ASSESS THE SECURITY LEVEL OF THE PERSONAL DATA IN YOUR ORGANISATION

Have you considered...?

FACTSHEET		MEASURE	
1	Raising user awareness	Inform and raise awareness among individuals handling data	□
		Write an IT charter and enforce its application	□
2	Authenticating	Define a unique identifier (login) for each user	□
		Adopt a user password policy conform to our recommendations	□
		Require each user to change his or her password whenever it has been resetted	□
		Limit the number of access attempts to an account	□
3	Access Management	Define authorisation profiles	□
		Remove obsolete access permissions	□
		Carry out an annual review of authorisations	□
4	Logging access and managing incidents	Implement a logging system	□
		Inform users of the implementation of the logging system	□
		Protect logging equipment and the information logged	□
		Organise the procedures for personal data breach notifications	□
5	Securing workstations	Organise an automatic session locking procedure	□
		Use regularly updated antivirus software	□
		Install firewall software	□
		Collect the user's consent before any intervention on his or her workstation	□
6	Securing mobile data processing	Organise encryption measures for mobile equipment	□
		Undertake regular data backups and synchronisations	□
		Require a confidential piece of information to unlock smartphones	□
7	Protecting the internal network	Limit the network traffic to the bare essentials	□
		Secure remote access to mobile computing devices via VPN	□
		Implement the WPA2 or WPA2-PSK protocol for Wi-Fi networks	□
8	Securing servers	Allow access to tools and administration interface only to qualified individuals	□
		Install critical updates without delay	□
		Ensure availability of data	□
9	Securing websites	Use the TLS protocol and check its implementation	□
		Check that no password or identifier are transferred via URLs	□
		Check that the user inputs correspond to what is expected	□
		Place a consent banner for cookies not required by the service	□
10	Ensuring continuity	Carry out regular backups	□
		Store the backup media in a secure place	□
		Organise security measures for the transport of backups	□
		Organise and regularly test the business continuity	□
11	Archiving securely	Implement specific access methods to archived data	□
		Destroy obsolete archives securely	□
12	Supervising maintenance and data destruction	Record maintenance in a register	□
		Have a responsible person from the organisation supervise work by third parties	□
		Delete the data from all hardware before it is discarded	□
13	Managing dataprocessors	Add a specific clause in the contracts of subcontractors	□
		Organise the restitution and destruction conditions of data	□
		Ensure the effectiveness of provided guarantees (security audits, visits, etc.)	□
14	Securing exchanges with other organisations	Encrypt data before sending it	□
		Ensure that it is the right recipient	□
		Send the secret information separately and via a different channel	□
15	Physical security	Restrict access to the premises via locked doors	□
		Install anti-intrusion alarms and check them periodically	□
16	Supervising software development	Offer parameters that respect the privacy of end users	□
		Avoid comment zones or supervise them strictly	□
		Carry out tests on fictional or anonymised data	□
17	Using cryptographic functions	Use recognised algorithms, software and libraries	□
		Keep the secret information and cryptographic keys in a secure way	□