



SP Commissioning

Unit 7a Ladycross Business Farm, Hollow Lane, Dormansland, Surrey RH7 6PB

Data Protection Policy for SP Commissioning (hereafter referred to as 'SPC')

Policy brief and purpose

SPC's 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.

Policy scope

This policy refers to all parties including employees (both PAYE and Sub contractors), job candidates, customers, suppliers and any others who provide any amount of information to us.

Who is covered under this Data Protection Policy?

Employees (including Sub contractors) of SPC must follow this policy. Consultants and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or who 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. A nonexhaustive list of the information covered by this policy includes any offline or online data that makes a person identifiable. These information types include names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data and so on.

SPC collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to us, the following rules apply.

Our data will be:

- Accurate and kept up to date
- Collected fairly and for lawful purposes only
- Processed by us within our 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 any 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 SPC has direct obligations towards people to whom the data belongs. Specifically we must:

- Let people know which of their data is collected
- Inform people about how we'll 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 held by us in either paper or electronic form.

Actions

To exercise data protection we're committed to:

- Restrict and monitor access to sensitive data
- Develop transparent data collection procedures
- Train employees in online privacy and security measures
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorisation et cetera).

Our data protection provisions will appear on our website.

Disciplinary consequences

All principles described in this policy must be strictly adhered to. Any breach of the above policy and any SPC guidelines relating to it will invoke disciplinary and possibly legal action.

Please note that there is also a specific Privacy Policy relating to our website which can be viewed at www.spcomm.co.uk.