Sharing data to tackle fraud: Guidance for telecoms providers

Created by: Comms Council UK (CCUK), the Home Office, Ofcom, and with input from the Information Commissioner's Office (ICO).

About this guidance

This guidance has been produced by the Comms Council UK, the Home Office, Ofcom and with input from the Information Commissioner's Office (ICO). It is aimed at telecommunications providers of all sizes operating in the United Kingdom and is designed to give organisations confidence in sharing data for fraud prevention purposes, explaining what is lawful, what frameworks exist to support it, and how to get started. It reflects the shared commitments set out in the government's Fraud Strategy 2026–2029 and the Telecommunications Fraud Charter (November 2025), both of which recognise multi-sector data sharing as central to detecting and disrupting fraud at scale.

Fraud causes serious harm to individuals, businesses and the wider economy. Telecoms providers are at the centre of the challenge, and tackling it effectively requires collaboration – including sharing relevant data with industry partners, law enforcement and fraud prevention organisations. The legal framework, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and the Data Use and Access Act 2025 (DUAA) provide a strong foundation for organisations to refer to, so that data can be shared confidently.

As part of the work undertaken for this guidance, we collected real-world examples of data sharing from across the sector. Appendices 4 and 5 set out real examples and case studies — including the initiatives involved and their impact — demonstrating what effective cross-sector collaboration makes possible in practice.

Key Principles

This guidance is built on three principles:

1. Sharing data appropriately helps disrupt fraud faster, reduce losses, protects customers, and helps to prevent bad actors move undetected between providers;
2. Good practice and network management builds trust with industry partners, carriers and law enforcement – and the market credibility that comes with that; and,
3. Improved regulatory confidence, and a demonstrable record of responsible governance that reduces the likelihood of increased regulatory scrutiny.

Remember:

- Fraud prevention is usually a lawful reason to share information.
- Share the minimum necessary.
- Keep a brief record of your decision.
- Use established schemes wherever possible.
- If unsure, seek advice – but don't assume data protection law prevents sharing.

Not sure whether or how to share? See the Data-sharing decision flow chart on page 10 of this document.

The risks of not sharing information and of sharing badly

Providers who fail to engage in appropriate fraud prevention collaboration may expose themselves to significant operational, commercial and regulatory risk:

- Providers with limited monitoring, poor engagement with industry partners or a reluctance to share relevant information may become attractive targets for misuse, scam traffic, spoofing activity or account compromise.
- Once a provider develops a reputation as an easy route for fraudulent traffic, it can spread quickly across the industry, damaging relationships with suppliers, carriers and interconnect partners.
- Upstream providers increasingly expect customers to investigate abuse reports, respond to traceback requests and cooperate on fraud prevention activity. Providers that repeatedly fail to engage may face increased commercial scrutiny, additional contractual restrictions, service suspension or even termination of supply arrangements.
- Failure to take appropriate steps to ensure numbers are not misused[1] could result in or contribute to breaches of telecoms rules[2]. Enforcement action could lead to a significant fine, the suspension of the provider's network/service and other remedies. In some instances, misuse of networks and services may also lead to criminal prosecutions.

Government is under pressure to expand financial liability beyond the finance sector into tech and telcos. Appropriate and lawful information sharing is increasingly becoming part of demonstrating responsible network management and regulatory compliance before further interventions may need to be imposed onto the sector.

Poor or unlawful sharing carries its own serious consequences: Providers that share data carelessly, disproportionately, or without appropriate safeguards risk privacy breaches, misidentification, customer detriment, legal challenge, reputational harm, and regulator attention. This is why the proportionality test (see the "What data can be shared" section on page 2 of this document) and the practical checklist: before you share data (see the "How to navigate the ecosystem: practical steps" section on page 5) are central to this guidance.

What data can be shared

The proportionality test

- What harm am I trying to prevent, and how serious is it?
- Is sharing this information likely to contribute meaningfully to preventing that harm?
- Am I sharing the minimum amount of data necessary for the purpose?

[1] Including by failing to carry out appropriate Know Your Customer checks, monitor for misuse, investigate and address concerns or cooperate with other organisations

[2] Including numbering rules under Ofcom's General Conditions, rules under sections 127 and 128 of the Communications Act 2003 and rules relating to the security of networks and services from section 105A the Communications Act 2003

- Are there appropriate safeguards in place – such as anonymisation, restricted access, or a data sharing agreement?
- Have I kept a record of my decision and reasoning?

Accuracy is central to sharing responsibly. Sharing inaccurate or poorly-defined information can cause real harm to the people it concerns and undermine trust in the wider system, so providers should be confident the data is accurate, up to date, and clearly distinguishes fact from suspicion before sharing. Getting this right depends on well-defined internal responsibility and governance: clarity over who is accountable for sharing decisions, how they are recorded, and how errors are corrected. The ICO's Data Sharing Code of Practice and its guidance on sharing personal information to prevent, detect and investigate scams and frauds set out how to put these frameworks in place. Please see Appendix 2 for more detail.

The Data-sharing decision flow chart in the "How to navigate the ecosystem: practical steps" on page 10 of this document walks you through these questions step by step.

Types of data that are currently shared within existing schemes and mechanisms:

- Telephone numbers associated with fraudulent activity.
- Call records associated with a number known to be used for fraud to identify potential victims.
- Domains used by threat actors for fraud, phishing, and malware.
- Keywords and phrases fraudsters use in malicious SMS.
- Personal data for actionable intelligence.
- Calling Line Identification (CLIs) and traffic associated with mass marketing fraud.

Personal data (indicative examples):

- "Personal data" means any information relating to an identified or identifiable natural person (the "data subject"); an identifiable natural person is one who can be identified, directly or indirectly.
- In the fraud prevention context, this includes information such as: names, dates of birth, addresses, telephone numbers, email addresses, IP addresses, online handles (usernames), financial account details and transactions, facial images and call content (recordings/transcripts).
- Such data can be shared for fraud prevention purposes where it is necessary and proportionate.

Anonymisation, pseudonymisation and Privacy Enhancing Technologies (PETs):

- Where there is uncertainty about sharing personal data, reducing its identifiability can provide a practical route forward — but it is important to be precise about what this achieves.
- Genuinely anonymised data (from which individuals can no longer be identified by anyone), falls outside data protection law and can be shared with fewer constraints.
- Much of fraud-related data, however, is only pseudonymised: a list of telephone numbers, for example, is likely pseudonymised where the provider holds (or is seeking) information linking those numbers to individuals. Pseudonymised data remains personal data and

must be treated as such. This does not prevent sharing, but providers should not assume that anonymisation applies where it does not, as this can give a false sense of security.

- Aggregation is not the same as anonymisation either: aggregated intelligence (such as broad call patterns) may still allow individuals to be identified, and should be assessed on that basis. Privacy Enhancing Technologies (PETs) can help reduce identifiability and support safer sharing where full anonymisation is not possible. Organisations should consider whether the purpose can be achieved with less identifiable data before concluding that sharing fully-identifiable personal data is necessary.

How to navigate the ecosystem: practical steps

A guide for UK Telecoms Providers: UK telecoms providers are expected to be proactive rather than purely reactive. A smaller provider is unlikely to operate the same anti-fraud mitigations as, for example, a major mobile operator, but it should still demonstrate reasonable and effective oversight and risk management. In practice, this means:

- **Monitoring for suspicious activity (Know Your Traffic):** maintaining reasonable visibility of network and customer activity such as:
    - unusual traffic spikes or patterns;
    - high-risk destinations or routes;
    - invalid or suspicious CLI usage;
    - customer complaints or abuse reports;
    - compromised accounts or unusual spend; and
    - maintaining abuse/security reporting processes. Controls may be manual or automated depending on provider size and capability.
- **Carrying out reasonable due diligence on customers and understanding their activity (Know Your Customers)** such as:
    - verifying customer identity;
    - understanding intended service use;
    - reviewing unusually high-risk requests;
    - monitoring newly onboarded customers more closely; and
    - maintaining accurate contact details, and, for business customers, checking company details against Companies House as part of identity verification.

If you have seen evidence of failed KYC checks from a specific entity, please consider contacting one of the relevant stakeholders in the key organisations list on pages 8 and 9 of this document.

- **Acting promptly when issues are identified:**
    - suspending or restricting compromised services,
    - blocking suspicious traffic or routes,
    - removing invalid CLI presentation,
    - notifying affected customers,
    - escalating internally through appropriate channels,
    - preserving logs and evidence, and cooperating with upstream or downstream providers such as wholesale carriers or ISPs.

Contact the appropriate organisation — see contact information in the key organisations list on pages 8 and 9 of this document. Providers should maintain a simple, documented escalation process.

- **Maintaining records:** of incidents, investigations and actions taken. This helps demonstrate compliance and supports learning and improvement.

Detailed guidance on due diligence and handling misuse can be found here. Further guidance on scam mobile messaging can be found in Ofcom's guidance[3] (see paras. 2.87–2.95).

You do not need to start from scratch: Getting involved in a data sharing arrangement that already exists is often faster, lower-cost, and lower-risk. Smaller providers can connect directly with established organisations such as CIFAS and NTS), who are actively looking for telecoms providers to engage with them. For real-world examples of successful cross-sector data sharing see Appendices 4 and 5. These organisations have the frameworks, and your data may be more valuable than you think. Smaller providers are sometimes the entry point of choice for fraudsters precisely because they are less well-monitored, which means the intelligence you hold can be highly relevant to the wider picture. Reporting into CIFAS or NTS as a smaller provider also means you benefit from intelligence flowing back to you.

When to consider data sharing:

- You have reason to suspect a customer is perpetrating fraud or facilitating others to do so.
- A customer has been rejected following know-your-customer (KYC) checks for reasons related to suspected criminal activity.
- You have received a report or complaint about potential misuse of numbers or services that suggests criminal activity.
- You have identified patterns of behaviour, such as unusual call volumes, CLI spoofing, or account characteristics, consistent with fraud.
- You have been asked to share data by a law enforcement body, a Specified Anti-Fraud Organisation (SAFO) – see Appendix 2 –, or another organisation operating under an established data-sharing framework.

Practical checklist: before you share data

1. Identify your Lawful Basis (see Appendix 2 if unsure).
2. Check whether the purpose can be achieved with less identifiable data (bearing in mind that data such as a list of telephone numbers is usually pseudonymised, not anonymised) – if so, use it.
3. Share only the minimum data necessary to achieve the desired outcome.
4. Send to the intended recipient only, avoiding cc/bcc addresses.
5. Keep a brief note: what you shared, with whom, why, and the expected outcome.
6. Be aware of the additional factors if sharing special category or criminal record data.
7. If the concern later proves unfounded, record that too and report it into the relevant scheme so the record is updated

[3] Note: the relevant measures do not come into force until January 2027

Use this checklist alongside the Data-sharing decision flow chart on page 10 of this document. See also paragraphs 2.26-2.29 of Ofcom's guidance on scam mobile messaging for further guidance.

Map: The Functional Data Flow

Note: The map categorises organisations into three distinct layers based on their role in the fraud prevention chain, allowing providers to see where they fit in and where responsibilities lie. Contact details can be found at the end of this document.

STRATEGY / POLICY Stakeholders responsible for providing the legal frameworks required for lawful sharing.	Home Office
	Ofcom
	National Crime Agency (NCA)
	Information Commissioner's Office (ICO)
	National Economic Crime Centre (NECC)
	National Cyber Security Centre (NCSC)
	Stop Scams UK
DATA SHARE Where data is analysed and shared across sectors. Entities facilitate the exchange of confirmed fraud risks to protect the wider ecosystem.	Cifas
	Telecommunications UK Fraud Forum (TUFF)
	Stop Scams UK
	Information Commissioner's Office (ICO)
	Ofcom
	Cyber Defence Alliance (CDA)
	Global Signal Exchange (GSE)
	National Cyber Security Centre (NCSC)
DATA FEED The operational entry point for data/intelligence.	Communications Crime Strategy Group (CCSG)
	UK Finance
	Report Fraud, City of London Police
	National Trading Standards (NTS)
	TechUK
	Comms Council UK (CCUK)
	NICC Standards Limited
	Global Signal Exchange (GSE)
	National Cyber Security Centre (NCSC)
	Ofcom

How to navigate common barriers

Note: This section addresses the most common blockers raised during the development of this guidance. Some concerns, including those relating to competition law and rights of defence, fall outside the scope of data protection law and are not fully resolved by this guidance alone. Providers with specific concerns in these areas should seek legal advice.

I'm unsure if I can respond to a request from Law Enforcement or a SAFO: Most people and organisations want to cooperate by responding to a law enforcement request on suspected fraudulent activity (to inform other communication providers and further investigations).

➔ So long as the request is made under recognised legislation (see Appendix 2) you should normally respond in full. Be careful to only provide the data requested. If you have additional data you would like to share, contact the requesting officer and advise them to make an additional request.

I want to report fraudulent activity I've spotted: You are encouraged to share information in order to inform wider communication providers, law enforcement and relevant SAFOs in order to prevent or detect crime.

➔ It is important that you share data safely and with organisations that will process it correctly. Refer to the practical checklist: before you share data on page 5 in this document or contact a recognised scheme (see Map on page 6) for support or follow the "proactively report activity" route in the Data-sharing decision flow chart on page 10.

I have been a victim of fraud and don't know what to do: If you have been a victim of telephony fraud you should seek support, this is a serious crime.

➔ You should report all cases of fraud to Report Fraud. You should also notify your supply chain if applicable as they may have additional resources to support you. See the key organisations list on page 9 for the full list of organisations and contact information providers can contact when responding to suspected fraud or misuse.

My data protection officer (DPO) or legal team is blocking requests: Requests from the ICO and Law Enforcement are usually permissible, guidance from the ICO makes this clear (see Appendix 3) and this document works to give confidence in the decision to respond to formal requests.

➔ Share this guidance or relevant ICO guidance (see Appendix 3) with your legal team, DPO or equivalent

I've received an informal request from National Trading Standards (NTS) or similar organisation: Where a body such as NTS is investigating potentially unlawful calls on your network (for example through its own call-record data) you may be asked to share data to assist their investigation.

➔ You can normally share the information on a voluntary basis without a formal legal request[4]. You should share only what is necessary and proportionate, keep a brief record of what you shared and

[4] As outlined in Appendix 2, under the DUAA 2025, preventing crime (including fraud) is a "recognised legitimate interest." This means you have a lawful basis to share for that purpose without carrying out a separate legitimate interests assessment.

why, and satisfy that the request is genuine — but data protection law should not be treated as a reason to refuse.

I'm having difficulty establishing data sharing agreements with telecoms providers: If you wish to proactively share data with another organisation on a regular basis, it can be sensible to establish an agreement between you. However, for infrequent exchanges there may be a simpler way.

➔ Join an existing scheme to avoid starting from scratch. The "How to navigate the ecosystem: practical steps" section in this guide sets out how to get involved.

I find a lack of consistent mechanism and limited visibility of existing schemes: Methods for sharing fraud intelligence between providers and with law enforcement vary, including the terminology used, particularly across sectors.

➔ Multiple mechanisms now exist. Refer to Map on page 6 to see what role an organisation plays in the fraud prevention chain. Contact a provider to establish common terms.

I have competition concerns: Sharing intelligence between providers could potentially constitute a collective boycott under competition law, for example where shared information leads to providers refusing to interconnect or do business with a specific operator.

➔ The key distinction is between sharing intelligence for fraud prevention purposes and using shared intelligence as the basis for collective commercial decisions.

➔ Competition law concerns should not be used as a default reason to avoid sharing altogether.

I have pre-judgement concerns: Data sharing is most effective when done quickly, meaning there is a risk, if handled poorly, that a provider or individual could be labelled as culpable before a full investigation has been completed. The law generally allows for 'rights of defence' to allow organisations and individuals to review evidence and challenge information.

➔ It is important to distinguish clearly between observed facts, indicators and conclusions — for example, by stating that traffic patterns have been observed which are consistent with known scam campaigns, and being clear where information is unverified.

➔ Information shared before an investigation is complete may later turn out to have an innocent explanation, by which point a data subject may already have been wrongly identified to multiple other providers. Responsible and appropriate data sharing therefore includes dealing with the consequences of good-faith but wrongful sharing: if a concern later proves unfounded, this should be recorded and reported back into the relevant scheme so the record is corrected (see point 7 of the Practical checklist: before you share data on page 5). Sharing on a "fire and forget" basis, with no mechanism to correct the record, is likely to breach the first data protection principle.

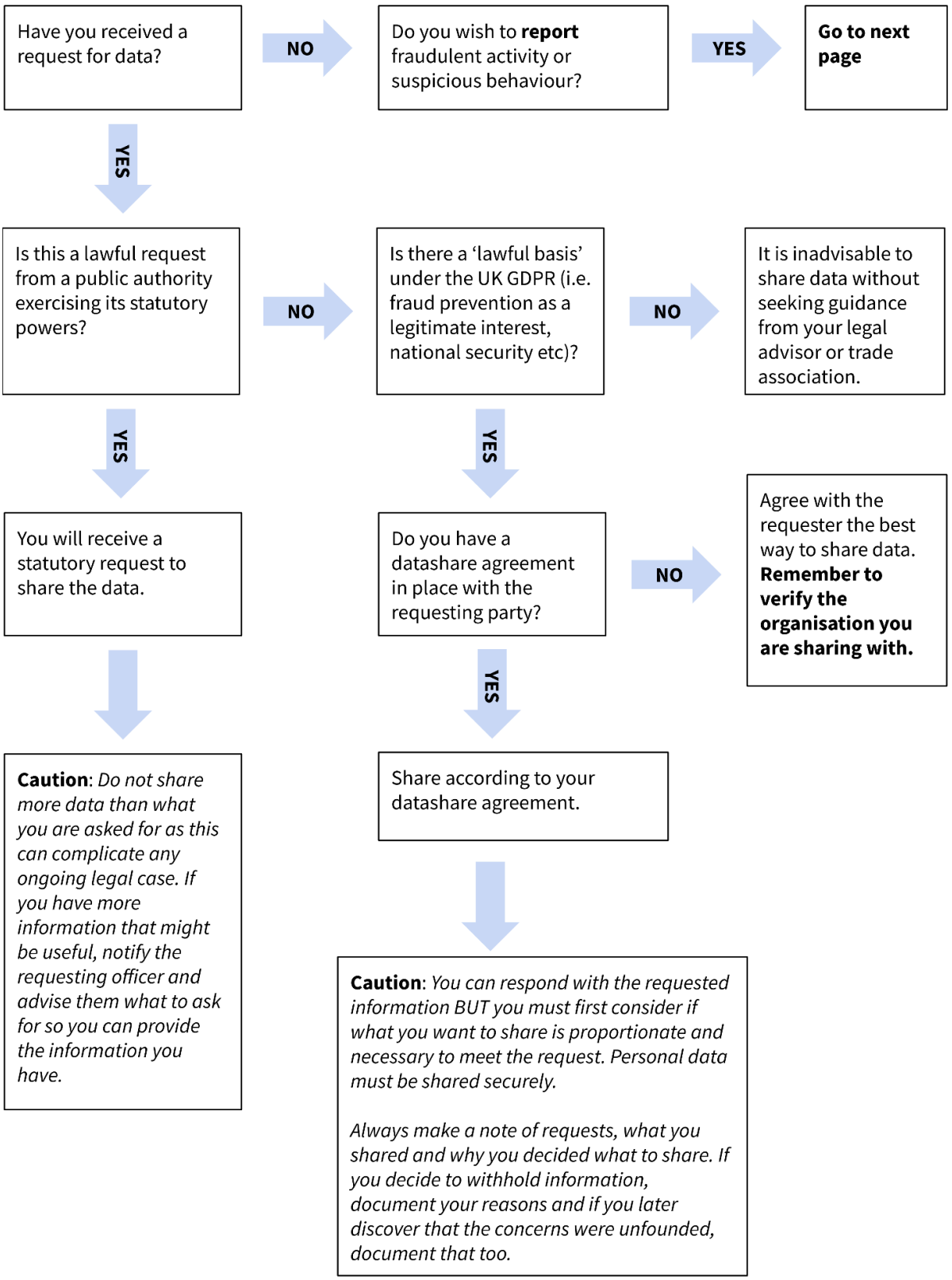
For more information on why data sharing is permitted, which regulation and legislation is relevant and where to find additional guidance please visit the Appendices that accompany this document. If you would like more support and guidance, you can try one of the organisations below or speak to the Information Commissioner's Office (ICO).

Key organisations:

This lists key organisations that telecoms providers can contact when responding to suspected fraud or misuse.

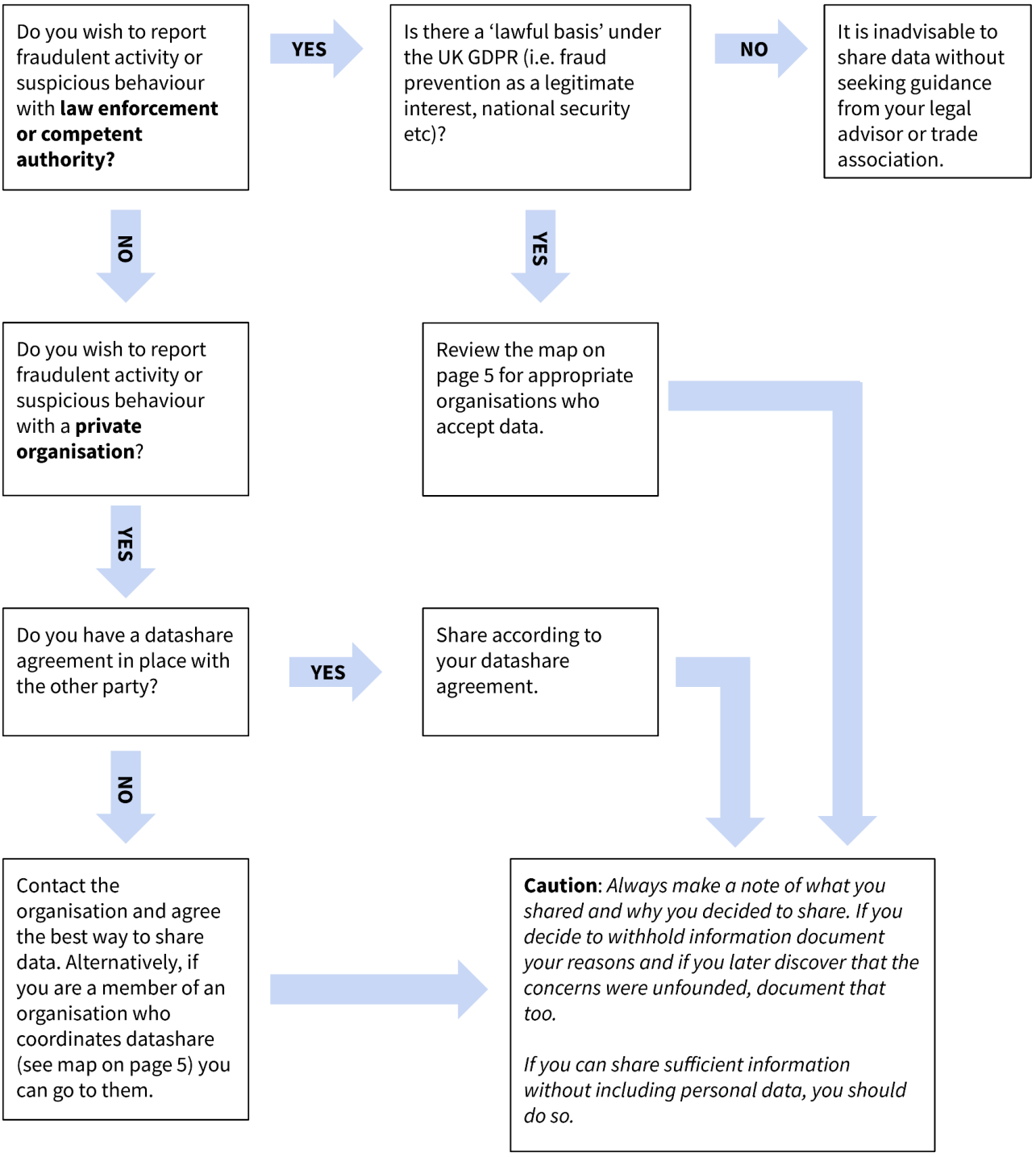
ORGANISATION	CONTACT DETAILS
CIFAS (members only)	Get help and advice on Scams here.
TUFF (members only)	Contact the organisation here.
Stop Scams (members only)	Call 159. More details here.
National Trading Standards	To report – contact Report Fraud on 0300 123 2040. For advice – contact Citizens Advice Consumer Service on 0808 223 1133 or 0808 223. More details here.
Report Fraud	To make a report click here. To get help and support click here.
National Crime Agency	Contact the organisation here.
Ofcom	For scam/nuisance texts and calls: forward suspicious texts to 7726 (free), then report to the ICO (see below) Report persistent silent or abandoned calls to Ofcom: online here or call 0300 123 3333.
Information Commissioner's Office (ICO)	Report via the ICO website here or or call 0303 123 1113.
Cyber Defence Alliance (CDA) (members only)	Contact the organisation here.
Global Signal Exchange (GSE) (members only)	Contact the organisation here.
Mobile UK (members only)	Contact the organisation here.

Data-sharing decision flow chart



Ask yourself… *Can you minimise the amount of personal data you share? For example, partial phone numbers and post codes and anonymised data patterns.*

If you wish to proactively report activity start here…



Ask yourself… *Can you minimise the amount of personal data you share? For example, partial phone numbers and post codes and anonymised data patterns.*