

Security and Privacy Policy

1. Definitions

- Neutral Territory Limited (“company” “us” “we”)
- Anyone who chooses to provide us with data (“user” “you” “your”)

2. Identity and Access

The privacy of user data is very important to us. We will only ever access your data to provide you with services you have requested from us, or to provide services which we think might be of interest to you.

When you choose to work with us, we will ask you for your name, email, phone number and any organisation with which you are associated. We will never sell your personal information to third parties, and we won’t use your name or organisation in marketing statements without your permission.

When you contact us to use our services, we will keep your personal details for future reference. When you browse our marketing pages, we track that for statistical purposes such as conversion rates and to test new designs. We also store any information you volunteer, like surveys, for as long as it makes sense, but not exceeding the data retention as stated in paragraph 7. Deleted data.

The only times our company ever shares users’ information are:

- To provide products or services that the user has requested, with the users’ permission.
- To investigate, prevent, or act regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms of Service, or as otherwise required by law.

If our company is acquired by or merged with another company, we will notify users well before any information about them is transferred and becomes subject to a different privacy policy.

3. Sensitive and Personally Identifiable Data

Neutral Territory does not store or process credit card details within the our web site. Any credit card processing is out-sourced to a PCI/DSS compliant payment gateway provider and all payment details pass directly between your browser software and the payment gateway via a secure SSL encrypted session.

If user bank account details are stored in by our company, access is restricted to authorised users only and protected at the database layer for access only by authorised employees of our company.

All data used by our company for product development such as proof-of-concept, demonstration or testing purposes, will contain no personally identifiable data and sensitive data such as bank account data will be anonymised.

4. Security and Encryption

Any data shared is encrypted via SSL/TLS when transmitted between our servers and your browser application. Database backups are also encrypted. Data isn’t encrypted in production database, but we go to great lengths to secure your data whilst at-rest. This includes the use of perimeter network detection and prevention tools, vulnerability scanning, segregation of duties, privileged access management, anti-virus and malware protection and a strict change and release management process.

5. Individual’s Rights with Respect to their Information

The General Data Protection Regulation (“GDPR”) gives people under its protection certain rights with respect to their personal information collected by our company. Accordingly, we recognise and will comply with GDPR and those rights, except as limited by applicable law. User rights under GDPR include:

- **Right of Access.** This includes an individual’s right to access the personal information we gather about them, and their right to obtain information about the sharing, storage, security and processing of that information.
- **Right to Correction.** This is an individual’s right to request correction of personal information.

- **Right to Erasure.** This is an individual's right to request, subject to certain limitations under applicable law, that your personal information be erased from our possession (also known as the "Right to be forgotten"). However, if applicable law requires us to comply with your request to delete your information, fulfilment of your request may prevent you from using our services.
- **Right to Complain.** This is an individual's right to make a complaint regarding our company's handling of their personal information with the appropriate supervisory authority.
- **Right to Restrict Processing.** This is an individual's right to request restriction of how and why their personal information is used or processed.
- **Right to Object.** This is an individual's right to, in certain situations, object to how or why their personal information is processed.
- **Right to Portability.** This is an individual's right to receive the personal information the Company has about them and the right to transmit it to another party.
- **Right to not be subject to Automated Decision-Making.** This is an individual's right to object and prevent any decision that could have a legal, or similarly significant, effect on them from being made solely based on automated processes. This right is limited, however, if the decision is necessary for performance of any contract between them and our company, is allowed by applicable European law, or is based on their explicit consent.

For questions about exercising these rights or any assistance required, please contact us at itsfun@neutralterritory.com and you will receive a response within 10 working days.

6. Processors we Use

For GDPR purposes, our company is considered a Data Processor and the user is considered the Data Controller. As part of the services provided by our company, and only to the extent necessary, certain third-party processors may be contracted to process some or all personal information. All Processors are vetted for GDPR compliance and a full list can be requested by emailing itsfun@neutralterritory.com and you will receive a response within 10 working days.

7. Deleted Data

When you ask to remove your data, we will ensure that nothing is stored on our servers beyond 30 days. Anything you delete in any Neutral Territory application will have an immediate effect on the operation of the software but may be retained in the security backups for the contracted retention period.

8. Law Enforcement

We will not hand your data over to law enforcement unless a court order says we are required to do so, and unless we're legally prevented from it, we will always inform you when such requests are made.

9. Disclosures

We will disclose any security or data breach relating to our users' data to the user's Data Controller within 10 working-days of the security incident or breach being discovered. The disclosure will be limited to the users' Data Controller unless agreed otherwise between the user and us, or if there is a legal requirement to make such disclosure more widely known.

10. Location of Site and Data

All user data, electronic or otherwise, is stored only within the United Kingdom, European Union or European Economic Area.

Last Updated: October 1st, 2020