How To Protect Patient Data for Digital Health Technologies

A Primer on the GDPR:

GDPR.EU

DataGuard

“

It is not data that is being exploited,

It's people that are being exploited.

-Edward Snowden

This carousel is made using resources from:

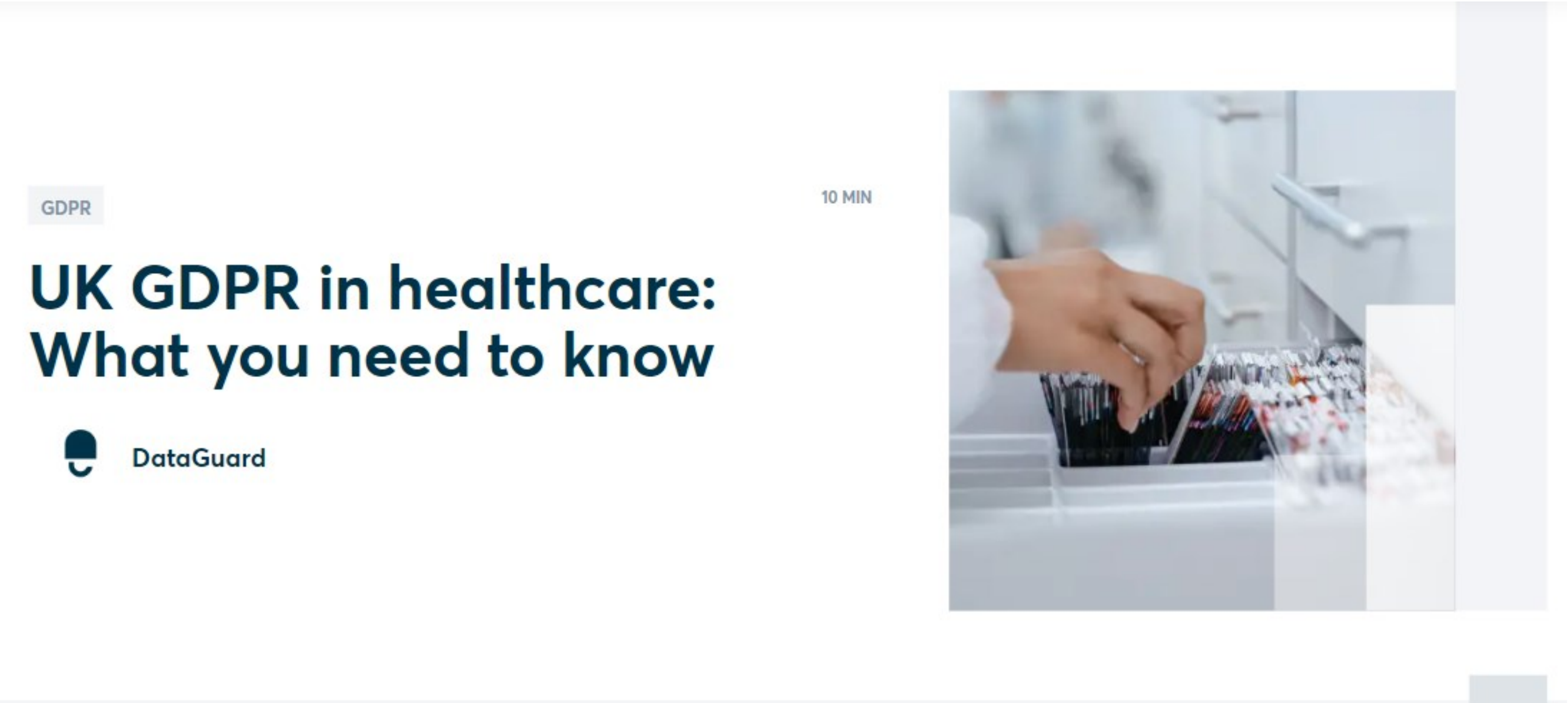
1. The official GDPR.EU Website

GDPR.EU
This project is co-funded by the Horizon 2020 Framework Programme of the European Union
Search...
Search
Home
Checklist
FAQ
GDPR
News & Updates

Complete guide to GDPR compliance

GDPR.eu is a resource for organizations and individuals researching the General Data Protection Regulation. Here you'll find a library of straightforward and up-to-date information to help organizations achieve GDPR compliance.

2. The DataGuard Website



UK GDPR in healthcare: What you need to know

DATA PRIVACY

One of the key tenets of medicine is patient confidentiality. In an increasingly advanced technological age, patient information is often stored in the form of electronic data.

In order to **build and maintain trust** amongst public members of society towards digital health technologies, every effort must be made to ensure that this trust is not violated.

In this carousel, we will explore the General Data Protection Regulation (GDPR) that exist to do just that.

SECTION 1:

WHAT IS THE GDPR?

GDPR

The **General Data Protection Regulation (GDPR)** is a European Union-wide law that affects every company collecting and storing EU citizens' data regardless of where they're located.

The General Data Protection Regulation (GDPR) is the **toughest privacy and security law in the world.**

Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they **target or collect data related to** people in the EU.

PENALTIES

The regulation was put into effect on May 25, 2018.

The GDPR will levy harsh fines against those who violate its privacy and security standards.

The **maximum penalty is** €20 million or 4% of global revenue, whichever is higher.

Data protection authorities can also issue sanctions, such as bans on data processing or public reprimands.

WHAT ABOUT THE UNITED KINGDOM?

The GDPR is **retained in domestic law as the UK GDPR**, it sits alongside an amended version of the DPA 2018.

The **key principles, rights and obligations** remain the same.

However, there are implications for the rules on transfers of personal data between the UK and the EEA.

IMPORTANT TERMS

The GDPR defines an array of legal terms at length. Below are some of the most important ones:

Personal data — Personal data is any information that relates to an individual who can be **directly or indirectly identified.**

Data processing — **Any action performed on data,** whether automated or manual.

Data subject — **The person whose data is processed**. These are your customers or site visitors.

Data controller — **The person who decides why and how** personal data will be processed. If you're an owner or employee in your organization who handles data, **this is you**.

Data processor — **A third party** that processes personal data on behalf of a data controller.

SECTION 2:

WHO HAS TO COMPLY WITH THE GDPR.

IN NO UNCERTAIN TERMS,

Any organization that processes the personal data of people in the EU/UK must comply with the GDPR.

"Processing" is a broad term that covers just about anything you can do with data: collection, storage, transmission, analysis, etc.

"Personal data" is any information that relates to a person, such as names, email addresses, IP addresses, eye color, political affiliation, and so on.

EXTRA-TERRITORIAL

The whole point of the GDPR is to protect data **belonging to EU citizens and residents**.

Even if an organization is not connected to the EU itself, if it **processes the personal data of people in the EU** (monitoring their behaviour or offering goods and services), it must comply.

The law, therefore, applies to organizations that handle such data whether they are EU-based organizations or not, known as "extra-territorial effect."

IN A NUTSHELL

If you are a HealthTech company that creates a product that **collects or processes data** of citizens within the EU/UK — You must comply with the GDPR .

Be it a wellness app used in the **community** or one used in a **clinical setting.**

It is very important to check your compliance BEFORE starting any data processing activities.

SECTION 3:

HOW TO COMPLY WITH THE GDPR.

OVERVIEW:

1. The first step is to conduct a GDPR assessment to determine what personal data they control, where it is located, and how it is secured.

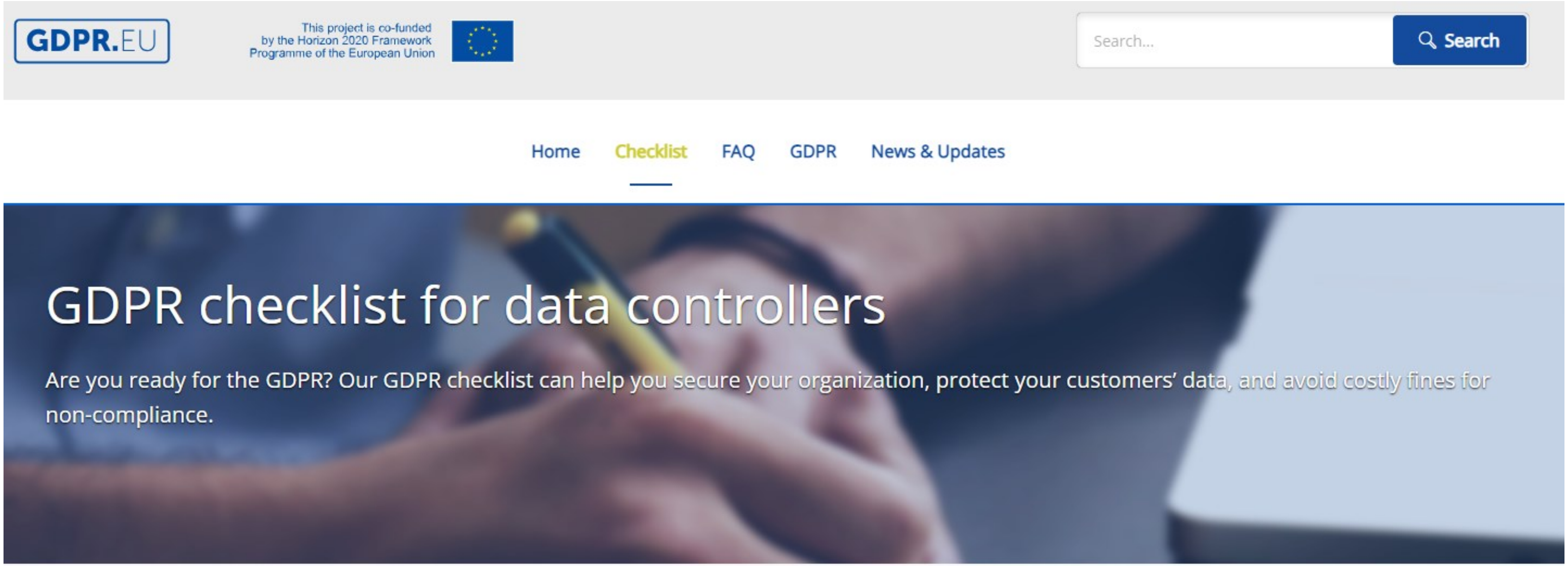
2. Organizations can comply with the GDPR by implementing technical and operational safeguards to protect personal data they control.

3. They must also adhere to the privacy principles outlined in the GDPR, such as obtaining consent and ensuring data portability.

4. You may also be required to appoint a Data Protection Officer and update your privacy notice, among other organizational measures.

GDPR CHECKLIST

Review the **GDPR checklist** to learn more about the steps to compliance.



GDPR.EU
This project is co-funded by the Horizon 2020 Framework Programme of the European Union
Search...
Search
Home
Checklist
FAQ
GDPR
News & Updates

GDPR checklist for data controllers

Are you ready for the GDPR? Our GDPR checklist can help you secure your organization, protect your customers' data, and avoid costly fines for non-compliance.

Available here at:

https://gdpr.eu/checklist/

TECHNICAL VS ORGANIZATIONAL

You're required to handle data securely by implementing "**appropriate technical and organizational measures**." For Example:

TECHNICAL

- Requiring your employees to use two-factor authentication on accounts where personal data are stored.
- Contracting with cloud providers that use end-to-end encryption.

ORGANIZATIONAL

- Staff trainings, adding a data privacy policy to your employee handbook.
- Limiting access to personal data to only those employees in your organization who need it.

DATA PROTECTION INFORMATION ASSESSSMENT

A **Data Protection Impact Assessment (DPIA)** is required under the GDPR any time you begin a new project that is likely to involve “a high risk” to other people's personal information.

Specific to Digital Health Technologies, a DPIA is recommended if:

“you're processing personal data related to “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, **data concerning health or data concerning a natural person's sex life or sexual orientation”**

WHAT IS IN A DPIA?

As outlined in Article 35, the GDPR requires DPIAs to contain the following elements:

- A systematic description of the envisaged **processing operations and the purposes of the processing**, including, where applicable, the legitimate interest pursued by the controller.

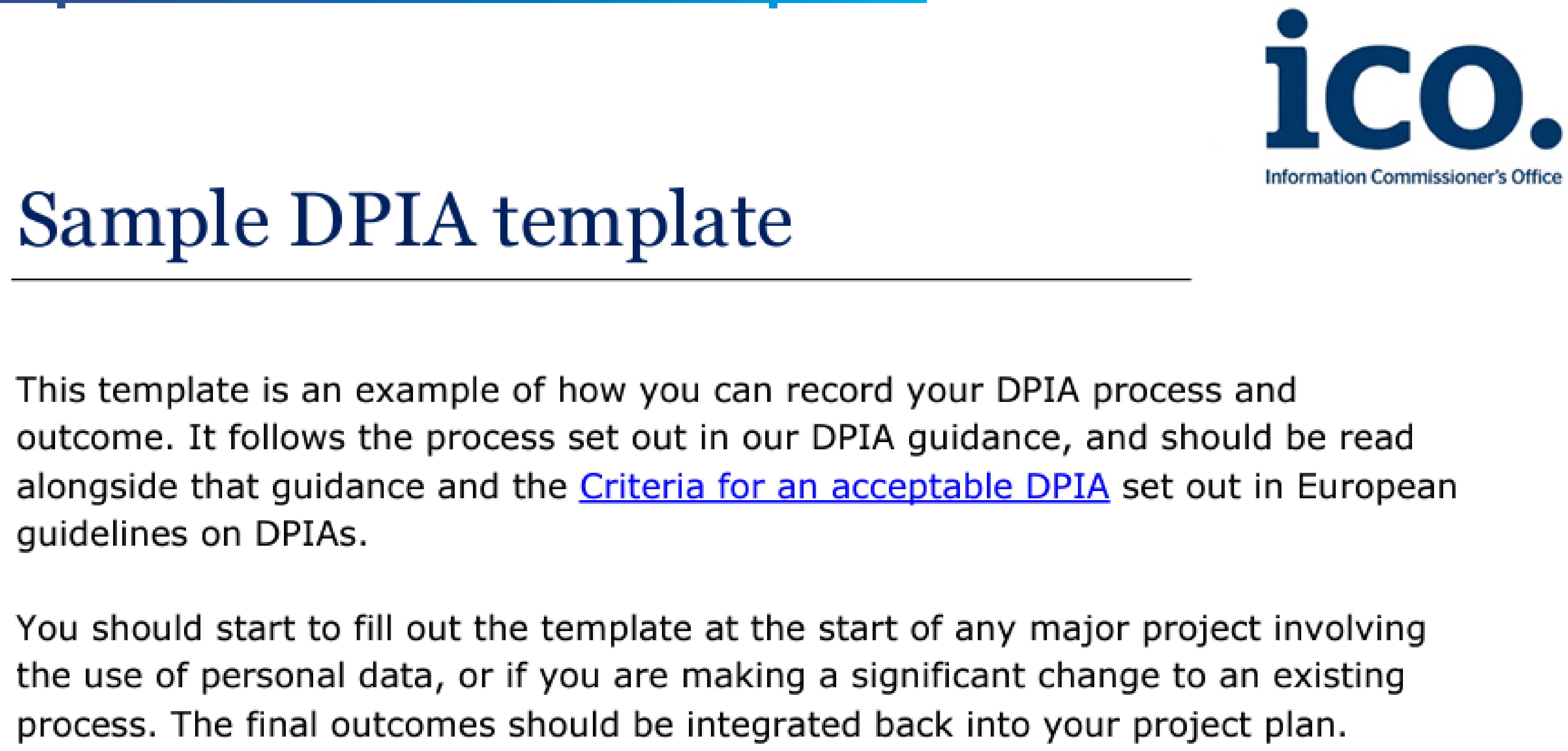
- An assessment of the **necessity and proportionality** of the processing operations in relation to the purposes.

- An assessment of the risks to the **rights and freedoms** of data subjects.

- The measures envisaged to address the risks, including **safeguards, security measures and mechanisms** to ensure the protection of personal data and to demonstrate compliance with the GDPR.

MORE ON THE DPIA

The UK's Information Commissioner's Office, which is responsible for enforcing the GDPR in that country, has prepared a Data Protection Impact Assessment template.



ico.
Information Commissioner's Office

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

The document will guide you through the process of determining **whether your data processing activity** requires a DPIA.

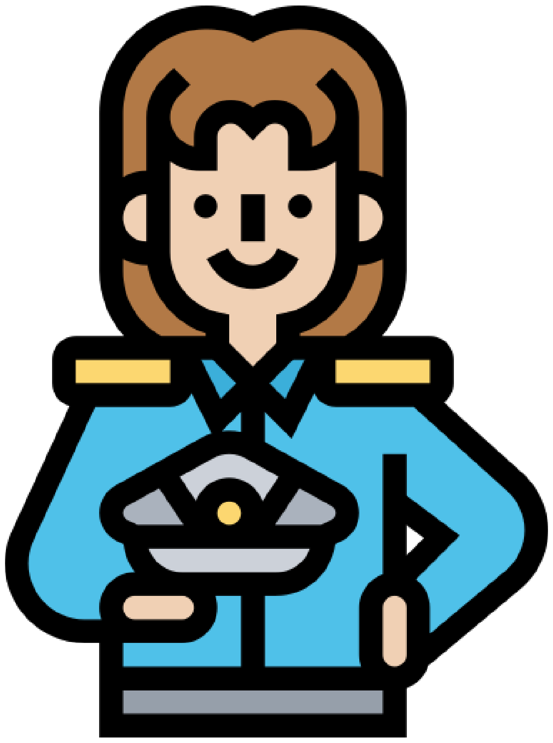
TO NOTE:

You must prepare your DPIA BEFORE beginning any data processing activity.

Ideally, you should conduct your DPIA **before and during** the planning stages of your new project.

If you have a Data Protection Officer you must consult with that person, and any other key stakeholders involved in the project, throughout the course of the DPIA.

DATA PROTECTION OFFICERS



A Data Protection Officer (DPO) role is to:

- Understand the GDPR and how it applies to the organization,
- Advise people in the organization about their responsibilities,
- Conduct data protection trainings,
- Conduct audits
- Monitor GDPR compliance,
- Serve as a liaison with regulators.

DO YOU NEED A DPO?

There are **three conditions** under which you are required to appoint a DPO:

- You are a public authority other than a court acting in a judicial capacity.
- Your core activities require you to monitor people systematically and regularly on a large scale.
- Your core activities are large-scale processing of special categories of data listed under Article 9 of the GDPR (e.g. **processing health data such as patient health records**) or data relating to criminal convictions and offenses mentioned in Article 10.

SECTION 4:

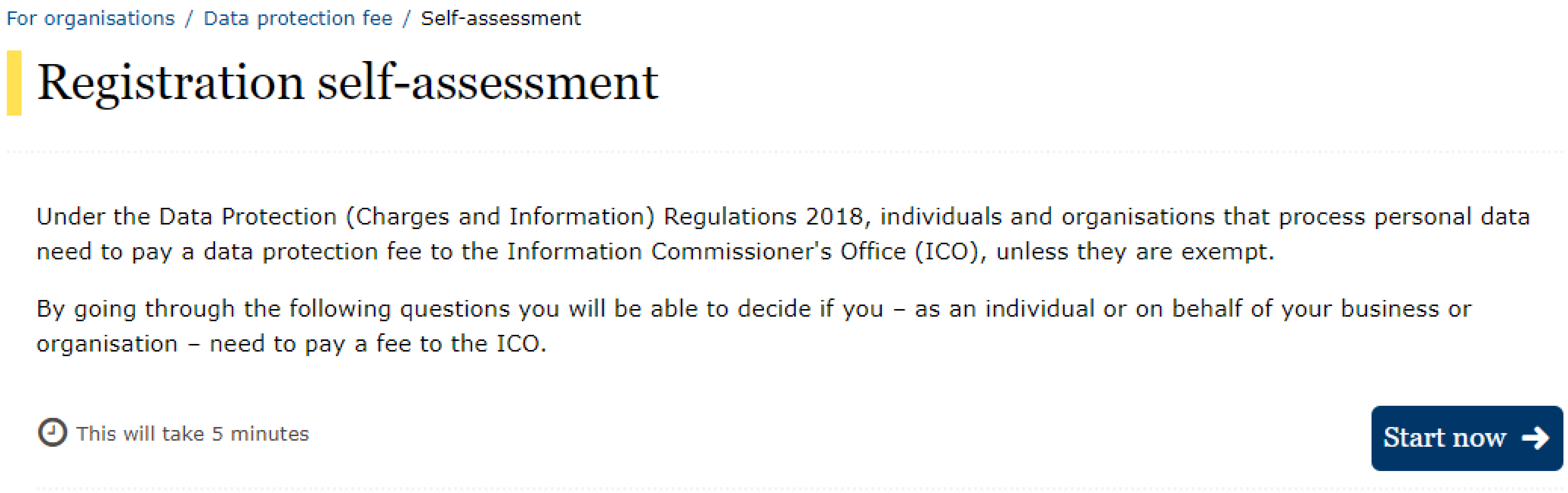
UK SPECIFIC CONSIDERATIONS.

INFORMATION COMMISSIONER OFFICE

ico.

Under the Data Protection (Charges and Information) Regulations 2018, individuals and organisations in the UK that process personal data need to **register and pay a data protection fee** to the Information Commissioner's Office (ICO), unless they are exempt.

EXEMPTION FROM THE ICO


For organisations / Data protection fee / Self-assessment

Registration self-assessment

Under the Data Protection (Charges and Information) Regulations 2018, individuals and organisations that process personal data need to pay a data protection fee to the Information Commissioner's Office (ICO), unless they are exempt.

By going through the following questions you will be able to decide if you – as an individual or on behalf of your business or organisation – need to pay a fee to the ICO.

There are a **few circumstances** where you may be exempted from paying the ICO fee.

The ICO has helpfully created an online registration self assessment to help you determine whether you are exempted or not.

NHS Digital

DATA SECURITY AND PROTECTION TOOLKIT

The **Data Security and Protection Toolkit** is an online self-assessment tool that all organisations must use if they have access to NHS patient data and systems.

You will need to identify a Data protection Officer.

It enables organisations to measure and publish their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems **must use this toolkit to provide assurance** that they are practising good data security and that personal information is handled correctly.

Hope you found this helpful!

This is a series we are making to help HealthTech Innovators access better resources.

Just our small way of helping!