bioventus™

PRIVACY HANDBOOK

2024

Table of Contents

Back to TOC

Bioventus Global Privacy Program

Bioventus is committed to the protection of Personal Data. In support of this commitment, Bioventus has adopted a set of Privacy Principles to guide us regarding how we use and protect Personal Data in the course of our work. The Privacy Principles are established in our **Global Privacy & Data Protection Policy**, as well as the following supporting policies:

- Data Processing Policy
- Data Subject Request Policy

These policies can be found on Bionet.

The Privacy Principles are based on internationally recognized standards related to the treatment of Personal Data. The Privacy Principles express and support Bioventus' commitment to our customers and vendors, our employees, and all other individuals with whom we interact in the course of our business.

All employees are expected to proactively seek guidance and raise concerns about privacy issues to the Privacy Officer. You can email the Privacy Officer at **privacy@bioventus.com**.

FAQ 1: WHAT IS DATA PRIVACY? IS IT DIFFERENT THAN DATA SECURITY?

A: Data Privacy allows individuals to control access to and the use of their Personal Data. Privacy also ensures that such data is protected from unauthorized use. Because of this, Security and Privacy are interrelated, though they are not the same.

What is Data Privacy?

Data Privacy is about **why and how we use** Personal Data. It is the practice of safeguarding Personal Data by limiting its collection, using it only for appropriate purposes, and protecting it from inappropriate sharing or dissemination.

Privacy requires us to implement certain security measures to put guidelines into practice.

What is Data Security?

Data Security or Information Security is about **how we protect** information. It refers to the technical and procedural safeguards in place to ensure that the integrity, availability, and confidentiality of information are not compromised.

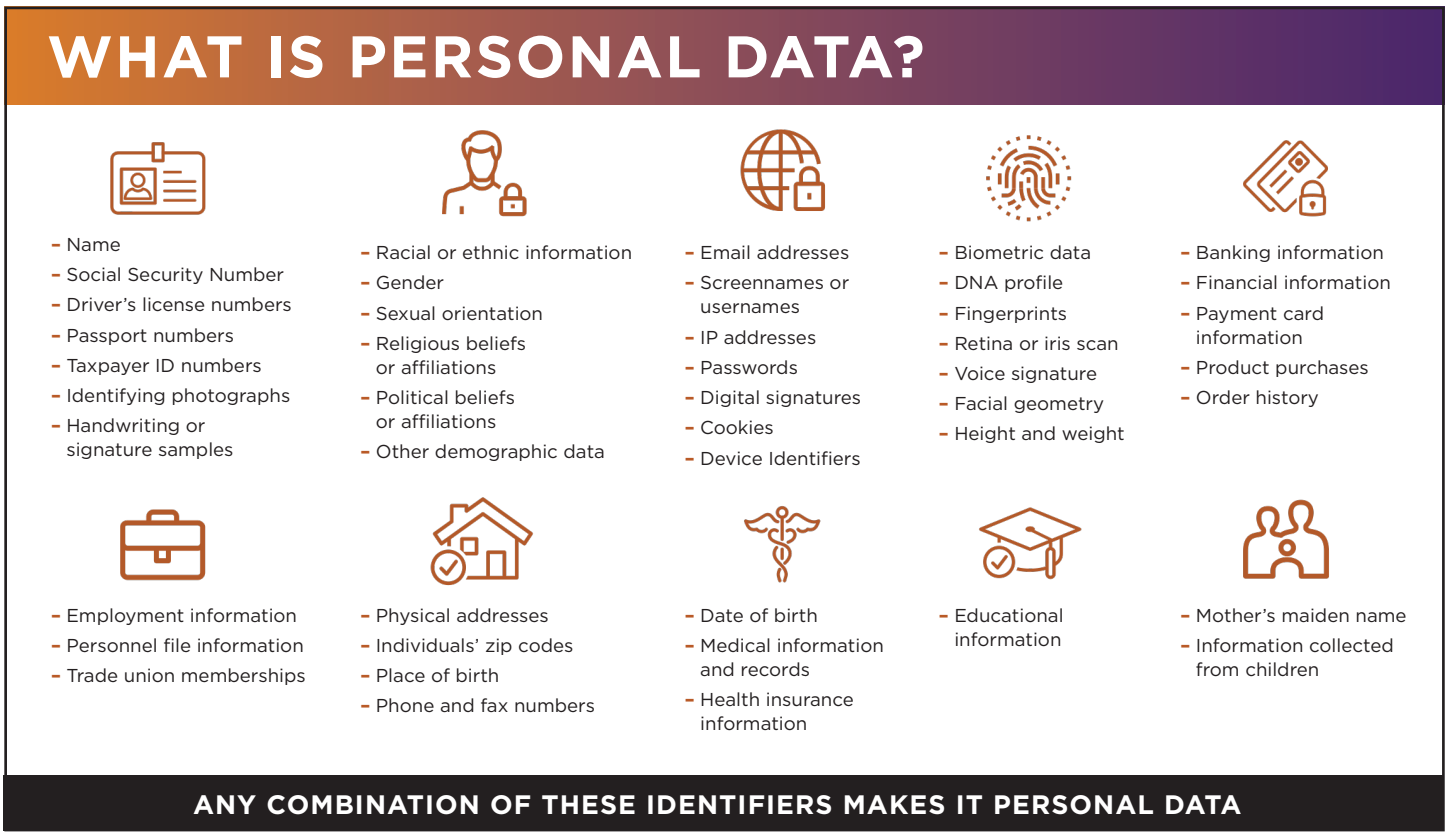
Security involves implementing controls that govern the access, storage, and transmission of all data, including Personal Data.

As you can see, Information Security is an important component of Privacy, helping protect Personal Data from unauthorized access or use. Privacy is also an important component of Security, ensuring that we do not collect, store, or use Personal Data without a legitimate purpose, which reduces the amount of Personal Data in our possession and minimizes the impact of security incidents. At Bioventus, the Privacy Team and Information Security Team work closely together, but they are distinct. It is important to understand that when Personal Data is involved, it is not sufficient to rely on Information Security alone.

FAQ 2: WHAT IS PERSONAL DATA?

A: Personal Data is any information about an identified or identifiable person. It is broader than the typical categories of information we think of, such as names, phone numbers, addresses, and Social Security numbers or other government ID numbers. Personal Data is any information that relates to a specific person where you know or could discover that person's identity.

You're probably familiar with the terms "Personally Identifiable Information" (PII) and "Protected Health Information" (PHI). **PII and PHI are no longer the international legal standard.** However, for U.S, healthcare entities, PHI is still an important concept as discussed below in "FAQ 4: What About HIPAA?". Instead, any data about a person falls within the definition of Personal Data and is regulated under modern privacy laws. For example, any data connected to a Customer ID is personal data, and many privacy laws consider IP address to be personal data.



FAQ 3: WHAT IS AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL?

A: An **identified** person is an easy concept – if you can tell who somebody is from the information, then that is Personal Data.

An **identifiable** person is a trickier concept. Someone is identifiable if you can take the information you have that does not directly identify the person and combine it with additional information available to you to discover their identity. For example, records such as payment history will be attached to a Customer ID number representing the person who has made payments. This ID number identifies that person's record in the database that holds their name and contact details. So even though the payment records don't list the person's name and address, you can easily use the ID number to link the payment history to the person's identity. This means the person in the payment records is identifiable.

FAQ 4: WHAT ABOUT HIPAA?

A: Because Bioventus is typically a HIPAA "Covered Entity," we have a duty and responsibility to protect the privacy and security of Protected Health Information "PHI", as defined by HIPAA. Specifically, because of the sensitive nature of health information, PHI typically requires higher standards of care than just Personal Data.

HIPAA Identifiers

PHI is a subset of Personal Data. Health Information becomes PHI when it meets two criteria:

- includes at least one of the 18 identifiers specified by HHS.
- It is handled by a Covered Entity (a health care provider, health plan or insurer, or healthcare clearinghouse), or a Business Associate (service provider) of a Covered Entity.

PHI can be any health data that includes one or more of the following 18 identifiers:

- Names
- Dates, except year
- Telephone numbers
- Geographic data
- FAX numbers
- Social Security numbers
- Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers including license plates
- Web URLs
- Device identifiers and serial numbers
- Internet protocol addresses
- Full face photos and comparable images
- Biometric identifiers (i.e., retinal scan, fingerprints)
- Any unique identifying number or code

Our **HIPAA Privacy Policies and Procedures** should be read in conjunction with Bioventus's supporting policies:

- Global Privacy & Data Protection Policy
- Data Processing Policy
- Data Subject Request Policy

These policies can be found on Bionet.

All PHI is Personal Data. Not all Personal Data is PHI.

Back to TOC

FAQ 5: WHAT OTHER PRIVACY LAWS APPLY TO BIOVENTUS?

A: While HIPAA is a very important privacy law for Bioventus, it is not the only law to which Bioventus is subject across the globe. In fact, in the past few years, many countries have passed legislation requiring much tighter controls on Personal Data. For example, the EU General Data Protection Regulation (GDPR) is one of the world's most rigid privacy laws, and Canada, Singapore, Brazil, Vietnam, India, and China have all recently passed more stringent controls on the use of Personal Data.

In the United States, over 10 states have passed their own "GDPR-like" laws, and California became the first U.S. state to have a specialized privacy regulatory agency. At the federal level, the Federal Trade Commission (FTC) has started investigating and enforcing certain privacy principles, and the FTC has required companies to delete algorithms and products developed without proper privacy controls and has imposed personal liability on company executives.

As an added complication, some of these laws can reach beyond their borders. For example, the GDPR can apply to Personal Data about European residents *anywhere in the world* that the information is being used. The GDPR follows the data globally.

If you are unsure whether a particular use of Personal Data is lawful, please reach out to the Privacy Officer for guidance.

FAQ 6: What Are Bioventus' Privacy Principles?

A: We adhere to a common set of principles that guide us regarding the use and protection of Personal Data. You should apply these Privacy Principles any time you encounter Personal Data in the course of your work.

PRINCIPLE ONE: LAWFULNESS, FAIRNESS, AND TRANSPARENCY

Personal Data should be used lawfully, fairly, and in a way that is transparent to the individual whose personal data we use.

FAQ 7: WHAT DOES "LAWFULNESS" MEAN?

A: We use Personal Data lawfully, fairly, and in a manner that is transparent to the individual whose data Bioventus is using. Lawful bases for using Personal Data include:

- Voluntary, informed consent for the use;
- The use is necessary to perform a contract or complete a transaction with the individual whose Personal Data is being used;
- The use is necessary to preserve human life or safety from serious threat;
- The use is required by law;
- The use is in the public interest; or
- The use is in the legitimate business interest of Bioventus , if the use does not cause undue risk to the privacy rights of the individual whose data is being used.

It is important that we only collect the Personal Data that we need for a project and that we use Personal Data only for the purpose for which we collected it. Don't collect Personal Data "just in case" it might be useful in the future.

Additionally, many countries, especially European countries, restrict the export of Personal Data to certain countries, such as the United States. If you are sending data outside of Bioventus to a third party or vendor, please first contact the Privacy Officer at privacy@bioventus.com, to ensure that transfer is legal.

FAQ 8: WHAT DO WE MEAN WHEN WE SAY WE MUST USE PERSONAL DATA "FAIRLY?"

A: "Fairness" is a broad and vague term, but it often boils down to using a person's data in a way that they would expect the data to be used.

FAQ 9: HOW DO WE ENSURE TRANSPARENCY AND INFORMED CONSENT?

A: We must tell people why and how we collect and use their Personal Data. Privacy notices are the most common way we communicate this information.

In some cases, we have to get voluntary, informed consent from individuals before collecting or using their Personal Data for certain purposes. This type of consent is stricter than simply asking individuals if it is ok for Bioventus to use their Personal Data. Instead, to be valid, a request for consent must:

- Describe what Personal Data will be used and why;
- Disclose whether the Personal Data will be shared and, if so, with whom;
- State how long the Personal Data will be maintained before deletion; and
- Inform individuals that they may withdraw their consent and provide instructions for doing so.

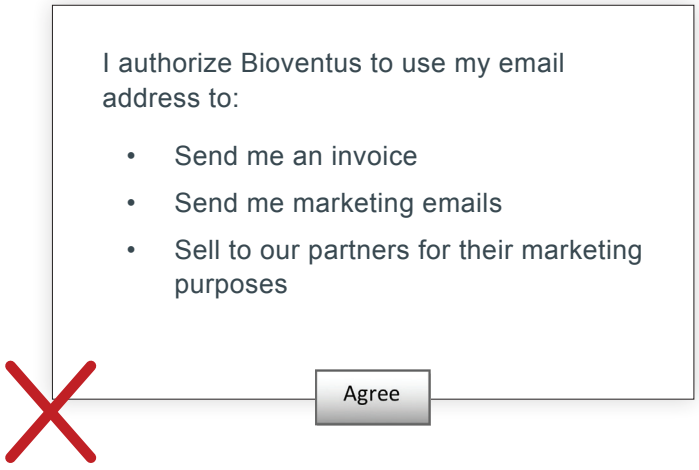
This information must be communicated in a clear and concise form that people can easily understand. It must also be "unbundled," meaning it is clearly distinguishable from other matters included in the same disclosure.

If the Personal Data will be used in multiple, distinct ways that require consent, the request for consent should be "granular," separately asking the individual for consent about each use of the Personal Data. The consent for one use case cannot require the individual to provide consent for an unrelated use case.

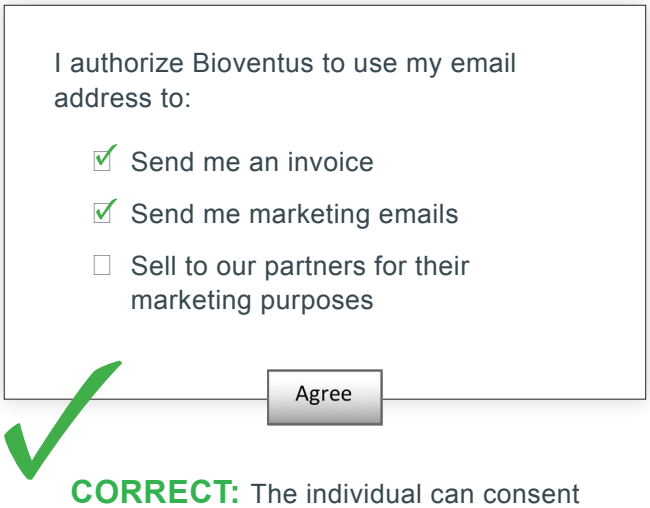
Contact the Privacy Officer for assistance with designing consent forms that comply with these consent requirements.

Practical Privacy Pointer: The more granular the consent, the more likely it is to be compliant.

Examples of Granular Consent:



INCORRECT: The individual is required to consent to everything or nothing. The three purposes need to be separated.



CORRECT: The individual can consent to specific separate uses of his or her email address.

PRINCIPLE TWO: PURPOSE LIMITATION

Personal Data may only be collected for specific, legitimate purposes and may not be reused in a way that does not align with those purposes.

Any time Bioventus collects or uses Personal Data, it must be for a specific, legitimate purpose. We must not conduct blanket Personal Data collection in the hopes that the information becomes useful someday. Instead, the reason for collecting the Personal Data must be explicit and determined at the time of collection.

FAQ 10: WHAT MEASURES DO I HAVE TO TAKE IF I WANT TO USE PERSONAL DATA IN A NEW WAY?

A: If we have already collected Personal Data but you want to use it in a **new way**, contact the Privacy Officer at privacy@bioventus.com to document the changes. If you want to use a **new system** or **vendor** for a project involving Personal Data, contact the Privacy Officer to determine if you need a Privacy Impact Assessment. Bioventus maintains a list of the ways we collect and use Personal Data, which may need to be updated to reflect your new process, system, or vendor. We call this Personal Data inventory a “Record of Processing Activities” or “ROPA.”

The Privacy Officer will check whether the proposed new or revised process, system, and/or vendor may pose a risk to individuals and therefore need a Privacy Impact Assessment to measure and reduce those risks. We cover Privacy Impact Assessments later in these FAQs.

PRINCIPLE THREE: DATA MINIMIZATION

The Personal Data collected or used must be limited to only the information necessary for achieving the specified, legitimate purposes for collecting the information.

We do not collect more Personal Data than is necessary to fulfill the purposes we specified when we collected it. In other words, we only collect the minimum amount of Personal Data needed to meet our specified business goals. Then, we only use the minimum amount of the collected Personal Data necessary for each step in meeting those goals.

FAQ 11: WHEN DO I HAVE TO CONSIDER DATA MINIMIZATION?

A: Data minimization must be considered at every stage of the data life cycle:

- **Collection**: Only collect or purchase the minimum Personal Data necessary to achieve the specified business purposes. Do not collect information that might be nice to have in the future but does not have a currently defined use.
- **Access**: Only provide access to Personal Data to individuals who need it for their job functions.
- **Use**: Only leverage the minimum Personal Data necessary to complete the task at hand. Filter out extraneous or unnecessary information. If possible, transform the data into a less-identifiable format, such as age ranges instead of dates of birth. Where possible, pseudonymize or tokenize the data (*e.g.*, replace names with ID numbers) so that the individuals cannot be easily identified.
- **Storage**: Only store Personal Data in appropriate systems. Do not create unnecessary copies or store information in unapproved locations. Once Personal Data is no longer necessary for the original purposes or archiving needs, we should remove it.

FAQ 12: HOW DO I MINIMIZE DATA?

A: Properly minimizing Personal Data is a multi-step process related to how, when, why, and by whom the Personal Data will be used. Data minimization can be achieved in several ways. For example:

- Do not ask for unnecessary Personal Data;
- Use only the documents and information relevant to the task at hand (e.g., hide or remove unnecessary information from working documents);
- Tokenize or pseudonymize data (e.g., replace names with ID numbers) to hide individuals' identities when the identities are unnecessary for the task at hand;
- Do not forward or give access to Personal Data to large groups of individuals who do not have a legitimate need for it; and
- Anonymize or aggregate data so that it can no longer be connected to specific individuals.

ANONYMIZATION

Anonymization involves modifying data so that it can never be retraced to specific individuals, even if combined with other information. Because anonymous data cannot be used to identify an individual, it is no longer considered Personal Data and is not subject to the same level of privacy and security restrictions.

True anonymization can be hard to achieve since individuals' identities can often be deduced by linking the data to other information available to us. Ask the Privacy Officer for assistance with anonymization.

Be careful! Anonymization can be hard to achieve. Consult the Privacy Officer to make sure data is anonymized before using it further.

PRINCIPLE FOUR: ACCURACY

Personal Data must be accurate and, where necessary, kept up to date.

We try to make sure that Personal Data is accurate and, where necessary, kept up to date. We take reasonable steps to ensure that inaccurate Personal Data is erased or rectified without delay if the purposes for which it is intended allow for the information to be updated.

PRINCIPLE FIVE: STORAGE LIMITATION

Personal Data should be kept only as long as necessary for the specified, approved uses or to meet Bioventus's legal obligations, after which it should be deleted or fully anonymized.

Once Personal Data has served its purpose, it must be deleted, encrypted, anonymized, or otherwise rendered unidentifiable or unreadable to protect the rights of the individuals the information concerns.

This does not mean Bioventus is necessarily obligated to delete all the information once it has served its purpose. We may also uphold the storage limitation principle if we anonymize the information so that it is no longer Personal Data capable of being linked to any particular individual.

FAQ 13: HOW LONG SHOULD WE KEEP PERSONAL DATA?

A: Generally, Personal Data should only be kept for as long as needed for the specified purpose for which it was collected or as required by legal considerations. For questions regarding storage limitation reach out to the Privacy Officer at privacy@bioventus.com.

PRINCIPLE SIX: SECURITY

Personal Data should be appropriately secured against unauthorized or unlawful access, loss, destruction, or damage. Bioventus maintains the confidentiality, integrity, and availability of Personal Data.

We use reasonable and appropriate information security measures to prevent theft, leaks, breaches, cyberattacks, or inappropriate access to or alteration of Personal Data. This involves establishing protections limiting unnecessary access to and use of Personal Data, such as multi-factor authentication and encryption, to reduce the chance of theft or breach.

FAQ 14: WHAT IS A PRIVACY INCIDENT?

A: A privacy incident is any event that might compromise the privacy, security, or confidentiality of Personal Data. There are three basic types of privacy incidents:

Confidentiality Incidents

Confidentiality requires us to have rules that limit access to information.

A confidentiality incident occurs when that limited access to Personal Data is compromised. In other words, a confidentiality privacy incident is inappropriate or accidental disclosure of Personal Data, including Personal Data sent to the wrong email recipient, accessed by a hacker, or otherwise disclosed unlawfully.

Example
Unauthorized disclosure of customer or employee sensitive information.

Integrity Incidents

Integrity is the assurance that information is trustworthy and accurate.

An integrity incident occurs when someone alters Personal Data without authorization.

Example
Someone inappropriately accesses a database and manipulates the data so that it is no longer accurate.

Availability Incidents

Availability is a guarantee of reliable access to information.

An availability incident occurs when Personal Data fields, files or records are no longer available due to a nefarious act such as ransomware or a lost or stolen device.

Example
Ransomware encrypts Personal Data so that it is unusable.

Notify the Privacy Officer at privacy@bioventus.com **immediately** of any privacy incident.

In making your notification, please do not use terms like “breach” or “data breach” because these terms carry with them legal meanings that should only be ascribed to an incident with guidance from the Bioventus Legal Team after taking into account the applicable laws and facts. In addition, please keep to the facts as you know them without speculating as to other details and causes. Investigations into privacy incidents move quickly and what we believe at the beginning of an investigation is often very different from what we later find out to have occurred.

Immediate reporting is critical because Bioventus may have to notify authorities in a very short time frame. When in doubt, err on the side of reporting a potential privacy incident.

PRINCIPLE SEVEN: INDIVIDUAL RIGHTS

Individuals have the right to request access and make changes to their Personal Data, and to object to the use of such Personal Data.

Most privacy laws require Bioventus to provide individuals with certain rights regarding their Personal Data. Depending on local law, individuals usually have the right to:

- Know how their Personal Data is used & shared;
- Access their Personal Data;
- Receive a copy of their Personal Data; and
- Request that we delete their Personal Data.

Some privacy laws may provide individuals with additional rights beyond those listed here. Forward any customer requests regarding these rights to the Privacy Officer for resolution.

Individuals can exercise their rights in many ways. They can ask a customer support representative or another Bioventus employee to exercise their rights. They can also click “unsubscribe” on email marketing campaigns.

Forward any requests or complaints you receive regarding an individual’s Personal Data or privacy rights to the Privacy Officer for resolution. Do not take further action unless instructed to do so. In some cases, there may be legal or legitimate business reasons why Bioventus cannot fully comply with a request. The Privacy Officer will make those determinations.

PRINCIPLE EIGHT: ACCOUNTABILITY

Bioventus is responsible for demonstrating compliance with all of the Bioventus Privacy Principles.

PRIVACY BY DESIGN (PBD)

A primary way Bioventus demonstrates compliance with the Privacy Principles is via Privacy by Design (“PbD”). PbD is a concept that integrates privacy into the creation and operation of new projects, devices, IT systems, networked infrastructure, and even corporate policies.

Bioventus adheres to PbD, which means that we consider the privacy implications of new business processes and information systems and build privacy into those processes and systems as an integrated part of the design process. PbD requires that Bioventus consider privacy from the very beginning of the development process of any initiative involving Personal Data, such as new or significantly updated business processes, software, or vendors handling Personal Data.

Privacy must be proactive, not reactive. PbD helps Bioventus anticipate privacy issues throughout the information lifecycle and mitigate those issues before they affect individuals. Privacy should be the default setting, meaning individuals should not have to take additional action to secure their privacy. Bioventus should not assume consent for sharing or reusing Personal Data for new purposes.

PRIVACY IMPACT ASSESSMENTS (PIA)

Another way Bioventus demonstrates compliance with the Privacy Principles is through Privacy Impact Assessments ("PIA"). A PIA is a cycle of fact finding, evaluation, risk mitigation, documentation, and monitoring designed to assess privacy risks from the point of view of the individuals whose Personal Data will be used. Bioventus ensures Privacy-by-Design by performing PIAs on **new or changing** business processes involving Personal Data that are likely to impact individuals, in particular where the processing is high risk, such as collecting sensitive information or creating profiles about individuals. The requirement to perform PIAs varies between different countries and jurisdictions, so if you're not sure whether you need a PIA, just ask!

Practical Privacy Pointer: There are some initiatives that almost always require a PIA.

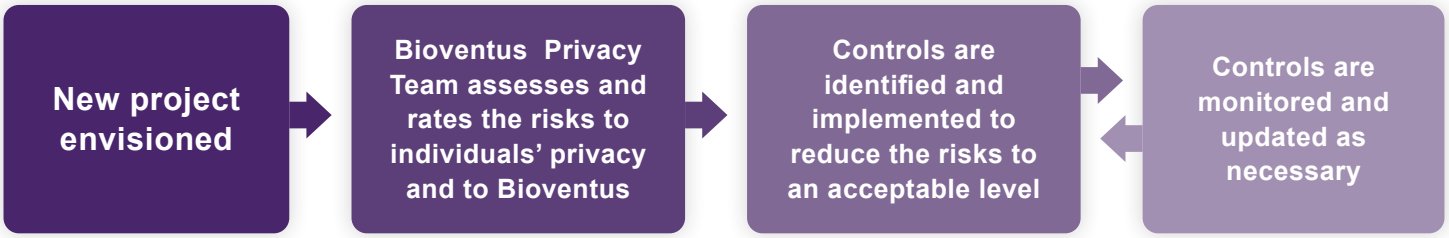
Examples of such initiatives are:

- An expansion of a project or system using Personal Data to new countries;
- Acquiring or enriching data sets containing identifiable data;
- Social media, email, or SMS marketing campaigns that rely on tracking consumer behavior;
- Personalized giveaways, contests, or incentive programs;
- Video surveillance of individuals or public spaces;
- Biometrics, including facial recognition and thumbprint authentication;
- Any process that involves the transfer of Personal Data across national borders, including for storage in a system located in a different country or providing data access to users located in a different country;
- New financial software that processes identifiable individuals' financial data;
- A credit card processing or payment system;
- Any online behavioral monitoring, including targeted advertising; and
- Geolocation tracking, RFID, or other track-and-trace methodologies that allow for individuals' whereabouts to be monitored directly or indirectly.

This is not a complete list of all projects or processes that may require a PIA. Please reach out to the Privacy Officer at privacy@bioventus.com for any projects involving Personal Data to see if you need a PIA.

FAQ 15: HOW DOES A PIA WORK?

A: Stakeholders should reach out to the Privacy Officer as early as possible in a new project to begin a PIA. PIAs are not static assessments; as the project changes and evolves, the PIA process will adapt to those changes. The PIA process works as follows:



PIAs are **collaborative**. The Privacy Officer will work with the project team to identify the privacy risks for each envisioned use of Personal Data, then rate each identified privacy risk based on the likelihood that it will occur and the potential impact on the individual should it occur. These risk ratings are inherently subjective but should be based on a consideration of the privacy risks to the individuals, the potential risks to Bioventus (including financial and reputation damage), and Bioventus's objectives and obligations (both regulatory and contractual).

For each identified risk, the Privacy Officer will work with the business process owner to determine what steps can be taken to reduce the likelihood that the risk will occur and/or the impact should the risk occur. Some of the more common risk-mitigating steps or controls are:

- Consent;
- Privacy notice;
- Cookie notice;
- Data minimization;
- Pseudonymization (i.e., making Personal Data identifiable rather than identified);
- Anonymization;
- Information separation;
- Access controls;
- Increased security measures or settings;
- Policies and procedures;
- Training;
- User-facing privacy controls;
- Updated or amended contracts;
- Storing the data in specific geographic locations; and
- Deletion of unnecessary pieces of information.

It is important to continually balance the costs and risks to the individual against the benefits to Bioventus. In rare cases, the costs of implementing sufficient protections to make the project compliant will outweigh the potential benefits of the project. If the Privacy Officer and the business process owner agree that the benefits do not justify the costs, Bioventus may decide not to proceed with the project.

Each risk-mitigating measure will be assigned a risk owner and a projected due date. When all mitigating measures are identified and assigned, the PIA will be completed pending the implementation of the identified measures. Once the measures are in place and the appropriate business owner accepts any residual risks, the Privacy Officer finalizes and records the PIA.

Back to TOC

Sharing Personal Data with Third Parties Outside of Bioventus

We only disclose Personal Data to a third party when sharing the Personal Data is necessary for a business need or to comply with a legal requirement. Before sharing Personal Data, Bioventus and the third party may need to enter into specialized privacy contracts.

DATA PROCESSING AGREEMENTS

If you would like to engage an external service provider, vendor, or business partner in your area of responsibility, Bioventus may need to sign certain privacy and security related agreements with the external party to ensure appropriate privacy protections are in place. Bioventus's vendor onboarding process involves an assessment of whether a Data Processing Agreement may be required.

The content of these agreements may vary depending on the circumstances of the engagement. The terms of a Data Processing Agreement often involve defining:

- Which of the parties can make decisions about how Personal Data is used;
- The categories of Personal Data that will be shared between the parties;
- The ways in which Personal Data may be used and the restrictions on other uses;
- Data breach response obligations;
- Whether the contract involves a "sale" of Personal Data;
- Whether and with whom the Personal Data may be further shared; and
- The technical and organizational measures in place to protect the security and confidentiality of Personal Data.

DATA TRANSFER AGREEMENTS

If the engagement will involve the transfer of Personal Data across national borders, including for storage in a system located in a different country or providing data access to users located in a different country, Bioventus and the vendor may need to sign a contract that governs the import and export of Personal Data.

Practical Privacy Pointer: If Personal Data will be transferred from one country to another, always speak with the Privacy Officer to understand the rules around such transfers.

Considerations for Marketing

REUSING PERSONAL DATA FOR MARKETING

If you want to send advertising or marketing content to individuals whose information Bioventus has already collected for other purposes, you may need to obtain that individual's consent for the additional use, depending on the circumstances.

Factors that may affect this determination include the purposes for which we originally collected the Personal Data, the ways we currently use it, the communication channel(s) we plan to use (e.g., email, telephone, mail, etc.), and whether we plan to target the marketing messages to certain individuals based on their behavior or preferences.

The general rule is that we can use Personal Data only for purposes we have already disclosed to the individual. Often, we notify people that we will use their Personal Data for multiple purposes, such as email marketing, online ad targeting, and providing them with promotions. If we have informed the individual of the ways we will use his or her Personal Data and the individual has provided either opt-in or opt-out consent (depending on country-specific requirements), then we may use the Personal Data for the specified purposes.

Contact the Privacy Officer at **privacy@bioventus.com** for an assessment to determine whether you need to ask individuals for permission before using their Personal Data for direct marketing (opt-in or sometimes double opt-in) or whether you merely need to provide individuals with an option to unsubscribe or object to the use of their Personal Data for marketing (opt-out).

ONLINE, SOCIAL MEDIA, BEHAVIORAL, AND LOOKALIKE ADVERTISING

Many of the newer privacy laws explicitly regulate online advertising practices, such as conducting lookalike audience advertising and using advertising cookies, pixels, or other online trackers to advertise based on a user's behavior or preferences. Please contact the Privacy Officer to establish the proper controls and consent mechanisms before engaging in these advertising practices.

bioventus®

Innovations For Active Healing

privacy@bioventus.com