

The **10 things** you need to know about the GDPR



GDPR

Learning objectives

- **Understand** what GDPR is, the consequences of not being GDPR compliant and what constitutes a breach
- **Better knowledge** of how to manage the risk and best prepare for GDPR
- **Recognise** the benefits of being GDPR compliant

Agenda



Introduction and
background



10 things you need
to know about
the GDPR



Questions?

Introduction and background

Hosted by Rob Walton, Chief Operating Officer, Intelliflo

15+ years experience in cyber security and data protection

ISO27001 Certified organisation



Active members of:

- UK Government National Cyber Security Centre (NCSC)
- Cyber Security Information Sharing Partnership (CiSP)



security.help@Intelliflo.com



@rawalton1910

GDPR – Intelliflo Working Group

Intelliflo Customer Working Group in place since July 2017

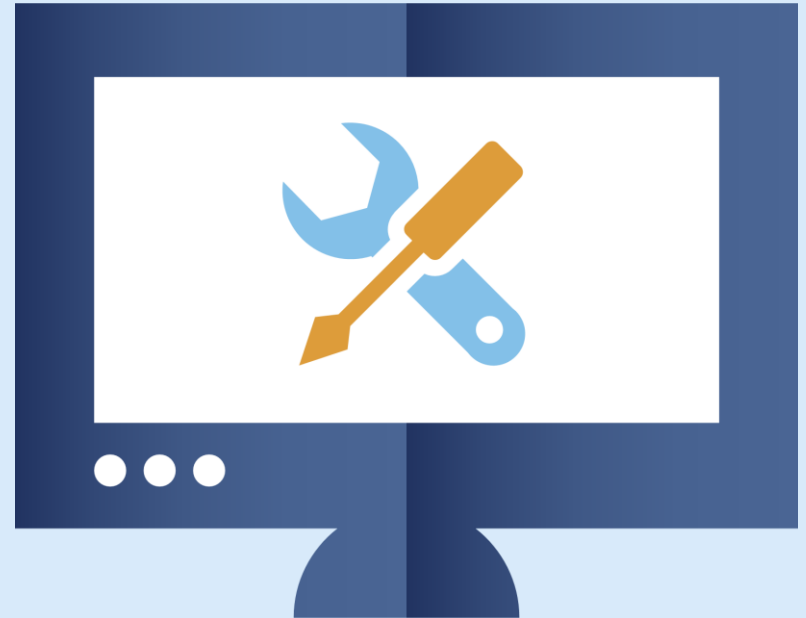
- Define iO product changes
- Assist wider industry to understand impact of GDPR
- Published consultation papers explaining challenges and how your peers are solving them.



intelliflo.com/gdpr-financial-advisers

GDPR – Free readiness toolkit

- GDPR Toolkit for Financial Advisers
- Developed in partnership with Brooklands Technology Limited
- Incorporates learnings from the customer working group
- Includes free assessment + 30 minute call with GDPR expert



intelliflo.com/gdpr_toolkit

1. GDPR - What is it?



- The EU General Data Protection Regulation (UK Data Protection Bill)
- Becomes UK law on 25 May 2018
- Gives power back to the data subject
- Brings data protection regulation in to the age of the internet

2. The core principles (Article 5)

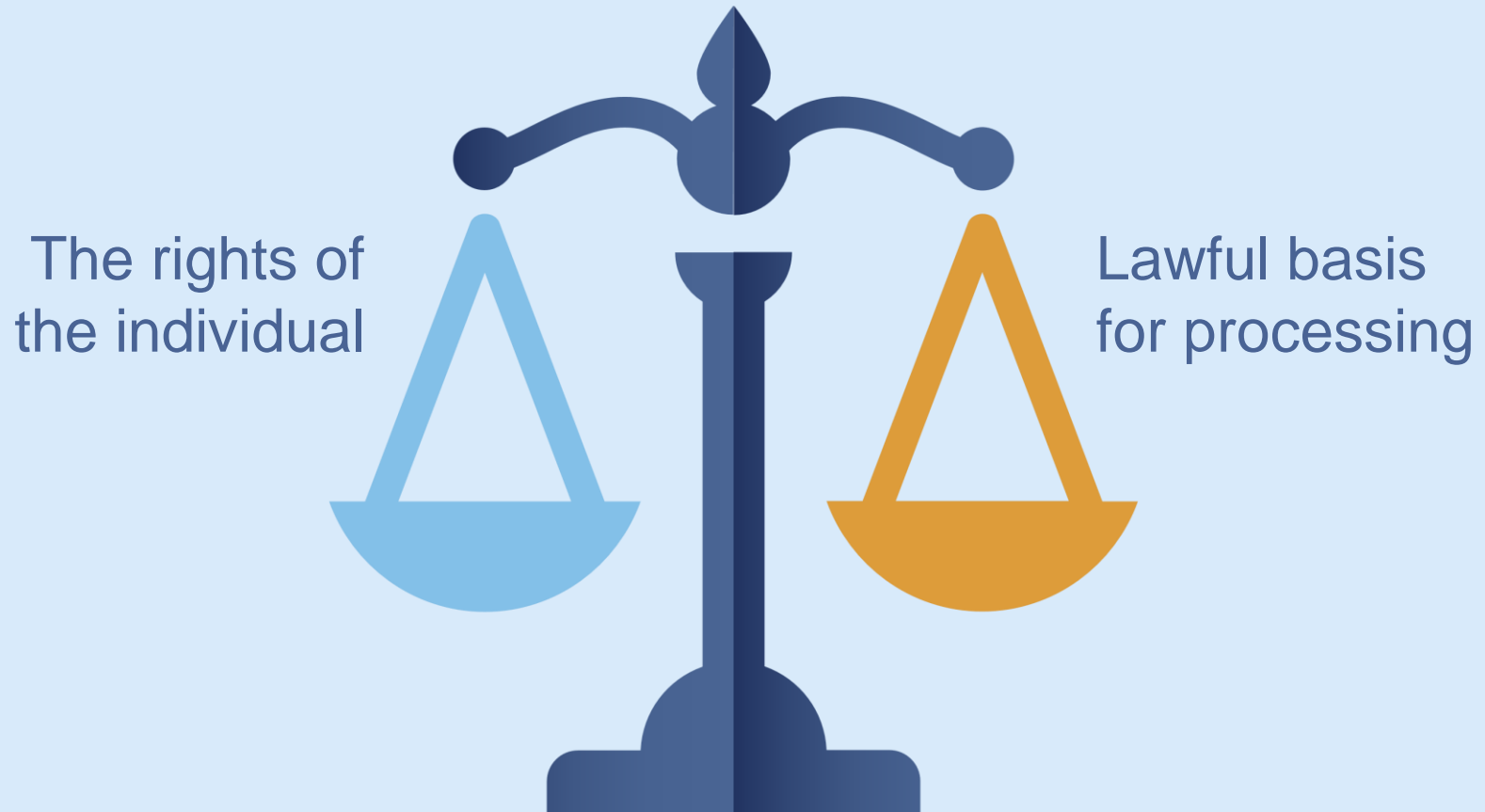
- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for only as long as is necessary
- Processed in a manner that ensures appropriate security of the personal data

2. The core principles (Article 5)



“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

How the GDPR finds the right balance



3. The rights of the individual

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated individual decision making

3. The rights of the individual

- You **MUST** have a documented process covering each right
- You **MUST** have trained your staff to be able to identify a request to exercise a right
- You **MUST** have trained appropriate staff on how to process a request to exercise a right
- You **MUST** have auditable records to show the training you have given to staff

4. Lawful basis for processing

- Consent – received clear and unambiguous permission by data subject, does not cover marketing by default
- **Contractual** – delivering on a contractual obligations
- **Legal** – meeting FCA requirement
- Vital interest – unlikely to be used by an advice firm
- Public task – unlikely to be used by an advice firm
- **Legitimate interests**
 - To be able to defend a legal claim in the future (FOS)
 - To be able to provide a high quality and tailored service

5. Your GDPR data inventory

This is a key GDPR asset that will help you to:

- Respond to right of individual requests
- Effectively manage a breach
- Undertake risk assessments on your business
- Evidence effective data management

Covered in the GDPR toolkit

The data inventory will document:

- What type of data subject?
- What type of personal data is held?
- What systems it resides in?
- What 3rd parties are used to process the data?
- What regions is the data stored in?
- What is the lawful basis for processing?
- What is the retention policy?

Description of business/data scenario	Lawfulness of processing	Data retention period	Response to right to erasure request	Response to right to object/restrict processing request
Data subject provides contact information and consent to be marketed to. No customer agreement have been signed and no advice has been given.	6(1)(a) – Consent of the data subject.	Two years from the point of consent if consent has not been given again.	Consent has been revoked so delete.	Consent has been revoked and there is no reason to actively process the data, so restrict process of data.
Data subject has signed a customer agreement however no meeting with the client occurred.	6(1)(a) – Consent of the data subject. 6(1)(c) - Processing is necessary for compliance with a legal obligation 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject	Until data subject is deceased on the basis of potentially needing to defend a legal claim.	Within five years, rejected on the grounds of 6(1)(c) - Processing is necessary for compliance with a legal obligation. Thereafter, rejected on the grounds of 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.	Consent has been revoked and there is no reason to actively process the data, so restrict process of data.
Data subject has signed a customer agreement and consent to be marketed to. Advice has been given but was not taken up by the data subject. There is no longer an ongoing relationship.	6(1)(a) – Consent of the data subject. 6(1)(c) - Processing is necessary for compliance with a legal obligation 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject	Until data subject is deceased on the basis of potentially needing to defend a legal claim.	Within five years, rejected on the grounds of 6(1)(c) - Processing is necessary for compliance with a legal obligation Thereafter, rejected on the grounds of 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.	Consent has been revoked and there is no reason to actively process the data, so restrict processing of data.
Data subject has signed a customer agreement and consent to be marketed to. Advice has been given and the data subject has transacted. There is an ongoing relationship.	6(1)(a) – Consent of the data subject. 6(1)(b) - processing is necessary for the performance of a contract 6(1)(c) - Processing is necessary for compliance with a legal obligation 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject	Until data subject is deceased on the basis of potentially needing to defend a legal claim.	As they are being actively serviced then 6(1)(b) processing is necessary for the performance of a contract and 6(1)(c) - Processing is necessary for compliance with a legal obligation. Thereafter, rejected on the grounds of 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.	Reject on grounds of 6(1)(b) processing is necessary for the performance of a contract and 6(1)(c) - Processing is necessary for compliance with a legal obligation
Data subject has signed a customer agreement and consent to be marketed to. Advice has been given and the data subject has transacted. There is no longer an ongoing relationship.	6(1)(a) – Consent of the data subject. 6(1)(b) - processing is necessary for the performance of a contract 6(1)(c) - Processing is necessary for compliance with a legal obligation 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject	Until data subject is deceased on the basis of potentially needing to defend a legal claim.	Within five years, rejected on the grounds of 6(1)(c) - Processing is necessary for compliance with a legal obligation Thereafter, rejected on the grounds of 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.	Consent has been revoked and there is no reason to actively process the data, so restrict processing of data.

Description of business/data scenario	Lawfulness of processing	Data retention period	Response to right to erasure request	Response to right to object/restrict processing request
<p>Data subject has signed a customer agreement and consent to be marketed to. Advice has been given and the data subject has transacted. There is no longer an ongoing relationship.</p>	<p>6(1)(a) – Consent of the data subject.</p> <p>6(1)(b) - processing is necessary for the performance of a contract</p> <p>6(1)(c) - Processing is necessary for compliance with a legal obligation</p> <p>6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject</p>	<p>Until data subject is deceased on the basis of potentially needing to defend a legal claim.</p>	<p>Within five years, rejected on the grounds of 6(1)(c) - Processing is necessary for compliance with a legal obligation</p> <p>Thereafter, rejected on the grounds of 6(1)(f) - Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.</p>	<p>Consent has been revoked and there is no reason to actively process the data, so restrict processing of data.</p>

6. Consent and privacy notices

Need to understand that consent to process data is not necessarily consent to market to the individual.

- Capturing information on individuals prior to them signing a client agreement (web forms etc)
- Marketing to non-clients
- Marketing to clients, not all communication is marketing...
- For consent to be valid it must be GDPR compliant:
 - Freely given
 - Unambiguous
 - A positive affirmation
 - As easy to withdraw as it was to give

6. Consent and privacy notices

Let's consider marketing to clients....

	Contractual communication	Legitimate interests marketing	'Marketing' marketing
Client 1	×	×	×
Client 2	×	×	
Client 3	×		

Your systems need to be able to cater for this differentiation.
You must support the right to object to legitimate interests marketing.

6. Consent and privacy notices

Article 13 – “**Information to be provided where personal data are collected from the data subject**”

- Privacy notice must be GDPR compliant
 - Why you store their data?
 - Where? In what regions?
 - What 3rd parties are involved?
 - How to contact your DPO (or equivalent)?
 - Retention periods or retention logic?
- You should, at a minimum, provide GDPR compliant privacy notices to all actively serviced clients before 25 May 2018
- Put it on your website too

6. Consent and privacy notices

Article 14 - "Information to be provided where personal data have not been obtained from the data subject"

- Privacy notice must be GDPR compliant, this includes but not limited to:
 - What data you store on them
 - Why you store their data, the lawful basis
 - Who gave you it
- This potentially means:
 - Partners
 - Dependents
 - Children over the age of 13

6. Consent and privacy notices

Article 14 shall not apply where and insofar as..... the provision of such information proves impossible or would involve a disproportionate effort.

- You should provide GDPR compliant privacy notices to partners of all actively serviced clients before 25 May 2018 where you hold PII data about them.
- You should capture in client agreements that it is your understanding that your client has consent to provide any information on other data subjects and that you may send the data subject a privacy notice.

7. GDPR - The *three* sticks...

- 1 Big fines are possible
- 2 The big risk is **Article 82** aka the Ambulance chasing article
- 3 Some breaches will become public record

€20m

or 4% of global
revenue fine for breach
or non-compliance



7. GDPR – The fines...

- €20m or 4% of global revenue fine for breach or non-compliance
- €10m or 2% of global revenue fine for failure to meet obligations of a data controller

But it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm.

The ICO's commitment to guiding, advising and educating organisations about how to comply with the law will not change under the GDPR. We have always preferred the carrot to the stick.

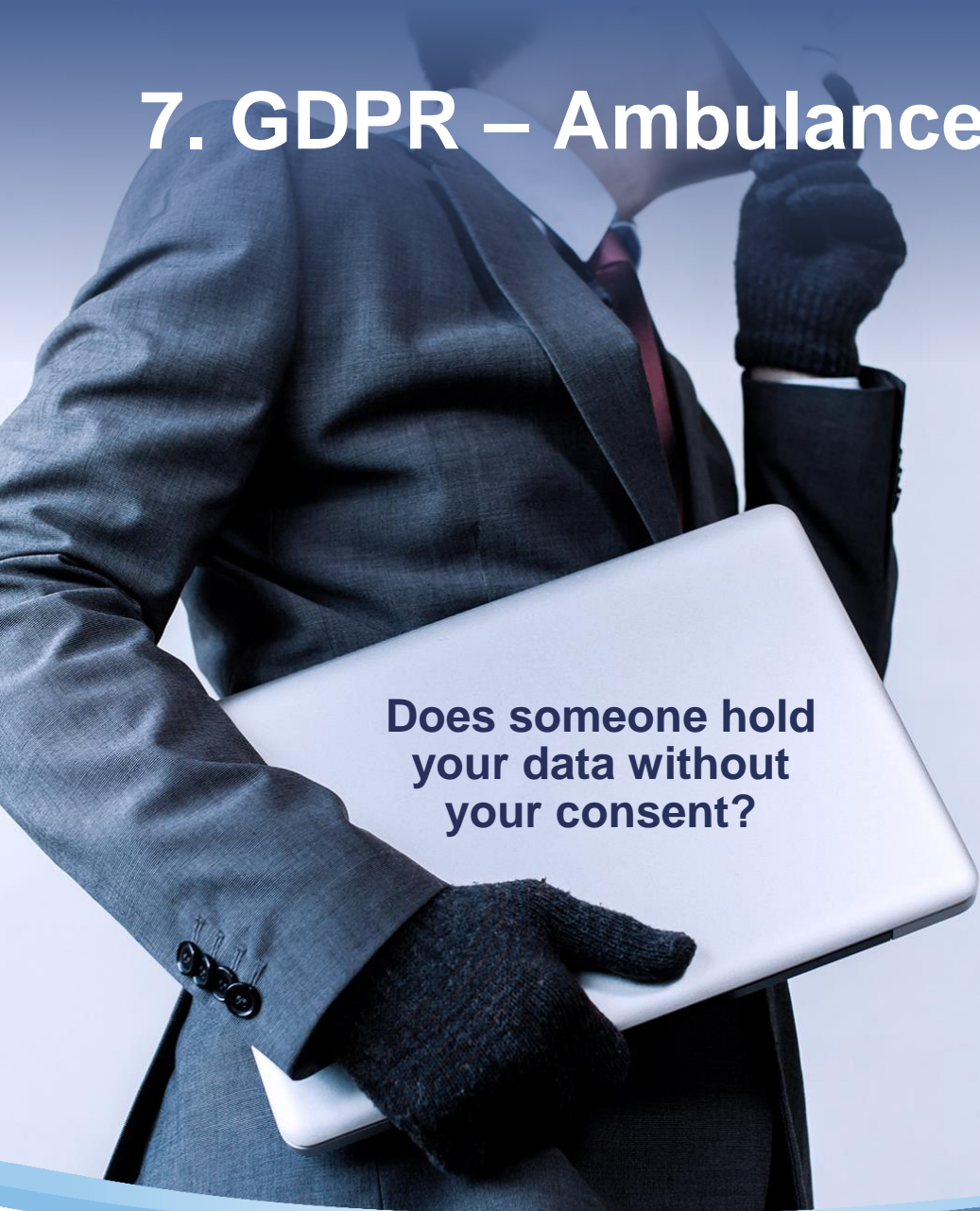
<https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/>

7. GDPR – The fines...

...impact on companies such as Facebook, who could face huge fines for breaches. Facebook COO Sheryl Sandberg has said the company has already **adjusted privacy settings** in anticipation. At its recent earnings call, Facebook specifically warned that GDPR could be an impediment to future growth.

<http://www.bbc.co.uk/news/entertainment-arts-42974551>

7. GDPR – Ambulance chasing



**Does someone hold
your data without
your consent?**

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Article 82(1) – Right to compensation and liability

8. GDPR - Ending up before the regulator

How?

- **A member of the public** may make a complaint
- **You** (the Data Controller) may report yourself
 - In the event of a data breach
 - You may have to tell your customers in that time period too

72

hours to report any
breach to the regulator



8. GDPR - What could a complaint be for?

- ✗ Not upholding an individual's rights
- ✗ Experiencing a data breach (CIA)
- ✗ Holding data you don't need anymore
- ✗ Holding inaccurate data
- ✗ Not having provided a privacy notice to an individual

8. GDPR - What could a complaint be for?

Data breaches don't
just look like this....



8. GDPR - What could a complaint be for?

Data breaches are anything in CIA (ISO27001)

- Confidentiality
 - A member of staff accessing a neighbour or friend's client records
 - A portfolio report being delivered to your client's next door neighbour
- Integrity
 - A member of staff accidentally entering incorrect data due to lack of knowledge or training resulting in a client making a decision based on incorrect valuation data
 - An aggrieved member of staff deliberately modifying data to cause damage
- Availability
 - An office flood or fire destroying only copies of client documents
 - Losing data after an IT outage and an untested, or insufficient, back-up process

9. GDPR - Data protection by design

Managing risk

Article 83:

“Fines will be imposed depending on technical and organisational measures implemented”

Ultimately you may have to explain why you work the way you do...

- Need to show your workings
- You are accountable for implementing appropriate governance

9. GDPR - Data protection by design

Real world examples



Customer data on unencrypted mobile devices



Physical documents



Not communicating securely with customers



Inaccurate customer data



Lack of security awareness

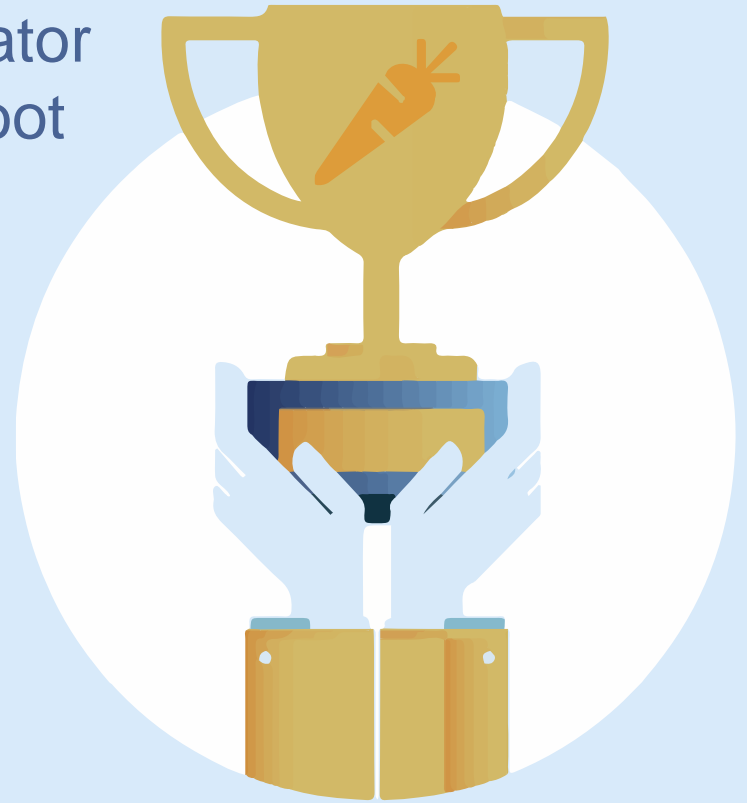
9. GDPR - Data protection by design

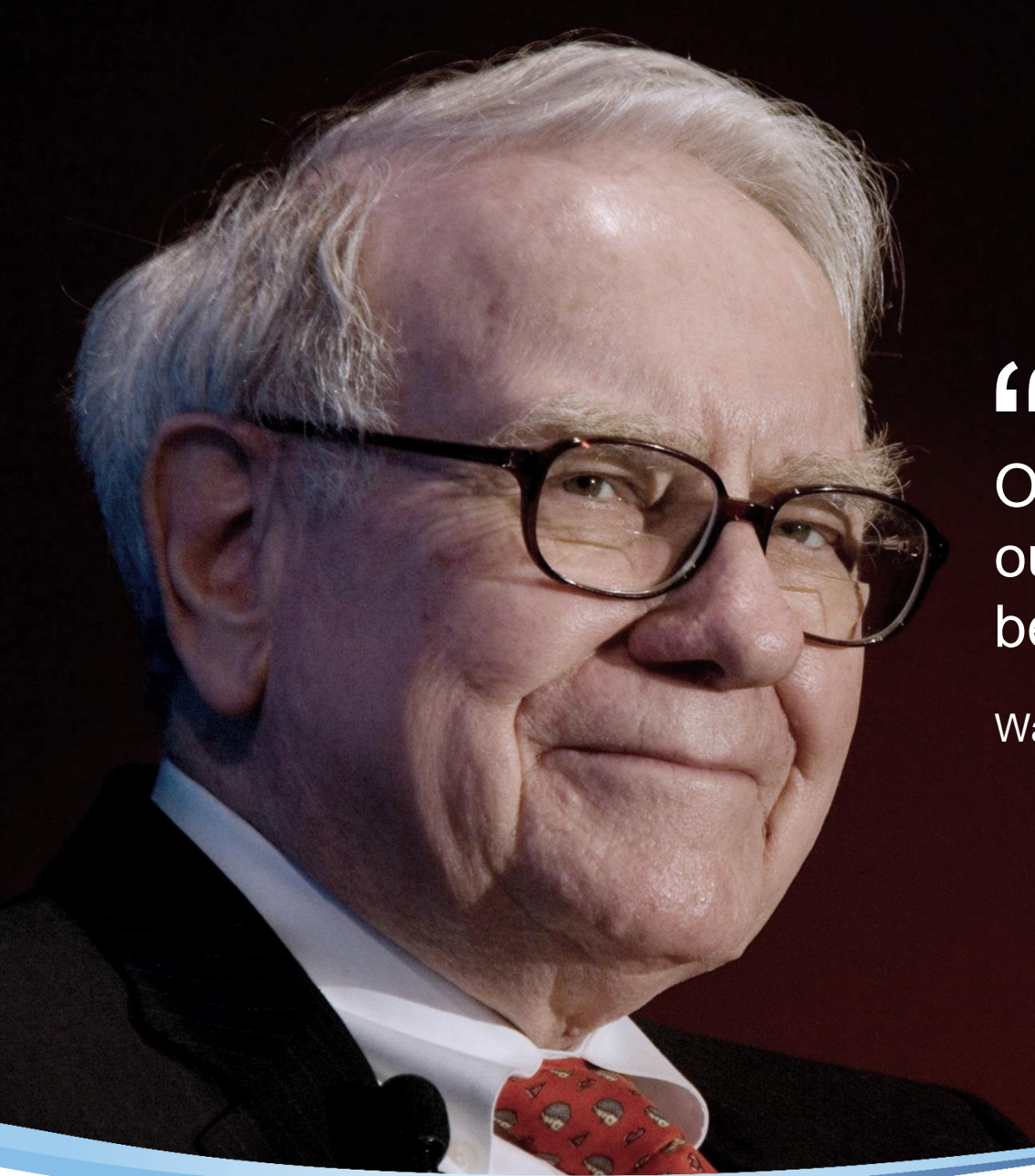
Real world solutions available right now

- Paperless office environment, online secure storage
- Secure and online customer portals
- Electronic contract (DocuSign)
- Leverage cloud services to improve your security
 - <https://www.ncsc.gov.uk/blog/saas-offerings>
- Ensure your 3rd party processors have ISO27001
- Ensure all of your IT is kept patched up to date
- Secure offsite physical storage
- Ensure your staff have appropriate training annually
 - GDPR
 - Information Security
 - Phishing Awareness

10. The GDPR silver lining....

- A badge of honour and a differentiator in the short term, get on the front foot
- Brand enhancing and business defending
- Most changes generally bring operational ROI and cost savings
- Real risks to every business
 - Cyber attacks double YoY
 - Ambulance chasing
 - Public naming and shaming





“

Only when the tide goes out do you discover who's been swimming naked. ”

Warren Buffett

GDPR free stuff

- Intelliflo GDPR Working Group Consultation Papers:
 - <https://www.intelliflo.com/gdpr-financial-advisers>
- Intelliflo Cyber Security guidance:
 - <https://www.intelliflo.com/cyber-security>
- Intelliflo and Brooklands partnered GDPR Toolkit plus free readiness assessment plus free 30 minute consultation with GDPR expert:
 - https://www.intelliflo.com/gdpr_toolkit

GDPR free stuff (Intelliflo customers)

- 6 free GDPR and Security eLearning courses with structured CPD minutes for Intelliflo customers
- Free knowledge assessment here:
 - <https://www.intelliflo.com/gdpr-awareness-assessment>
- Intelliflo Flashlight Data Cleansing Service
 - Uses data science techniques to help you clean your data and reduce time spent on valuations
 - Speak to your account manager

Learning objectives

- **Understand** what GDPR is, the consequences of not being GDPR compliant and what constitutes a breach
- **Better knowledge** of how to manage the risk and best prepare for GDPR
- **Recognise** the benefits of being GDPR compliant

Questions

- Is contacting a client because their mortgage deal is ending classed as legitimate interests marketing or marketing marketing?
 - If you have advised them on their mortgage or have offered mortgages as part of your regular and ongoing service, then that would be classed as legitimate marketing.
- Will you be providing a training module on the academy for the GDPR changes being made in iO?
 - Yes, we host a monthly webinar, that shows and explains all the latest enhancements made to iO. We will be hosting a GDPR specific webinar on 4 June, which will also be hosted in both the User Guide and the Academy.
- Can you send me the link to the GDPR Data Inventory template please?
 - A copy of the Data Inventory template can be found in the toolkit, which can be found on our GDPR page.

Thank you

0330 102 8402 | www.intelliflo.com



GDPR