Frequently Asked Questions

Your cyber security and data compliance questions, answered.

naq.

As a limited company contractor, am I liable for a cyber attack?

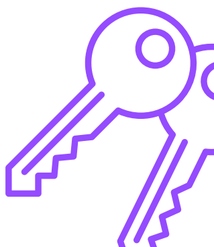
Yes. Any type of legal liability lies with the entity which is responsible for carrying out work, processing data, etc. Contractors usually have professional indemnity insurance or business liability insurance because they know that if they give the wrong advice or if they break something that belongs to their client, they can be held liable.

This is not different in the cyber security context. You are the entity responsible for your client's information and if you cause any of their data or systems to be compromised you are the one responsible for it.

As an umbrella contractor, am I not protected by the umbrella company?

The Umbrella organisation must be secure and compliant. Your relationship with the umbrella organisation is important. If you're a director of the umbrella organisation, then something called directors liability applies.

This means that you can be held liable for the actions and omissions of the company, usually if they're a result of mismanagement. But as an employee, you also have a responsibility to ensure you protect the umbrella organisation and yourself.



What are the top 5 quick wins for being cyber safe?

- Train your team! The vast majority of cyber attacks are due to user mistakes.
- Make sure everybody has read and signed policies on what they should and shouldn't do
- Practice what you would do if a cyber incident took place
- Ensure you keep accurate, up to date records of all the accounts you use and all the IT you use and if it is owned by the company or owned by the employee.
- Backup all the data you cannot afford to lose to something other than your computer or server

How do I back up client data? Surely I can't do this as the responsibility should be with the end client?

Are you allowed to store your client's information on your own infrastructure? If the information is on their own infrastructure, they have the obligation to back up their information. In this case, you can't do that. But, **your clients' information is not the only type of information you have!** For all your other types of information, the handling and backing up thereof remains your responsibility.

What is GDPR?

The General Data and Protection Regulation was originally developed by the European Commission, and subsumed into British law after Brexit. It introduces strict controls on the privacy of personal information. **The UK GDPR has strict requirements on how you should handle personal data**, which types you are allowed to process and the security controls you must have in place to protect this data. It also mandates what you must do in the case of a data breach.

The UK GDPR will soon be changing after the recently announced Data Reform Bill which may remove some of the paperwork required but may make it much more difficult to work with companies outside of the UK. Companies that do not abide by the GDPR can face fines of up to 4% of global turnover.

As a limited company I have been contacted by letter by ICO, what is my responsibility for this communication?

If you run a Ltd company, **you must register with the ICO** and pay the registration fee. It is almost impossible that a company does not process any personal data so we recommend that you pay the registration fee right away. You can find more information here: https://ico.org.uk/for-organisations/data-protection-fee/

Our top 5 recommended software options

Of course, number 1 is Naq but we recommend the following software and processes as a good starting point:

- **Turn on full disk encryption on your computers.** It is free on all macOS versions and Windows 11 - this will mean that if your laptop is lost or stolen, the thief will not be able to access any of your data.

- **Offsite backup** - It is critically important you back up all the data you cannot afford to lose to a completely separate environment from your computers. The easiest way to do this is to backup all your data to your cloud drive environment (such as Google Drive or Sharepoint) and secure this with 2FA and a strong password. You can also use a third-party tool such as CloudAlly (a partner of Naq) to backup your drive data to their third-party data centres.

- **2FA app** - Two-factor authentication is super important as it guarantees that it is really you who is trying to log in. The best thing is, it is free! Most web applications now support 2FA wither via an authenticator app such as Google Authenticator or SMS text message.

Our top 5 recommended software options

- **Anti-virus** - All Naq customers are provided with next-generation endpoint protection but a good place to start is Windows Defence on Windows (which is completely free) or a product such as F-Secure for MacOS computers

- **Password Manager** - It is vital that all of your passwords are unique and strong but of course this quickly turns into a nightmare memory game. The best way to do this is to use a password manager such as NordPass. By using a trusted password manager, you can generate super strong and unique passwords without having to memorise them. All you need to do is remembr your master password and turn on 2FA.

Have any other questions?

Send us a message on info@naqcyber and a member of our team will be in touch!