

Local Planet Solutions Ltd T/A Why Settle Data Protection Policy

Policy brief & purpose

Our Data Protection policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality.

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

Scope

This policy applies to all parties (employees, job candidates, customers, suppliers etc.) who provide any information to Why Settle. Employees of Why Settle 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.

Policy elements

As part of our operations, we need to obtain and process information. This information refers to 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.

Why Settle commits to collect this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to the company, 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 unauthorised 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 organisations, 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 those to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we will 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 we store

Actions

To exercise data protection we are committed to:

- Develop transparent data collection procedures
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorisation etc.)
- Build secure networks to protect online data from cyberattacks
- Include contract clauses or communicate statements on how data will be handled
- Inform individuals of the amount of time that their data will be preserved
- Declare its data protection provisions publicly (e.g. on website)
- Ensure all concerned parties have read the policy and adhere to it
- Train employees in online privacy and security measures
- Restrict and monitor access to sensitive data
- Establish clear procedures for reporting breach of privacy or data misuse

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.