INFOSECTRAIN

Azpirant TECHNOLOGIES

GDPR ASSESSMENT CHECKLIST

@infosectrain

SWIPE LEFT

INFOSECTRAIN

Azpirant TECHNOLOGIES

01 Governance & Accountability

Article	Requirement	Compliance
5	Do you have a comprehensive data protection policy that shows compliance with processing, privacy by design, and record keeping requirements?	
5	Do you provide comprehensive training to all staff members on GDPR standards and principles, including processing activities, controls, privacy impact assessments, audits, data subject rights, reporting lines, and privacy by design, as well as the potential consequences of noncompliance?	
5	Do you frequently check your employees' comprehension of GDPR regulations by testing, retraining, and maintaining records of training?	
38	Does the data protection officer (DPO) you need to ensure GDPR and other data protection rules are followed have the appropriate resources, independence, and reporting power to the highest level of management?	
38	Is the DPO required to carry out his or her duties in confidence or secrecy?	
38	Have the DPO's additional responsibilities been evaluated to prevent conflicts of interest, if any?	
37	Does the DPO possess the skills and expertise necessary to carry out the duties listed in Article 39?	
37	Have you given the necessary supervisory authority, the general public, and internal staff members access to the DPO's contact information?	
24	Do you have a policy to protect people's personal information?	
24	Do you have a policy and procedures for handling data breaches, incidents, and notifications?	
24	Do you have a set of procedures that are documented for obtaining, processing, and storing personal data?	

INFOSECTRAIN

Azpirant TECHNOLOGIES

02 Data Protection Impact Assessment

Article	Requirement	Compliance
35	Is the Data Protection Officer (DPO) always involved when a Data Protection Impact Assessment (DPIA) is being carried out?	
35	Do you, if applicable, seek the opinions of the data subjects or their representatives on how the data are intended to be processed?	
35	Do you conduct DPIA whenever there is a possibility that the processing may involve a high risk or will have a substantial impact on a data subject?	
35	Do you have a procedure in place for detecting changes in risks, and do you evaluate DPIAs for changed risks?	
35	Does the DPIA include an analysis of whether the processing activities are absolutely necessary and in what proportion they should be in relation to the purposes?	
24	Do you have any established policies and processes that you follow while carrying out a DPIA?	
36	Do you give the measures and safeguards that are provided to preserve the rights and freedoms of data subjects, in the event that you consult with the Supervisory Authority?	
36	Do you give the Data Protection Officer's contact information when contacting the Supervisory Authority?	
36	Are there measures in place to protect against any risks that each DPIA may present?	
36	Do you specify the specific duties of the controller (if relevant) while consulting the Supervisory Authority?	

INFOSECTRAIN

Azpirant TECHNOLOGIES

03 Privacy by Design & Secure Processing

Article	Requirement	Compliance
24, 25, 28, 32	Do you use encryption and/or pseudonymization to protect personal data?	
24, 25	Do you limit access to personal data to just the personnel who are actually responsible for processing the data?	
25, 32	Do you set up all of the systems and networks with defaults that have a high level of security?	
32	Do you regularly audit and test systems and services to make sure that continuing confidentiality, integrity, availability, and resilience are maintained?	
	Do you have business continuity strategies that are well-documented, sturdy, and tested to quickly restore access to and availability of personal data in the case of a technical or physical incident?	
24, 25	Do you use redaction and other storage and processing techniques on tangible copies of personal data?	
32	Do you guarantee that, in the event of physical or technological incidents, processes and systems can be restored?	
24, 25	Do you have established, documented processes for destroying data that is no longer required, and do you take steps to ensure that personnel follow those processes?	
25	Do you support gathering and processing only the minimal amount of data required for the outlined purposes?	
25	Is information gathered electronically (through forms, websites, surveys, etc.) minimised so that only the fields necessary for the processing goal are used?	

INFOSECTRAIN

Azpirant TECHNOLOGIES

04 Processing Principles

Article	Requirement	Compliance
32	Have you conducted a risk assessment to determine, evaluate, quantify, and track the impact(s) of processing?	
24	Do you uphold your data retention and records management policies?	
30,32	Do you internally audit every processing activity?	
5	Are personal records only preserved as long as necessary to fulfil the processing goals?	
6	Do you recognise and demonstrate the legal justification for each and every processing of personal data?	
5	Are personal records current and accurate, and are all practical measures made to guarantee that incorrect records are immediately deleted and corrected?	
9	Are you processing special category in accordance with one or more of the requirements of Article 9(2)?	
5	Have the principles used to support detention durations been documented?	
6	Do you conduct a review to ensure compliance with one or more of the lawfulness of processing conditions before receiving & processing personal information?	
5, 6	Has personal data been handled fairly, legally, and openly?	

INFOSECTRAIN

Azpirant TECHNOLOGIES

05 Data Protection Officer (DPO)

Article	Requirement	Compliance
38	Is the DPO required to maintain the privacy of any information?	
37	Has the Supervisory Authority received the DPO's contact information?	
38	Has the DPO identified, established, and disseminated the data protection governance structure's reporting lines?	
37, 39	Has the DPO been evaluated and confirmed to possess the necessary skills and knowledge to oversee adherence to the GDPR and the company's own data protection goals?	
37	Have you given a certain individual the authority to manage data protection compliance?	
38	Has the DPO's other responsibilities been examined to rule out any potential conflicts of interest?	
37	Have you made the Data Protection Officer's contact information available?	
38	Does the Data Protection Officer (DPO) have enough access, resources, and funding to carry out their duties?	
38	Are the DPO's appointment and contact information known to all employees?	
37, 39	Has the DPO been evaluated and confirmed to possess the necessary professional qualifications and competence to work with the Supervisory Authority?	

INFOSECTRAIN

Azpirant TECHNOLOGIES

06 Data Subject Rights

Article	Requirement	Compliance
18	Do you limit processing when the veracity of personal data is questioned to allow for verification?	
15	Do you make sure that the categories of personal data involved are communicated to the data subject when they exercise their right to access?	
19	Do you inform all processors and other receivers of personal data about corrections, erasures, and processing limitations?	
18	Do you have a procedure for limiting processing when data subjects ask for it when processing is no longer required or legal?	
12	Do you have policies and safeguards in place to guarantee that every piece of personal data can be delivered electronically?	
15	Do you make sure that all of the things stated in Article 15(1) are disclosed to a data subject who exercises their right to access?	
22	Do you make sure that data subjects have the right to be exempt from choices that have a legal basis or have a similar impact on them?	
20	Do you provide personal data to another controller in a machine-readable format upon a subject's request?	
16	Do you have procedures in place for updating incorrect personal data and finishing up incomplete personal data?	
21	Do you stop processing data from data subjects who object to it being used for direct marketing?	
15	Do you make sure that a data subject who exercises their Right to Access has the option to file a complaint with a supervisory authority?	

INFOSECTRAIN

Azpirant TECHNOLOGIES

07 Consent and Information Disclosures

Article	Requirement	Compliance
13, 14	When data is collected from data subjects, are privacy notices and policies given to them? If not, are they given to them within a month if not?	
13	Do you make sure that the contact information for the Data Protection Officer is supplied at the time of consent when personal data is obtained directly from the data subject?	
7	Are consent requests legibly distinct from other topics, presented in an understandable and accessible format, and worded in a simple and straightforward manner?	
12	Are all exchanges with data subjects conducted in writing, using language that is straightforward, clear, and concise?	
7	Do you have proof that the individuals whose data were processed gave their consent?	
7	Do you have transparent audit trails that can be used to prove consent and the source of it?	
7	Are data subjects prompted to voluntarily opt-in (using distinct, unchecked opt-in boxes in accordance with Recital 32)?	
7, 13, 14	Does the privacy notice detail the various ways you intend to use the personal data?	
7	Do individuals who provide their personal information have the right to withdraw their consent at any time, and is doing so as simple as providing it?	
7	Is the procedure for revoking consent straightforward, easy to use, and quick?	
6, 7, 13, 14	Does your privacy notice specify the legal justification for processing clearly?	

INFOSECTRAIN

Azpirant TECHNOLOGIES

08 Breach Management

Article	Requirement	Compliance
33	Do you keep track of information on data breaches, their effects, and the corrective steps that were taken?	
34	Does the report provide a description of the nature of the personal data breach when informing the Supervisory Authority?	
33	Do you, as a processor, promptly inform the controller of any data breaches as soon as you become aware of them?	
34	Does the report include the categories and approximate number of data subjects in question when alerting the Supervisory Authority?	
34	Do you notify affected data subjects of breaches without excessive delay and in simple and understandable language?	
34	Regardless of their size or breadth, are all breaches looked into and fixed?	
32	Are security procedures (such as backup, pseudonymization, encryption, and testing) in place and suitable for the dangers associated with data?	
34	Does the report provide a description of the likely effects of the personal data breach where informing the Supervisory Authority?	
33	Do you have an updated plan for responding to data breaches?	
34	Does the report to the Supervisory Authority contain actions to mitigate any potential detrimental effects?	
24, 33, 34	Do you have policies and processes in place for breach incidents and notification?	

INFOSECTRAIN

Azpirant TECHNOLOGIES

09 Data Transfers & Sharing

Article	Requirement	Compliance
28, 32	Do you do a data sharing evaluation, identify the benefits and dangers of sharing the data, and record them before sharing or disclosing personal information?	
45	Do you frequently review the Official Journal of the European Union for the withdrawals and modifications to data transfer authorizations made by the Commission?	
28, 32	Do you perform a data sharing evaluation before sharing or disclosing personal information, identifying and recording how it should be shared?	
46	Do administrative agreements or contractual terms include procedures to ensure proper data transfer safeguards?	
46, 47	Do you make sure that applicable safeguards are in place and that binding corporate rules are applied where you are transferring?	
32	Do all of your communications—including email, file transfers, website forms, and payments—involve secure data transmission methods?	
47	Are all of the items in Article 47(2) specified in enforceable corporate rules?	
32	Do you use encryption and communicate just the information that is required when transferring or exposing personal information?	
28, 32	Do you do a data sharing evaluation and identify and record the aims and intent of sharing when sharing or disclosing personal information?	
44	Have you found every global data export method and flow?	