



# GDPR

What to do about it



Elizabeth Denham, Information Commissioner

GDPR rebalances the relationship between individuals and organisations.

It gives greater control to people about how their data is used and it compels organisations to be transparent and account for their actions.

As individuals, most of us applaud a stronger framework. As heads of agencies, some of you may have a different view.

Those organisations that thrive under the new rules will see the GDPR as an opportunity to commit to data protection and embed it in their policies, processes and people.

Those that merely comply, that treat the GDPR as another box-ticking exercise, miss the point. And they miss a trick.

Because this is about restoring trust and confidence. Only one in five people in the UK trust organisations to look after their data. That's not good enough.

The GDPR is an opportunity to reset the equilibrium.

You can expect that the ICO will uphold the law and that I will stand up for the rights of UK citizens.

While there will be no grace period – you've had two years to prepare – I know that when 25 May dawns, there will be many organisations that are less than 100 per cent compliant.

This is a long haul and preparations will be ongoing. But if you self-report a breach, engage with us to resolve issues, can demonstrate effective accountability arrangements, you will find us to be fair.

Enforcement will be proportionate and, as it is now, a last resort.



V Sign

Bugs in home



Baby monitors hacked

Is Google tracking everything  
you do?



Is that link real

# Paranoia



# How to get Hacked

- Use a BAD Pa55w0rd
- Use the Same Pa55w0rd everywhere
- Don't use 2<sup>nd</sup> factor authentication
- Don't use common sense
- When Microsoft Calls you – let them in
- It'll never happen to me attitude
- Use Social Media – without a thought

# This is Why GDPR was developed?

- 
- Economy Increasingly becoming digitised. DPA was created 1998
  - Companies are assessing customer behaviour based on data
  - Recent breaches show there is Significant risk
  - Strengthens Data Protection of personal data
  - Will change our approach to information security
  - Focuses on EU Subjects – not companies
  - All European companies must comply

# Why is it important for you?

- 
- Required by Law
  - You will receive requests
  - Improved efficiency
  - Better reputation
  - You will be attacked
  - Protection against breaches/fines

# 52%

of global IT decision makers think they will be fined due to the GDPR





# The GDPR is structured around six principles:

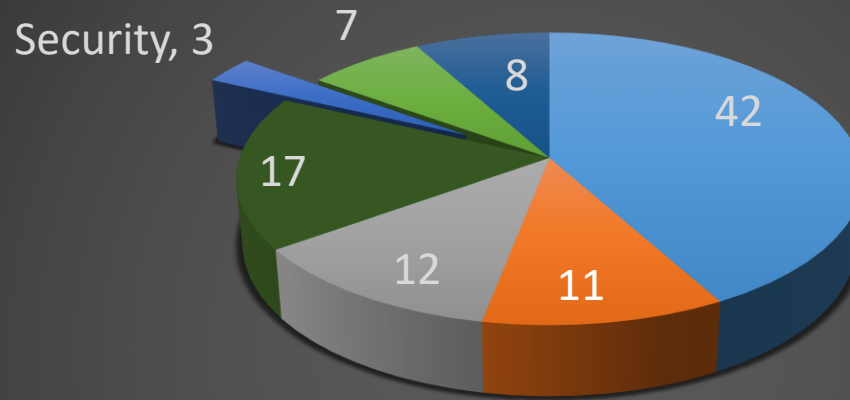
- 
- Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Confidentiality, Integrity and Availability

# What is the GDPR?

- **11 Chapters**  
99 Articles (the law)
- **Recitals**  
Describe how to implement the Articles



## GDPR Article Focus (%)



- Administration
- Data Subject Rights
- Security
- Remedies

- General and Principles
- Controller Responsibilities
- Sending out of EU

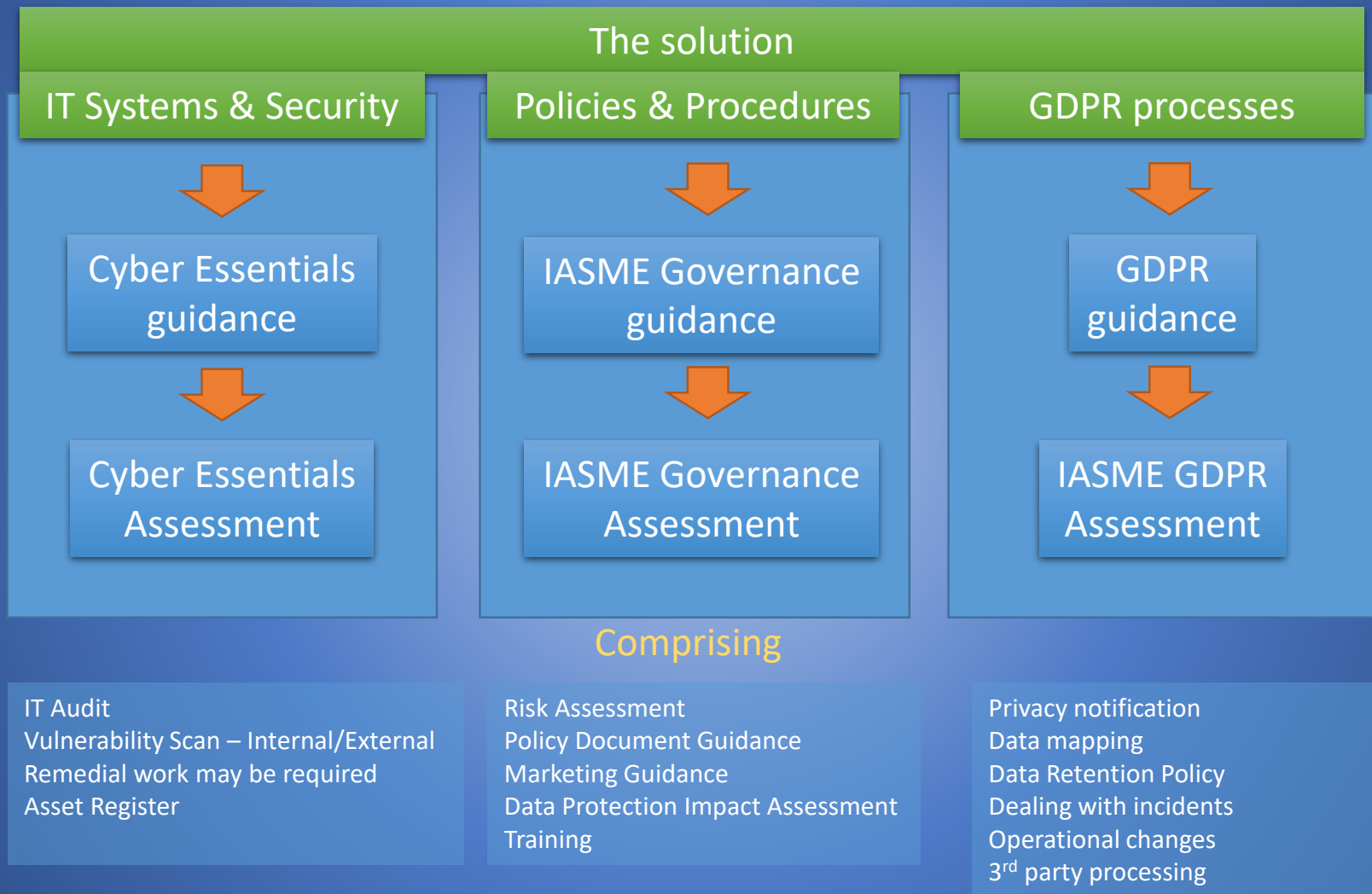


# IASME Consortium<sup>®</sup>

**Governance assessment including  
Cyber Essentials and GDPR**

# How do you become GDPR ready?

The GDPR can be categorised into 3 main sections.







Consent



Breach notification



Right to Access



Right to be Forgotten



Data portability



Privacy by Design



Data Protection Officer

## MUST BE



Given by a statement  
or clear affirmative  
action



Freely given, specific,  
informed and  
unambiguous



Proven by the data  
controller



Withdrawn as easily  
as it is given

## MUST NOT



Be inferred from  
silence, pre-ticked  
boxes or inactivity



Make consent a  
condition for receiving  
a service unnecessarily

!?!?

Use confusing  
unclear language



Bundle with other  
terms and conditions



Consent



Breach notification



Right to Access



Right to be Forgotten



Data portability



Privacy by Design



Data Protection Officer



You have 72 hours from the breach discovery, to inform the ICO and any subjects that may have been affected.



Consent



Breach notification



Right to Access



Right to be Forgotten



Data portability



Privacy by Design



Data Protection Officer



Personal Data	
<div>Subjects have the right to obtain data held about them. An easy to read electronic copy must be provided. - for free</div>	Name
	Home Address
	Business Address
	Identity Card No
	Passport No
	Driving License
	Income Tax No



Consent



Breach notification



Right to Access



Right to be Forgotten



Data portability



Privacy by Design



Data Protection Officer



When data is no longer relevant to a company, subjects can have it erased.





Consent



Breach notification



Right to Access



Right to be Forgotten



Data portability



Privacy by Design



Data Protection Officer



All data should be easily transferrable between computer systems.





Consent



Breach notification



Right to Access



Right to be Forgotten



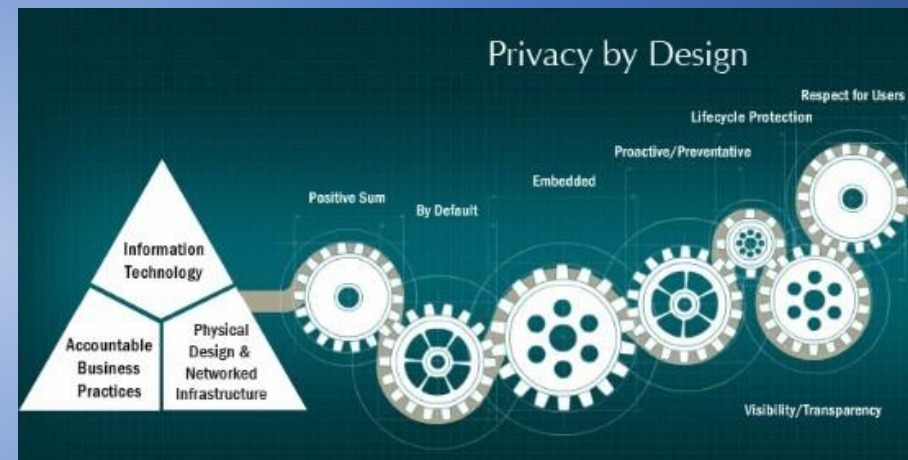
Data portability



Privacy by Design



Data Protection Officer





Consent



Breach notification



Right to Access



Right to be Forgotten



Data portability



Privacy by Design



Data Protection Officer



**Only for LARGE Companies**

# The **RISK**



**Just Eat** has come under fire after a delivery man sends **unsolicited texts** to a customer

Date **16 January 2018**

Type **Statement**

An ICO spokesperson said:

“

If a customer's phone number is used for reasons for which it was not originally taken, it could be a breach of the Data Protection Act.

"Organisations have a legal duty to make sure personal data is only used for the purposes for which it was obtained. We are aware of reports of an incident involving Just Eat and will be looking into it."



## Flybe fined £70,000

In August 2016, Flybe sent an email to 3.3 million people in their database with the subject line “Are your details correct?”

It sounds like a smart strategy in theory, but unfortunately, these 3.3 million people had previously opted out (unsubscribed) to marketing emails and thereby gave no consent to be contacted.

Elliot, if this email is not displayed properly, [click here](#).  
Ensure you receive your Flybe emails by adding [admin@news.flybe.com](mailto:admin@news.flybe.com) to your address book.



Hi Sven,

It's been a while since we last saw you and as a valued customer, we'd like to ensure the information we hold for you is up-to-date.

To check and update the personal data we hold for you, please click the button below to go to your account where you can amend any out of date information and update your marketing preferences. This will only take a moment.

We respect your personal data and will never share it with any third party.

To say thank you, if you click and update your information by 24/08/16 you will be given the option to enter into our prize draw to win one of ten pairs of tickets to any destination on the Flybe network. T&C's apply.

**Key take away:** If your customers have opted-out of marketing emails, don't email them – it's as simple as that. You are breaking the law if you do.



## **Honda Motor Europe fined £13,000**

In a separate incident, Honda Motor Europe sent an email to 289,790 subscribers between May and August 2016 asking their database “would you like to hear from Honda?”.



This email was sent in order to clarify how many of the 289,000 subscribers would like to receive marketing emails going forward. But, once again, this email was sent to individuals who had specifically opted out.

This mistake earned Honda a [£13,000 fine](#) as a result.


**Key take away:** If you do not have explicit consent to email your customers, then don't email them! Even asking for consent is classed as marketing and is in breach of the upcoming GDPR regulations.






Royal Mail, members of [Royal Mail Group](#)  and [Post Office](#)  would like to contact you about products, services and offers that might interest you. Click on the Register button to submit this form and indicate your consent to receive marketing communications by post, phone, email, text and other electronic means. If you **do not** wish to receive such communications, please tick the relevant box(es) below.

☐ Post ☐ Telephone ☐ Email ☐ SMS and other electronic means

If you would like to receive information about products, services, special offers and promotions from carefully selected  third parties, please let us know by ticking the relevant box(es) below.

☐ Post ☐ Telephone ☐ Email ☐ SMS and other electronic means

Royal Mail takes your privacy very seriously. The information you provide through the website will be held under the Data Protection Act 1981. Please read our [Privacy Policy](#) 

# How **NOT** to do it

# Preparing for the General Data Protection

## Regulation (GDPR) 12 steps to take now

1

### Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2

### Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3

### Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4

### Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.



5

### Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6

### Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7

### Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8

### Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9

### Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10

### Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11

### Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12

### International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.



# What Data?

What data do you collect?

Where is it stored?

Any third parties?

Do you need it?

How is it shared amongst your team?

Where did it come from?

Where is it going?

How long to you keep it?



# Individuals Rights

Right to  
information

Right to access

Right to  
rectification

Right to be  
forgotten

Right to  
restriction of  
processing

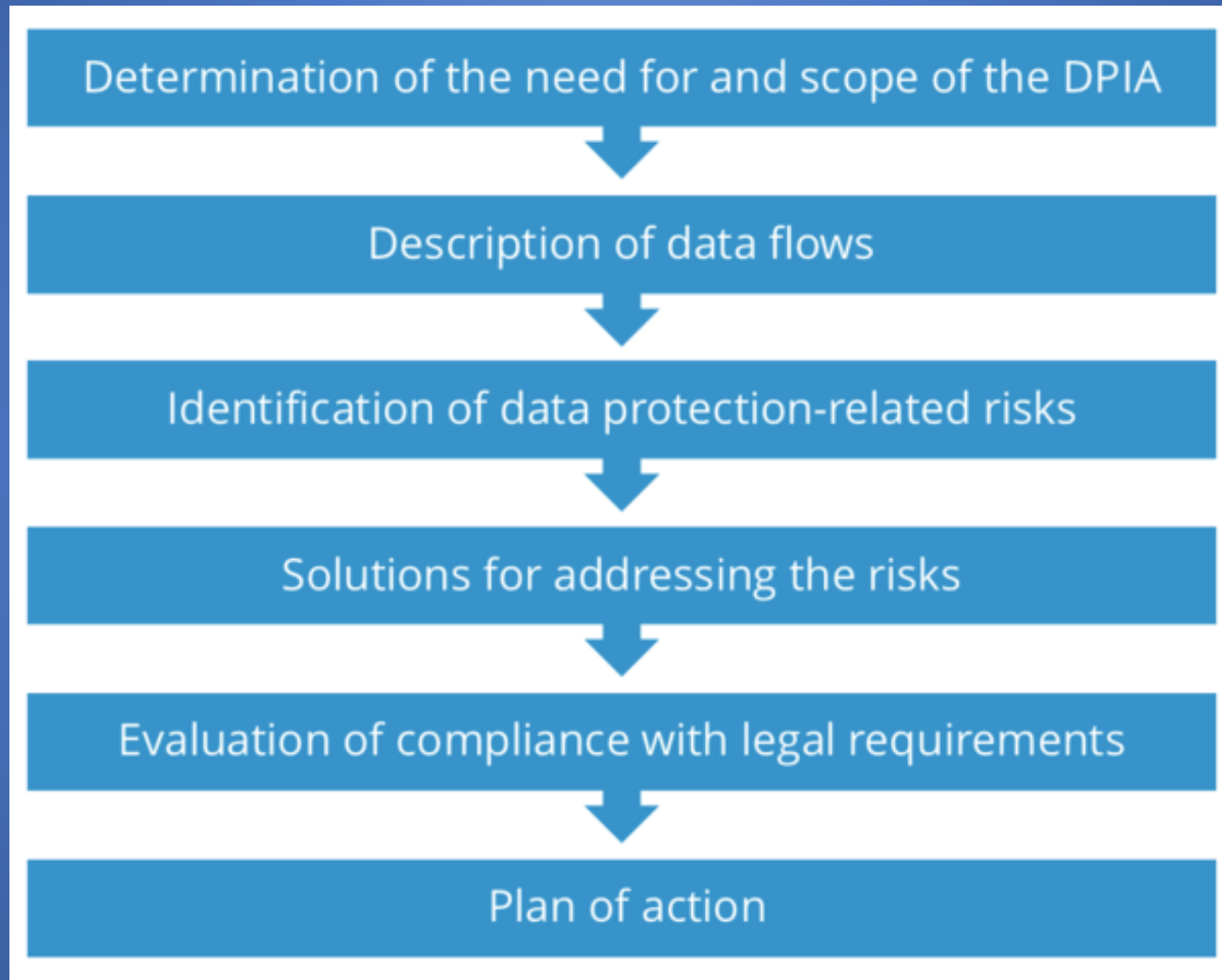
Right to  
notification

Right to  
portability

Right to object

Right to  
appropriate  
decision making

# Data Protection Impact Assessments (DPIAs)



What can you do?

**Now!**

# Cyber Essentials

Secure the  
Boundary

Configure  
securely

User access  
control

Malware  
protection

Patch  
Management



# Ensure security measures are practical

Controls can ***stop*** people acting in a way that places the organisation at risk.

...but they must  
be consistent  
with the way  
people behave  
and think.



Password fatigue

Monitoring - trust & private life and business.

Complacency

Move beyond technical education

Tackle the Millennials





# A password is like a toothbrush



Choose a  
good one

Don't share it  
with anyone

Change it  
occasionally

PASS **PHRASE**

Ilcft1tm!

I Like Coffee First Thing In The Morning

Ilcft**L**1tm!

# Cyber Security...



...is an attitude. It is not just an IT issue.



...is a behaviour, and a way to life and should become part of your culture.



...transcends your relationships with Suppliers, Customers, Sub-contractors and Co-workers.



...is there to protect your assets and protect the personal data of those you work with.

# Core Policies and Documents





# Your Action Plan



Know what data you have & where it is



Educate and Raise Awareness



Create a Business Culture around Security



Mitigate Vulnerabilities



Get the Cyber Essentials tick



# How can we help



Advise



Training



Work with your existing IT



Prepare your system for you



Assess you

# Final thought

HACKED

200 days

Before discovery



You may have already been hacked – you just don't know it



[www.bc-technologies.co.uk](http://www.bc-technologies.co.uk)