Global Policy

Data Privacy

Policy No.:	5.02 (Version 2.0)
Issue Date:	22 January 2024
Applies to (Region):	All
Applies to (Department):	All
Contact Persons:	Corinne Mignon, Global Data Privacy Business Partner
	Nicolas Hubert, General Counsel and Chief Compliance Officer
Approvers:	Gilles Galliou, Chief Executive Officer
	Troy Randolph, Chief Financial Officer

Signatures of Approvers:

DocuSigned by: Gilles Galliou CA6C0C62004B48B...

DocuSigned by: Troy Randolph F11F2A098E2F4D7...

Contents

1 Executive Summary

As information becomes more available, more valuable and is stored in more places, individuals have an understandable interest in protecting the privacy of information about them. Envu commits itself to protecting individuals' Personal Data. Envu's ability to operate effectively depends on a positive relationship with our stakeholders. They entrust Envu with their Personal Data and expect that Envu will protect their privacy. Meeting that expectation is a key principle and critical to the success of the company.

Data Privacy laws vary widely from country to country, with some countries having no Data Privacy legislation at all, some having Data Privacy protection scattered in several different laws and others having comprehensive Data Privacy laws. Data Privacy is an essential right in many countries where Envu does some business. Because Data Privacy is an important topic, and especially because there is not a single global standard, a group-wide approach to Data Privacy is required to establish an appropriate common standard that adequately protects Personal Data while allowing for the secure, legal exchange of Personal Data and efficient execution of our business.

This Policy explains the general principles that govern the management and protection of Personal Data at Envu.

2 Purpose Statement

2.1 Policy Rationale

This Policy establishes minimum principles for Processing Personal Data within Envu. Envu recognizes that an individual's interest in privacy has to be acknowledged, and that the misuse of Personal Data could result in significant harm to an individual. As a result, Envu is committed to processing each individual's Personal Data in a lawful manner that respects Data Subjects' privacy.

2.2 Risks to be mitigated

Envu is committed to protecting and securing Personal Data out of fairness to and respect for the privacy of affected individuals.

In the event that Personal Data of individuals is not processed in line with the Data Privacy principles in Section 3 below, Envu may need to stop using the affected Personal Data until curing the non-compliance or, if that is not possible, even delete such Personal Data. Non-compliance can cause:

- substantial fines
- criminal sanctions
- government audits
- mandatory individual and government notifications
- claims for damages by customers, competitors or others
- reputational damage

- exclusion from publicly funded business in major markets
- internal and external legal and administrative costs in defending cases, and / or
- breach of contracts or contract terms

2.3 Groups Affected

This Policy applies to all employees in all legal entities of the Envu group.

The Data Privacy principles in Section 3 of this Policy may apply even if in local jurisdictions Data Privacy laws are less strict or not available at all, depending on the laws applicable to the Processing Activity. To the extent Data Privacy laws are stricter than the principles in this Policy, Envu will adhere to these stricter privacy laws where applicable.

This Policy covers the protection of the privacy of information about individuals (i.e., human beings), and may be connected with information that Envu wishes to protect from unauthorized access by third parties, such as Envu's trade and business secrets.

Each country and country group Managing Director must assign responsibility for Data Privacy Policy compliance management to appropriate individuals (hereinafter "**Responsible Managers and Data Privacy Ambassadors**"). Data Privacy Compliance is a responsibility of all employees. However, for Data Privacy – as for every compliance topic – accountability (final non-delegable responsibility) remains with country or country group Managers and Managing Directors and all employees remain responsible for Data Privacy Compliance in their day-to-day activities.

The Envu Global Data Privacy Business Partner is supporting Managing Directors in their endeavour to achieve sustainable compliance with Data Privacy within the organizations of the respective functions and commercial operations.

As explained below in these graphs, the Responsible Managers and the Data Privacy organization have different, though complementary, roles and responsibilities. The two must therefore collaborate while remaining separate and distinct. As a consequence, an employee may not be assigned two roles in both parts of the organizations.

Achieving Data Privacy compliance requires action in three major areas: **Regulation**, **Implementation** of Regulations, as well as **Monitoring**. In these three areas the Responsible Managers for Data Privacy and the Data Privacy organization have different roles and responsibilities as shown in the following Figure 1.

Figure 1: General roles & responsibilities in ensuring Data Privacy compliance

RACI model: **R**: Responsible, **A**: Accountable, **C**: Consulted, **I**: Informed

	Regulations	Implementation	Monitoring
Data Privacy organization	R, A	C, I (work towards)	R, A
Management Responsibles	C, I (enact[2])	R, A	I, R, A (e.g. for corrective actions)

Regulations: The Data Privacy organization defines Data Privacy regulations in consultation with global functions. Each Legal Entity has to enact these regulations formally.

Implementation: Country, country group and legal entity level are responsible and accountable for confirming that their functions have taken adequate steps to implement the Data Privacy regulations. This includes assignment of Responsible Managers and Data Privacy Ambassadors for Data Privacy Policy Compliance Management and the Data Privacy organization, allocating adequate resources, and putting appropriate measures and processes in place. The Data Privacy organization supports implementation with counselling and advice and should be consulted during all phases of implementation. The Responsible Managers and Data Privacy Ambassadors for Data Privacy should be in continuous dialogue with the Data Privacy organization and the two should align on Data Privacy relevant topics, in connection with Country and / or Country Group Organization.

Monitoring: The Data Privacy organization monitors Data Privacy compliance with regards to selected high-risk activities. When corrective and preventive actions are necessary as a result of such monitoring, Responsible Managers are responsible for initiating and implementing those corrective and preventive actions. The global functions remain responsible for self-monitoring their Integrated Compliance Management (ICM) Data Privacy functional processes.

The respective roles of Responsible Managers and Data Privacy Ambassadors and the Data Privacy organization – at group level, country or country group level and legal entity level – are shown in Figure 2. Responsible Managers and Data Privacy Ambassadors will be appointed by country or country group Managing Directors as quick as possible in order to make sure Data Privacy rules are understood and applied by their organizations. In some countries where it is mandatory by law, those Data Privacy Ambassadors may be also registered as Data Protection Officer (DPOs) towards their local Data Privacy authority.

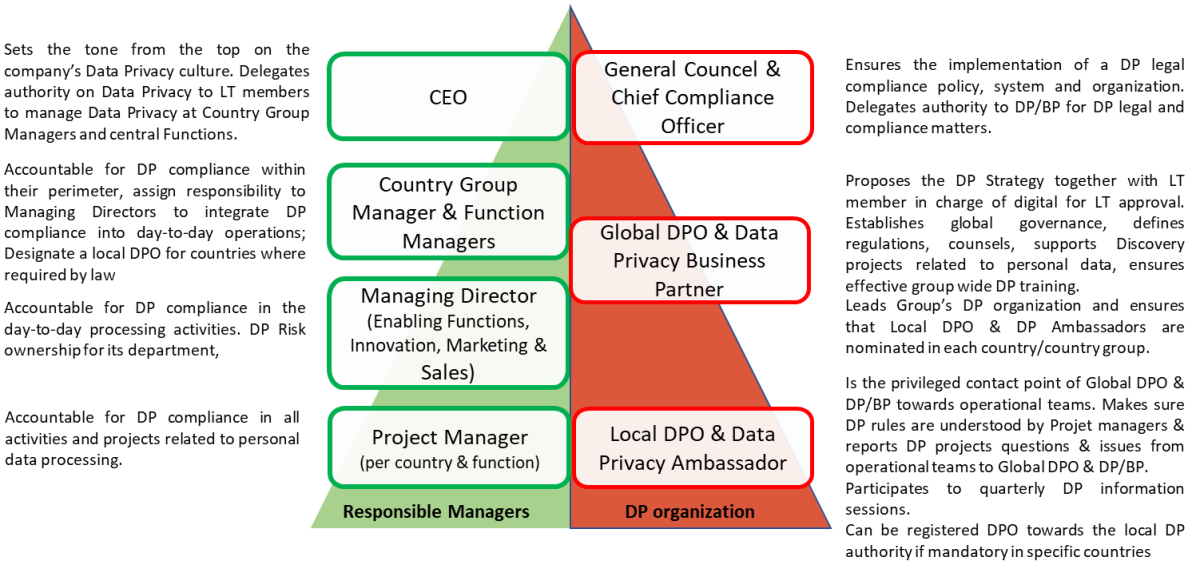


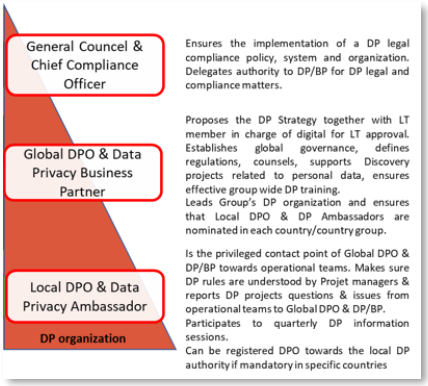
Figure 2: DP roles and responsibilities

CEO: He or she sets the tone from the top on the company's Data Privacy culture and delegates his or her authority on Data Privacy to his or her Leadership Team members to manage Data Privacy at Country Groups' level and central functions' level.

Country Group Manager & Function Manager: They are accountable for Data Privacy compliance management for their perimeter. For this purpose, they assign responsibility to Managing Directors in each country of their perimeter to integrate Data Privacy compliance into day-to-day operations. They also have the responsibility to nominate a Responsible Manager and Data Privacy Ambassador, that may be the Data Protection Officer (DPO) in each country where it is required by local laws. If a DPO is not mandatory, the Country Group Manager & Function Manager will nominate a Responsible Manager and DP Ambassador for all Legal Entities and Branches of their perimeter to facilitate and remind to local employees that each time they are using personal data in their day-to-day activities, they should follow Data Privacy Principles.

Managing Directors (Enabling functions, Innovation, Marketing and Sales): They are accountable for Data Privacy Policy compliance Management for their perimeter and support addressing the ownership for any Data Privacy risk that occurs within their department.

Project Manager (per country and function): They are accountable for Data Privacy compliance in all activities and projects related to personal data processing in their areas of responsibility. For this purpose they should follow all principles described in the section 3 of the present policy.



General Counsel and Chief Compliance Officer: He or she ensures the implementation of the Data Privacy compliance policy, system and organization. He/she delegates his authority to the Data Privacy Business Partner (DP/BP) for all Data Privacy legal and compliance matters.

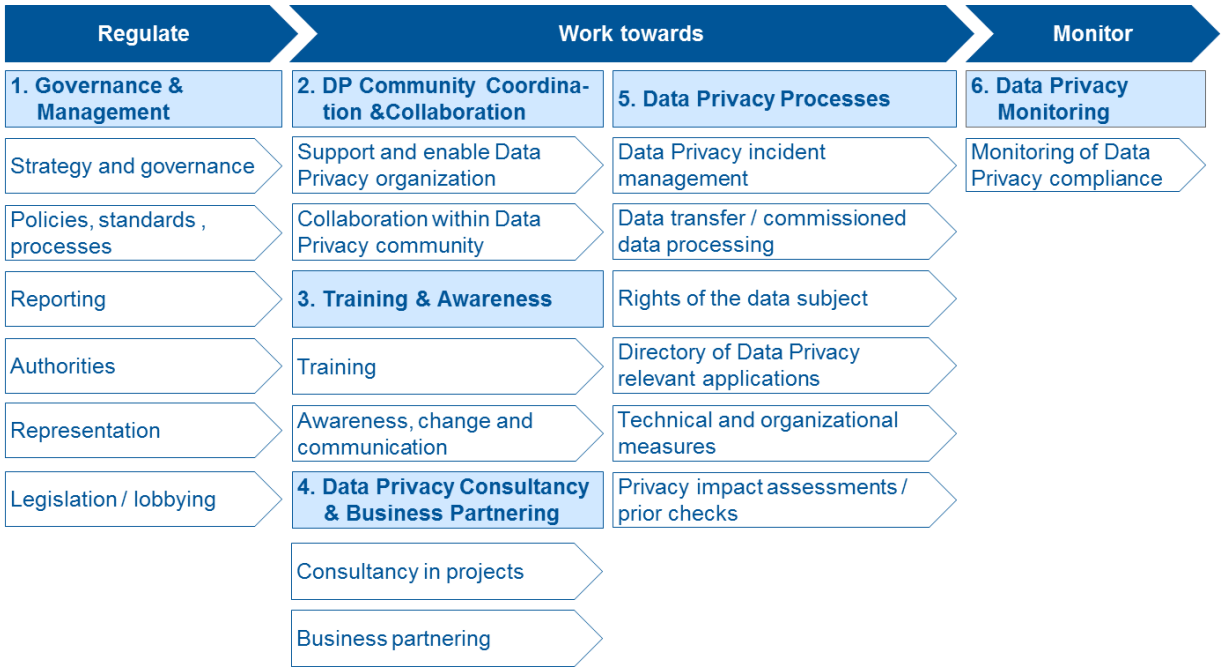
Global Data Protection Officer (global DPO) and Data Privacy Business Partner (DP/BP): He or she receives the delegation from the General Counsel and Chief Compliance Officer to ensure the implementation of the Data Privacy compliance policy, system and organization. He/she proposes the Data Privacy strategy together with the Leadership Team member in charge of digital, for Leadership Team approval. He or she establishes global governance, defines regulations, counsels, support projects related to personal personal and ensures effective group wide Data Privacy training. He or she also leads the Envu's Data Privacy organization and may be appointed local DPO where there is no local resource available, working in collaboration with the Responsible Managers and DP Ambassadors in each country / country group. Finally, he or she reports Envu's Data Privacy compliance level to Envu Governance, Risk & Compliance Manager on a quarterly basis and proposes corrective actions when necessary.

Local Data Protection Officer (local DPO) and Data Privacy Ambassador (DP Ambassador): He or she is the privileged contact point of the Global DPO and DP/BP towards the operational teams. For this purpose, he or she should be close to the operations and has to be aware of all local data processings in place or in project. He or she makes sure that Data Privacy rules and principles are communicated to any employee of his perimeter. He or she facilitates and reminds them that each time they are using Personal Data in their day-to-day activities, they should follow Data Privacy Principles. He or she participates to quarterly Data Privacy information sessions lead by the Global DPO and DP / BP, integrating the Data Privacy Community.

For countries where a DPO is mandatory by law, the Global DPO / DP Business Partner may be registered towards the Data Privacy authority of the said countries if there is no local resource available, unless if the law requires a in country DPO. If a DPO is not mandatory by law, Envu's decided to nominate a DP Ambassador which will have exactly the same role than the local DPO, with the difference that it will not be registered towards the local DP Authority.

In general, the responsibilities of the Data Privacy organization can be summarized as shown in Figure 3

Figure 3: Overview of main responsibilities in Data Privacy



3 Policy Content

3.1 Policy Statement

3.1.1 Personal Data

Personal Data is information that directly or indirectly identifies a particular individual, such as a customer, employee, business partner, shareholder or supplier. Your home address, personal or business email address, mobile phone number, and credit card information are examples of Personal Data. In addition, any information related to an identified or identifiable

individual also constitutes Personal Data, including characteristics or preferences (e.g., gender, marital status, income), behavior (e.g., job performance, purchasing activities, hobbies) or communications (e.g., an individual's opinions, beliefs or written text). The individuals to whom Personal Data belongs are called "**Data Subjects**".

Personal Data does not necessarily need to contain information directly identifying an individual (e.g., name and address of a person). Information is still considered to be Personal Data, if it can be linked to an individual with reasonable effort (considering the technical, organizational, time and financial investment required).

> *Example:* An internet protocol ("**IP**") address is a unique string of numbers that identifies each computer in order to communicate over a network. Although this information does not contain any direct identifiers from individuals, it is still considered Personal Data in many jurisdictions because it is possible to link this information to an individual with reasonable effort. IT service providers, who assign each IP address to their customers, are able to identify individuals, and applicable legal remedies may require IT service providers to reveal the identity behind an IP address.

Further, Personal Data is not limited to private information. Even information generated in a business context about an individual (including information collected by Human Resources about an employee) is considered Personal Data.

> *Example:* Your professional phone number is an example of this type of Personal Data, just like your job title, business email address or salary.

In contrast, information about a company, business or a department, as distinguished from an individual, is not considered Personal Data for purposes of this Policy.

> *Example*: Envu's company address.

Information that does not relate to an identified or identifiable natural person is called "**Anonymous Data**". Anonymous Data is not subject to Data Privacy laws. Personal Data can be modified so that it becomes Anonymous Data.

> *Example:* Human Resources summarize the results of an employee survey in a report. HR deletes the direct identifiers (e.g., name) from the report. Then, HR aggregates the indirect identifiers (e.g., gender, function or department), resulting in groups that are large enough that no data can be linked to a specific employee. The data in the report are then Anonymous Data.

Some Personal Data, called "**Special Categories of Personal Data**", are subject to heightened protection (e.g., additional restrictions for Processing or more stringent technical and organizational data security requirements for protecting this Personal Data from unauthorized access). For purposes of this Policy, Special Categories of Personal Data include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, health information, sex life and sexual orientation. Local law may add additional categories, such as criminal convictions, government identification numbers, or financial information.

DO	*DON'T*
☑ Determine whether data is Personal Data and if it belongs to the Special Categories of Personal Data before handling it.	☒ Don't forget that Personal Data can be present in any format (hard copy or digital format, and in writing, picture or audio).
☑ Always consider whether you can use Anonymous Data (versus Personal Data) to accomplish your business purpose.	☒ Don't assume that data is not Personal Data just because it does not include a name.
☑ Record your Personal Data Processing as a "New DP request" on Envu's DP COCKPIT.	☒ Don't collect any Special Categories of Personal Data (i.e. Religion, Political opinions, Health Data) except if you have the express consent of concerned individuals.

3.1.2 Data Processing Lifecycle

Data Privacy laws regulate the Processing of Personal Data. For this Policy "**Processing**" or "**Processing Activity**" means any operation or set of operations that are performed on Personal Data. Thus, basically anything that is being done with Personal Data qualifies as Processing and can thus be subject to applicable Data Privacy laws.

Often, this is not limited to operations performed on Personal Data with the use of automated means (meaning using a computer). Rather, Data Privacy laws can be applicable even in situations where no computers are used, e.g. when Personal Data form part of a filing system.

> *Example:* Human Resources organize certain employee information using files and folders with printed documents instead of using digitalized documents on a computer. Since the printed information is organized in a filing system, it is subject to applicable Data Privacy laws.

In order to better organize Data Privacy assessments required for any kind of operation performed on Personal Data, Envu developed a "**Data Processing Lifecycle**". It consists of the following Processing phases, which contain the most relevant operations that are usually performed on Personal Data in the corresponding Processing phase:

- **Collect:** Operations such as gathering or recording Personal Data.
- **Transfer:** Operations such as disclosure of Personal Data by transmission, dissemination or otherwise making such data available to other entities within the Envu group or to external parties.
- **Analyze:** Operations such as use, consultation, organization, structuring, adaptation, alignment, combination, alteration or restriction of Personal Data for the intended legitimate purpose as initially defined at the time of its collection.
- **Store:** Operations such as storage of Personal Data on Envu's own storage media (e.g., data center, data backups, mobile apps, local computers) or on third parties' storage media (e.g., cloud solutions).
- **Delete:** Operations such as erasure or destruction of Personal Data.

When planning a new Processing Activity, Envu will consider this Data Processing Lifecycle along with the Principles for Processing Personal Data in Section 3.1.3 below.

DO	*DON'T*
☑ Remember to assess a new Processing Activity along the Data Processing Lifecycle (from the collection of data to their deletion).	☒ Don't forget that Personal Data can also be collected by third parties on behalf of Envu. ☒ Don't forget that making Personal Data available to third parties, including by granting access to Envu's IT systems, qualifies as a transfer. ☒ Don't forget that even transfers of Personal Data within the Envu group can be subject to applicable Data Privacy laws.

3.1.3 Principles for Processing Personal Data

3.1.3.1 Lawfulness

Any Processing of Personal Data must be lawful. This means that Envu must follow the Data Privacy laws and regulations that are applicable to Envu's handling of Personal Data.

3.1.3.2 Legal Basis

In some jurisdictions, Processing Personal Data is not permitted without a legal basis. In such cases, Envu must Process Personal Data only in accordance with such legal basis. In general, there are two types of legal bases:

- **Statutory permission:** Data Privacy laws may contain statutory justifications for companies like Envu to Process Personal Data in important situations.

  Example: Processing Personal Data is necessary for Envu to fulfill its responsibilities for a contract to which the Data Subject is party, or for Envu to comply with its obligations under applicable law, such as employee tax reporting or for payroll purposes.

- **Consent**: Means any freely given, specific, informed and unambiguous indication of a Data Subject's wishes by which a Data Subject, by a statement or by a clear affirmative action (i.e., opt-in), indicates agreement to the Processing of his or her Personal Data. Consent should be obtained only where required by applicable law, such as when there are no statutory permissions available.

  Example: Pest control operators' emails addresses collected may be processed to send them marketing communications only on the basis of their valid consent.

3.1.3.3 Privacy Agreements

In addition to confirming legal basis, Envu must enter into special agreements with third parties (e.g., suppliers) prior to sharing Personal Data with them ("Privacy Agreements") where

required by local Data Privacy laws.

DO	*DON'T*
☑ Make sure that what you want to do with Personal Data is permitted by local statutes, rules or regulations, or that you obtain a valid consent. ☑ Make sure to document consents you obtain from Data Subjects or to check whether another legal basis is possible before processing personal data. In case of doubt, you must be able to provide proof that you have a valid legal basis. ☑ Check with Envu Global DP Business Partner to determine whether sharing Personal Data with a third party is permitted, and whether Envu must enter into a Privacy Agreement with the third party before transferring Personal Data for the first time.	☒ Don't place any conditions or requirements on consent – consent must be given freely. ☒ Don't assume that you may use Personal Data for any purpose simply because you may have access to it. ☒ Don't assume that you may Process Personal Data in a particular way because another company does it that way. ☒ Don't transfer Personal Data unless you are certain that you have any needed statutory permission or consent. ☒ Don't assume that you are allowed to transfer Personal Data to a third party just because Envu has a contract with that party – a legal basis and/or a Privacy Agreement may still be required. ☒ Don't assume that you may access and share Personal Data with anyone within Envu without first checking whether it´s legally acceptable and if transfer to a different legal entity is permitted.

3.1.3.4 Transparency and Fairness

The principle of transparency and fairness requires informing individuals that their Personal Data are being processed. In many jurisdictions, Data Privacy laws require Envu to inform Data Subjects accordingly. Information about a Processing Activity must be given in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. In order for information to be concise, transparent and intelligible, it must be limited to information relevant to the particular Processing Activity. Documents that contain this kind of information are called "**Privacy Statements**".

> *Example: Envu* includes Privacy Statements on its websites to provide website visitors with information about how their Personal Data is processed on those websites.

Envu will provide at least the following information to Data Subjects, if it is legally applicable, commercially reasonable and feasible to do so:

- The identity of the Envu entity that is primarily involved in the Processing Activity
- Purpose of the Processing
- For jurisdictions that provide rights to Data Subjects, information about these rights, including how they are able to exercise them

- Any further information needed to promote fair and transparent Processing of Personal Data

DO	*DON'T*
☑ Make sure that you always provide a Privacy Statement to Data Subjects that informs them about the Processing of Personal Data in a concise, transparent, intelligible, and easily accessible form, using clear language.	☒ Don't hide or disguise Processing Activities from affected Data Subjects. ☒ Don't provide information to Data Subjects that are irrelevant to the Processing of their Personal Data. It might confuse them. ☒ Don't confuse Privacy Statements with privacy policies. Privacy statements are mainly used externally to inform Data Subjects, whereas Privacy Policy is an internal document. ☒ Don't confuse Privacy Statements with obtaining Data Subjects' consent. Privacy Statements are only information / notification documents. Don't ask Data Subjects to confirm that they agree with or have read a Privacy Statement.

3.1.3.5 Purpose Limitation

Envu will collect Personal Data only for specified, explicit and legitimate purposes.

> *Example:* Collecting Personal Data for the general purpose of conducting "Big Data" analyses would not qualify as a specified and explicit purpose. However, collecting Personal Data to conduct a "Big Data" analysis for the purpose of identifying a relationship between information A and information B could qualify as a specified and legitimate purpose.

In addition, Envu will not further Process Personal Data in a manner that is incompatible with the initial purposes for collecting such Personal Data.

> *Example*: A sales representative from the Envu team collected Personal Data from professional rodent control prospects in order to offer them a service against rodent control. A few weeks later, the same sales representative would like to use the Personal Data collected to invite these prospects to an event on railway weed control. Envu's sales representative will not be able to use this Personal Data without a legal basis adapted to this new purpose (e.g. the consent of the prospects).

Further, Processing for scientific research purposes will not be considered incompatible with the initial purposes for collection if Envu respects the rights of the Data Subjects (such as by only using Pseudonymized Data or Anonymous Data).

DO	*DON'T*
☑ Determine legitimate purposes for Processing Personal Data at the time you plan to collect it and try to be comprehensive and specific.	☒ Don't collect Personal Data unless you have a specific, definable business need for the data, and have a legal basis for the Processing Activity.

3.1.3.6 Data Minimization

Envu will collect Personal Data only if the purpose of the Processing cannot reasonably be fulfilled in another way. This means that Envu must completely refrainfrom collecting Personal Data where collecting Personal Data is not absolutely necessary.

> *Example:* An Envu customer call center receives a report of an incident involving use of a product of Envu, which report includes the name, contact information and health information of the impacted individual. The call center needs to report the incident to the quality department to help to identify any potential problems with its products and prevent further damages. For this purpose, however, it is not necessary for the quality department to collect the name or other identifying information of the impacted individual – instead, it is sufficient for the quality department to receive Anonymous Data. Therefore, the call center removes the name and other identifying information from the incident report before transmitting it to the quality department.

Further, when Envu needs to collect Personal Data, Envu's collection must be limited to the Personal Data that is absolutely necessary to fulfill the purposes for which it is processed.

> *Example:* Sending an electronic newsletter that includes a personalized greeting generally requires obtaining only the recipients' email addresses and names. Other unrelated information (e.g., date of birth) is not necessary to send a newsletter and should therefore not be collected from recipients.

Another method that supports data minimization is the use of "**Pseudonymized Data**": data that is separated from direct identifiers so that it cannot be linked to an individual without additional information held separately and securely from the Processed Personal Data. Unlike Anonymous Data, Pseudonymized Data is still considered Personal Data as long as it can be tied to an individual with reasonable effort.

> *Example:* Before sharing Phyto Pharmacovigilance data to the ANSM Authority, Envu's Phyto Pharmacovigilance team replaces all direct identifiers of data subjects (e.g., name, contact details) with a subject ID. Envu's Phyto Pharmacovigilance team keeps the information linking each data subject to a subject ID separately and securely from the Phyto Pharmacovigilance data shared with the Authority. The data are thus pseudonymized.

Finally, when you plan to develop a new tool or application that will contain Personal Data, make sure that this tool or application integrates the principle of "**Privacy by Design**", i.e. taking into account the protection of users' privacy even before designing a system involving the processing of Personal Data.

DO	*DON'T*
☑ Make sure that the Personal Data you collect is absolutely necessary to fulfill the purpose for which you are authorized to collect the Personal Data. ☑ Use Pseudonymized Data instead of direct identifiers when possible. ☑ Make sure the principle of "Privacy by Design" is integrated in each new project involving the processing of Personal Data.	☒ Don't collect more Personal Data than required just because you are concerned that you might want it at a later date or for a different purpose. ☒ Don`t forget that Pseudonymized Data can still be Personal Data.

3.1.3.7 Data Retention & Deletion

Envu will limit the Processing of Personal Data to what is necessary for the purposes for which it was collected. This requires, in particular, making sure that the period for which Personal Data is stored is limited to the time needed to support the initially defined purpose. Envu will establish retention periods and / or periodic review periods for the Personal Data to make sure that Personal Data are not kept longer than necessary. When the Personal Data are no longer needed to support a business purpose, Envu will delete or destroy the Personal Data in accordance with local law and Envu regulations or will continue to Process only Anonymous Data.

Example: Envu's customer relationship department manages information about customers in order to:

- fulfill current agreements, and / or
- actively engage with (potential) customers (e.g., by sending marketing information about new products).

For each purpose, the customer relationship department needs to define retention and deletion periods and / or periodic reviews for the Personal Data involved:

- Tax law in most jurisdictions requires information related to agreements (e.g., invoices) The time period for keeping customers' Personal Data for marketing purposes depends on whether the respective customer remains a potential customer. A pest control operator who ceases to work as a pest control operator may no longer be interested in receiving marketing information from Envu. In periodic reviews, these customers need to be identified and their Personal Data must be deleted.

DO	*DON'T*
☑ Determine the retention period (or at least the criteria for determining it) before starting a new Processing activity. ☑ Consult with the Global DP Business Partner	☒ Don't delete Personal Data until you confirm that applicable retention obligations do not require you to keep them. ☒ Don't keep Personal Data beyond established

for retention and deletion requirements. ☑ Delete or destroy Personal Data in accordance with local laws and Envu procedures. ☑ Delete of Personal Data when it is no longer necessary for the purpose for which it was collected and Envu is not legally required to retain it. ☑ Implement regular checks for the current status of retention / deletion obligations. ☑ Include Personal Data from back up or archiving systems into your retention and deletion process.	retention periods unless required by law (e.g., legal hold).

3.1.3.8 Integrity and Confidentiality

Envu will Process Personal Data in a manner that provides appropriate security and confidentiality of Personal Data, including preventing unauthorized access to or use of Personal Data and the equipment used for its Processing.

DO	*DON'T*
☑ Consider the security requirements you need to put in place to protect Personal Data – including appropriate technical and organizational data security measures – *before* collecting them. ☑ Make sure to agree on appropriate technical and organizational measures with any third party that processes Personal Data on Envu's behalf. ☑ Remember to regularly check the appropriateness of technical and organization measures.	☒ Don't share Personal Data with a third party who is supposed to process Personal Data on Envu's behalf without first assessing that the technical and organizational measures taken by this third party to protect it.

3.1.4 Risks derived from the usage of Artificial Intelligence tools

Artificial Intelligence (AI)-based tools such as ChatGPT, Otter AI, are becoming increasingly popular, and many businesses are convinced that their use is a must today.

Envu does not wish to restrict opportunities to use innovative new tools but will ensure that their use does not put at risk the rights that individuals have over their Personal Data, nor undermine the confidentiality of business data. All potential internal Envu users must first make a joint request to their Data privacy Business Partner and IT Global Lead before installing such tools on their Envu Devices.

In the context of the coming into force of the Artificial Intelligence Act (AI Act), which foresees penalties of up to 6% of worldwide annual sales or 30 million Euros (whichever is higher) for the use of AI based tools that are prohibited or with a lack of data governance rules, Envu is committed to ensuring the legitimate use of such tools, while respecting the rights of individuals who may be required to share their personal data as a result of their use.

DO	*DON'T*
☑ Consult your IT Global Lead and Global DP Business Partner prior any use of new AI-based tools	☒ Don't share any Personal Data except if you collected prior consent from concerned individuals ☒ Never share Envu Business information with AI-based tools

3.1.5 Data Subjects' Rights

In many jurisdictions, Data Privacy laws grant Data Subjects certain rights vis-à-vis those that Process their Personal Data. For instance, many jurisdictions grant Data Subjects a right to receive access to their Personal Data or a right to delete or correct their Personal Data under certain conditions.

In case applicable Data Privacy laws in the respective local jurisdictions do not grant such rights to Data Subjects, Envu will at least respond as follows:

- respect a Data Subject's request by giving it due consideration and by responding within a reasonable time; and
- grant a Data Subject's request if it is commercially reasonable to do so, taking into account time, cost and resources.

DO	*DON'T*
☑ Immediately contact Envu Global DP Business Partner when receiving a request from a Data Subject who would like to get access to all his Personal Data or would like to edit, delete or transfer his Personal Data. ☑ Make sure that all Personal Data are accurate and correct any errors, even if an error seems minor or unimportant.	☒ Don't dismiss or take lightly a request from a Data Subject, no matter how trivial the concern may seem to you. ☒ Don't ignore a request for deletionbecause it is not possible due to retention obligations – If the deletion is not possible in the system, make sure the said Personal Data are archived in order not to continue using them.

3.1.6 Data Privacy Incident and Personal Data Breach

A "**Data Privacy Incident**" is a situation where Envu learns about a possible Personal Data Breach. A "**Personal Data Breach"** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

A Personal Data Breach may, if not addressed in an appropriate and timely manner, result in material or non-material damage to individuals such as:

- Discrimination
- Identity theft or fraud
- Financial loss
- Loss of control over their Personal Data
- Limitation of rights
- Loss of confidentiality of Personal Data, or
- Other significant economic or social disadvantage to the individual concerned.

In some jurisdictions, Personal Data Breaches that could result in risk to Data Subjects require notification to the impacted Data Subjects and / or applicable government authorities within a short period of time (e.g., in the EU, Data Privacy authorities must be notified within 72 hours after Envu of a Personal Data Breach).

Further, Personal Data Breaches may have a negative impact on Envu's reputation. Therefore, even if applicable Data Privacy laws in the respective local jurisdictions do not require immediately notifying authorities or Data Subjects, Data Privacy Incidents will always require expedient notification to Envu's Data Privacy Business Partner.

For proceeding with an incident or breach notification to Envu's Data Privacy Business Partner, any employee who is aware of such an incident should report it promptly on the **SharePoint DP Cockpit**

DO	***DON'T***
☑ In the event of a suspected Data Privacy Incident, involve Envu Global DP Business Partner **promptly and not later than 72 hours**, in order to facilitate meeting legally required notification periods.	☒ Don't try to handle a Data Privacy Incident on your own.

3.1.7 Interactions with Authorities

In many jurisdictions, there are government authorities dedicated to monitoring compliance with Data Privacy laws. Authorities may reach out to Envu in different contexts, such as to conduct a general Data Privacy audit or because the authority follows-up on a complaint rose by Data Subjects or other third parties. Some jurisdictions even require Envu to proactively consult with authorities in certain situations.

Any interaction between Envu and authorities must be managed by Envu Global DPO/Data Privacy Business Partner, Region Legal Counsel and Local DPO if such function is requested by local law.

DO	*DON'T*
☑ Immediately notify Envu Global DP Business Partner, Region Legal Counsel or Local DP Ambassador when an authority reaches out to you.	☒ Don't try to answer or handle any request from an authority by yourself.

3.1.8 International personal data transfers

Data Transfer means to make Personal Data available to any person who does not work for the same legal entity (including another legal entity within Envu), i.e. a third party. This may occur in many ways, such as by sending Personal Data to a third party or providing a third party access to the Personal Data. Even just allowing a third party to see the Personal Data on a computer screen can constitute a data transfer. Hosting data on a cloud from a service provider also constitutes a data transfer.

Depending on the role and the location of the parties involved there are different data transfer constellations possible.

- Controller to Controller

  When a Controller transfers data to another Controller.

- Controller to Processor

  When a Controller transfers data to a Processor.

- Processor to Processor

  When a Processor transfers data to another Processor.

- Processor to Controller

  When a Processor transfer data back to the Controller.

Depending on the location of the parties involved:

- **Within the EU / EEA or from the EU / EEA to a safe third country outside the EU / EEA**
  When one of the above mentioned data transfers takes place between legal entities within the EU / EEA or to a safe third country outside the EU / EEA. As of March 10th, 2022, as safe third countries, we can consider: Andorra, Argentina, Canada, Faroe Island, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, United Kingdom and Uruguay.

- **From the EU / EEA to an unsafe third country**

  When one of the above data transfers takes place between a legal entity within the EU / EEA and a legal entity located in an unsafe third country, i.e. outside the EU / EEA / safe third country.

  When a data transfer is planned, depending on the type of data transfer and destination the following requirements may need to be observed:

- **Third Party Due Diligence**

  Contact your Global DPO/DP Business Partner to perform such due diligence check.

- **Technical and Organizational Measures**

  Assess, implement and document adequate technical and organizational measures. Please note, that documentation of such measures is also part of the relevant contract to be concluded with the third party.

  Contact Global DPO/DP Business Partner who will indicate you which template to be used inside the relevant contract with the third party.

- **Conclude appropriate Data Privacy Contract**

  Contact Global DPO/DP Business Partner who will indicate you which template to be used inside the relevant contract with the third party.

- **Additional Data Transfer Safeguards where Data is Transferred to an unsafe Third Country**

  Contact Global DPO/DP Business Partner who will indicate you which template to be used inside the relevant contract with the third party.

DO	*DON'T*
☑ Before deciding to share personal data with a third party, immediately contact Envu Global DP Business Partner to check if the transfer project is legally possible and applicable requirements.	☒ Don't implement any data transfer to third party without preliminary check that you have a legal basis to implement it.

3.1.9 Accountability & Data Privacy Management System

In many jurisdictions, Envu is legally obligated to demonstrate compliance with Data Privacy laws by managing and documenting:

- all Processing Activities conducted by Envu (in the **Record of Processing Activities,** "**RoPA**")
- all privacy-related legal assessments of Processing Activities
- all Data Subject requests, Data Privacy Incidents and interactions with authorities
- an evaluation of risks associated with a Processing Activity that are likely to result in a high risk to the rights and freedoms of natural persons (**Data Privacy Impact Assessment**, "**DPIA**"), and
- all measures to mitigate any identified risks, including technical and organizational measures, to ensure confidentiality, integrity, availability and resilience of IT applications, infrastructure and services that are used to Process Personal Data.

3.1.10 Risk Cases

Derived from the Data Privacy principles laid down in Section 3 above, Envu has identified the following risk cases which Envu seeks to address with its Data Privacy regulations:

- Lack of legal basis for Processing Personal Data
- Lack of transparency on the Processing of Personal Data
- Lack of proper purpose limitation
- Lack of proper data minimization
- Lack of proper data retention and deletion of Personal Data
- Lack of integrity and confidentiality when Processing Personal Data
- Lack of proper management of a DPIA
- Lack of proper management of Data Subject requests
- Lack of proper management of Data Privacy Incidents and Personal Data Breaches
- Lack of proper management of authority interactions
- Lack of ability to demonstrate compliance with Data Privacy laws

3.2 Implementation, Training and Control

The principles of this Policy are to be implemented when Processing Personal Data.

The following measures are to be implemented in all legal entities of Envu by local management in alignment with Envu's Data Privacy Business Partner:

- Provide local availability of this Policy
- If necessary, translate content of this Policy into local language

4 Appendix

4.1 Definitions and Abbreviations

Anonymous Data	Information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable
DPIA	Data Privacy Impact Assessment, a privacy-related evaluation of risks associated with a certain Processing Activity in cases where a Processing Activity is likely to result in a high risk to the rights and freedoms of natural persons

Data Privacy Incident	Situation where Envu learns about a possible Personal Data Breach
DPMS	Data Privacy Management System (please refer to 3.1.7 for more details)
DPO (Data Protection Officer)	Role within a company or organization whose responsibility is to ensure that the company or organization is correctly protecting individuals' personal data according to current legislation.
Privacy Agreement	Special agreements required with third parties prior to sharing Personal Data with them
Data Processing Lifecycle	Processing phases, which contain the most relevant operations that are usually performed on Personal Data in the corresponding Processing phase
Data Subjects	The individuals to whom Personal Data belong to
IP	Internet protocol
Personal Data	Information that directly or indirectly identifies a natural person
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data
Pseudonymized Data	Personal Data that is separated from direct identifiers so that it cannot be linked to an individual without additional information held separately and securely from the Processed Personal Data
Privacy Statements	Information about a Processing Activity, given in a concise, transparent, intelligible and easily accessible form, using clear and plain language and limited to information relevant to the individual Processing Activity
Processing / Processing Activity	Any operation or set of operations which are performed on Personal Data or on a set of Personal Data
RoPA	Record of Processing Activities, a comprehensive and sustainable documentation of all Processing Activities conducted by Envu
Special Categories of Personal Data	Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, health information, sex life and sexual orientation or other categories of Personal data as defined by local laws