	Review Considerations	Control in Place	Reference / Link	Comments
	The EU General Data Protection Regulation (the GDPR or the Regulation) is the primary data protection law in the European Union. While it builds on the principles of the 1995 directive on data protection (Directive 95/46/EC), its extra-territorial scope and the introduction of significant changes entail extensive and considerable efforts for organizations worldwide. It imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation went into effect on May 25, 2018.			Click Here for the Regulation
GOVERNANCE AND ACCOUNTABILITY	We maintain company policies that cover privacy and data protection principles and are current			
	We have documented GDPR requirements and best practices in a formal program			
	We review the 99 articles of the GDPR and related guidance to determine how the regulation applies to our operations			
	We record identified areas subject to GDPR and review these at least annually with our data protection officer/contact, legal and compliance to determine continued application			
	We conduct a regular data mapping exercise is conducted to remain current on our data processing activities			
	We conduct our data mapping exercise to collect information on:- • What personal data we hold • Where it came from • Who you share it with • Legal basis for processing it • What format(s) is it in • Who is responsible for it • Access level			
	We make sure that our GDPR Program requires the design of systems to include from the beginning appropriate technical and organizational measures to help meet the requirements of the Regulation and protect the rights of data subjects			
	We require implementation of appropriate technical and organizational measures not only to ensure compliance, but also to demonstrate these measures are in place using the GDPR's Six Principles: - Lawful, Fair and Transparent Processing - Purpose Limitation - Data Minimization - Data Accuracy - Storage Limitation - Integrity and Confidentiality			
	We have designated and documented key roles and responsibilities for our GDPR program			
	We keep HR policies and procedures current (and if applicable, revised) to ensure that employee's individual rights under the GDPR are considered and complied with			
	We have a current resource to assist with questions from data subjects as further documentation to help demonstrate compliance with GDPR			
	We maintain our GDPR program through periodic reviews that are conducted at least annually to make sure program components are current and compliant against internal and external changes			
DATA PROTECTION OFFICER (DPO)	We have designated responsibility for GDPR compliance to a Data Protection Officer (DPO) or similar role			
	We provide the DPO with sufficient access to senior management, ongoing support and the budget to perform the role			
	We have instituted a reporting mechanism between the DPO and senior management			
	We have informed relevant stakeholders of the DPO's appointment and contact details			
	We have published the contact details of our DPO			
	We have communicated the DPO's contact details to the relevant Supervisory Authority(ies)			
	Our DPO has sufficient expertise in GDPR requirements and any other relevant and applicable data protection laws and practices, as well as our			

	Review Considerations	Control in Place	Reference / Link	Comments
	The EU General Data Protection Regulation (the GDPR or the Regulation) is the primary data protection law in the European Union. While it builds on the principles of the 1995 directive on data protection (Directive 95/46/EC), its extra-territorial scope and the introduction of significant changes entail extensive and considerable efforts for organizations worldwide. It imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation went into effect on May 25, 2018.			Click Here for the Regulation
CONSENT	We can always demonstrate that consent has been given			
	If processing is based on consent, we request for consent is made in a clear and transparent format, using plain language			
	Our consent request is made in an easily accessible format			
	Our consent request is always presented in a manner that is clearly distinguishable from the other matters			
	We require consent to be active and not based on silence, inactivity or pre-ticked boxes			
	We clearly state that the data subject has the right to withdraw consent at any time and provide a simple, accessible and quick process to submit withdrawals			
	We retain clear audit trails to evidence consent and where it came from			
	We maintain a Privacy Notice/Policy (on our website, contracts, emails, etc.) that is used to ensure compliance with the conditions for consent and information disclosure rules			
	We maintain a policy that the provision of good and services cannot be made contingent on consent to processing which is not necessary for the service being supplied			
	We maintain a policy not to obtain or process the personal data of a child under 16 years			
NOTICES	We have notices that include the requisite information as applicable including: - purposes of processing and legal basis for processing - details of data transfers outside the EU - recipients, or categories of recipients - retention period - rights of individuals (e.g., access, erase, rectify, objection to processing, withdrawal, etc.) - automated decision making - how to submit a complaint - the categories of information and the source(s) of the information			
	We maintain data subject request processes and timeframes that are reviewed and updated as needed to comply with GDPR requirements			
DATA BREACHES	We maintain current and documented data breach procedures are maintained as part of our incident response program			
	We make sure relevant stakeholders are advised periodically of the GDPR data breach procedures, including what constitutes a breach, who to			
	We maintain a log of all reported / identified breaches and sent to our DPO periodically for review			
	We require all identified and reported breaches to be investigated to resolution			
	Where a data breach has been evaluated in consultation with the DPO and deemed likely to result in a risk to the rights and freedoms, we make a report of the breach to the Supervisory Authority within 72 hours			
	We maintain records related to our data breach investigations			

	Review Considerations	Control in Place	Reference / Link	Comments
	The EU General Data Protection Regulation (the GDPR or the Regulation) is the primary data protection law in the European Union. While it builds on the principles of the 1995 directive on data protection (Directive 95/46/EC), its extra-territorial scope and the introduction of significant changes entail extensive and considerable efforts for organizations worldwide. It imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation went into effect on May 25, 2018.			Click Here for the Regulation
DATA SUBJECT REQUESTS	We maintain procedures to process data subject requests on a timely basis			
	If we cannot identify the data subject/individual, the request will not be processed			
	No fee is charged to process data subject requests UNLESS certain exceptions apply and the fee is reasonable ("repetitive requests", "manifestly unfounded or excessive requests" or "further copies)			
	If this right is exercised, we provide the data subject with: • Purpose of processing; • Categories of data; • Recipients of data; • Data storage period; • Rights to rectify or erase personal data • Rights to restrict processing of personal data or to object to such processing • Right to file a complaint with a supervisory authority • Source of data; • Existence of automated processing, associated logic and consequences; and • Safeguards for transfer to third countries or international organizations.			
SECURITY & RECORDKEEPING	Daily data backups are performed and all backups are kept in a secure, restricted access location			
	Pseudonymization and/or encryption methods are used to secure personal data			
	Pseudonyms and their personal identifiers and/or encryption methods and their secret keys are always kept separate			
	Minimum information necessary for the purpose specified is obtained			
	Data by electronic means and use is collected only the relevant fields relevant to the processing purpose			
	Documented destruction procedures are in place for information that is no longer necessary, or part of an individual's consent withdrawal or right to erasure			
	Hard copy data is used for storing or processing to ensure data minimization			
	Strong passwords are required and enforced across our organization through documented procedures published to our staff			
	Passwords to networks, computers and backups are changed periodically			
	Access to personal information is restricted to only those authorized individuals processing the data			
	Strong security defaults are activated on all systems and networks			
	Audits and reviews are conducted to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services			
	Documented audit and review process are in place for regularly testing, evaluating and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing			
	Remediation of issues and gaps resulting from our documented audit and review processes are monitored			
BCP	We maintain documented and tested business continuity plans to restore the availability and access to personal data in a timely manner in the event of a business interruption or breach			

	Review Considerations	Control in Place	Reference / Link	Comments
	The EU General Data Protection Regulation (the GDPR or the Regulation) is the primary data protection law in the European Union. While it builds on the principles of the 1995 directive on data protection (Directive 95/46/EC), its extra-territorial scope and the introduction of significant changes entail extensive and considerable efforts for organizations worldwide. It imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation went into effect on May 25, 2018.			Click Here for the Regulation
DATA PRIVACY IMPACT ASSESSMENT	We conduct a DPIA if processing is likely to be high risk or cause significant impact to a data subject			
	Our DPO is included in the evaluation and mitigating action plan			
	We include an evaluation of the risks to the rights of data subjects			
	We require remediation measures to address/mitigate identified risks			
	We factor data protection measures into new projects			
	Data protection measures are factored in as early as possible within any new project lifecycle, so that evaluations and recommendations can be incorporated into the design of the processing operation			
	We report DPIA results where required to regulators and external stakeholders			
	We monitor resolution of privacy / data protection issues flagged during our DPIA			
AWARENESS & TRAINING	We educate/train employees, management and other stakeholders on the GDPR requirements and our GDPR program			
	We provide Periodic notices on the GDPR and our GDPR program are provided to maintain awareness			
	We have measures in place to verify and evidence employee knowledge and understanding of the GDPR			
	We deliver training or communications on the GDPR requirements at least annually			
	We provide GDPR awareness notices and training to third-parties engaged to process or store personal data related to our processing activities			
MONITORING & TESTING	We document and include audit and Monitoring plans for our GDPR program			
	We audit all GDPR and associated data protection procedures periodically			
	We include compliance with the GDPR and relevant data protection laws into our monitoring , reporting, evaluations measures			
	We evaluate new processes and/or systems for risks to data protection and GDPR compliance			
	We include GDPR in our risk assessment program, including reviewing processing activities regularly to ensure they are still valid and effective			
	We have mechanisms in place to spot check processing activities to measure compliance with the GDPR			
	We report monitoring, evaluation, and audit results to management and responsible areas for action			
	We monitor remediation measures related to GDPR monitoring and audit results to their resolution			
	We keep records and results of our audit and monitoring reviews and make sure to refer them to our DPO or similar role			
DATA TRANSFERS	When transferring or disclosing personal information, the data is encrypted and includes only what is necessary			
	Secure data transfer methods for communications are used			
	A transfer of personal data to a third country or international organization (outside of the EU) is effected only if one or more of the below conditions applies:			
	if the receiving country/organization ensures an adequate level of protection (Adequacy Decision)			
	In the absence of an Adequacy Decision, we rely on appropriate safeguards			
	We use compliant standard contractual clauses			
	Provisions are inserted into administrative arrangements which include enforceable and effective data subject rights			
	DPO and other relevant stakeholders are involved in the setup of any personal data transfers			