GDPR Compliance Policy

Policy Owner: <Job title of policy owner>

Effective Date: <Date you choose, after which there will be consequences for personnel for non-compliance>

Application

This policy applies to all employees, contractors, and vendors while doing business with <Company Name> and others who have access to European Union (EU) and the European Economic Area (EEA) data subject information ("personal data") in connection with <Company Name>'s operating activities.

Policy

<Company Name> is committed to protecting the security, confidentiality, and privacy of its information resources including EU and EEA personal data in accordance with the requirements set forth in the General Data Protection Regulation (EU) 2016/679 ("GDPR", "Regulation"). Personal data shall only be processed when there is a legal basis to do so, data shall be managed to ensure that security, confidentiality, and privacy are maintained, and data will be used only for authorized purposes. All employees and contractors of <Company Name> share the responsibility for safeguarding personal data to which they have access.

When performing commercial activities in support of <Company Name> products and services that impacts EU/EEA personal data, <Company Name> may engage in certain activities which may require it to receive, store, process, transmit, create, or access and use data which may trigger compliance requirements with the provisions applicable to GDPR. This policy and the GDPR Policies adopted hereunder are intended to support the mission of <Company Name> and to facilitate data processing activities that are important to <Company Name> by:

- Ensuring compliance with requirements imposed by GDPR and <Company Name>'s regulatory obligations
- Providing for the establishment of GDPR Policies that set forth, among other things, the required technical, physical, and administrative safeguards to maintain the security, confidentiality, and privacy of personal data
- Setting forth the roles and responsibilities necessary for <Company Name> to meet its obligations with respect to activities related to the processing of personal data in accordance with GDPR

Roles and Responsibilities

Policy Adoption

<Company Name> shall, in cooperation with relevant stakeholders, develop and adopt necessary and appropriate GDPR Policies, which will include, among other things, the technical, physical, and administrative safeguards required to ensure the confidentiality, integrity, and privacy of personal data, and protect personal data against reasonably anticipated threats or hazards and unauthorized uses or disclosures. All relevant <Company Name> stakeholders shall cooperate with <Company Name> in the development and implementation of the GDPR Policies.

The <Company Name> Information Security and Data Privacy Policies are a component of the GDPR Policies and implement controls which support GDPR compliance.

Responsible Person

<NAME>, <TITLE>, <EMAIL>, <PHONE> has been assigned responsibility for overall oversight of <Company Name>'s GDPR compliance program.

Data Protection Officer

The Data Protection Officer (DPO) shall have the responsibilities set forth in this Policy and GDPR Article 39. The DPO is tasked with daily and ongoing oversight and management of <Company Name>'s GDPR Compliance Program, which includes the following responsibilities:

- Monitoring <Company Name>'s internal compliance with GDPR
- Providing guidance at the earliest stage possible on all aspects of data protection
- Keeping <Company Name> stakeholders appraised of changes to GDPR and other relevant laws and regulations
- Assisting the controller or processor in monitoring internal compliance with the Regulation, including:
    - Collecting information to identify processing activities
    - Analysing and checking the compliance of processing activities
    - Informing, advising and issuing recommendations to the controller or the processor
- Acting in an independent manner, and ensuring there is no conflict of interest in other roles or interests that the DPO may hold
- Maintaining inventories of all personal data stored on behalf of the data controller or processor
- Responding to security, privacy, and data access requests and complaints from data subjects
- Managing data security and critical business continuity issues that could impact personal data
- Providing guidance, as requested, to the data controller to complete a data protection impact assessment ("DPIA")
- Providing guidance on responding to accidental or malicious activity that could impact personal data
- Cooperate with the supervisory authority as needed
- To act as the contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter

The **Data Protection Officer** is: <NAME>, <TITLE>, <EMAIL>, <PHONE>

Article 27 Local Representative

For entities operating outside of the EU, Representatives must be named (a Representative is defined in Article 4 as "a natural or legal person established in the [EU] who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under the GDPR."). Representatives must be established in one of the EU Member States where the data subjects whose personal data the company processes are located. Companies operating in the UK must also appoint a UK Representative. Primary responsibilities include:

- Serving as the contact point for all issues related to the company's processing of personal data under the GDPR, including as a contact point for supervisory authorities
- Understanding current data protection laws, legal or compliance requirements, and interfacing with regulatory authorities

Representative(s) is/are:

EU Representative: <NAME>, <TITLE>, <EMAIL>, <PHONE>, <COUNTRY>

UK Representative: <NAME>, <TITLE>, <EMAIL>, <PHONE>, <COUNTRY>

Implementation

Data Protection

All personal data requires a legal basis for processing, and will be accessible on a strict need-to-know basis. Personal data is to be kept confidential and must be protected and safeguarded from unauthorized access, modification and disclosure.

- Storage and Transmission: Personal data must be encrypted, with strong cryptography, whenever stored on or transmitted by <Company Name> systems
- Disposal: Paper records must be securely shredded prior to disposal. Electronic media must be securely wiped, sanitized or physically destroyed prior to disposal or reuse
- Awareness Training: Relevant personnel will receive appropriate training on their information security and data privacy responsibilities with regard to GDPR and the handling of personal data as well as the Data Subject Access Request (DSAR) procedure
- <Company Name> will not transmit EU or UK PII to any third-party or vendor until an appropriate Data Protection Addendum has been fully executed by <Company Name> and the third-party.
- The company shall retain Record of Processing Activity in accordance with Article 30 of the GDPR. Records shall include:

○ the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
○ the purposes of the processing;

- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Breach Notification

Notification of any reportable unauthorized use or disclosure of personal data will be sent to affected parties in accordance with the GDPR notification requirements and the Incident Response Policy.

Data Subject Access Requests (DSAR/SAR)

Subject to the exceptions noted below in this policy, <Company Name> will comply with any SAR concerning the following rights of the data subject:

- Access (a copy of the personal data undergoing processing)
- Rectification of personal data (correction of data stored or processed)
- Erasure ('right to be forgotten')
- Restriction of processing
- Notification regarding rectification or erasure
- Data portability (In the event of a Data Portability Request, <Company Name> will export the customers data in an industry standard format and make it internet accessible for download only by the data subject)
- Objection to processing (withdrawal of consent to processing)
- Automated individual decision-making, including profiling
- Do Not Sell requests under the CCPA

SAR when <Company Name> is the data controller:

- A SAR must be made on <Company Name>'s privacy page <Company Name>.com/privacy. <Company Name> may provide an "interface" or self-service mechanism that the data subject is instructed to use to initiate the SAR process.
- A SAR can also be made using the email address privacy@<Company Name>.com.
- Where required, the data subject must provide reasonable evidence of their identity in the form of valid identification of identity, for example, email verification.
- When submitting the SAR via the interface, the data subject must identify the SAR type that is being requested, e.g., erasure.
- If a SAR is submitted by an agent, the submission must include the identification of the data subject.

SAR when <Company Name> is the data processor:

- The SAR must be submitted via the user interface in the <Company Name> Services.
- The controller must identify the SAR that is being requested.

SAR requirements:

- The date by which the SAR is submitted, identification is verified, and the specification of the SAR request type must be recorded; <Company Name> will acknowledge any manual requests within 3 business days.
- <Company Name> has one month from the initial request date to complete the request. There are very limited circumstances in which an extension to that one month will be provided.
- The SAR application will be documented and can be audited using the <process or interface> or <Company Name>'s internal processes.

<Company Name> as the data processor

- Customers will be provided instructions on how to access the data through the user interface or APIs.
- To the extent the customer is unable to access the data or has issues with accessing the data, <Company Name> will assist the customer in accessing their data.
- <Company Name> will collect the data specified by the data subject and process according to the instructions provided by the data controller.
- <Company Name> will maintain a record of requests for data and of its receipt, including dates.

<Company Name> as the data controller

- Collect the data specified by the data subject
- Search all databases and all relevant filing systems (manual files) in <Company Name>, including all back up and archived files, whether computerised or manual, and including all email folders and archives. <Company Name> maintains a record that identifies where personal data in <Company Name> is stored.
- <Company Name> will maintain a record of requests for data and of its receipt accessible by <Company Name>'s Data Protection Officer, <Chief Legal Officer>, and/or any other designated <Company Name> representatives. <Company Name> will also keep a record of processing to include dates.
- Provide data subjects an online mechanism to making request and all such requests will be logged.
- <Company Name> will acknowledge the SAR within three (3) days of the initial request and respond to any SAR within 25 days of the initial request.
- SARs from employees or previous employees will be coordinated with HR and the employees' current or previous departmental leadership.

SAR Exemptions

- <Company Name> may withhold information requested under SAR in accordance with Article 23 of the GDPR or any similar exemption under applicable law. Any such exemption must be reviewed and approved by the Data Protection Officer or <Chief Legal Officer>.

SAR Limits

Where permitted by law, such as Article 15 of the GDPR, for any further copies of personal data collected by <Company Name> that are requested by the data subject, <Company Name> may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic format.

Compelled Disclosure

<Company Name> governs the compelled disclosure of customer Personally Identifiable Information pursuant to valid third-party legal demands for such information, such as court orders, search warrants, subpoenas, government investigations, and similar demands, and is incorporated by reference into <Company Name>'s Privacy Policy.

Upon receipt of legal demands for information,<Company Name> will immediately notify the <Chief Legal Officer>, and Data Protection Officer. <Company Name>will investigate the demands, and if it is determined at <Company Name>'s sole discretion that they are valid, we will search for and disclose the information that is specified and that we are reasonably able to locate and provide. We are unable to process overly broad or vague demands, and we will not disclose information that is not specifically demanded, except in response to follow-up demands.

<Company Name> may contact customers if we are compelled to disclose their information pursuant to valid legal demands for such information, but we are not required to do so, and in some instances, we may be legally prohibited from doing so.

All external communications with customers, regulators and law enforcement shall be approved by <Company Name>

Enforcement

The <roles responsible for the enforcement of this policy, e.g., Chief Human Resources Officer, HIPAA Security Officer, Chief Information Security Officer and Legal Counsel> are responsible for the enforcement of this policy.

Employees who may have questions should contact <who employees should contact with questions about the enforcement of this policy, e.g., their local Information Security, IT or HR management representative> as appropriate.

Disciplinary Action

Failure to comply with any provision of this policy may result in disciplinary action, including, but not limited to, termination.

Reporting

All suspected violations or potential violations of this policy, no matter how seemingly insignificant, must promptly be reported either to <recipient(s) or policy violation reports, e.g., Legal Counsel, or <Company Name>'s Data Privacy Officer immediately, or via the incident reporting process at <incident reporting email, e.g., incidents@companyname.com>>.

As long as a report is made honestly and in good faith, <Company Name> will take no adverse action against any person based on the making of such a report. Failure to report known or suspected wrongdoing of which you have knowledge may subject you to disciplinary action up to and including termination of employment.

Version History

Version	Date	Description	Author	Approved by
<1.0>	<Date of change>	Initial policy	<Author of changes>	<Approver of changes>