

GDPR – Introduction



Welcome to the Chess ICT GDPR Training course, the aim of this course is to:
Inform you of the details within the new GDPR legislation and how this may impact your day to day business operations.

We'll cover the history of the Data Protection Act and how you can seamlessly transition to the new GDPR regulations

And finally, we can start to prepare you and your organisation on your new responsibilities and procedures you may have to put in place



In Module 1 we will explain how to assess where you currently are in relation to GDPR and your overall data privacy controls.

Module 2 is aimed at helping you understand the moving parts of GDPR and to help align your operations to these areas.


After that, Module 3 covers the role of the Data Protection Officer.

In Module 4 we delve into the roles and responsibilities involved in GDPR.

The documents, Processes and information which you may need are addressed in Module 5.

Module 6 covers the important process of handling a data breach or incident. And Finally, In Module 7 we will discuss where Chess can help you going forward.

Disclaimer



Chess have invested a great deal in our interpretation of the General Data Protection Regulation (GDPR) to ensure that our customer data is safe , that our processes are considered and necessary, and so that we will continually improve our data governance as we grow as a company.


This course however is very specialized, and certain points are open for interpretation.

This means that the views within this course are not necessarily shared by lawyers or courts, but are just what we reasonably expect to be the case.

Chess therefore does not guarantee that all information is factual and interpreted correctly, wherever possible we have included reference links to ICO or other organisations and we encourage you to research as much as possible from these reference links.

If you wish to ensure your company is legally covered by GDPR, consider consulting legal or specialised GDPR consultancy.

Chess will work collaboratively with you and your company to protect the privacy of your customers and employees.




Chess have invested a great deal towards our interpretation of the General Data Protection Regulation (GDPR) to ensure that our customer data remains safe , that our processes are necessary and effective, and that we continually improve our data governance practices as we grow as a company.


This course is very specialized, and certain points are open for interpretation.
We wish to emphasize that Chess ICT is primarily an IT & telecommunications company, and not a legal firm.

This means that the views/opinions made throughout this course may not necessarily be shared by all data controllers, lawyers or courts, but are just what we reasonably expect to be the case and have been independently assessed for compliance by a privacy specialist.

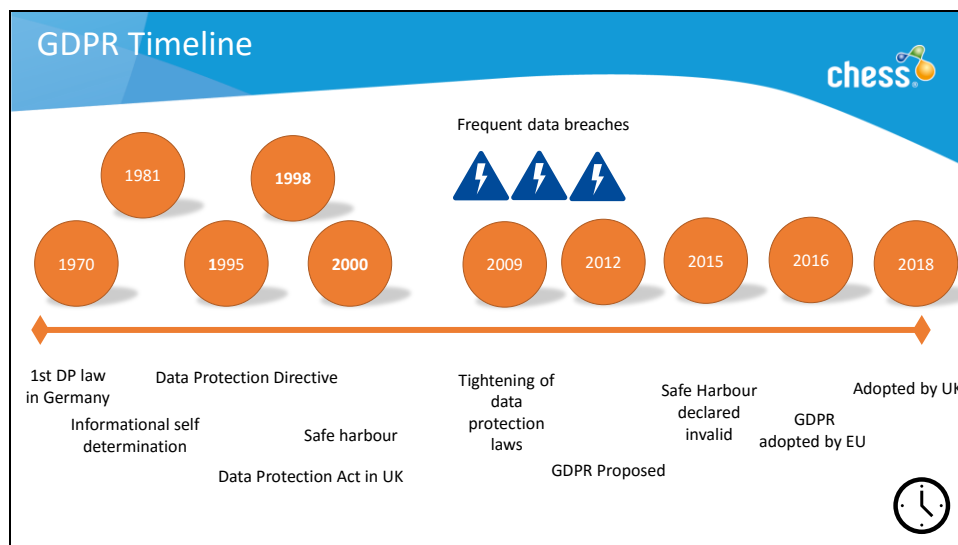
Where possible we have included references and links to the Information Commissioner and we encourage you to research as much as possible from these reference links.

In addition to this training course, its recommended that you seek further advice from a privacy expert or legal practitioner should you feel that your business may require specific guidance.

In a nutshell
chess 

What	The EU General Data Protection Regulation (GDPR) is a new law that strengthens privacy for EU citizens.	When	25 May 2018.
Where	Anywhere that holds data on EU citizens.		
	Access to information has never been easier. The digital age has brought with it additional complexities	Why	
Who	Everyone who deals with Personal Information will have to be aware of the law, you will need to assess whether it applies to you on a constant basis.		
How	We will be going through that on this course		

- **What** the EU General Data Protection Regulation (often GDPR) is a new law that strengthens privacy regulations for its citizens.
- **When** 25 May 2018
- **Where** Anywhere that holds data on EU citizens.
- **Why** Access to information has never been easier the digital age has brought with it additional complexities
- **Who** Everyone who deals with Personal Information will have to be aware of the law, you will need to assess whether it applies to you on a constant and continuous basis.
- **How** We will be going through that on this course



The need for privacy has been a topic of discussion for decades , firstly with paper based systems and lately with the growth of the internet and cloud storage SOLUTIONS for electronic data SYSTEMS.

Here are a few significant events that ultimately have led to the GDPR being adopted in 2018

In **1970** 1st DP law was introduced in Germany

On 28 January **1981**: The treaty regarding the protection of individuals with regard to automatic processing of personal data was signed as Council of Europe Convention 108 and went into effect on 1 October 1985. All 47 members of the Council of Europe have ratified the treaty, except Turkey.

In **1983** Informational self-determination proclaimed in German after census

in 1995 because the Data privacy laws varied across EU and impeded the free flow of data. the European Commission proposed the **Data Protection Directive**, which the GDPR will replace.

The European Data Protection Directive was created as an essential element of EU privacy and human rights law. The directive came into force on 13 December 1995 and required EU member states to implement the corresponding provisions in national law by 24 October **1998**.

For this reason, in 1998 the Data Protection Act was introduced in UK

The Safe harbour' agreement in **2000** allowed for the export of personal data to the US, wherever in Europe it came from. It required no need to ask for consent, or to enter into bilateral agreements. This was generally regarded as a bad thing if you were an EU Citizen

Since the Data Protection Act 1998, there have been several high-profile data breaches. Most notably...

- **2006 A Company called TJX, compromised the records of 94 million credit card customers**
- In 2008 Heartland Payment Systems had a data breach which resulted in the exposure of 134 million credit cards records
- In 2011 **Sony's PlayStation Network were hacked which exposed the records of 77 million PlayStation Network accounts; it was estimated that incurred losses were \$171 M**

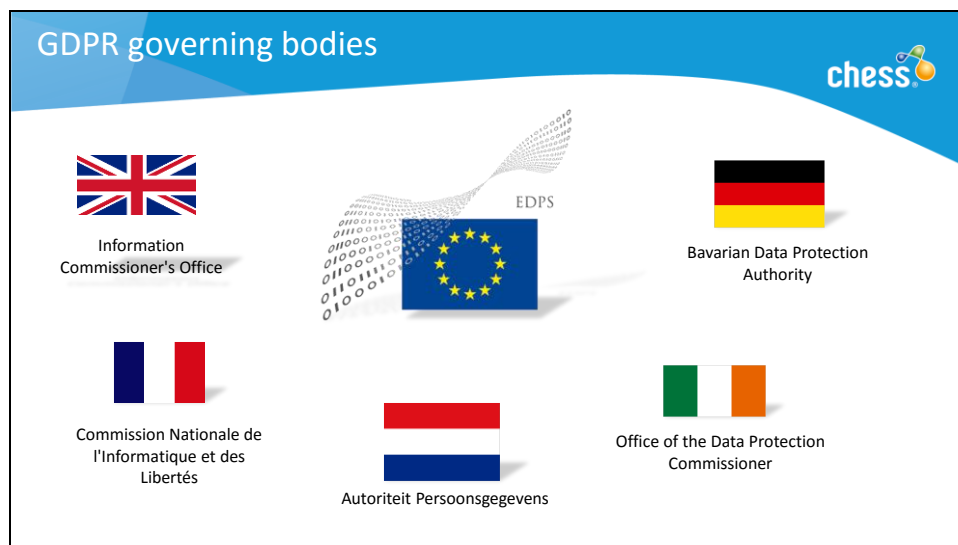
In 2009 The European commission called for tougher privacy *laws to react to these new types of cyber threats as the current legislation didn't take into effect the new ways of keeping personal information*

In 2012 GDPR was proposed, and after two years of discussions was approved.

In 2015 US Safe Harbour declared invalid, this forced the big US companies such as google, Apple and Microsoft to build EU based data centres that are covered by European privacy laws

In 2016 the GDPR was adopted by the EU, this meant that member countries had to agree to create new legislation to adhere to these new principles

In May 2018, GDPR will come into force in the UK





The organisation that oversees each EU member applies the GDPR is the European Data Protection Supervisor
The EU's independent data protection authority.
European Data Protection Board

Although the regulations are sourced in the EU council each country will have its own governing body and interpretation of the regulations

The French, Dutch, Irish and German all have their own specific organisation for example, and here in the UK it's the ICO

If history is any judge, Germany and Spain will be the toughest on data protection laws, whereas the Republic of Ireland, which has gathered a reputation for leniency, will be the softest

- <https://www.itgovernance.eu>
- <https://www.dataprotection.ie>
- <https://www.cnil.fr>
- <https://www.lida.bayern.de>
- <https://autoriteitpersoonsgegevens.nl>

What has changed		chess	
 DPA		 GDPR	
1995	2018		
8 Principles	6 Primary Principles		
100+	99 Articles		
Only applies to UK	Any org that holds data on EU citizens		
Negative opt-in	Positive opt-in		
Fee for requests	Can no longer charge		
the right of access to a copy of the information	the right to be forgotten		
Only covered by the Privacy and Electronic Communications Regulations 2011	within 72 hours		
Fines up to £500,000	Up to 20 million euros		

Let's take a look at some of the differences

As many businesses have become comfortable with the rules and requirements of the existing Data protection act.

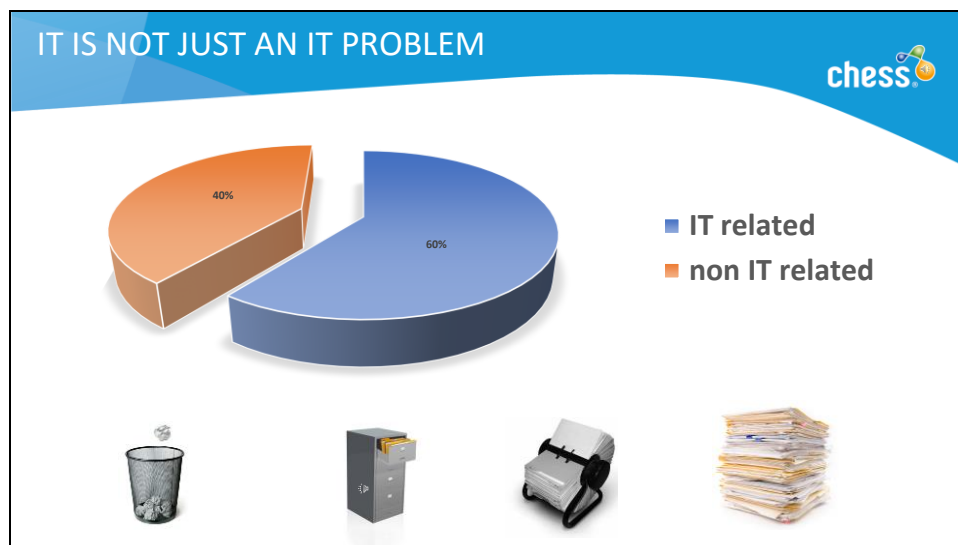
the GDPR can be seen by many as a complete overhaul towards privacy practices businesses must adopt.

The good news is that in essence the GDPR regulations are actually not that different from the current DPA, they merely plug some of the gaps to combat the new type of Cyber Threats

Here we can see a comparison of the main differences between the DPA and GDPR.

Some of the key changes here are.

- A simplification from 8 to 6 principles
- There are roughly the same number of articles
- The GDPR is applicable across the whole of European (and beyond) previously each member state had its own individual legislation
- Marketing consent, primarily opt in rather than opt out.
- You can no longer charge for supplying data to data subjects
- There are new data subject rights, particularly the right to be forgotten.
- There is now a Mandatory 72-hour window to report an incident to the ICO
- And the headline grabbing Increased fines for data breaches and incidents.



Its important to remember that The GDPR is not entirely focussed on electronic data, there are considerations for all data however its processed and retained.

For example, The HR function in each company will need to be aware on how they control the information of their employees. For example company directories, appraisals forms from existing employees and CV's from candidates wishing to apply for positions within the company - are all within scope of GDPR.

Could you answer this simple question?

Can you locate all the paper records for a person if they evoke any one of their data subject rights?

How easy is it to find out how many copies of these documents you hold, and where they are?

Do you keep paper based document that contain personal information safe?

Are you disposing of paper based records when they're no longer relevant and how are you doing this?

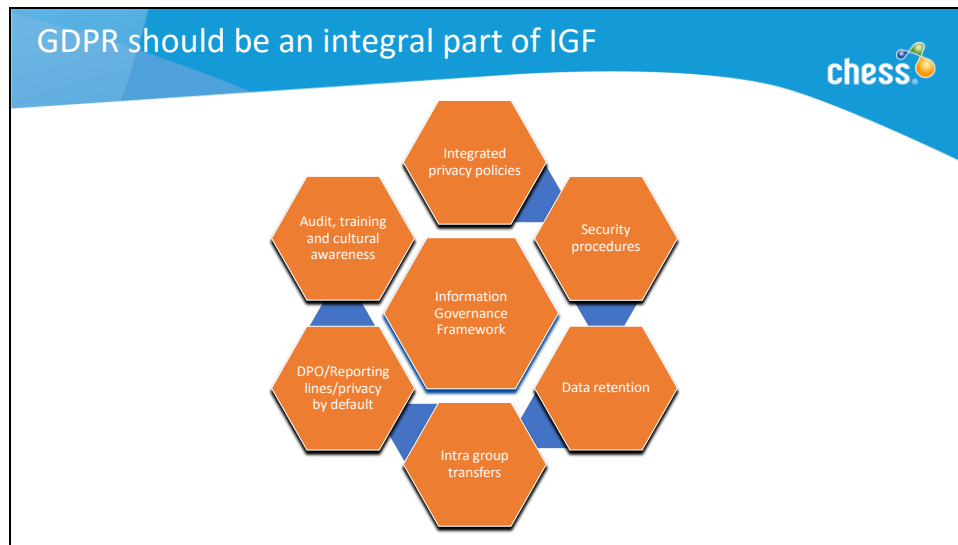
If you can't answer these questions then an audit of your current processes may be in order.



Apart from the obvious database records, file systems and cloud storage files you may have which involve customer records, there's a variety of other elements to consider when implementing the GDPR regulations to understand where data could exist:

Here are a few examples;

- Website cookies
- Mobile device Management
- Cloud storage
- Backup and recovery tapes
- Filing cabinets and Paper Stores such as Filing cabinets & Confidential Waste Bins, their security and location
- IT equipment disposal such as Hard drive destruction.
- Internal procedures
- Email retention logs and audit files




GDPR should be an integral part of IGF Information Governance Framework

The purpose of the Information Governance framework is to formally establish an organisation's approach to Information Governance.

This framework is used by organisations to guide all staff that create, store, share and dispose of information.


The GDPR regulation should be addressed by your internal data/privacy policy and form part of your Information Governance framework

The GDPR 99 Articles


Recitals are guidance on spirit of content of the chapters

1. General Provisions Articles 1-4
2. Principles Articles 5-11
3. Rights of the Data Subject Articles 12-23
4. Controllers and Processors Articles 24-43
5. Third Countries Articles 44-50
6. Supervisory Authorities Articles 51-59
7. Cooperation and Consistency Articles 60-76
8. Penalties , Liabilities and Remedies Articles 77-84
- 9,10 & 11 Specific Provisions Articles 85-99

<https://ico.org.uk/>



the GDPR is split into 99 articles across 11 chapters, preceded by recitals that give guidance on how the articles are to be interpreted.

- **Chapter 1** includes Articles 1-4 which deal with General Provisions and definitions
- **Chapter 2** deals with principles of processing and includes Articles 5-11 Principles
- Articles 12-23 make up **chapter 3** and address the Rights of the Data Subject
- **Chapter 4** deals with your obligations and responsibilities when dealing with PI these are detailed in Articles 24-43 Controllers and Processors
- Remember the safe harbour agreement ? **Chapter 5** deals with this in the articles for third countries. Specifically details what organisations must do to protect PI when they move data outside the EU. Articles 44-50
- **chapter 6** contains Articles 51-59 which deals with Supervisory Authorities As we mentioned before , here in the UK our supervisory authority is the ICO
- The co-operation between supervisory authorities is contained within **chapter 7** this includes Articles 60-76 Cooperation and consistency
- The section that has everybody worried is chapter 8(Articles 77-84) which contains information on Penalties , Liabilities and Remedies.

Worth noting that these sanctions are generally imposed for repeat offences. and as long as you are actively implementing procedures and policies these sanctions will probably be suspended until you can reasonably comply.

9,10 & 11 Articles 85-99 specific provisions exclusions and additional requirements such as churches and charities

