DATA PROTECTION COMPLIANCE POLICY AT NEXTWEBI

Nextwebi delivers high-end IT solutions to businesses. We are one of the most experienced and trusted **Web Design & Web Development Company in Bangalore** and we are also a Google partner digital agency having 7+ years' experienced professional team from designing a simple website to robust web application development, crafting a digital campaign & SEO. Currently, we are serving domestic and international customers of all sizes of business. We enable the brands & corporates to look good online using their websites so that the website can welcome its customers and give a pleasant user experience across the devices.

While serving the clients at global level with vast amounts of digital data, we are entrusted with the responsibility of securing the data with utmost confidentiality and security measures.

Policy brief & purpose

Our company's **Data Protection Policy** refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. The policy is framed in adherence to the rules and regulations stated under Information Technology Act, 2000 (IT Act) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and European Union's (EU's) General Data Protection Regulation (GDPR).

With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

Who is covered under the Data Protection Policy?

Employees of our company and its subsidiaries must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

Scope

This policy refers to all parties (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

Policy elements

As part of our operations, we need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc.

Our company collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up-to-date
- Collected fairly and for lawful purposes only
- Processed by the company within its legal and moral boundaries
- Protected against any unauthorized or illegal access by internal or external parties

Our data will not be:

- Communicated informally
- Stored for more than a specified amount of time
- Transferred to organizations, states or countries that do not have adequate data protection policies
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities)

In addition to ways of handling the data the company has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll process their data
- Inform people about who has access to their information
- Have provisions in cases of lost, corrupted or compromised data
- Allow people to request that we modify, erase, reduce or correct data contained in our databases

Actions

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyber attacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.)

Our data protection provisions will appear on our website.

The rules and regulations:

The major points of the GDPR policy are stated below. **The 'company' mentioned refers to 'Nextwebi IT solutions pvt ltd.'**

1. Data protection principles

The company is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;

b. collected for specified, 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 not be considered to be incompatible with the initial purposes;

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

a. This policy applies to all personal data processed by the company..

b. The Responsible Person shall take responsibility for the company's ongoing compliance with this policy.

c. This policy shall be reviewed at least annually.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the company shall maintain a Register of Systems.

b. The Register of Systems shall be reviewed at least annually.

c. Individuals have the right to access their personal data and any such requests made to the company shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

b. The company shall note the appropriate lawful basis in the Register of Systems.

c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the company's systems.

5. Data minimisation

The company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The company shall take reasonable steps to ensure personal data is accurate.

b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the company shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. The company shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

c. When personal data is deleted this should be done safely such that the data is irrecoverable.

d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the concerned legal authorities.

This policy also includes all terms and conditions stated under GDPR policy(see for more information https://cis-india.org/internet-governance/files/gdpr-and-india , https://gdpr.eu/checklist/ ,https://gdpr.eu/compliance/), Information Technology Act (see for more information https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf) and India's Personal Data Protection Bill (see for more information https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf).

Disciplinary Consequences

All principles described in this policy must be strictly followed. A breach of data protection guidelines will invoke disciplinary and possibly legal action for the company. Every employee is liable to adhere to the rules and regulations stated in the policy, failure in doing so will result in legal actions stated in the mentioned policies and all the official documents(like experience letter, character certificate, salary) from the company will be made null and void.

Quick summary for clients:

- Any confidential data (such as login details,hostings, domain details, email address) should be shared only on the following email address- ajay@nextwebi.com
- The client should refrain from sharing any confidential data over Whatsapp messages, SMS, phone calls, social media etc.
- The clients are advised to change the confidential password and relevant login details once the project is completed and handed over to them. This is entirely the client's responsibility to make sure that they have made necessary changes and taken suitable actions once the project is completed and handed over to them.
- All employees are trained to follow the GDPR compliance to maintain the confidentiality of the client's data.
- The employee's are strictly instructed not to share client's confidential information to any colleagues, friends, relatives or family members.
- If there is a breach of confidentiality and policy, an investigative procedure will take place and appropriate legal actions will be taken.
- If found guilty of breaching confidentiality and policy in any form, the legal actions will be taken in context of GDPR policy which includes 18years imprisonment or severe fines up to 4% of annual global revenue, depending on the severity and circumstances of the violation.

_____	_____
Employee's Signature	**Date**
_____	_____
Company's Official Signature	**Date**