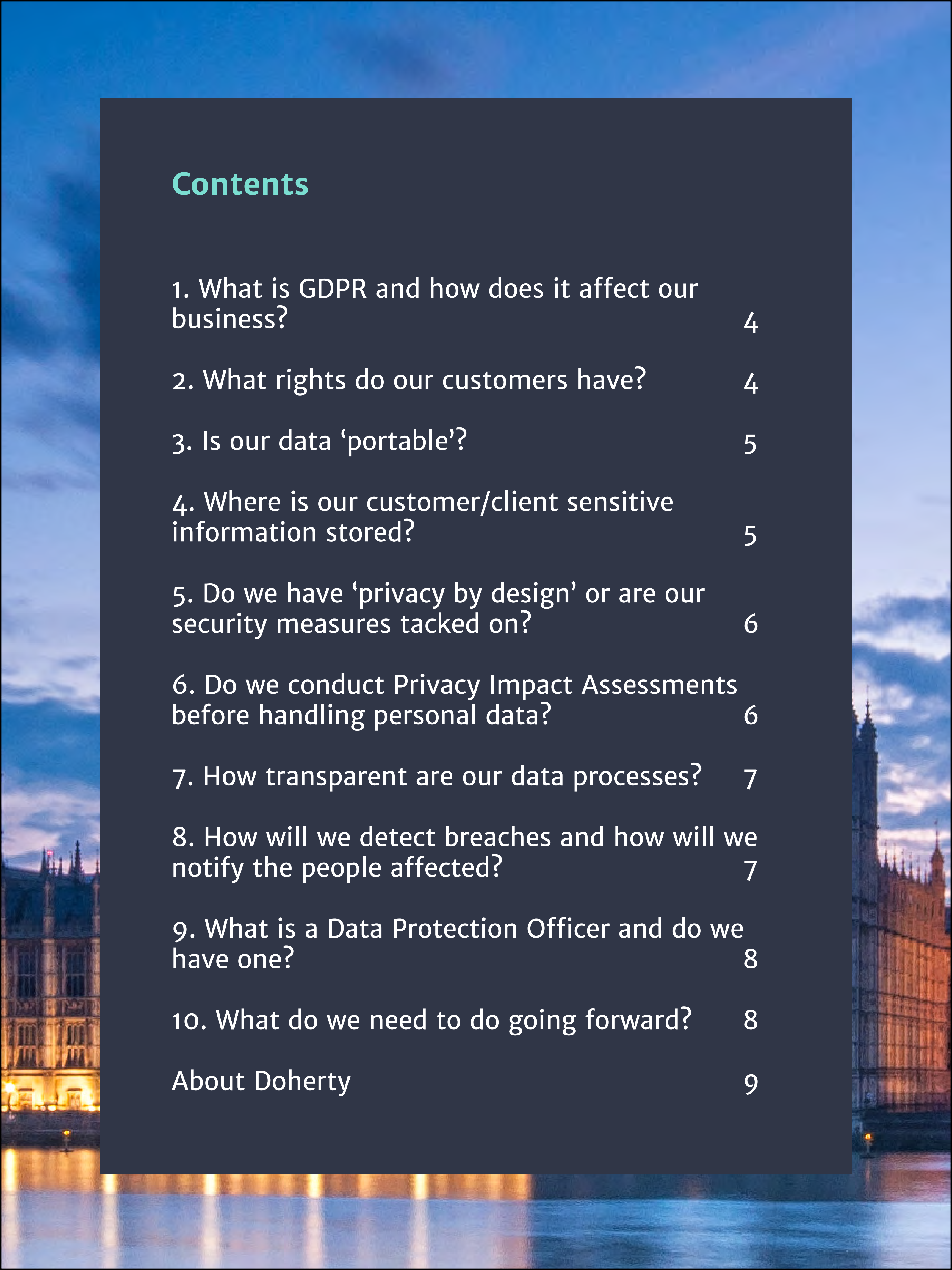
10 questions to ask your IT provider about GDPR today

dohertyassociates

If you own a business within the UK, the chances are you've heard of the new General Data Protection Regulation (GDPR). However, despite it being the biggest business buzzword of the last year, many businesses are still unaware about what GDPR is and how it will affect them.

In fact, 46 percent of UK businesses state GDPR is still **not a priority** at their organisations, according to a recent survey. Even more worryingly, only five percent of businesses are properly prepared for when the policy takes effect in May 2018. This law could have a dramatic impact on how you handle data and, as a result, it should not be ignored.

To ensure you don't end up paying hefty fines and breaking the law, it's vital you discuss GDPR with your IT provider. So, grab a pen and paper, note down the following questions and start booking up a call with your IT provider as soon as possible.



Contents

1. What is GDPR and how does it affect our business?

Did you know that almost a third of UK businesses still don’t understand how GDPR will affect their business? With the deadline looming, your company cannot afford to be unprepared.

So, first and foremost, it’s important to ask your IT provider about GDPR and how it’ll affect your business specifically. Be sure to ask any questions you have about the new law, what areas of your company will be affected by the regulation and how you can prevent your business from paying penalties in the event of a data breach.

2. What rights do our customers have?

GDPR enforcement is for the sake of your staff and customers’ privacy. As a result, they’ll be given a bigger voice and more rights.
Instead of privately processing and managing your customers’ data, you’ll be expected to provide:

- **Consent.** Are your terms and conditions fair and easy to understand? Under the new law, it’ll be illegal to present your customers with illegible and leading documents. It should be as easy to say ‘no’ to your policies as it is ‘yes’. Consent is everything.

- **Right to access.** Your data subjects will have the right to access their personal data free of charge and make any alterations they feel is necessary. If asked for their data, your business is responsible for providing a document of their information in electronic format.
- **Right to be forgotten.** In short, the 'Data Erasure' act allows your customers to request for their data to be deleted. This includes ceasing further processing of their information by both your business and other relevant third parties.

Make a note of what rights your customers and clients already have. If they don't have consent, the right to access and the right to be forgotten, consult your IT provider and discuss the actions you should be taking.

3. Is our data 'portable'?

As of May 2018, when asked to provide a physical copy of a data subject's information, you are legally required to send the appropriate documents in electronic format. But, before you can share data with your subjects, it's important to ensure you have the capability to do so first.

Therefore, be sure to ask your IT provider how portable your data is. Are you currently able to format and send sensitive data? Have you ever sent data to your clients or customers before?

4. Where is our customer/client sensitive information stored?

Ensuring your customers' data is stored securely is **essential** for both their safety and yours. As a result, it's important to ask your IT vendor the following questions:

- Is our customer data stored on-premise or in the cloud?
- Who has access to this sensitive data? Do we have appropriate admin controls?
- What are our current data policies?
- Do we have suitable access controls, security tools and training in place?
- Do we have a disaster recovery plan?

Your systems and security measures should be water tight. Discuss every crack and crevice with your IT provider to ensure that you're not missing any gaps.

5. Do we have 'privacy by design' or are our security measures tacked on?

Security measures should never be implemented as an afterthought. GDPR states that businesses should implement 'privacy by design' in an effort to ensure organisations create systems with data protection in mind **before** adding extra security.

Implementing this policy can help your business to:

- **Stay informed** of your data processes and policies
- **Identify problems** early on and act quickly
- **Stay compliant** and avoid legal repercussions

ICO suggest creating new systems specifically for storing and accessing personal data to help stay compliant, but be sure to ask your IT partner for their recommendations.

6. Do we conduct Privacy Impact Assessments before handling personal data?

A Privacy Impact Assessment (PIA) is an audit that determines how your business's sensitive data is collected, maintained, protected and shared. Under the new data regulations, these assessments will become mandatory within the ‘privacy by design’ law. The overall aim is to ensure every business handling sensitive information assesses their privacy, security and best practices **before** they begin processing data.

Ask your IT provider whether they are conducting PIAs and the benefits of pre-assessment. You’ll find that these audits can help to reduce costs, build trust with your customers and keep your organisation compliant.

7. How transparent are our data processes?

A PIA can help your organisation’s data processes become more transparent and easier to understand, but that’s not where your efforts should stop. Your business can never be too prepared and ensuring complete transparency is a GDPR best practice.

According to Microsoft, your organisation should be:

- Providing notice of **data collection**
- Discussing information **processing purposes and use cases**
- Defining data **retention and deletion policies**

Before you take action, ensure you consult with your IT provider to see what actions, tools or processes they suggest deploying.

8. How will we detect breaches and how will we notify the people affected?

In compliance with GDPR, your business must notify your customers and data controllers of a breach as soon as you’re aware of the problem. What’s more, you must legally notify the authorities of a breach within 72 hours.

Although it’s up to you to notify your customers and the authorities of a data breach, it’s vital that you **ask your IT provider if you have the right technology** in place to detect threats immediately. At the end of the day, investing in threat detection and advanced analytics can help you stay compliant, reduce costs and act fast in the event of a compromise. If your IT provider hasn’t got the right defence tactics in place, they will never be able to help you stay compliant.

9. What is a Data Protection Officer and do we have one?

Under the GDPR, it is not mandatory for your business to employ a Data Protection Officer (DPO), unless you are:

- A public authority
- Carrying out large scale systematic monitoring of individuals
- Carrying out large scale processing of special categories of data.

These officers must have expert data protection knowledge and should ensure that your organisation's data processing is compliant with the law.

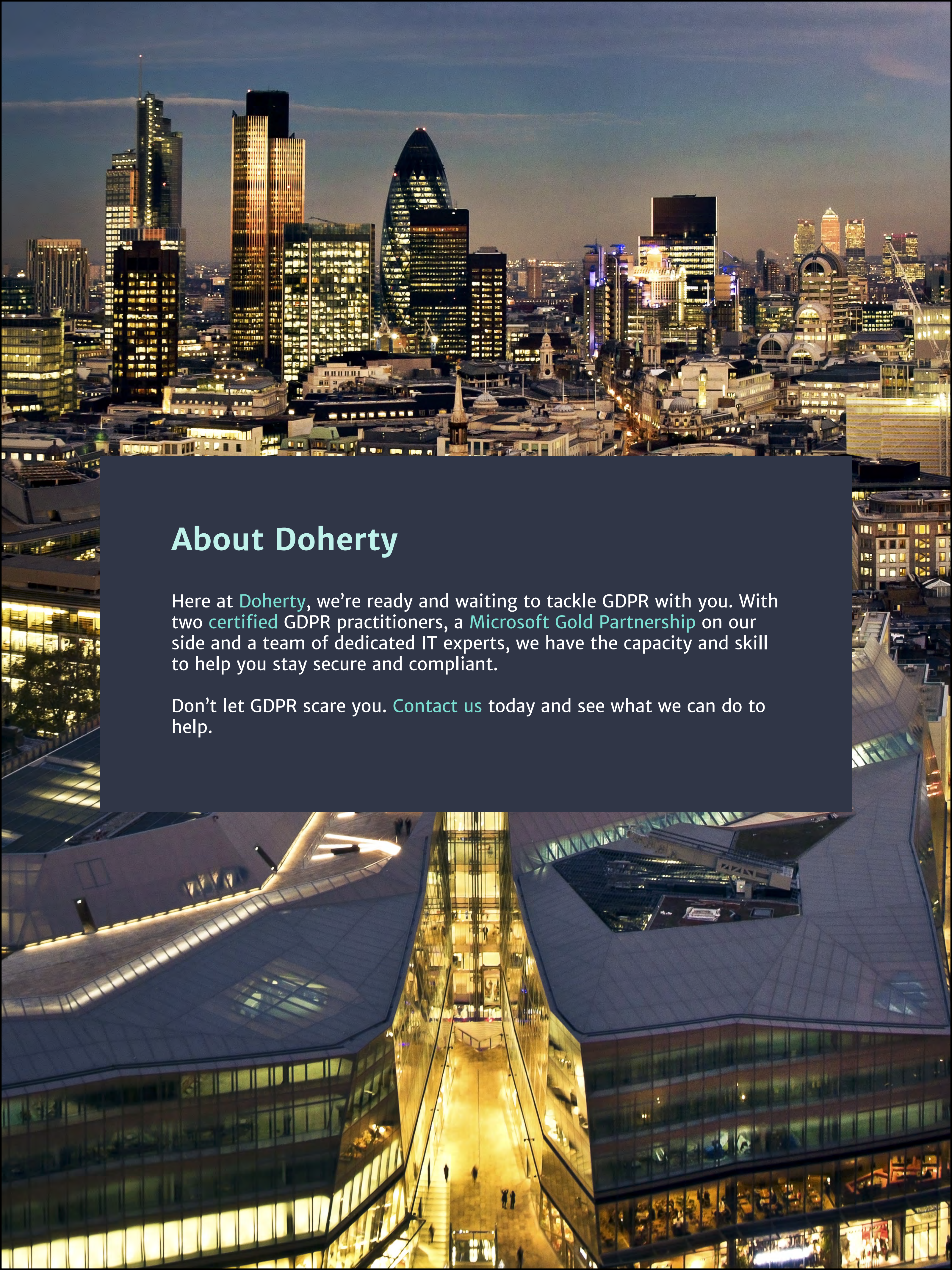
A DPO can either be a staff member or an experienced service provider. Any organisation can appoint a DPO if they wish, but regardless of whether it is mandatory or not, you must ensure your organisation has sufficient staff and skills to discharge your obligations under the GDPR.

10. What do we need to do going forward?

Becoming compliant with GDPR is not a one-time fix. Your organisation and your IT provider must look to the future, discuss plans and discover how you can make your data processes **better**.

As a starting point, try discussing the following questions:

- **Where have we fallen short on this checklist?** There shouldn't be any loopholes in your data processes. If you can't answer these questions satisfactorily, you'll need to discuss taking immediate action with your IT provider to remedy the situation.
- **How secure are our systems, servers and processes?** If your organisation hasn't completed an audit or assessment recently, now is the time. If you discover any immediate security issues, sit down with your IT partner, redefine your policies and talk through the tools and products you could be using.
- **Are we as educated as we could be?** When it comes to GDPR, the more you know the better. If your employees don't know the best practices for data sharing, collection or privacy, they may compromise your compliancy. Be sure to find out whether your IT provider offers training days or events around GDPR and compliance.



About Doherty

Here at Doherty, we're ready and waiting to tackle GDPR with you. With two certified GDPR practitioners, a Microsoft Gold Partnership on our side and a team of dedicated IT experts, we have the capacity and skill to help you stay secure and compliant.

Don't let GDPR scare you. Contact us today and see what we can do to help.