



Scotforth Ltd – Data Protection Policy 2019

Personal Data - Clients / Potential Clients

There are two types of core individual we work with, clients and potential clients. As a service provider in the Exploration & Production sector we are likely to hold personal data on clients / potential clients which will allow us to meet their needs adequately.

This personal data is likely to be name, business address, and contact details.

Personal Data – Directors & Consultants

There are two Directors of the business, Peter Hutchison and Dmitri Balabayev, and there is one additional consultant who we work with, Stuart Hutchison.

Why we hold Personal Data

We hold the data to be able to:

- Communicate with clients, potential clients and the directors and consultants of the business
- Assess requirements, negotiate and agree contracts
- Work with clients on the delivery of their services.

How do we hold the Personal Data?

Many conversations occur verbally, but also via e-mail. With e-mail we use Outlook via Microsoft 365. Predominantly we hold data for contact purposes using email and mobile phones.

How do we process the Personal Data?

We access the personal data for contacting clients / potential clients, for holding conversations, taking notes on requirements and keeping them informed as appropriate.

Third Parties and Data Processors

Presently we use [Design Farm](#) to manage the SFL website and [CMS Broadband Ltd](#) to manage our IT services. Both companies adhere to GDPR.

Permissions for Personal Data

We use two core reasons for holding and processing Personal Data:

1. Legitimate Interest
2. Contractual relations.

Access and deletion of the Personal Data

Any of our clients / potential clients are entitled to access the data we hold on them, and request for such data to be deleted.

We anticipate being able to provide Personal Data to clients or candidates within 24 hours, and being able to delete such data on request within 24 hours.



Data Breach

If in the unfortunate case of a data breach (deliberate or accidental) the business due to its size will likely be aware of a breach, as all forms of data storage are accessed daily. Where a client / potential client or third party informs the business of a breach, this is likely to be within working hours.

Where a breach occurs

1. The business will secure the data and notify the storage provider of such a breach.
2. Those whose Personal Data is subject to the breach will be notified immediately and informed of how the breach will be dealt with. Agreement from those affected will also be sought.
3. The ICO will be informed immediately of the breach.
4. Where necessary trade bodies and the Police will be notified.