GDPR - Checklist

JESI is considered to be a Processor that engages and integrates with Sub-processors

Definition: Processor
A natural person or legal entity that processes personal data on behalf of the controller (e.g., a call centre acting on behalf of its client) is considered to be a processor. At times, a processor is also called a *third party*.

JESI provides cloud-based software that ‘customers’ or ‘controllers’ purchase and as a company JESI has a responsibility to ensure that the security provisions maintained in the SAAS are compliant to the obligations under the GDPR.

	Activity	**Commentary**	**Expected Time Line or Completed**
1	Conducted an information audit to map data flows		Completed
2	Documented what personal data JESI holds, where it came from, who the data is shared with and what is done with it.		Completed
3	Appropriate data protection policy		Completed
4	Nominated a data protection lead or Data Protection		Completed

	Officer (DPO)		
5	Decision makers and key people in the business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business	Agenda item on monthly team meetings	Compliant & Ongoing
6	Business manages information risks in a structured way so that management understands the business impact of personal data related risks and manages them effectively.	Ongoing and reviewed regularly using a risk management matrix.	Compliant & Ongoing
7	Business has implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities	Risk Management Matrix that captures and manages all JESI technology and identifies security gaps.	Compliant & Reviewed Monthly
8	Business provides data protection awareness training for all staff.	Processes are adjusted to comply with OAIC Australian Privacy Principles and UK Gov Data Protection	Compliant & Ongoing
9	Business only processes data on the documented instructions of a controller and there is a written contract setting out the respective responsibilities and liabilities of the controller and the JESI business.		Comply
10	Business has sought prior written authorisation from the controller before engaging the services of a sub-processor, and there is a contract in place		Comply

11	If the business operates outside the EU, an appointed representative within the EU in writing.		Comply
12	The business has effective processes to identify and report any personal data breaches to the controller	See JESI Data Security and Risk Management Policy April 2018	Ongoing
13	The business has a process to respond to a controller's request for information (following an individual's' request to access their personal data)	Controllers have full access to any data logged in the JESI system and when required provide email authorisation for specific reporting	Completed
14	The business has processes to ensure that the personal data held remains accurate and up to date.	Controllers are responsible for ensuring the accuracy of their own personal data.	Completed
15	The business has a process to routinely and securely dispose of personal data that is no longer required, in line with the agreed timescales as stated in your contract with the controller.	JESI is a technology tool that is used for a legislative safety requirement and is required to retain data for a period of time as determined by the controller.	Completed
16	The business has procedures to respond to a data controllers' request to suppress the processing of specific personal data.	Controllers are responsible for their own specific personal data.	Completed
17	The business can respond to a request from the controller to supply the personal data process in an electronic format.	Controllers have full access to any data logged in the JESI system. Accessible when required by providing email authorisation for specific reporting	Completed
18	Your business has an information security policy	See JESI Privacy Policy April 2018	Completed

	supported by appropriate security measures.		