

Information and Data Security

Your personal information is **kept strictly confidential and secure**. We **prioritise your privacy**, ensuring that your data remains **safe from unauthorised access or disclosure**. We use the highest standards of data protection and privacy control.

Privacy

Your **privacy is paramount** to us. We take **advanced measures to protect** it.

You could refer to the standards used by the best in the world and compare the same with eIRED.

 Google	https://safety.google/security-privacy/
 Microsoft	https://www.microsoft.com/en-in/trust-center/privacy
 Meta	https://about.meta.com/actions/protecting-privacy-and-security/
 LinkedIn	https://security.linkedin.com/content/security/global/en_us/index/our-security-practices

Data Protection

Transport layer encryption adds a security layer by encrypting data transmitted over a network, safeguarding sensitive information from unauthorised interception. HTTPS is commonly used for this purpose. This encryption protects sensitive information from being intercepted by unauthorised parties, safeguarding the confidentiality and integrity of data during transmission.



All data transmitted between your device and our servers is encrypted using HTTPS.

We strive to maintain the security and safety of Your Personal Data in line with industry standards. Once we have received your information, we use strict procedures and security features as per industry standards and the Data Protection Laws to try to prevent unauthorised access, loss, misuse, unauthorised disclosure and dissemination, destruction and alteration of Your Personal Data.


The security controls and practices implemented by el Red to protect Your Personal Data under its Privacy Policy shall be in accordance with the reasonable security practices and procedures under Section 43A of the Information Technology Act, 2000.

We aim to protect from unauthorised access, alteration, disclosure or destruction of Your Personal Data or other information that We hold. The security measures we adopt to protect your Personal Data or other information include the following:

- We use encryption to keep Your Personal Data or other information private while in transit;
- We offer security features like an OTP verification to help You protect Your User Account on the Platform;
- We restrict access to Your Personal Data or other information to Our employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be subject to disciplinary action if they fail to meet these obligations;
- We ensure compliance with the Data Protection Laws as well as other Applicable Laws;
- We ensure that Your Aadhaar number is not disclosed in any manner and is stored in accordance with the extent of Aadhaar laws and regulations.

Threats detection and blocking

Our system, integrated with tools like New Relic and Sentry, automatically detects and blocks potential threats in real-time. By employing advanced threat detection algorithms, we swiftly identify suspicious activities, bolstering our ability to prevent unauthorised access or malicious attacks. This automated protection ensures the safety and integrity of your data and systems, enhancing overall security.



Aadhar verified accounts

Accounts that have been Aadhar verified undergo a stringent authentication process, providing an added layer of credibility and trustworthiness. This verification ensures that the account holder's identity is authenticated using Aadhar, a government-issued identification method, enhancing security and reliability for all interactions and transactions. Additionally, we employ sandbox environments to further bolster security measures and ensure the integrity of our authentication processes.



Control of user data

Users have the flexibility to modify or remove entered data at any time, empowered by features like JWT authorization and authentication. This advanced security measure ensures that only authorised users can access and modify their information, maintaining the integrity and confidentiality of their data. Additionally, our system employs OTP-based login, adding an extra layer of security to user accounts. Whether it's correcting errors or updating preferences, users have control over their data, enhancing their overall experience and satisfaction.



User Data

Transparent Purpose for your Data

We may monitor the use of the Platform through the use of cookies and similar tracking devices. To illustrate, We may monitor the number of times You visit the Platform or which pages You viewed. This information helps Us to build Your User Account and render better Services to You. Some of this data will be aggregated or statistical, which means that We will not be able to identify You individually.

The following table lists the information We may collect from You and how We will use it.

What we collect	Why we collect it
<p>Registration and onboarding of Users: Your first and last name, mobile number, email-ID, username, gender, date of birth, location, current profession, name of the employer, or any information We ask You on the Platform during on-boarding.</p> <p>Alternatively, You can also register on the Platform via your existing social media handles including Instagram and LinkedIn and fetch certain information from such accounts. We collect only public profile information, depending on the social media account used by You to log in while registering on the Platform. However, We do not collect/store any account passwords.</p>	<ul style="list-style-type: none"> ● To set-up Your User Account on the Platform and facilitate login. ● To notify You about products and services being offered by other Users on the Platform. ● To notify You about changes to the Platform, including the Terms of Use and this Privacy Policy. ● To help you network and connect with users. ● To provide you information regarding products, services, events, and opportunities. ● To facilitate communication with You and give customer support. ● To verify Your identity and pre-populate relevant fields in Our application's UI/UX.
<p>Other particulars submitted by Users: These are the particulars that are accessible on Your User Account but are not mandated to be provided during the onboarding/registration process, such as (a) reviews submitted by</p>	



other Users presented as 'Testimonials', (b) 'Leads' and 'Needs', (c) Bio, (d) User's skills, (e) awards and certificates, (f) education details including details about the User's school and college, and (g) the details of the User's employer and the role performed by the User therein.

Log Data: Information We automatically collect when You use the Platform, whether through the use of cookies, web beacons, log files, scripts, or any other information of similar kind.

Creating Leads on the Platform: The following particulars are to be populated/uploaded by Users who intend to post and share a Lead with other users on the Platform - (a) location, (b) images from the Users' device that fits the description of the Lead, and (c) description of the services sought to be offered along with its price range. The Leads outline the specific services that can be offered by their respective Users.

Creating Needs on the Platform: Users are also allowed to create Needs on the Platform highlighting their specific requirements, which includes particulars such as the location of the User. These can be shared by other users on the Platform or on other third-party platforms.

Sharing of Needs and Leads outside the Platform: The Platform allows the sharing of Needs and Leads posted by El Red Users on other platforms as well, and the Needs/Leads

- To allow other Users to assess if You would be a relevant fit for the specific Needs of the former basis your skills and other professional achievements, insofar as transacting in products and/or services is concerned.
- To allow Us to match a User with a specific Need with such other Users that best match the requirements of the former.
- To allow Our Users to reach out to a wider user base, and to introduce other potential Users to the Platform.
- To allow us to incorporate automated measures to expedite the process of matching El Red Users with complementary requirements. This is undertaken via the 'tags' selected by Users while creating their Need/Lead on the Platform.

so shared include the following particulars (a) the display picture of the respective El Red User, (b) location of the User, (c) title and company of the User, and (d) the description of the concerned Need/Lead.

Surveys: We may ask You to undertake surveys or fill questionnaires from time to time. Some of these will require You to give Us additional Personal Data or other information. These surveys or questionnaires may also be conducted by Our Partners, Our Service Providers, or any other third-party.

Device data: Information We collect from the devices You use to access or operate the Platform. This includes, without limitation, information about Your device attributes and identifiers, plugins, name of Your mobile operator or ISP, SMS sent by El Red, device language, time zone, IP address, connection speed, device applications, contact list, or any information available on such device.

- To develop new services, improve existing services on the Platform, and integrate User preferences, feedback, and requests.
- To administer the Platform and facilitate internal operations, including but not limited to, troubleshooting, data analysis, testing, research, security, and fraud-detection.
- To enable You and other users on the Platform from gaining access to your network.
- To better understand how You use and access the Platform and to improve Your User experience.
- To assess effectiveness of and improve advertising and other marketing and promotional activities.
- To keep the Platform compatible with the supported device(s).
- To provide You with automatic updates and security measures so that Your User Account is not used in other User's devices.
- To provide Us feedback on Your device behaviour, which helps Us to improve Our quality of Services but also provide an enhanced and customised User experience.

<p>Customer support data: Any information that You provide to Our customer support team or Our Grievance Redressal Officer periodically.</p>	<ul style="list-style-type: none"> ● To investigate Your support issue and assist You in resolving your query. ● To internally help Us in improving and developing Our User support systems. ● To pass on relevant queries from Users to Our Partners or Service Providers.
<p>Phonebook and contact data: We will seek your consent to access your phonebook data, specifically (a) the numbers you have saved, along with (b) the names by which you have saved each of the respective contacts on your device.</p>	<ul style="list-style-type: none"> ● To give Users the ability to interact and connect with a 'network of networks' in its truest sense, by showing them profiles of people already added on the phonebooks of their respective contacts and unlock those contacts for access by other users on the Platform. ● To allow Users to connect with people from varying backgrounds in an expedited manner, driven by the ease of identifying accounts that have been saved as contacts by the Users' connections.
<p>Location data: Information that We derive from Your device or from the location/address details You provide Us while using the Platform.</p>	<ul style="list-style-type: none"> ● For security and account management. ● To provide You with location customization.

We use Your Personal Data to send You promotional emails and messages. However, We will provide You the ability to opt-out of receiving such emails and messages from Us. If You opt out, El Red may still send You non-promotional emails and messages, such as emails and messages about the Services and Your User Account on the Platform.



Storage, Processing And Retention Of Personal Data

We will store Your Personal Data and other information only to the extent required by Us to carry out the Services as provided herein, and if there is a legal requirement to retain the same. We shall not retain any of Your Personal Data and other information if the purpose for which We collected it has been fulfilled, and there is no legal requirement for Us to retain the same.

The Personal Data collected by Us would be stored and/or processed on servers located in India, and such storage shall be in compliance with the Data Protection Laws. El Red will also be entitled to use third-party service providers such as MongoDB Atlas to store Your Personal Data. The storage location(s) are chosen to operate efficiently, improve performance, and reduce probability of errors while protecting Your Personal Data in the event of an outage or other problems.

Withdraw Consent: You may also choose to withdraw Your consent (including consent provided for processing of Your Personal Data or other information by Us or by any third party on Our behalf, or Your consent provided for data retention purposes) provided to the Platform at any point of time. In order to withdraw Your consent for the use, processing, disclosure, sharing or transferring of any Personal Data, You may raise a request on the Platform or by mailing Us at feedback@elred.io

Right to erasure: You may request the deletion or removal of Your Personal Data at any time. Such right of erasure can be exercised in a manner prescribed by the Central Government, by writing to Us at feedback@elred.io. On such a request for erasure, We shall delete all Your Personal Data stored by Us, as well as ensure that any third party Service Providers processing Your Personal Data on behalf of Us deletes the same as well, unless its retention is necessary for ensuring compliance with Applicable Laws.

Disaster recovery

Data backups are essential, especially in the face of natural calamities. Our system implements robust backup strategies, including AWS regional-wise live backups, daily local backups, and snapshots. By regularly backing up data to secure offsite locations and leveraging AWS infrastructure, organisations can mitigate the risk of data loss due to events like floods, earthquakes, or hurricanes. These backups serve as a crucial safety net, ensuring that vital information remains accessible and intact, even in the wake of unexpected disasters.

