Magrathea Telecommunications Limited,
5 Commerce Park, Brunel Road, Theale,
Berkshire RG7 4AB

0345 004 0040 info@magrathea-telecom.co.uk

Guidance on good practice relating to due-diligence in the UK

This document is for clarity and guidance but does not seek to replace official regulations or guidance and all Service Providers are responsible for satisfying themselves that they are adhering correctly to current standards and rules. Magrathea accepts no liability whatsoever for any errors, omissions or statements in this guidance or for any loss which may arise from your use of this guidance.

Who should make use of this guidance

Any provider obtaining numbers, either directly from the regulator or through a wholesale provider like Magrathea, and provides them to another party (i.e. sub-allocation). Also, any provider who is providing call origination services to their customer.

Each party in the provision chain needs to carry out their own checks and monitoring relevant to the services being provided. The following guide is designed to help consolidate Ofcom's good practice guidance in order for our clients to quickly and easily understand their obligations.

Key actions to take

- Check you have carried out recent and relevant due diligence on any of your customers to whom you provide service, and that you have documented your findings.
- Check you have a documented policy and procedures for your due diligence process, including ongoing monitoring and identifying risk.
- Check your contracts or user agreements help you to meet your regulatory obligations.
- Check you have a documented policy in place for dealing with reports of misuse.

The rules and regulations

Under the Communications Act 2003, Ofcom have the authority to regulate the allocation and use of UK telephone numbers. The regulation is set out in General Condition B1 (Allocation, adoption and use of telephone numbers)[1]. This general condition sets out the terms for effective and efficient use of numbers.

In November 2022, Ofcom released good practice guidance[2] to sit alongside GC B1, in order to bring clarity to the steps required by providers to prevent misuse of telephone numbers, specifically in relation to scams.

Most recently, in February 2024, Ofcom launched an enforcement programme[3] to make sure that providers are following the rules and will use adherence to their good practice guide as a measure of compliance.

Due Diligence Checks – Know your Customer

A key part of this process is to take reasonable steps to understand your customer and what risk there is of misuse of sub-allocated numbers or with call origination through your service.

The checks you carry out as part of your process will be determined by a number of factors, such as:

- The nature of your relationship with the customer
- The longevity of the relationship with the customer and relevant history
- The customer's target market

Below is a list of expected checks you may need to carry out to know your customer properly:

- Registered company details including trading names and registered office address
- Nature of business
- Existing telephone numbers and business websites
- Contact details of the senior manager with responsibility for numbering
- Information about the customer's network and the services provided

It is also likely to be appropriate to carry out more detailed checks by doing some or all of the following:

- Using the Companies House register:
    - confirm the information matches what you've been told
    - check the person acting as a director has not been disqualified
    - check the details of all individuals with influence in the business
    - check the details of individuals who receive a share of the revenue generated by the business
    - gather the names and details of any parent or holding company
- Ask the customer to confirm that no other party is operating in the capacity of a shadow director;
- Check the Cifas register to ensure the person you are dealing with is not listed;
- Check the Financial Conduct Authority (FCA) register to ensure the customer has permission to carry out regulated financial activity (if applicable);
- Check Phone-paid Services Authority (PSA) for banned individuals or companies;
- Check the ICO website for enforcement action taken;
- Check if the business has links to any other current or previous accounts with you;
- Obtain and verify details of place of business;
- Check the Individual Insolvency Register to see if influential individuals have gone bankrupt or agreed a deal to manage debt;
- Check for relevant industry registrations.

Due Diligence Checks – Intended use of your service

The next key part of the process is to fully understand why your customer requires the service from you and how they intend to use it. For example, do they have a specific target market or service they are promoting.

Some examples of specific things to check are:

- If providing numbers, is the volume requested consistent with the service as described to you?

- What is the customer's process for allocating numbers to their users (or customers)? Are their KYC checks and monitoring procedures adequate?

- What is the customer's process for validating caller ID, compliance with marketing regulations and compliance with all other key regulations and guidance?

- Do you have a main point of contact to discuss any concerns of issues relating to misuse of the service provided?

- How will you monitor your customers compliance with the terms of service under which you have provided numbers or calls?

- How often will you revisit your checks on the customer? For example, at set intervals or when additional services are requested?

Remember – your process and procedure should be proportionate to the risk of harm or abuse

Due Diligence Checks – Identify high risk customers

An important part of your onboarding and monitoring process is to flag any customer that could be considered 'high risk' and therefore take extra precautions. Examples of things that might raise concerns for you include:

- Inaccurate, vague or otherwise unclear information provided about the intended use of your service.
- Vague or absent checks being performed on their own customer (if not the end user).
- A request for numbers not matching the intended use of numbers (e.g. requesting too many numbers for intended use) or a request for concurrent calls not matching the intended volume of calls.
- Incorrect or incomplete information (such as address information).
- Not using UK contact details (including IP addresses), when the business claims to be in the UK.
- Signing up outside business hours (to try and circumvent checks).

- Key information (e.g. name, address etc) matching a disabled or dormant account already on your system.
- Use of generic, non-business email addresses or using the same email for multiple accounts.
- Payment information being changed frequently.
- Use of a virtual private network (VPN).
- Adverse information from a public database or media website.

Continued compliance

You must have a documented process for both onboarding and the ongoing monitoring of your customers. This process must include provision for reassessing risk, particularly after complaints of misuse or changes within a customer's organisation.

You should also consider if contractual controls are appropriate, to require your customers to act appropriately and to pass on any obligations to their customers, if they are not the end user.

It is important to keep a record of all the checks you carry out and ideally have one senior person responsible for compliance, however, anyone in your team who is involved in service provision should be trained in the process of compliance and best practice and know how to deal with complaints.

Incidents of misuse

Once again it is important to have documented how you will respond to non-compliance and what will trigger it.

Your response must be proactive and prompt to reduce the risk of consumer harm. The responsibility is on you to decide an appropriate and proportionate course of action and to keep records of your decisions and actions should you be challenged.

Once you have identified a concern you must take steps to prevent further potential misuse as far as reasonably possible, for example this may be blocking a customers access to your service or reporting them to a fraud agency.

It is your responsibility to support affected consumers where appropriate and co-operate with the regulators or other organisations that may investigate the matter.

If an incident includes number ranges held by Magrathea, or calls that have transited Magrathea's network, please do notify us. We often receive complaints directly and we can manage those more effectively if we have the full information available to us.

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0023/256343/unofficial-consolidated-general-conditions-May-2023.pdf
[2] https://www.ofcom.org.uk/__data/assets/pdf_file/0022/247504/annex2-good-practice-guide.pdf
[3] https://www.ofcom.org.uk/about-ofcom/bulletins/enforcement-bulletin/open-cases/enforcement-programme-phone-and-text-scams