Privacy Policy

Privacy is a cornerstone of building trust in **The Fab Tap, LLC**, a Minnesota limited liability company ("**we**", "**us**" and "**our company**") in all the ways we serve our customers, employees, vendors and clients. It is our policy to comply fully with all applicable data privacy and security laws that regulate our company in the state of Minnesota and all other states within the United States of America in which we do business. Furthermore, our company also strives to implement best practices and principles in the use of all personal data.

The purpose of this Data Privacy Policy (this "**Policy**") is to establish a company culture of respect for the privacy of personal data and to inform our employees, agency employees, independent contractors, interns, volunteers and vendors of our company-wide commitment to protect privacy in all aspects of our global business. It is important that all of those who have access to, or process personal data, comply with this Policy.

Scope

We are committed to complying with all applicable data privacy laws, rules and regulations applicable to our business. We shall collect, process, and transfer personal data responsibly in accordance with the principles and obligations as set forth below, unless this or any company policy conflicts with stricter requirements of local law, in which case, any local law will prevail. This Policy is intended to articulate our core data privacy principles that are applicable worldwide and which we seek to integrate into all company operations, policies and procedures. This Policy is not intended to be exhaustive and encompassing of all explicit privacy requirements that may apply to particular businesses or in particular countries. Rather, this Policy sets the foundational privacy and data protection policy requirements that shall be universally present in all our operations involving the processing of personal data.

This Policy applies to all full and part-time employees, agency employees, interns, volunteers, and independent contractors of our company. It also applies to all suppliers and vendors who process personal data from us or that provide personal data to us, regardless of geographic location or of any form or medium in which personal data may be processed (i.e. oral, paper, electronic). All who process personal data on behalf of our company are responsible for ensuring that they comply with the principles stated in this Policy, as well as any supporting data governance policies, procedures, contracts or directives developed by individual business units to meet the requirements of this Policy.

Failure to comply with this Policy will be treated seriously and may result in disciplinary or legal action, including termination of employment. Any breach of this Policy may result in personal liability and even criminal prosecution, as well as exposing our company to regulatory enforcement actions, fines and contractual claims, including claims for compensation from individuals.

Definitions

"Data Subject" "means the individual person to which Personal Data applies. Data Subjects can be our employees ("**Associates**"), customers, clients, independent contractors and our vendors. Data Subjects cannot be businesses.

"External Personal Data" means Personal Data Processed about Data Subjects that are external to us, such as our customers, clients, vendors and contractors.

"Internal Personal Data" means Personal Data Processed about Data Subjects that are internal to us, such as Associates, independent contractors, volunteers, and interns.

"Personal Data" means any information relating to an identified or identifiable natural person (Data

Subject) that enables a Data Subject to be identified from a larger group of people, directly or indirectly, in particular by reference to an identifier or data element. Personal Data does not include data that has been made anonymous, aggregated, de-identified or otherwise rendered incapable of identifying an individual Data Subject.

Examples of Personal Data

It is important for all of us to be aware of how Personal Data can be used in different ways to intentionally and unintentionally identify an individual Data Subject or disclose information about a Data Subject. For this reason, we should be aware of both Direct Identifiers and Indirect Identifiers in the Personal Data we use at our company.

Direct Identifiers. Some Personal Data can directly identify a Data Subject, such as someone's name, email address, driver's license number or credit card number. Generally, the following Personal Data elements, alone, can provide the ability to directly identify a Data Subject from a larger population. For example, a Social Security Number or an email address is specific to one individual. At the same time, the ability of a Direct Identifier to isolate one person from a larger population can still vary in the context of the information to which someone has access, and other data available to the user. For example, a typical Direct Identifier such as first and last name may not sometimes still not be specific enough, as would be the case with a more common first and last name, such as "John Smith."

First and Last Name	Employee performance data (e.g., ratings, reviews, salary bands)
Telephone Number	Social Security Number or National Identification Number
Email Address	Driver's license number
Employee Identification Number	Tax identification number and category
Date of Birth	Information about criminal history, civil judgments, or administrative sanctions
IP address	Biometric data (Pictures, fingerprints)
Home Address	Genetic data
Credit card information	

Indirect Identifiers**.** However, other Personal Data that are not Direct Identifiers are still capable of identifying a Data Subject when combined with other data. Indirect Identifiers have the potential to identify a Data Subject, depending on the context in which it is made available and what other information is accessible, such as one's age, gender, marital status or eye color. For example, if a male, age 89, lives in Zip code 44111, it is quite possible those three indirect identifiers of gender, age and ZIP code would be enough to identify that male by name if he were the only male of the age in the ZIP code, or possibly the only person of that age in the ZIP code.

Marital Status	Nationality
Number of Children	Ethnicity
Geographic subdivisions (i.e. ZIP Code or Area Code)	Health Information
Skin color	Disability Status
Gender	Sexual orientation
Hair color	Number of sick days or days off
Behavioral data (e.g., number of visits to a website, log details, how long employee works on a specific task)	Records about working times, breaks, holidays
Salary or bonus information	IP Address

The preceding lists are for illustrative and awareness purposes only, and are not intended to be exhaustive. The ability to identify a Data Subject, directly or indirectly, continually evolves with the

addition of data, changes in Processing purposes and technology capable of Processing such Personal Data. Therefore, we should always be thoughtful about which Personal Data elements we are using and how to ensure we are not unintentionally disclosing more about an individual than intended.

"Processing" of Personal Data means any operation that can be carried out in relation to data, such as collection, use, analysis, disclosure, storage, deletion, retention or transfer.

"Sensitive Personal Data" means certain sensitive subcategories of Personal Data, as defined by applicable laws or legal agreements with the company. What constitutes sensitive data can vary from country to country. At our company, Sensitive Personal Data can include personal health data, financial data, credit worthiness data, student data, Personal Data collected online from children under the age of 13 (U.S.) or 18 (E.U.), and information that can be used to carry out identity theft or fraud.

Privacy Principles

We see privacy and data protection as essential, fundamental components of our business and commitment to customers, business partners and our Associates. Accordingly, this Policy and our approach to privacy are firmly rooted in the globally-recognized Fair Information Practice Principles, which include the following core principles.

1. Transparency in Processing. We will be open and transparent to the degree possible about our developments, practices and policies with respect to Personal Data. To the degree possible and allowed by law, we will seek to provide notice of such data Processing practices in advance of such Processing, be it in form of agreements, disclosures, privacy policies or procedures. Likewise, when possible, we shall always seek to disclose the relevant parties involved in any such Processing of Personal Data and for what purposes.

When the informed consent of a Data Subject is required by law and whenever feasible, we will obtain it. All Personal Data held by us must be treated as confidential at all times, regardless of the form in which such Personal Data are Processed (i.e. oral, paper, electronic). All Personal Data shall be fairly and lawfully collected, Processed and/or transferred in accordance with the rights of the Data Subject and applicable law. We shall not transfer Personal Data to another entity, country or territory unless appropriate steps have been taken to transfer such Personal Data in accordance with the company's representation to the Data Subject's, applicable agreements, or applicable law. We will make all notifications or filings to applicable data protection authorities as may be required by local laws.

2. Limited Processing. In our Processing of Personal Data, we will place limits on the purposes for which Personal Data are Processed.

- Purpose Specification Principle. The purposes for which Personal Data are Processed should be specified no later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. When possible, we will provide choices to Data Subjects on the purposes for which Personal Data will be Processed.

- Collection and Use Limitation Principle. Personal Data should not be collected, disclosed, made available or otherwise used for purposes other than those specified in any posted policy, contract or other notice, except with the consent of the Data Subject or under applicable law. Furthermore, we shall seek to use only the minimum Personal Data required to complete any transaction, respond to any request, or provide any service.

- Retention Principle. Personal Data shall not be kept for a period of time longer than necessary for the purpose for which it was collected and/or Processed and shall be deleted, de-identified or otherwise rendered incapable of identifying the Data Subject by the end of such a lawful retention period.

3. Data Subject Rights in Processing. A properly authenticated Data Subject shall be able to exercise the following rights in relation to any Personal Data we control about the Data Subject.

- to obtain from us, or any party authorized by us, a confirmation of whether or not we have Personal Data related to the Data Subject;

- to know the source of, and have access to, any Personal Data under our control relating to the Data Subject within a reasonable time of any valid request by the Data Subject; such a request may be processed at a charge, provided it is not excessive;

- if required by applicable law, request a portable data set of such Personal Data that is usable by the Data Subject, the access to which shall be provided in a reasonable manner and the Personal Data in a form the Data Subject can readily understand and use, if such provision is within the company's capabilities and not overly burdensome;

- to challenge Personal Data relating or attributed to the Data Subject and, upon validation of the challenge, have the data erased, rectified, completed or amended; and

- to be given reasons if a request or challenge is denied, and to be able to challenge or escalate such a denial for review.

4. Quality and Accuracy in Processing. Personal Data should be relevant to the purposes for which it shall be Processed, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. To the extent possible, applicable, or as required by law, Data Subjects will have direct access to any Personal Data held about them and have the ability to modify or delete such Personal Data.

5. Security in Processing. We cannot promise the privacy of Personal Data without also ensuring the security necessary to keep such data private. Personal Data shall be protected by all reasonable safeguards to protect against such risks as loss or unauthorized access, destruction, use, modification or disclosure. we shall use security measures comprising layered administrative, technical and physical security safeguards to protect the confidentiality, availability and integrity of Personal Data.

6. Accountability and Redress in Processing. We are accountable for implementing data governance measures to fulfill the requirements of this Policy. We shall continually assess our Processing practices and implement the policies, procedures and data governance measures required to ensure Personal Data are Processed in accordance with this Policy to give effect to these principles. Each company shall ensure its personnel are properly trained on the proper use of such Personal Data and have access only to the Personal Data necessary to fulfill assigned job duties. Any individual who fails to comply with this Policy or any other data privacy or security policy may be subject to discipline, up to, and including termination of employment or contract.

We may, from time to time, use third parties to Process Personal Data on its behalf. Our accountability for such data governance shall extend to such third parties and the company shall only choose third parties which comply with our data privacy requirements and information security controls, take reasonable steps to ensure compliance and enter into written contracts warranting such compliance.

Effective Date and Enforcement

This Policy is effective as of November 19, 2020. As of the effective date, this Policy replaces and supersedes any former policy related to our use of all Personal Data. Any person subject to this Data Privacy Policy that has questions or concerns or any person who needs further advice or has any concerns or issues about handling Personal Data, should contact hello@thefabtapco.com.