GDPR – Commonly Asked Questions

Do you have a GDPR statement?

Our statement regarding the protection of your data under GDPR can be found within our privacy notice which is available from our website.

What are the rules for GDPR?

Whilst we cannot provide legal advice to aid understanding on this, there are numerous sites available to help on this, including the ICO website here which includes some great explanations and advice.

As a data controller will you be sharing or giving access to my data to other organisations?

The minimal required data necessary to fulfil contracted services is only shared with specific parties. This information will be generally limited to the following:

- Contact Name
- Contact Email Address
- Site Address
- Telephone Number

Do you, or plan to, transfer personal data outside of the UK?

No data is transferred outside of the UK, unless specifically requested by the client data controller.

Are you storing any client data on premise or via a cloud based hosting solution?

Data is stored both on premise and in our own private cloud located in Tier 4 UK datacentres

Please describe what security arrangements are in place to protect this data

The Southern Communications Group comply with ISO27001 standards and are currently undertaking Cyber Essentials Plus accreditation.

When using client data in a non-production environment, is the data anonymised or copied from the production environment?

The data is not anonymised and is copied from the production environment, however access is restricted to personnel involved in the test procedures and is covered under the same ISO27001 standard as per the prodcution data.

At the end of the contracted period how will you ensure that you no longer hold personal data that the client is the data controller for?

Upon expiry of the contract we will remove any personal data that the client requests, subject to any contractual or legal requirement to retain the data.

How do you ensure the safe and secure storage of voice recordings in the cloud and/or on your servers?

All call recording data is stored on servers housed within a data centre that complies with ISO27001 (information security standards).

The servers can only be accessed through internal private network address space and is not publicly accessible.

All access to the servers are also 2 factor encrypted. We secure the recordings with a 256-bit encryption & we have a unique code generator to prove that they are the original although I would highlight that a considered risk would be access to your portal as this is publicly accessible.

Whilst we ask you to change your passwords and only allow individuals access that have the right, we cannot be in control of your own security and policies so if security was compromised locally, i.e. someone let their password known to another person, this would be your responsibility and you would be considered a "controller".

Portal Interfaces are held within the core of our network and protected externally through industry standard firewall units operating in High Availability mode.

Do you provide individuals with information about how their Personal Data will be used?

Specific information will be provided upon request; however, our privacy statement is available on our website.

How have you obtained our express consent regarding the use of Personal Data and how are such consents obtained?

We obtain consent through the completion of a GDPR form.

We will not normally share your data outside of the Southern Communications Group of companies but may be required to hand over this data as part of a legal or regulatory obligation.