



CLUEVEST



Privacy & Data protection policy

Table of contents

1: Introduction:.....	3
2. Fundamental concepts:.....	6
3: Principles for data privacy:.....	7
I: Fairness and lawfulness:	7
II: Restriction to a specific purpose:	7
III: Transparency:	7
IV: Data minimization & data economy:.....	8
V: Deletion:	8
VI: Accuracy; Keep up-to-dateness of data:.....	8
VII: Confidentiality and data security:	8
4: Privacy by Design:.....	9
5: Our staff Responsibilities:.....	9
6: Reliability of data processing:	10
6.1: Customers:.....	11
6.2: Stakeholders:	13
6.3: Employees:	14
7: Data transfer management:.....	17
8: Consent of the Data subject:	18
9: Rights of the Data subject:.....	18
10: Data Breach incidents:.....	20
11: Data protection officer:.....	21
12: Addressing compliance with the GDPR:.....	22

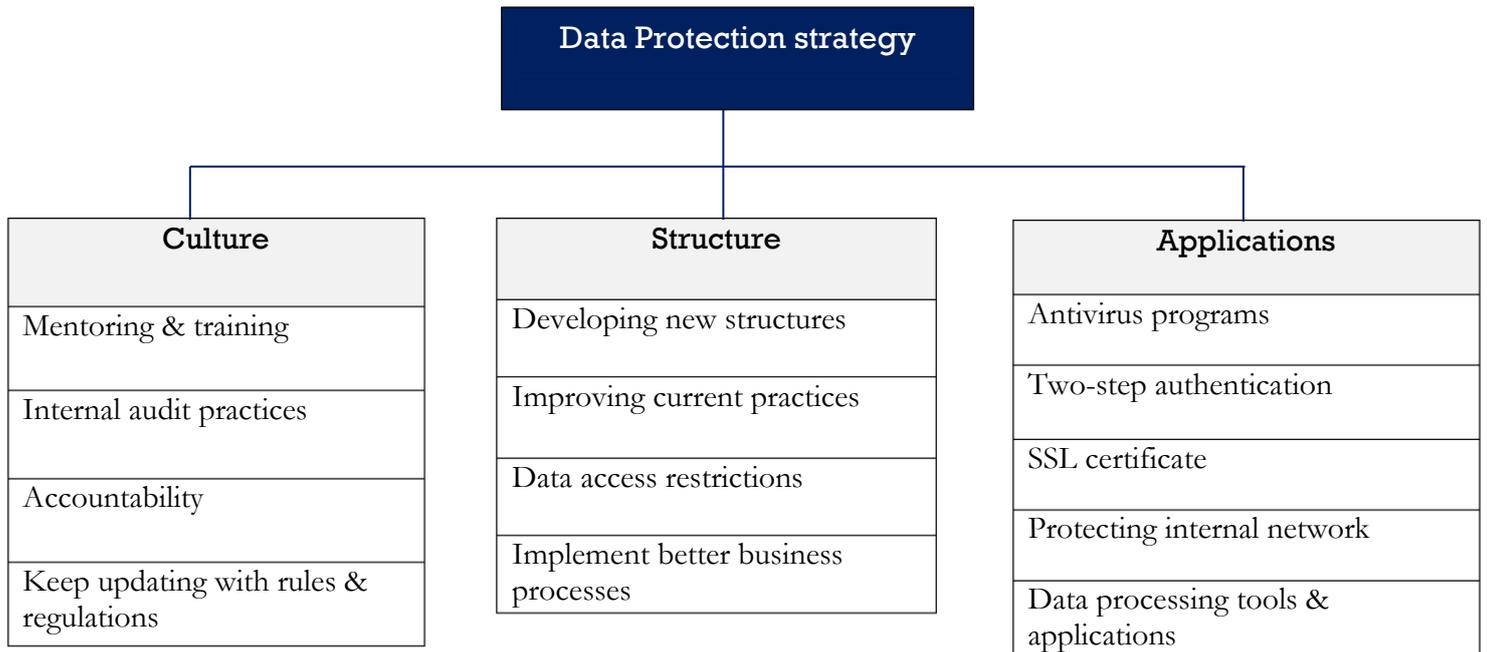
Privacy & Data protection policy

1: Introduction:

Cluevest is driven with its purpose and mission to create growth by adding maximum value in our customers' lives and in the society. Cluevest mission is to create growth but having the right policies, culture, internal structures at the place. Without a solid internal infrastructure and business processes, it would not be possible for us to give a best service to our customers, comply with rules & regulations and to protect our assets against any harmful attack. Cluevest invests heavy resources when it comes to have the right policies, culture and structure on the place that can give the best value to our customers and help us to succeed in our purpose and passion to adding maximum value in our customers' lives. Data privacy and protection have never been so important as it is in today's information and digital world. Cluevest has taken this very seriously even before we started to develop our products and services. We have invested heavy resources in consultancy and training, putting the right secure infrastructure and are working continuously every single day by training and developing our internal organization's culture to protect our customers' data and information.

The major driving force behind to invest heavily on these internal structures, policies and culture is to have a solid foundation to protect our customers' data from to be exposed to any other third irrelevant party that can harm our customers' privacy and integrity or can use data for any other purpose to get a benefit from our customers' data. Cluevest's management take it very seriously and is always one step ahead to invest and put the right policies and structures on the place to protect our customers' data. Cluevest is in a business of trust and reputation, and we want that our each and every customer and all of our stakeholders(suppliers, vendors, employees, investors, business partners) have a mental comfort and a peace of mind by having a strong trust on our values and business practices that we are here to not only help them, but we are here to help them by protecting their privacy and data. Cluevest also is very committed to work and collaborate with governmental agencies by following the guidelines, rules and regulation and keeping our business in compliance and also are working together to improve the data protection and our internal structures even more by following their recommendations and also keeping ourselves update by latest changing in rules and regulations related to data privacy and protection.

Cluevest has invested heavy resources and continues to invest more resources to improve our business practices in these following domains to protect our customers' data.



Cluevest is driven to create growth by building, maintaining and strengthening relationships with our stakeholders and our values are strongly tied by building trust and provide security to our stakeholders by protecting their data. Cluevest has very stricter requirements for data processing and complies with the general data protection regulations (GDPR) and other international standards and laws that are applicable globally in other markets.

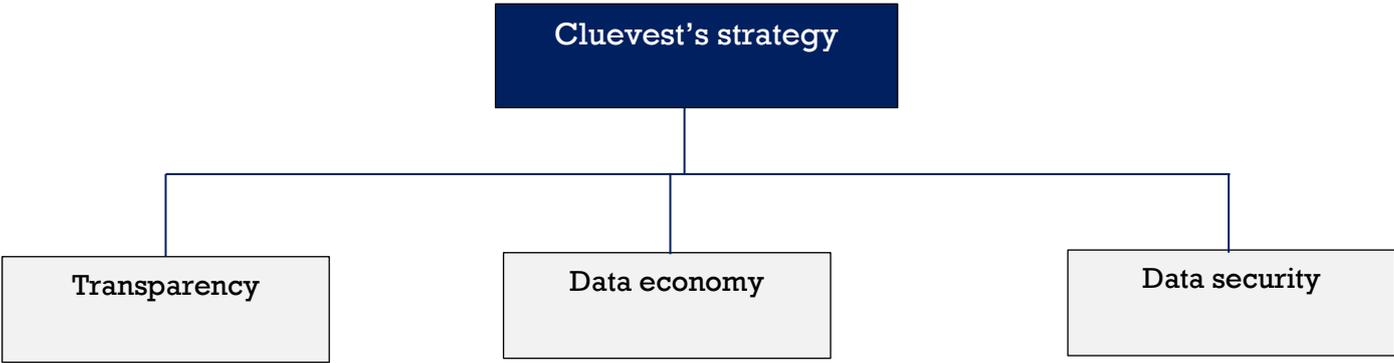
Cluevest collects and processes data in its daily business practices related to following data subjects:

- Current, past and prospective employees
- Customers
- Users of our websites
- Subscribers
- Other stakeholders

The purpose of this policy is to give more information to our customers and stakeholders about how we are processing and protecting their data from any misuse. In addition, the purpose of this policy is to give more information to regulators and governmental authorities about how we are complying with the rules and regulations by putting the right practices on the place.

This control applies to all systems, people and processes that constitute the organization's information systems, including management, employees, suppliers and other third parties who have access to Cluevest's stakeholders' information. GDPR is one of the most comprehensive framework to protect the customers' data and privacy. For to comply with rules and regulations, we have adopted principles within our organization that are in alignment with the

GDPR and other international data privacy standards. Our strategy is to follow these principles and develop the culture and implement the right tools and practices that will ensure the protection of customers' data. These principles are based on transparency, data economy and data security among others, and we strongly mirror these principles in our business practices to comply with rules and regulations.



2. Fundamental concepts:

Here below are the details of some of the fundamental concepts related to data privacy and protection.

Personal Data:

Any information relating to an identified or identifiable natural person ('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.

Processing of data:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller:

A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject:

As per data protection policy, data subject is any natural person whose data can be processed. In some countries; legal entities can be data subject as well.

3: Principles for data privacy:

Our data privacy principles are aligned with GDPR principles for data privacy and protection. We implement following principles in our business practices to comply with rules and regulations and also protect customers' data and privacy.

- I. Fairness & lawfulness
- II. Restriction to a specific purpose
- III. Transparency
- IV. Data minimization & data economy
- V. Deletion
- VI. Accuracy; keep up-to-dateness of data
- VII. Confidentiality and data security

I: Fairness and lawfulness:

The first principle strengthens that data should be processed lawfully and fairly. The individual rights of the data subject must be protected while processing personal data.

II: Restriction to a specific purpose:

Data should be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with GDPR Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

III: Transparency:

Data subjects should be informed about how his/her data is being handled. Generally, personal data should be collected directly from the individual concerned. When data is collected, the data subject must either be aware of or informed of:

- The identity of the data controller
- The purpose of data processing
- Third parties or categories of third parties to whom the data might be transmitted.

IV: Data minimization & data economy:

Before requesting and processing of personal data, we must determine whether or to what extent the processing of personal data is necessary in order to achieve the purpose for which data is undertaken. Data should be adequate, relevant and limited to achieve any purpose with the data. We need to pursue the goal by anonymization and minimization wherever it is possible. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

V: Deletion:

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with GDPR Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

VI: Accuracy; Keep up-to-dateness of data:

Personal data must be accurate, complete and correct and suitable steps should be taken to keep the data relevant, correct and up to date.

VII: Confidentiality and data security:

Personal data should be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

Cluevest's values, culture and business practices are in alignment with these privacy principles, and we ensure that we have put strategies and policies on the place to comply with these principles. Our business workflow, business processes and applications are in alignment to follow these principles, and we also provide guidelines, mentoring, training and have accountability on the place to comply with these principles. We do monthly internal audit and are working consistently to sustain and be persistent with our culture to protect customer data and use the data according to data privacy rules & regulations. We continue to strengthen and improve our business processes and applications for to be one step ahead when it comes to data privacy and data protection.

4: Privacy by Design:

Cluevest's management and the whole team are very committed to always think ten steps ahead when it comes to not only developing products and services but also the internal organization's culture and infrastructure which are the major foundation and backbone to deliver our products and services to our customers and add value in their lives. We think ten steps ahead when it comes to implementing the new internal organizational processes, integrating new applications and technological tools, hiring new employees or contractors. We build, design and hand over responsibilities by taking into consideration of data privacy and data protection. Whenever we start looking any technology or application into our platforms, we think the security aspects and how strong it can protect us and how it will work practically in our growing business. We build and design each element of our business process by taking into consideration the privacy of our stakeholders.

5: Our staff Responsibilities:

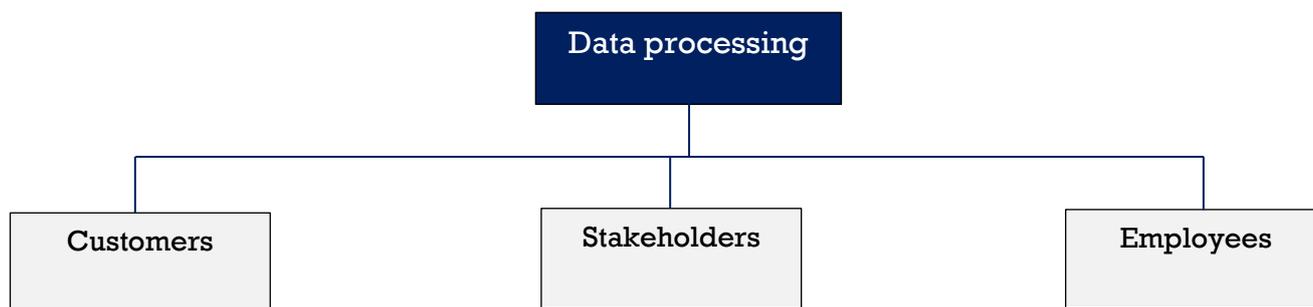
Cluevest's culture is built on our dedicated employees and other stakeholders who are committed to add value in our customers lives by holding themselves accountable and doing their best. Our employees are committed to do the best by holding themselves accountable. Our employees who share or have access to our customers and other stakeholders data share the same responsibilities at their working places:

- To obtain and process personal data fairly.
- To keep such data only for explicit and lawful purposes.
- To disclose such data only in ways compatible with these purposes
- To keep such data safe and secure.
- To keep such data accurate, complete and up-to-date.
- To ensure that such data is adequate, relevant and is not excessive.
- To retain such data for no longer than is necessary for the explicit purpose.

These work ethics and responsibilities of our employees are aligned with our privacy principles and each one hold each other accountable.

6: Reliability of data processing:

Cluevest's management and employees are committed to live their culture, values, work ethics and designed policies for data privacy. Employees and management whoever have access to the personal data is committed that they follow the organizational policy related to data privacy and make ensure that at each step their actions are aligned with our privacy principles. Cluevest processes the data of its customers, stakeholders and employees in their daily day to day business.



In our business practices, we process the data due to at least one or multiple reasons within our organization.

- Due to contractual obligations
- To meet our legal obligations
- When there is a legitimate interest
- To protect the vital interest of the data subject itself
- By getting consent to use for marketing & promotions, research and historical analysis, for future job opportunities, for future business relationships

Cluevest processes the data by taking into consideration of rules and regulations and complies with the privacy rules. Cluevest is strongly driven to work with data minimization and have implemented data policies based on our data risk assessment. We do our best not to process the data which fall in risk group-3. Here below is a brief guideline about our risk scale. This risk scale is defined based on which data can be more harmful if data breach incident occurs.

Risk scale: 1 (low Risk)	Risk scale:2 (medium risk)	Risk scale: 3 (high risk)
In this includes: Name, email, phone/mobile number; address; IP address, etc.	In this include: Age; gender; Job title, career history, etc.	In this include: Personal identity numbers; credit card details; racial/ethnic origin; political opinion; religious/philosophical beliefs; trade union membership; health data; sex life/sexual orientation; genetic data; biometric data; personal data related to criminal convictions & offences.

Cluevest’s culture, internal structures are built based on our these risk scale analysis and we always strive to not only with data minimization but also avoid to process data which falls in risk scale-3, but there are minor exceptions and we do this only when we absolutely need to do this for our contractual obligations or when there is a legitimate interest. Even if we use the data which fall in risk scale-3, we always try to put the right structure and tools at the place to protect the data, this includes for example data encryption; data masking; data obfuscation; role minimization and we always comply with PCI standards whenever we process customers credit cards in our business transactions. Certain sensitive data is only processed if data subject has given consent or it is mandatory due to law for asserting, exercising, or defending legal claims regarding the data subject.

Here below are the more details about each type of data subject and how we process the data.

6.1: Customers:

I: For contractual obligations:

Customers data is processed for contractual obligations, which include serving our customers once they have bought our products/services. Customer data is stored and processed for to fulfil our contractual obligations to our existing customers and kept in use for a contractual purpose, for legal obligations, and for marketing as long as customers have given consent for this.

II: For legal Obligations:

Customers data is processed and kept within our organization for to comply with legal obligations. Personal data is kept as long as we need to comply with rules & regulations. This includes, for example, tax purposes, accounting purposes, national legislation request or any lawsuit, etc.

Data can also be processed if national legislation allows this. In that case, the type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions.

III: For legitimate interest:

Personal data of the prospective customers can be processed for to establish, execute or terminate a contract. Prior to offering products/services, personal data can be processed to prepare bids, informational and educational based selling purpose; consultative sale processes and to initiate the sale process. Prospective customers can be contacted for follow up, for give more insights information and details about our products/services to find the right fit and best match to serve our customers and to add value in our prospective customers's lives by helping them to choose the right products/services which will help them to live a better life. Any restrictions requested by the prospective customers are applied and complied with.

IV: For vital Interest of the data subject:

Cluevest arranges many free events and promotional educational programs for to make growth possible and to connect with our right prospective customers. Personal data can be processed for the vital interest of the data subject if there is any emergency, and our staff can help to save that data subject life. This can happen in situations if any data subject during these events and promotional educational programs face health crises, and we need to contact the relevant governmental agencies or to their friends and families. This even applies even when any data subject visits our office and if data subject faces health crises, then data can be processed to contact relevant governmental agencies and to data subject's friends & families.

V: For marketing & promotions:

Personal data is processed for marketing, promotions and to give away free contents and educational material to our customers and prospective customers. Cluevest is driven to create growth by connecting with our prospective customers, customers and audience. Generally, data is processed by getting the consent from the data subject, and data is used only for the purpose for which data subject has given his/her consent. Data can be accessed from third party sources but in that case data subjects are informed, and their consent are taken as soon as possible at the first contact with the data subject.

Data subject has a right to withdraw his/her consent for marketing & promotion, and they can withdraw automatically by using the application tools and opt-out buttons which are provided to them during our conversation and messages with them. If that will not be possible due to any technical issue, data subject can contact to our support team(support@cluevest.com), and our team will help them immediately at no cost to withdraw their consent for marketing and promotional purposes.

If data subject has withdrawn his/her consent, his/her data will not be used for marketing & promotional purposes, and data will be deleted immediately, if we do not need to retain the data due to any other solid ground, which includes(contractual obligations, legal obligations, legitimate interest, research & historical analysis).

Consent is taken electronically or in a written form. Consent can also be taken verbally, for example, on phone or in physical meetings. Consent is documented for to comply with rules & regulations. Consent is taken from a parent in

case age is below than 16.

Once data subject has withdrawn consent, data subject can give consent again at any time whenever he/she wants to accept our marketing & promotional material and marketing and promotions material will be sent again to data subjects at no cost, and their consent will be accepted at no cost to give them the best experience with our brand. Their new consent will be only used for the purpose for which they have given consent to.

6.2: Stakeholders:

Cluevest is driven with its purpose and mission to create growth, and this is not possible without our stakeholders. Cluevest believes on together, believes on sharing values and vision, believes on coming along together to give the best value and service to our customers. Our stakeholders are the most important assets for our business and for our organizations. Cluevest's stakeholders include partners, suppliers, vendors and contractors. Cluevest processes their data in our daily business transactions for the following means.

I: For contractual obligations:

Stakeholders data is processed for contractual obligations, which include all the formal/informal and legal contracts. Data is processed within the organization to hold each other accountable, deliver on each other promises, for protection and security, for legal obligations. Data is kept within the organization as long as it is required and is absolutely necessary by taking into consideration of the rules & regulations of data privacy and protection.

II: For legal obligations:

Stakeholders data is processed and kept within the organization for to comply with legal obligations. Personal data is kept as long as we need to comply with rules & regulations, for our legal protection. This includes, for example, tax purposes, accounting purposes, national legislation request, or any lawsuit protection; legal claims to fulfill each other promises according to the contracts.

Data can also be processed if national legislation allows this. In that case, the type and extent of data processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions.

III: For legitimate interest:

Personal data can be processed for market research for to find the best suitable match for our organization. Personal data can be processed for due diligence for to rely on any stakeholder for our business purposes and mission. Data is processed for legitimate interest once both parties are willing and are interested in future business relationships. Personal data is kept within our organization as long as it is necessary during the process. Personal data can be kept within organization after the processing by getting consent of the data subject and is kept within organization as long as both parties are interested in any future business relationship.

IV: For vital Interest of the data subject:

Cluevest invites and meets different stakeholders at its office locations and even at different private offices and hotels to find, test, negotiate and write contracts with our stakeholders. Our stakeholder/s data can be processed due to any urgent health emergency where we need to contact relevant governmental agencies, his/her/their family & friends to save and to protect his/her/their lives.

V: For marketing & promotions:

Our stakeholders are our major business partners and can be our customers as well. Cluevest is driven to make an impact by adding value by its products/services to each and every individual on this planet. Cluevest arranges, invites, sends, delivers different marketing, promotional, information material about our products/services to our prospective customers. Marketing & promotions material can only be sent to our stakeholders if they have given their consent. Marketing & promotions can be sent as long as they have given consent.

Data subjects have a right to withdraw consent at any time through digital applications and tools, if that would not be possible in any given situation, they can contact to our support team at (support@cluevest.com), and our support team will help them to withdraw their consent at no cost. Marketing and promotions will be stopped immediately, and data will be deleted immediately if there is no other legitimate reason. Data subject can give again consent at any time at no extra cost to accept marketing & promotions from Cluevest.

Consent is taken electronically or in written form. Consent can also be taken verbally for example on phone or in physical meetings. Consent is documented for to comply with rules & regulations. Consent is taken from a parent in case if age is below than 16.

6.3: Employees:

I: For contractual obligations:

Employees data is processed under contractual obligations for to process salaries, compensations and to provide other employment benefits. Employees data is also processed for other business purposes, for example, to track sick leaves and work performance. These all data processing occurs for to fulfil contractual obligations. Data is processed only that is relevant and is related to the purpose.

II: For legal obligations:

Employees data is processed to comply with employment labor law in certain statutory wherever it is required. Employee data is processed also for other legal purposes wherever it is required. Employees data is also kept for to protect the organization against lawsuits and to comply with legal obligations. Wherever data is used for legal obligations, employees are treated fairly and the maximum effort is taken to expose less data to protect employee integrity & privacy.

There must be a legal authorization to process personal data that is related to employment relationship but was not originally part of the employment agreement. This can include other legal requirements, collective regulations with employee representatives, consent of the employee or the legitimate interest of the company.

III: For legitimate interest:

Prospective employee's data can be processed wherever the data subject is willing to initiate an employment relationship with the organization. Personal data can be processed for screening the right candidate and for to do due diligence during the selection process.

Highly sensitive data which falls in risk scale-3 category are processed only under certain conditions. Certain data can be processed only under special requirements of the national law. The processing of highly sensitive data must be permitted or prescribes under national law. Additional processing can be permitted if it is necessary for the responsible authority to fulfil its rights and duties in the area of employment law. The prospective candidate/employee can also give consent to process sensitive data.

Other legitimate interests are generally of a legal nature for which data can be processed, which includes (e.g. filing, enforcing, defending against legal claims) or financials (e.g. valuation of company).

For processing the personal data, control measures and the interest of the employees are taken into consideration and if there is any risk for data subject related to data privacy, appropriate steps and measures are taken to protect employees data privacy.

IV: For vital Interest of the data subject:

Cluevest is driven to create growth and bring along right candidates that can help us with our mission and purpose to serve our customers better and at the same time help individuals to find the best suitable employer for their professional career. Cluevest participates in different job fairs/events and also arranges different sessions to meet the young talent to tell about its culture, future opportunities and what we are looking in the workforce so that they can prepare them better to find their next employer. It happens even prospective employees visit us at our offices, and even Cluevest meets prospective employees in hotels, private office and for different case competition and networking events. Data subjects's data can be processed due to any urgent health emergency where we need to contact relevant governmental agencies, his/her/their family & friends to save and to protect his/her/their lives.

V: For marketing & promotions:

Cluevest major assets are its employees and stakeholders that do their best at each single day to make the Cluevest even better and drives it towards its mission and vision to make growth possible by adding maximum value in our customers' lives. Cluevest needs to connect, make an impact, attract and motivate the prospective talent that Cluevest is the best employer for their professional career where they feel home, are excited, motivated, passionate, and cluevest culture is driven to challenge them to help them to grow by increasing their performance, skills and by helping them improve their personality attributes. Cluevest is driven to connect to help people to pursue their passion and dreams related to their professional career.

During the selection process, we choose the candidates who can be best fit for our organization. The candidates which are not relevant for our organization, we inform them through our suitable communication channel (phone/email/postal/third party), and their data is deleted immediately or maximum within 30 days from our systems.

The other candidates which can be interesting and relevant for us and can be a best match for our future job opportunities are kept in our employment data. These candidates' data are stored and protected for future job opportunities, as long as there is a mutual interest from the both sides. Candidates have a right to withdraw their application/interest at any time. If they choose to withdraw their interest/application at any time, their data is deleted immediately or maximum within 30 days at no cost. Candidates have a right to join our employment database again by giving a new consent.

Consent is taken electronically or in a written form. Consent can also be taken verbally, for example, on phone or in physical meetings. Consent is documented for to comply with rules & regulations. Consent is used only for the relevant purpose which is about employment opportunities or employment offerings as an independent contractual agreement.

Prospective candidates/employees have a right to know about their data with the Cluevest and also have a right to withdraw their consent for any future job opportunities. Prospective candidate/employees can contact to HR(career@cluevest.com) for any queries related to the data privacy, and the relevant team/person within the organization will be more than happy to help the data subjects with their queries at no cost.

VI: Monitoring & controlling:

Cluevest culture is strongly based on self-responsibility, freedom, passion, driving force and think and do best by yourself in each given situation and be committed to add maximum value to our customers lives by holding themselves accountable and comply with rules and regulations. Although Cluevest puts some monitoring and controlling on the place where this is important to protect the company infrastructure, prioritize security and to minimize the risk related to any harmful attack against the company structure, systems and privacy.

Company provides tools (email, telephone, access to intranet, internet, social networking related to work/projects) and these tools are organizational resources for to perform best and to drive growth and profitability. These resources can be used within legal regulations and internal company policies. In the event of authorized use for a private purpose, the relevant laws related to their use and communication should be observed.

Cluevest does not put any general monitoring to these applications for to give employees freedom and to respect their personal integrity and privacy, although protective measures can be enhanced to protect the network, tools, applications, security and privacy of the company and its associated stakeholders.

For security reasons, these organizational resources can be logged for a temporary period. Evaluation of this data from a specific person can be made only in a justifiable case of suspected violation of laws or internal policies of the organization. The investigation can be conducted only by the investigative department while ensuring the principle of proportionality is met. The relevant national laws are being observed to comply with rules & regulations.

7: Data transfer management:

Cluevest is driven with its purpose to create growth by protecting the data privacy of our stakeholders and customers, and collaborates with the governmental authorities to have their confidence on our business operations and at the same time to comply with all the rules and regulations. Cluevest is a small and medium-size company and for its daily day business operations, Cluevest needs to rely on suppliers, vendors and business partners to succeed in its mission to add maximum value in our customers' lives and to deliver on our promises.

Cluevest management is committed to comply with rules and regulations and implement the necessary steps for data privacy and protection that are in alignment with our privacy policy and more importantly with our privacy core principles. Some of the necessary steps which management take are to collect as less data as possible that is relevant to perform any business transaction and at the same time minimize its access by implementing role-based access to protect the privacy of the data. We use intensively risk scale parameters, and we do our best not to collect data, which falls in risk scale-3. If we need to collect the data that belongs to risk scale-3 for some of our business transactions, we always try to put the more necessary steps to protect the privacy of the data subjects.

Cluevest complies with rules and regulations when it comes to transferring of data within EEA and even outside EEA. Cluevest has some vendors, suppliers outside the US, EEA area. These include, for example, IT services, accounting services, office administration services and marketing services. Cluevest does this because of having long-term business relationships that we can trust, improve business processes and effectiveness to give the best service to our customers. Cluevest is committed to hold each of our business partner, supplier, vendor accountable by having right policies, structure on the place to comply with rules and regulations. Here are some of the key steps management took/takes to protect data privacy of the data subjects and to comply with rules and regulations.

- Have written contracts based on standard contractual clauses defined by general data protection regulations (GDPR).
- Educate, train and mentor our suppliers, vendors about data privacy and protection.
- Implementation of monthly accountability reports to all employees across our organization and to all of our vendors and suppliers.
- Evaluate regularly the capabilities and necessary steps which are taken by our suppliers and vendors to ensure that they provide enough protection for data privacy.
- Work effectively with data minimization and role-based access.
- Do our best in not to process data, which falls in risk scale-3 or put the necessary steps on the place for data protection and privacy.

Cluevest's management is committed to hold each of our supplier, vendor accountable and has made ensure that each and every supplier and vendor are obliged with our data privacy policy and do their best to take even more necessary steps for data protection. Suppliers and vendors are guided to cooperate related to any inquiry made by the supervisory authorities from the country wherever we are located as a legal entity (data exporter/controller) and are responsible to

comply with rules and regulations. Cluevest's management is also committed to cooperate with the respective supervisory authorities to make ensure that we are doing our best to protect the rights, privacy, integrity of the data subjects.

Cluevest's policies, internal structure and business processes are designed to make ensure that we can provide the required and necessary data privacy and protection to the data subjects and to comply with the rules and regulations. We have implemented Data breach processes to take necessary steps in case of a data breach incident to minimize the damage for the data subjects. We are committed to cooperate, support to the data subject in case of any data breach to provide protection to the data subjects.

8: Consent of the Data subject:

Cluevest is committed to create growth by complying with the rules and regulations and to give a best customer experience to our customers. Unless it is necessary for a reason allowable in the GDPR, Cluevest takes explicit consent from the data subject to collect and process their data. Data is used and processed only for the purpose for which it is collected. In case of children age below than 16, parental consents are obtained. Cluevest provides transparent information to the data subjects about the usage of their data and their rights as a data subject. Cluevest provides clear information where data subjects can contact about to execute their rights as data subjects and information related to their queries are provided to them in a clear and simple language without any cost.

If personal data are not obtained directly from the data subject, then data subjects are informed in a reasonable period and definitely within a one-month period.

9: Rights of the Data subject:

Cluevest is committed to respect the rights and privileges of the data subject itself and provide the best service at no cost to help them with their data queries for to help them to provide the comfort, security, trust and confidence on their own power to act on the behalf of their own data. These are the following major rights of the data subjects which we are committed to go beyond an extra mile to do our best to respect and act in accordance with the rights of the data subject.

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within Cluevest that allow the required action to be taken within the timescales stated in the GDPR. Here below in a table, there is a brief overview of these procedures.

Data subject rights	Cluevest's procedures
The right to be informed.	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection
Rights in relation to automated decision making and profiling	Not specified

Cluevest is committed to perform these queries as soon as possible or within a given timeframe of any specific procedures. Please note that data subject's data cannot be erased if we need to keep data due to fulfil our contractual obligations or any legal obligations. Data subjects can contact to us by the following provided sources:

Contact details related to the Data queries	
Data subject type	Contact
Customers & stakeholders	support@cluevest.com
Prospective employees & employees	career@cluevest.com

10: Data Breach incidents:

Cluevest has taken necessary steps to have procedures and actions on the place that need to take to minimize the risk in case of any data breach incident and also inform to the respective data protection authority (DPA) and to the data subject itself, if it is required by law and data breach can be harmful for the data subject. Data breach is any incident, which violates our data privacy policy. These incidents include:

- Improper transmission of a personal data to third parties
- Improper access of a personal data by any third party
- Loss of personal data

As per policy in case of any data breach incident, employees, vendors, suppliers are responsible to take the necessary steps to mitigate the risk and also to inform to the management as soon as possible about any data breach incident. Management is responsible to take the necessary steps together with the team to mitigate the risk of the data breach and also take other necessary steps according to the rules and regulations. Management will evaluate the incident, and if it is likely to result in the rights and freedom of the data subject, the relevant data protection authority (DPA) will be informed within 72 hours. This will be managed in accordance with our information security incident response procedure which sets out the overall process of handling information security incidents. In addition, if it is necessary depending on the nature of data breach incident and the level of risk, management and team will inform the data subject about the level of risk, about the incident and what actions they can take as a data subject to minimize the risk against any potential loss.

Under the GDPR, the relevant DPA has the authority to impose a range of fines of up to four percent of annual worldwide turnover or twenty million euros, whichever is the higher, for infringements of the regulations. Management is committed to cooperate with the relevant authorities to protect the privacy and against any potential loss to the data subject and also will work together with the national authorities to comply with rules, regulations.

11: Data protection officer:

A defined role of Data Protection Officer (DPO) is required under the GDPR if an organization is a public authority, if it performs a large-scale monitoring, or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Cluevest is a small and medium-size organization, and management took necessary steps to ensure the privacy of data subjects and to comply with rules and regulations. We are also committed to not process data, which is sensitive (risk scale-3) or lower the processing of risk scale-3 data as much as we can. Management invests consistently heavy resources in training, consultancy from external sources to make ensure that we are doing our best to protect the privacy of data subjects and are also complying with rules and regulations. Cluevest's management itself is responsible and act as data protection officer and is committed to have Data protection officer as our business will grow and there will be absolutely a necessity to appoint a data protection officer.

12: Addressing compliance with the GDPR:

Cluevest's management has taken following actions to ensure that the Cluevest complies at all times with the accountability principle of the GDPR:

- The legal basis for processing personal data is clear and unambiguous
- Management has taken responsibility to act as a data protection officer.
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
 - Organization name and relevant details
 - Purposes of the personal data processing
 - Categories of individuals and personal data processed
 - Categories of personal data recipients
 - Agreements and mechanisms for transfers of personal data to non-EU countries, including details of controls in place
 - Personal data retention schedules
 - Relevant technical and organizational controls in place

These actions are reviewed on a regular basis as part of the management review process to ensure their effectiveness and to continuously find ways to improve them and to comply with any changes in rules and regulations.

Please notice that we have not mentioned some of the details related to cookies which we use on our website in this privacy policy. Please read our cookies policy for to get more insights about which kind of information we collect from our website visitors for to improve our business processes and for to give best user experience on our website.



About the Cluevest

Cluevest, LLC is a business consultancy firm with focus on finance and growth. Cluevest offers business consultancy, business reports, business training programs, speaking engagements and has many other products for human resources and organizational development. Cluevest even owns brands: Legerwise, Starnox. Legerwise offers services in accounting & taxation. Starnox offers services in digital marketing and in content creations.