Data Privacy Policy

Table of Contents

1. Purpose

Protecting the security and privacy of Personal Data (defined below) is important to Bio-Techne and its subsidiaries and affiliated companies ("Bio-Techne", "we" or "our"). Our goal is to conduct our business in compliance with applicable laws on data privacy protection and data security.

In the course of our business, Bio-Techne needs to gather and use certain Personal Data about individuals. The Personal Data collected can include information related to individuals associated with our customers, suppliers, business contacts, as well as employees and other people the organization has a relationship with or may need to contact. This Data Privacy Policy ("Policy") describes how this Personal Data must be collected, handled and stored to meet the company's data protection standards and to comply with global data privacy laws.

The policies and procedures set forth in this Policy outline the Personal Data that Bio-Techne may collect, how Bio-Techne uses and safeguards that Personal Data, and with whom it may be shared.

Each employee, officer and director must accept responsibility for adherence to this Policy. Violations of this Policy may lead to serious sanctions including, for an employee, discipline up to and including immediate termination, at the sole discretion of the company. The Company may, in addition, seek civil recourse against an employee, officer or director and/or refer alleged criminal misconduct to law enforcement agencies.

2. Data Privacy Principles

To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully. Bio-Techne recognizes that personal information should be responsibly handled, which includes, collecting, using, and storing it based on the following Principles:

- Processing Personal Data lawfully, fairly, and in a transparent manner, consistent with the purpose for which is was collected;
- Limiting collection of Personal Data to what is necessary for the purpose of collection;
- Maintaining the accuracy of Personal Data;
- Deleting Personal Data when it is no longer needed;
- Using appropriate security measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage through appropriate technical or organizational measures.

3. Scope and Definitions

This Policy applies to Personal Data processed by Bio-Techne employees throughout the organization, including its subsidiaries and affiliates, and is enforceable among all Bio-Techne employees in all operating units of Bio-Techne globally. All employees should to adhere to the requirements of this Policy when handling Personal Data.

3.1. What Does this Policy Control?

This Policy governs the ***Processing*** of the ***Personal Data*** of a ***Data Subject***.

3.1.1. What is a Data Subject?

In short, a Data Subject is a person. We are only concerned with data about natural persons, or Personal Data. Businesses are not Data Subjects, although the employees of a business are typically considered Data Subjects. Bio-Techne may have data about businesses that is confidential, but not of concern under this Policy, (e.g., proprietary information of a customer relating to its proprietary technology would typically be governed by a non-disclosure agreement (NDA) and would not fall within this Policy).

3.1.2. What is Personal Data?

Legal definition: Personal Data "means any information relating to an identified or identifiable natural person (i.e. Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

In practice, Personal Data is any piece of information that allows you to identify a person (i.e., Data Subject). Examples include:

- contact information and general identifiers
  - name
  - home and business addresses
  - home and business cell phone or telephone
  - fax and pager numbers
  - home and business e-mail addresses
  - emergency contact information
  - dates of birth
  - marital status
  - citizenship information
  - birth date and place
  - information on related persons or beneficiaries
  - photographs and other visual images of an individual
- employment, performance, compensation and benefits
  - bank account and payroll information
  - employment history and letters of recommendation
  - resume and any information included in a job application
  - work restrictions and accommodations
  - work related accident information
  - grievance resolutions
  - disciplinary action
  - hire date
  - employee identification number

    - job title
    - position/grade
    - attendance
    - department
    - business unit
    - supervisor
    - work site/location
    - projects
    - performance reviews
    - salary, bonus, long term incentives
    - retirement
    - family member/dependents' names
- education and training
    - education level
    - institution and field/focus/major
    - competency assessments
    - professional licenses and certifications
    - training courses
- IT
    - computer or facilities access and authentication information
    - individual account login information and passwords
- expense and travel
    - passport information/number
    - corporate or personal credit card number
    - bank account information
    - travel booking details
    - other travel information (e.g. frequent flyer number, reward program number)

3.1.3. What is Sensitive Personal Data?

Sensitive Personal Data is a subcategory of Personal Data that requires special protection under some laws. Sensitive Personal Data includes the following information about Data Subjects:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- data concerning health
- data concerning a natural person's sex life or sexual orientation

3.1.4. What is Processing of Personal Data?

The term "processing" broadly means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means. The definition of Processing is extremely broad and includes, but is not limited to, any of the following:

- collecting
- recording
- organizing
- storing
- adapting or altering
- retrieving
- consulting (i.e. reviewing with another party)
- disclosing or transmitting
- disseminating or otherwise making available
- aligning or combining (i.e., confirming or comparing)
- blocking
- erasing or destroying

4. General Guidelines for Handling Personal Data

The following guidelines should be followed by employees processing Personal Data as a part of their job responsibilities. Even if an employee does not interact with Personal Data on a daily basis, it is important to be aware of these guidelines:

- Keep all Personal Data secure by taking sensible precautions and following the guidance in this Policy and the IT Policies identified in Section 14;
- Limit access to Personal Data covered by this Policy to those who need it for their work (i.e., Personal Data should not be unnecessarily disclosed either within Bio-Techne or externally);
- Use reasonably secure means to access Personal Data (i.e., ensure the computer or device used to access Personal Data has appropriate security measures installed, such as VPN; if you have question about your device you can contact IT); for example, don't use devices containing Personal Data when using publicly accessible WiFi, which is frequently available in public locations such as coffee shops and airports (for additional information about using secure means for accessing the internet and Personal Data, see the IT Policies in Section 14);
- Follow Bio-Techne's Password Policy, particularly when accessing Bio-Techne systems containing Personal Data;
- Regularly review and update Personal Data to keep it accurate.
- Delete and dispose of Personal Data when it is no longer required; and
- Request help from managers or subject matter experts if you are unsure about any aspect of this Policy or the protection of Personal Data.

5. Storage of Personal Data

In addition to the general guidelines for handling Personal Data above, employees should follow these specific guidelines when storing Personal Data either in hardcopy (i.e., on paper) or electronically.

When Personal Data is stored on paper (e.g. printed payroll reports), it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to Personal Data that is usually stored electronically but has been printed for some reason:

- Keep paper or files containing Personal Data in a locked drawer or filing cabinet when not in use;
- Ensure that paper and printouts with Personal Data on them are retrieved promptly, such as from a printer, so that unauthorized people are not exposed to them; and
- Shred and dispose of documents containing Personal Data securely when no longer required, such as in shredding bins.

When Personal Data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Adhere to the IT Policy 100: Password Policy;
- Keep removable media (e.g., CDs, DVDs, flash drives) containing Personal Data locked away securely when not in use;
- Minimize storage of significant amounts of Personal Data on laptops or other mobile devices, like tablets or smart phones. Incidental exchange of Personal Data via email or other incidental use of Personal Data storage on laptops or mobile devices for purposes of conducting business is acceptable (for example, email exchanges with individuals located in the EU that happen to contain an EU employee's signature block with name, address, and phone number is considered incidental); and
- Store Personal Data on designated drivers and servers – not on mobile devices (recognizing that incidental amounts of data may be sent as described above); only upload Personal Data to cloud computing services that have been vetted and approved for handling Personal Data;
- Maintain site servers containing Personal Data in a secure location, away from general office space and accessible only to employees that need access as a part of their job;
- Back-up Personal Data frequently, and test those backups regularly, in line with Bio-Techne's standard backup procedures; and
- Protect all servers and computers containing Personal Data through security software and a firewall approved by IT.

6. Use of Personal Data

In addition to the storage of Personal Data, employees must consider how they use the Personal Data they access and store. Personal Data is at the greatest risk of loss, corruption, or theft when it is accessed or used:

- Lock unattended computer screens when working with Personal Data;
- Do not share significant amounts of Personal Data informally (i.e. large amounts of personal data should not be sent via email). Incidental use of some Personal Data in the course of an email exchange is acceptable, but secure file transfer mechanisms (e.g., Egnyte) should be utilized when Sensitive Personal Data or large amounts of Personal Data are involved;
- Do not transfer Personal Data to a person, public authority, organization, agency or body other than Bio-Techne ("Third Party") unless you have confirmed with your manager or the legal department that such a transfer is appropriate. The law in some countries requires that data privacy issues be covered under a data transfer agreement or other compliance mechanism before Personal Data can be sent to a Third Party.
- Minimize use of personal computers or devices when accessing Personal Data.
- Use Personal Data consistent with the "Basis for Processing" explained in Section 7 below.

7. Basis for Processing

Based on the principles discussed in Section 2 of this Policy, Bio-Techne uses Personal Data for limited, specific, and transparent purposes (i.e., the "basis for processing"). The bases – or justifications - for processing specific kinds of Personal Data used by Bio-Techne are as follows:

- Personal Data of current, former, and prospective employees and their dependents: based on the employment contract between Bio-Techne and its employees and their mutual, legitimate interest in having employee data processed as a part of the employment relationship, e.g., for purposes of issuing payslips and administering benefits;
- Personal Data of Customers: based on the legitimate interest of Bio-Techne's customers to receive services and order products and of Bio-Techne in serving those customers.
- Personal Data of Prospective Customers, or "Leads" – based on the consent of the Data Subject.

8. Notice to Data Subjects

Data Subjects should be provided with a relevant "Privacy Notice" consistent with Bio-Techne's collection and processing practices and intentions relating to that Data Subject's Personal Data. Generally, this notice is provided at the time the Personal Data is collected, or within a reasonable time as consistent with this Policy and the law, consistent with the following:

- The employee notice is provided at the time of initial employment and can be obtained at all times through Human Resources.
- The customer notice is provided at all times on the Bio-Techne website and is linked to in relevant customer communication and in the footer of all web pages.
- Prospective customers are asked to consent to processing at the time information is collected and provided a copy of or link to the privacy notice on Bio-Techne's website.

In particular, the notice shall include:

- the identity and the contact details of Bio-Techne and its affiliates and, where applicable, of a specific Bio-Techne representative;
- the purpose(s) of the processing for which the Personal Data is intended as well as the basis for the processing as identified in Section 7;
- the recipients or categories of recipients of the Personal Data, if any;
- when applicable, the fact that the Personal Data will be transferred across borders to another country and details concerning the data protection precautions being used to protect the data associated with such transfer;
- the time period for which the Personal Data will be stored or, if that is not possible, the criteria used to determine that period;
- the existence of the Data Subject rights as described in Section 9 and, where the processing is based on consent (e.g., with Prospects), the existence of the Data Subject's right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority under the EU General Data Protection Regulation; and
- whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such Personal Data;

As required by the laws and regulation of a relevant jurisdiction, Bio-Techne will provide a Data Subject subsequent notice if Personal Data is to be processed differently than stated in the original notice.

9. Data Subject Rights

As described in this Policy, Bio-Techne is committed to the transparent processing of Personal Data consistent with applicable data privacy law, including the EU General Data Protection Regulation ("GDPR"), and as provided in our data privacy notices described in Section 8. Further, Bio-Techne is committed to fulfilling Data Subject rights under applicable data privacy law, including the rights to access, correct, delete, restrict use, move data, object, and receive specific information regarding automated decision making or profiling.

10. Disclosure of Personal Data

Bio-Techne discloses Personal Data to Third Party service providers in only limited circumstances consistent with the policies and procedures in this Policy and the law. Specifically, employees may only share Personal Data consistent with an existing data transfer agreement with the Third Party to which Personal Data will be disclosed. In addition, Personal Data can only be transferred to a Third Party if a Data Subject has received proper notice or, where required by law, provided appropriate consent.

Bio-Techne shall use data transfer agreements when sending Personal Data to Third Parties and/or outside of the EU. In particular Bio-Techne shall use:

- A contract consistent with Article 28 of the GDPR for transfers to Third Parties within the EU;
- A contract between Bio-Techne subsidiaries and Bio-Techne headquarters in the U.S. consistent with the Standard Contractual Clauses when transferring Personal Data within Bio-Techne outside of the EU;
- A contract between Bio-Techne and Third Parties consistent with the Standard Contractual Clauses when transferring Personal Data to Third Parties outside of the EU.

Bio-Techne will also disclose Personal Data to the extent required by law. Bio-Techne considers disclosure "required by law" in the event of a legal mandate that (a) compels Bio-Techne to make a disclosure of Personal Data and (b) is enforceable in a court of law. Examples of a legal mandate include, but are not limited to, the following:

- court orders and court-ordered warrants;
- subpoenas or summons issued by a court, grand jury, inspector general, or administrative body authorized to require the production of information;
- a civil or an authorized investigative demand; and
- statutes or regulations that require the production of information.

Requests for Personal Data that may be "required by law" but are not routine in nature should be reviewed with the Legal Department before Personal Data is provided (sending personnel files to a third party, unemployment inquiries regarding specific individuals, information requested on an anonymized basis such as inquiries from the dept of labor or relating to the Affirmative Action Plan or Equal Employment Opportunity).

11. Training

All Bio-Techne employees shall receive training on data privacy protections and this Policy. Employees performing certain functions, such as in the Human Resources or Marketing and Sales, may receive additional training if, through the course of their work, they regularly process Personal Data.

12. Record of Processing

Bio-Techne will maintain a record of processing Personal Data as required by law, including Article 30 of the GDPR, to be produced to regulatory authorities as appropriate and allowable.

13. Data Breaches

In the case of any unauthorized disclosure of Personal Data, Bio-Techne shall notify Data Subjects and proper regulatory authorities consistent with the laws and regulations of the relevant jurisdiction. The response shall be a joint effort among Legal, IT Security, and any relevant divisions or businesses with impacted Personal Data.

14. IT Security Policies

Bio-Techne will take reasonable precautions to keep Personal Data in its possession secure against loss, misuse, unauthorized access, disclosure, alteration and destruction. Further, Bio-Techne will hold Third Parties processing Personal Data on its behalf to security standards consistent with the jurisdictions in which they operate. Bio-Techne periodically reviews its security measures in an effort to protect the privacy of Personal Data.

IT Securities Policies applicable to the protection of Personal Data include, but are not limited to:

- IT Policy 100: Password Policy
- IT Policy 101: Network Security
- IT Policy 102: Technology Acceptable Use

15. Changes to this Policy

Bio-Techne reserves the right to modify this Policy from time to time to ensure it accurately reflects the regulatory environment and our Personal Data collection principles. When material changes are made to this Policy, corresponding changes will also be made to the relevant, outward facing notices to Data Subjects. When such a material change is made, Bio-Techne will post a revised version of this Policy and notify Data Subjects as required by law and consistent with this Policy.

16. Administration of this Policy

Bio-Techne expressly reserves the right to change, modify, or delete the provisions of this Policy without notice.

Responsibility for administration of this Policy rests with various functions, including but not limited to IT Security and Legal. All employees are responsible for consulting and complying with the most current version of this Policy. If you have any questions regarding this Policy or how to comply with it, please contact privacyinfo@bio-techne.com

17. Effective Date

This Policy is effective as of May 21, 2018.