Embracing GDPR

Taking a common sense approach and looking to the future.

Stacey Egerton & Gill Dickson
Policy & Engagement (Public Services)

ico.
Information Commissioner's Office

Outline

- Introduction
- Myth busting quiz – true or false
- Key messages
- Data processing activity
- What are your concerns?
- Feedback and discussion

Introduction

Don't need a DPO....

But still need to comply with the law.

Myth Busting

True

False

Question 1

Councillors do not need to pay a data protection fee?

(it depends)

Data protection fees

- Data controllers have to pay a data protection fee unless they are exempt (**The Data Protection (Charges and Information) Regulations 2018**)
- **Data controller** = determines the purposes and means of processing personal data.
- **Local council** is a data controller and will need to pay the fee
- **Councillors** – most of their duties will be undertaken on behalf of the council and covered by the councils DP fee.
- **HOWEVER** – where councillors are undertaking constituent casework (e.g. taking forward complaints made by their local residents) likely they will be a controller in their own right and need to pay a data protection fee (Tier 1 - £40)

https://ico.org.uk/media/for-organisations/documents/2259094/dp-fee-guide-for-controllers-20180601.pdf

Question 2

A local council does not need to keep personal data indefinitely?

(true)

Retention/storage limitation

- Article 5(1)(e) personal data shall not be kept for longer than is necessary
- Should periodically review the information you hold and delete or anonymise it when you no longer need it
- Should have a retention policy in place setting out how long you will keep information for and your justifications for this – will need to take into consideration any statutory requirements around retention.
- Keeping information 'just in case' is unlikely to be a sufficient justification

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

Question 3

All data breaches must be reported to the ICO?

(false)

Not every data breach needs to reported

Best way to report a breach is over the phone

72 hours

- Only applies to personal data breaches as per the definition in GDPR (Art 4(12)
- Only reportable where it is likely there is a risk to people's rights and freedoms
- **0303 123 1113 – Mon-Fri 9am-4:30pm**
- 72 hours – includes evenings/weekends/bank holidays (not just working hours)
- It is not a 72 deadline to just get in contact with the ICO - It's 72 hours, where feasible, to provide the information set out at Article 33 of the GDPR.

ico.
Information Commissioner's Office

Question 4

Consent is not always needed to share personal data?

(true)

Lawful Basis for Processing – consent is not the only one

- Consent
- Contract
- Legal obligation
- Vital interest
- Public task
- Legitimate interest

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Question 5

It is mandatory for all councillors and clerks to undertake data protection/GDPR training? *(false)*

Not mandated by GDPR/DPA 18....

BUT some organisations make GDPR training mandatory for staff

Accountability

Can you show how you are complying with the law?

ico.
Information Commissioner's Office

Thanks for your time today!

Get in touch

Talk to our advice services team via our:

- **Live chat** at ico.org.uk; or
- call our **helpline** on
- 0303 123 1113.

Keep in touch

- Subscribe to our **monthly e-newsletter** at www.ico.org.uk
- **Follow us** on:

@iconews

/iconews

YouTube

LinkedIn

ico.
Information Commissioner's Office