evaluation. AND B) A policy, procedure or a mechanism shall be in place to ensure that the security solution is kept up-to-date.	Inspection. Date of the last antivirus update.
T.2			**B**	**Extended Security Requirements** **IF the Target of Evaluation includes High Risk Data Processing as specified in the Certification Scheme**		
T.2.1				**Connectivity Checks for Internet access**		
				Condition: IF the Target of Evaluation includes Internet access, THEN:		
T.2.1.1	CP	G	B	HTTPS enabled	A) HTTPS shall be enabled by default for accessing the web interface.	Inspection and test
T.2.1.2	CP	G	B	SDNS enabled	A) Secure DNS (SDNS) shall be enabled for public domain names resolution.	Inspection and test
T.2.1.3	CP	G	B	SSL	A) Unsecure SSL shall NOT be used.	Inspection and test
T.2.1.4	CP	G	B	TLS	A) Unsecure TLS shall NOT be used.	Inspection and test
T.2.1.5	CP	G	B	SSH	A) Unsecure SSH shall NOT be used.	Inspection and test
T.2.1.6	CP	G	B	Backward incompatibility	A) Backward compatibility with unsecure SSL or TLS versions shall be disabled.	Inspection and test

T.2.1.7	CP	G	B	WiFi	IF the Target of Evaluation processes personal data through WiFi, THEN: A) The WiFi access shall be configured to use: a.1) WPA2 or higher; a.2) (OR) WPA2-PSK or higher; a.3) (OR) a solution as secure as WPA2. AND B) The WiFi network accessible to visitors shall be separated from the WiFi used for internal purpose.	Inspection and test
T.2.2				**Crypto Management**		
T.2.2.1	CP	G	B	Protection Tools Management Policy	A) There shall be a written policy framing the introduction, maintenance and phasing out of protection tools.	Policy. Inspection. Interview of employees.
T.2.2.2	CP	G	B	Cryptographic Policy	A) The Applicant shall have a cryptographic policy in place that specifies: a.1) the cryptographic algorithms to be used; a.2) (AND) the generation, update, escrow and revocation (destruction) of keys; a.3) (AND) the adequate key length requirements. a.4) (AND) the time period after which the keys must be changed.	Cryptographic policy.
T.2.2.3	CP	G	B	Key Length	A) The key length shall be sufficient to comply with the current state of the art, including a transactional data symmetric security level of at least: a.1) 80 bits for data stored less than 5 years; a.2) (OR) 128 bits for data to be stored for a period of 5 years or more.	Inspection Sample test
T.2.2.4	CP	G	B	Key Update	A) The keys shall be updated in due time according to the key management policy.	Inspection Sample test
T.2.2.5	CP	G	B	Key revocation	A) The compromised keys shall be effectively revoked.	Inspection Sample test
T.2.3				**Penetration Tests and Monitoring**		
T.2.3.1	CP	G	B	PEN Test	A) The Applicant shall perform penetration tests: a.1) on a yearly basis and after significant changes that may affect the security; a.2) (AND) the last penetration test shall be less than 12 months old; a.3) (AND) there shall be a procedure in place to ensure that the results of the PEN Tests are addressed.	Penetration test
T.2.3.2	CP	G	B	Intrusion Detection	A) The Applicant shall have rules, procedures or mechanisms in place to detect and report intrusions.	Documentation review Inspection Interiew of the CISO