



Data Protection Policy

Re:Ignite CIO, number 1183488, is committed to working with personal information lawfully and correctly. To this end Re:Ignite CIO adheres to the principles detailed in the Data Protection Act 2018, the General Data Protection Regulation (GDPR).

This is the Data Protection Policy for Re:Ignite Church. Re:Ignite complies with the following privacy principles with respect to personal data. It shall apply to all the staff and third parties involved in business with the company.

1. The company has access to lawfully acquired personal data, and it processes that data in a transparent manner.
2. The policy provides protection to any kind of data it collects with the consent of the data holders, including names, phone numbers, postal addresses, email addresses, and more.
3. The company will process the data only if and to the extent that
 - i. It has gained the consent of the data holders
 - ii. The processing is necessary for the relationship of the parties
 - iii. The processing is necessary for compliance with any legal obligations
 - iv. The processing is to further a legitimate business interest
 - v. It is necessary for the employee's performance
4. The company collects information with the explicit consent of the data holders, and it uses it for the explicit, legitimate purposes set forth in this policy and for no other purpose.
5. The company only collects data that is adequate, relevant, and limited for the purpose for which it is being collected.
6. The company collects and processes personal data as accurately as possible.
7. The company takes every measure reasonable and necessary to maintain the integrity and confidentiality of the information being collected. It does not provide or allow unauthorized persons to access it.
8. Data that is necessary to run the business and from which the company generates revenues, and it is collected with free consent and for a legitimate purpose will remain the company property, and the company will have the ultimate power to use that data legitimately.
9. Personal data shall be retained by the company as long as necessary, and it shall be deleted immediately after the need is over.
10. Personal data may be disclosed to the company's management, HR, or IT.
11. Personal data may be disclosed to third parties such as payroll and benefits vendors, background check companies, and more.
12. The data holder has the right to ask for any data from the company except which is adverse to the company's interest.
13. In case of a breach of the data, the company will notify the individuals and the appropriate authority within 48 hours of such breach.

Signature:

A handwritten signature in blue ink that reads "Alister Murdoch".

Date: 25th April 2023