

Data Protection Policy

Our Policy

1. Data Security
2. Sensitive personal data
3. Employee Information
4. Customer & client information
5. Domain names and email addresses
6. Financial information, including credit card details
7. Business associates' information
8. Client information
9. Information request
10. Disclosure to government & their agencies

The policy is addressed to staff members, but is relevant to all aspects of data protection.

The data protection policy exists to:

- Protect your data
- Protect the data of other members of our staff
- Comply with the law
- Protect the data of the company

Please remember that the data protection is the responsibility of all staff members at all times. It is very easy to disclose information about a colleague or a customer to a third party, friend or family member. If you do so, you are in breach of this policy and of your contract of employment. To avoid this, you should avoid discussing any aspect of your work outside of work and discuss issues about which you have strong feelings only with the appropriate person at work.

We are extremely concerned to protect your privacy and confidentiality. We understand that not only all employees but also customers, suppliers and others with whom we come into contact in our working day are quite rightly concerned to know that your or their data will not be used for any purpose unintended by them and will not fall into the hands of a third party. Our policy is both specific and strict. If you come across any instance of a failure of our policy, do tell us.

Information may be unlawfully available to computer hackers and unlawful visitors. We will take reasonable precautions against such events, but we take no responsibility for any unlawful act of any person.

Except as set out below, we do not share, or sell, or disclose to a third party, any personally identifiable information we collect.



Our policy

1. Security and management of personal data

- 1.1. Because personal data is or may be held on many computers within the office, please use the password system laid down. Do not change any password or insert password access where previously there was none.
- 1.2. Sensitive personal data is kept on one computer in the company. That computer is kept in a room, which is locked at night. Access to the sensitive data is protected and is limited to a maximum of 3 staff members. If it is necessary to extract any such data for use by another staff member, the data controller will follow the use and satisfy him/herself that the data has been deleted after use.

2. Sensitive personal data

We do not collect sensitive personal data.

3. Employee information

This information is used:

- 3.1. To maintain proper employment records for our own use;
- 3.2. To maintain salary records and to pay staff in accordance with our obligations;
- 3.3. To comply with our legal obligations relating to tax and money;
- 3.4. To comply with legal obligations relating to employment

4. Customer and Client information

This information is used:

- 4.1. To provide customers and clients with the services they have requested;
- 4.2. For billing and accounting purposes;
- 4.3. To enable us to answer their enquiries;
- 4.4. For verifying their identity for security purposes;
- 4.5. For marketing our services and products;
- 4.6. Information which does not identify any individual may be used in a general way by us or third parties, to provide class information, for example relating to demographics or usage of a particular page or service.

5. Domain names and e-mail addresses

Are recognised by our servers and the pages visited are recorded. This information is used:

- 5.1. In a collective way not referable to any particular individual, for the purpose of quality control and improvement of our site;
- 5.2. To send out news about the services to which web site visitors have signed up;
- 5.3. To tell customers and clients about other services of ours.



6. **Financial information, including credit card details**

This information is used to obtain payment for goods and services ordered from us. We do not use it for any other purpose. We do not store this information longer than necessary to process a payment. We are not responsible for such data once it has passed to our merchant service provider/bank.

7. **Business associates' information**

This information is given to us in the course of business. This information is used:

- 7.1. To maintain our accounts and business records;
- 7.2. To enable us to answer enquiries;
- 7.3. To verify identities.

8. **Client information**

All staff members are required to ONLY speak with account holders regarding their account unless otherwise permitted to by the client. Disclosing client personal information can lead to the termination of employment.

9. **Information request**

At any time you may review or update the personally identifiable information that we hold about you, by contacting us at the address below. To better safeguard your information, we will also take reasonable steps to verify your identity before granting access or making corrections to your information.

10. **Disclosure to Government and their agencies**

We are subject to the law like everyone else. We may be required to give information to legal authorities if they so request or if they have the proper authorisation such as a search warrant or court order.

Your signature below indicates that you have read the ESDS Software Solution Limited Data Protection Policy. Your signature does not mean that you agree with each and every provision of the policy. However, it does indicate that you will abide by the regulations set out in the above policy.

Signed 

Date 21-April-2025

(Print Name) Vikas Deshmukh