magora

№	Issues for self-management	Complaint ("+" or "-")
1.	Your company has a list of every type of personal information it holds, the sources of that information and details of how long this data will be retained, as well as a list of the organisations with whom the data is shared.	
2.	Your company has a list of sites where it stores personal information and the ways data flows between them.	
3.	Your company has a publicly accessible privacy policy that outlines all processes related to personal data.	
4.	Your privacy policy includes an explanation of your company's lawful basis for processing personal information.	
5.	Company employees are informed about upcoming changes enforced by GDPR.	
6.	The Data Protection Supervisory Authority relevant to your Member State is identified or representative (for non-EU countries) appointed.	
7.	Data sharing and processing agreements with other organisations are reviewed and their compliance with the GDPR evaluated.	
8.	The role of the Data Protection Officer (DPO) is established.	
9.	The contact details of the DPO are accessible to data subjects and the contact process is simple and appropriate.	
10.	Mechanisms for establishing and receiving consent from data subjects are implemented.	
11.	A simple and clear consent withdrawal method for data subjects is introduced.	
12.	Data subjects' consent is obtained specifically for each processing activity. (Bundled consent is not allowed).	
13.	Methods of obtaining and storing consent are determined and implemented.	

If you need support in development or automation of any GDPR-related procedures or wish to conduct an independent test for GDPR-compliance in your company, contact our representatives: Dmitry: +44 20 3393 1772 James: +44 07 397132798

14.	Procedures for responding to subject access requests by data subjects are developed.	
	Data for subject access requests is provided in appropriate digital format and, when required, can be transmitted to a new provider.	
15.	Procedures to fulfill data subjects' rights to object to data processing, rectify and erase their data are established.	
16.	Procedures for ensuring that all copies and extracts are provided, rectified or erased upon data subject's requests, are provided.	
17.	All data processes are documented and bought into alignment with GDPR requirements.	
18.	For services targeted directly at children, appropriate practices for verifying data subjects' age and, where necessary, for gaining parental or guardian consent are established.	
19.	Use of pseudonyms is implemented to replace direct and indirect personal data identifiers in data systems with meaningless data values that can be reversed under the right conditions.	
20.	Encryption of data in use, at rest, and in transit is provided.	
21.	Data breach identification, blocking and forensic investigation capabilities are established for rapid awareness of active breach attempts by malicious actors.	
22.	An automatic reporting system of data breaches involving personal data is created to inform local authorities and data subjects involved within timeframes established by GDPR.	
23.	Automated data deletion processes are functioning for data for which your business no longer has any use.	
24.	Customers are systematically informed about updates to the privacy policy.	
25.	Procedures for conducting a data protection impact assessment for high-risk processing of sensitive data are established.	
26.	You have a list of sub-processors, the use of which is mentioned in your privacy policy.	
27.	Check that you've addressed all points and have tested the implemented solution.	

If you need support in development or automation of any GDPR-related procedures or wish to conduct an independent test for GDPR-compliance in your company, contact our representatives: Dmitry: +44 20 3393 1772 James: +44 07 397132798