







TYFU CYMRU
GROW WALES



GDPR reflections and update: March 2019
Anna Bezodis

@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

1





What this session will cover

Overview of the GDPR:
key details to understand


Update on recent
developments

Q&A session

@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    


2

What is the GDPR?







= The General Data Protection Regulation.

EU law that we've had to comply with since 25 May 2018.



Will remain despite Brexit!! (we'll come on to that later)

@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

3

What does it do?




Improved data rights for individuals

Organisations must be more accountable and responsible when handling data

@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

4

What the GDPR applies to







Personal data = any info relating to a living person ('data subject') who can be directly or indirectly identified from that information.

Special category data = what was previously 'sensitive personal data', including information relating to an individual's:


- race
- ethnic origin
- political opinions
- religion
- TU membership
- genetics
- health
- sex life
- sexual orientation
- biometrics (for ID purposes)

(NB: Data on [criminal offences](#) is dealt with separately)





@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

5

Examples




















Directly identifiable	Indirectly identifiable	Not covered by GDPR
<ul style="list-style-type: none"> • Name • Contact details • Date of birth • Photograph or video 	<ul style="list-style-type: none"> • NI number • Passport no. • Driving license no. • Location data on device • IP address 	<ul style="list-style-type: none"> • Anonymised data • Data about deceased individuals • Data about an organisation (not an individual)





@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

6

Which of these activities would be classed as 'processing' personal data?




 Taking a call and logging a customer's name and contact details for an order 	 Passing a customers name and address to a courier for a delivery 	 Keeping a record of allergies your staff member has, for health and safety 	 Shredding paperwork relating to orders you've processed for customers 	 Receiving a person's order and contact details through a form on your website 
	 Logging details of a company that supplies you with goods 	 Taking photos of volunteers carrying out tasks for you 	 Saving orders you've received in to a file on your laptop 	

@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

7


Lawful basis for processing data







To process someone's data lawfully you must have a valid reason for processing it – known under GDPR as a 'lawful basis'.

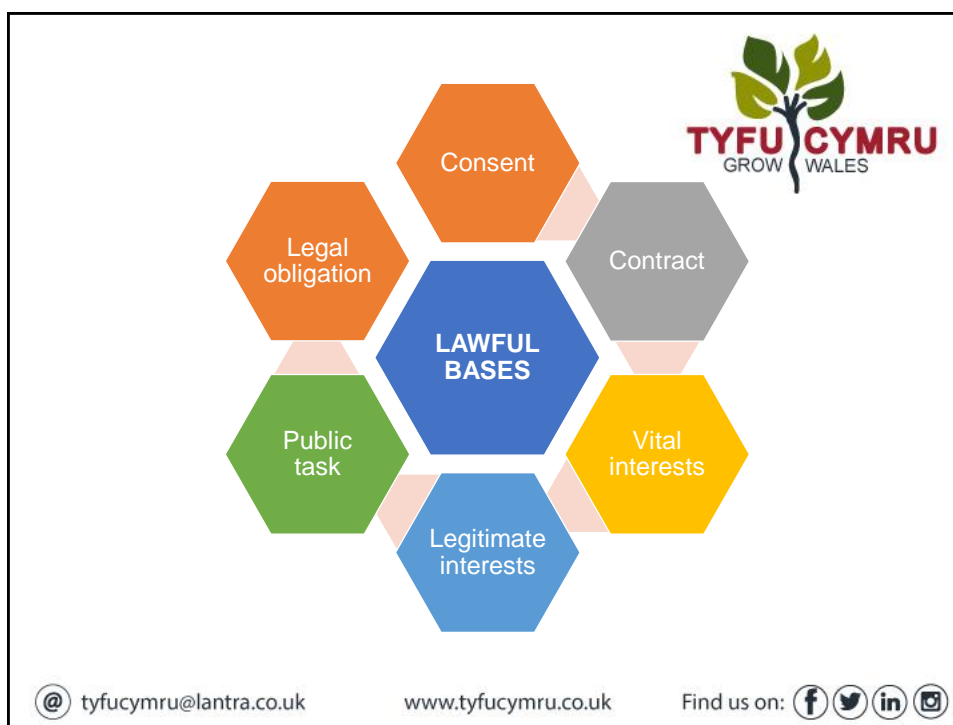
6 lawful bases to choose from, and the organisation you work or volunteer for will decide which of them you need to rely on and when.

Having consent from the individual the data relates to is one of the 6 options. This will be best in some cases but you **DON'T** always need consent to process someone's data – it's a myth!



@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

8



9

Key things to ensure (1)




- Know what lawful basis you're relying on
 - If it's consent, must be 'opt in' and keep evidence of it
- Have clear privacy notices / policy to tell people how you will process their data and what their rights are
 - Understand how to deal with any Subject Access Requests
- Only gather information you really need, and only keep it as long as is necessary, stored securely
- Photos/videos are personal data so remember to treat them in same way as other data you collect
 - If children/vulnerable adults, best to get written consent





@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:

10

Key things to ensure (2)


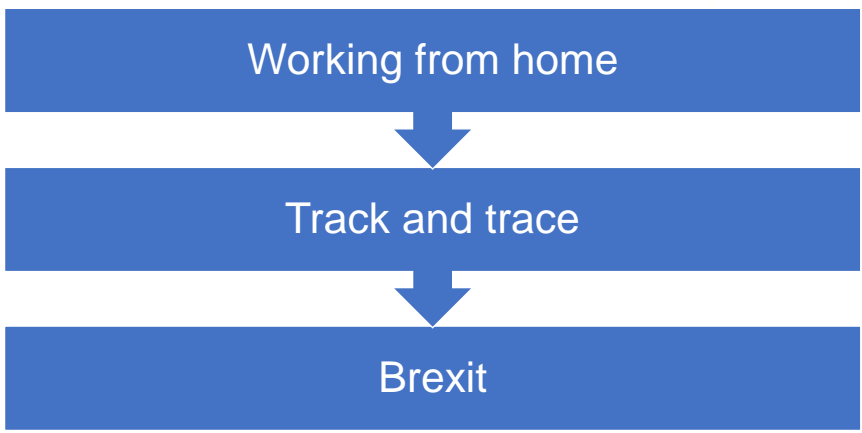


- Take care when sharing data, internally or externally
 - Who can you share it with?
 - Is the method secure (passwords/encryption/courier etc)?
 - With group emails, use Bcc and beware autofill / forward!
- If taking data out of office, is it secure?
 - Consider devices/papers/USB sticks/leaving overnight etc
- Dispose of data securely once you no longer need it
- If there's a breach, **MUST** report to ICO within 72 hrs!
 - Ensure all staff/volunteers are trained to identify and flag

@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    





11

Recent developments





```


graph TD
    A[Working from home] --> B[Track and trace]
    B --> C[Brexit]
  
```

@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

12







Working from home




Consider:

- **Potential IT security risks that can occur**
 - What policies/procedures/guidance/training do you have in place to help staff work in a compliant way?
 - → [ICO's top 10 tips for staff to follow](#)
- **Who supplies device/software being used? You/staff?**
 - Understand risks and benefits of both
- **Video conferencing**
 - Privacy/security settings? Are you using a safe VC tool with clear data processing terms?

→ See my infographics for further links to ICO guidance

@ tyfucymru@lantra.co.uk
www.tyfucymru.co.uk
Find us on:    

13





Contact tracing



If you need to gather details for contact tracing:

- **Only collect and use what is necessary**
 - Keep data to a minimum – just gather what you really need to implement measures effectively
- **Be transparent with individuals (staff, customers etc)**
 - Explain why you are collecting data / what you will use it for
- **Treat people fairly and ensure they can exercise rights**
- **Carefully store data**
- **Don't use it for other purposes – e.g. marketing**
- **Erase it securely in line with govt guidance**

→ See infographics for links to ICO guidance/case studies

@ tyfucymru@lantra.co.uk
www.tyfucymru.co.uk
Find us on:    

14

€ Brexit



There will now be EU GDPR and UK GDPR

- Brexit trade deal means **data can flow freely for now**
- Waiting to see if Euro Commission will grant UK '**adequacy**'
- If granted adequacy, no need for additional safeguards when data is transferred between EEA countries and UK **businesses**
- Now have up to **6 month 'interim period'** from 1st Jan 2021 for adequacy to be granted
- Some organisations need to appoint an **EU representative**
- **If you comply with UK GDPR you'll also comply with EU GDPR 😊**

→ <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/dp-transition-small-orgs/>

@ tyfucymru@lantra.co.uk

www.tyfucymru.co.uk

Find us on:

15

Useful tools from ICO



▪ [Self assessment checklist for small businesses](#)

Answer questions and get a short report to help identify areas you may need to work on.

▪ [Accountability Framework](#) and [self assessment](#)

ICO encourages all businesses to adopt a risk-based approach. Self assessment tool helps you see how your organisation is currently meeting ICO's expectations in relation to accountability.


@ tyfucymru@lantra.co.uk

www.tyfucymru.co.uk





Find us on:

16

Summary of steps to being GDPR compliant



- Be **open and clear** with people about what will happen to their data if they give it to you: explain this to them if necessary
- **Share data safely and responsibly**: stop to think if unsure
- Use **strong passwords** and/or **encryption**
- **Only take what you really need** out of the office and **keep it safe**
- If relying on **consent**, ensure you have **proof / record of 'opt in'**
- Ensure you deal with any **consent withdrawals** or other requests relating to a person's **rights** (e.g. request to erase data)
- Be familiar with procedure to deal with any **data breaches** or **Subject Access Requests**.








@ tyfucymru@lantra.co.uk www.tyfucymru.co.uk Find us on:    

17

Thank you!

www.annabezodis.com

Find us on:

18