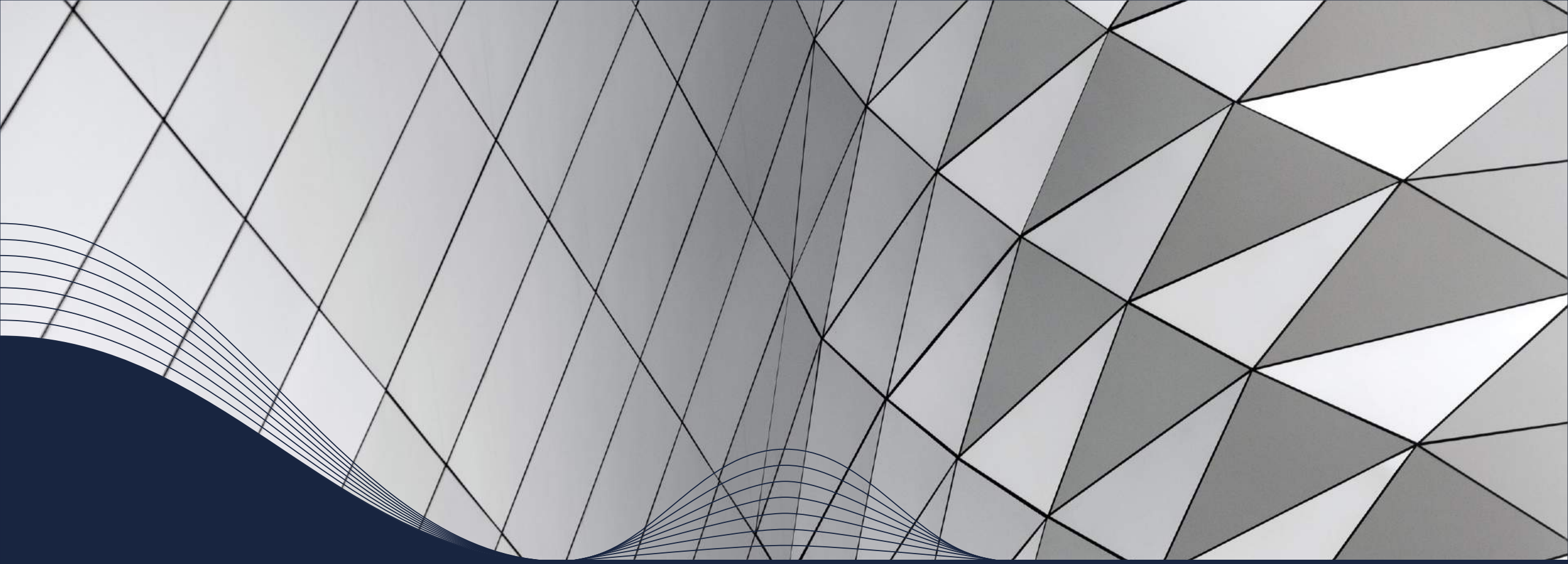


Refugee Action – Cyber Security and the GDPR

Training Session – Tuesday 9 June 2020

DLA PIPER

Agenda

1. Introductions
2. eSignatures
3. GDPR Principles
4. Cyber Security and Remote Working – Practical Tips
5. Questions

Eilís McDonald
Associate
+353 1 436 5450
eilis.mcdonald@dlapiper.com

Ataikor Ngerebara
Associate
+44 (0)20 7349 0296
ataikor.ngerebara@dlapiper.com

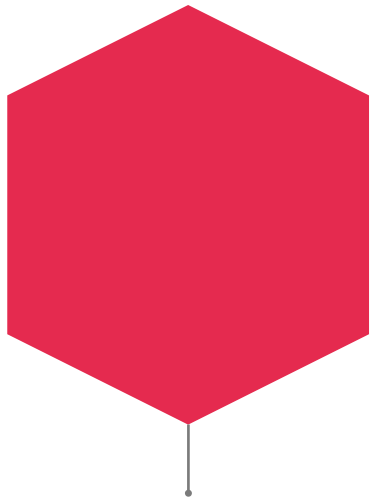
Cezary Bicki
Associate
+353 877 181 602
cezary.bicki@dlapiper.com

Introductions and Icebreakers

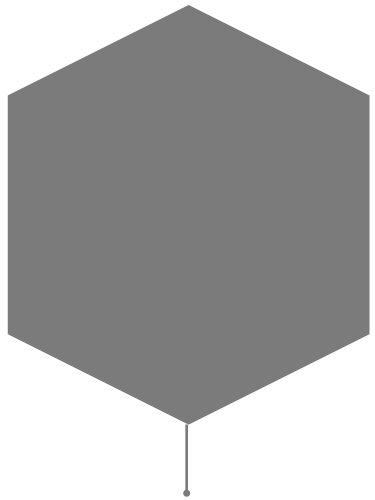
E-signatures

Cez Bicki – Key issues and practical tips

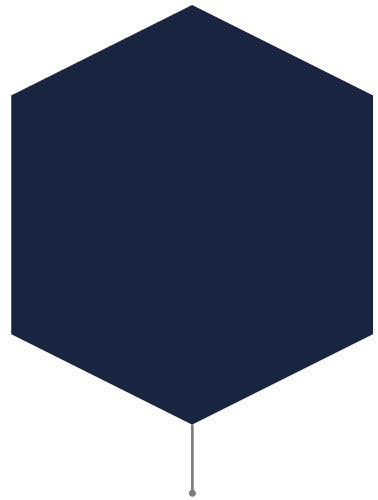
Electronic signatures: what do they include?



A person typing his/her name into an electronic version of a contract/deed



A person electronically pasting his/her signature (eg in the form of an image) into an electronic version of a contract/deed



The use of a web-based e-signature platform (eg Docusign) where the person clicks to have his/her name automatically inserted in the electronic version of the contract/deed

Electronic signatures: are they valid?

- An electronic signature can be used to validly execute deeds and other documents provided that:
  - the signatory intends to be bound by the document; and
  - any formalities relating to the execution of that document are satisfied (eg any formalities required under statute such as witnessing)
- It is legally possible to witness an electronic signature, but:
  - the witness must be physically present; and
  - video witnessing is not permitted
- Execution procedures similar to those set out in slides 7 and 8 should still be followed (eg for deeds and real estate contracts, only the complete, final versions of the documents should be circulated for electronic signature)

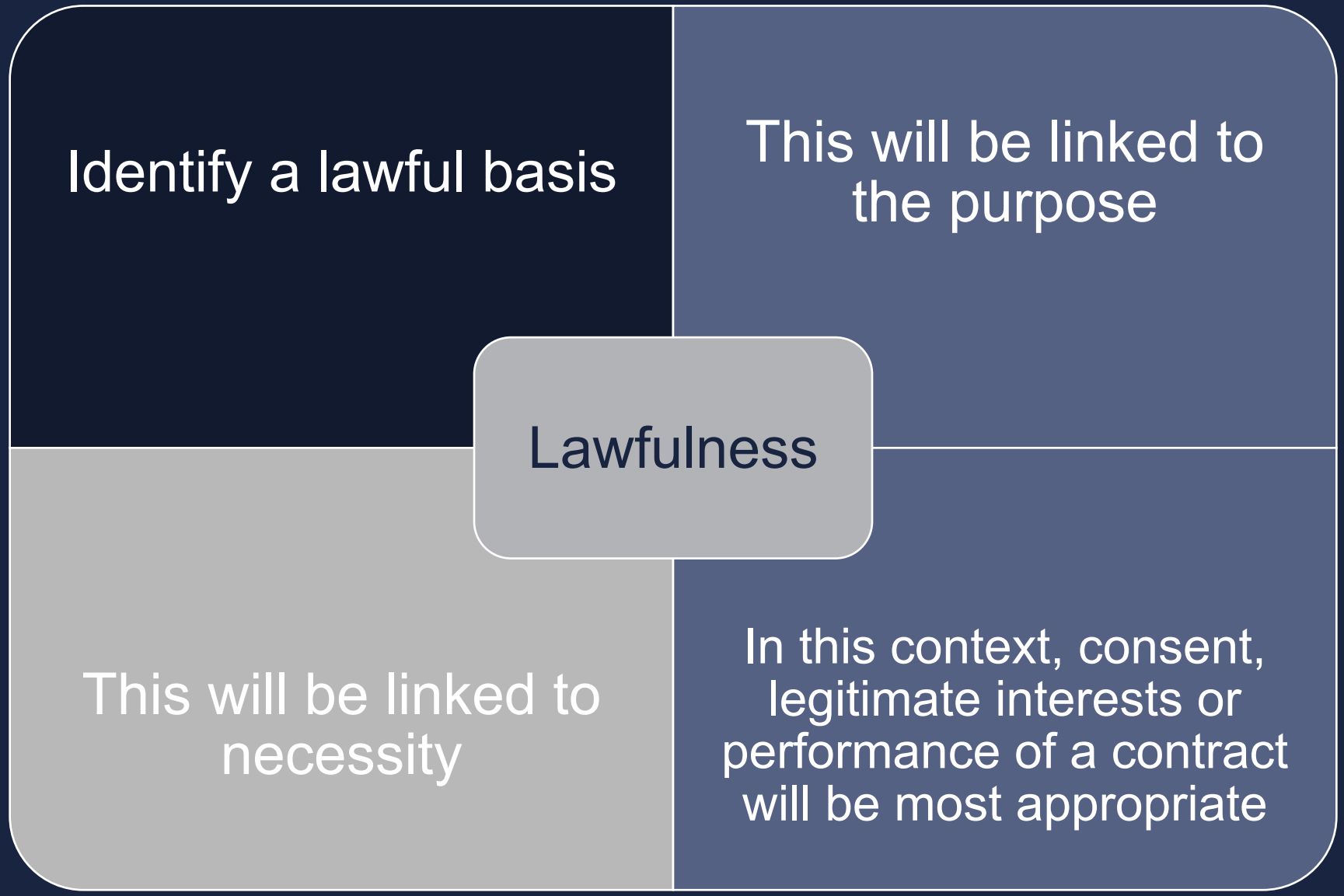
Electronic signatures: when they may not be appropriate

- Electronic signatures may not be appropriate:
  - if the document needs to be filed with an authority or registry (eg Land Registry, Stamp Office) which won't accept electronic signatures
  - if the place of signature or the location of the document has particular legal consequences (eg for stamp duty purposes)
  - if the signing party doesn't have the corporate capacity or authority to execute the document by electronic signature (eg there are restrictions in the constitutional documents)
  - if the signing party is using its common seal
  - if the document needs to be executed in front of a notary
  - if the transaction is cross-border in nature – you will need to check if the electronic signature of the document enables its recognition, registration or enforcement in the relevant jurisdictions

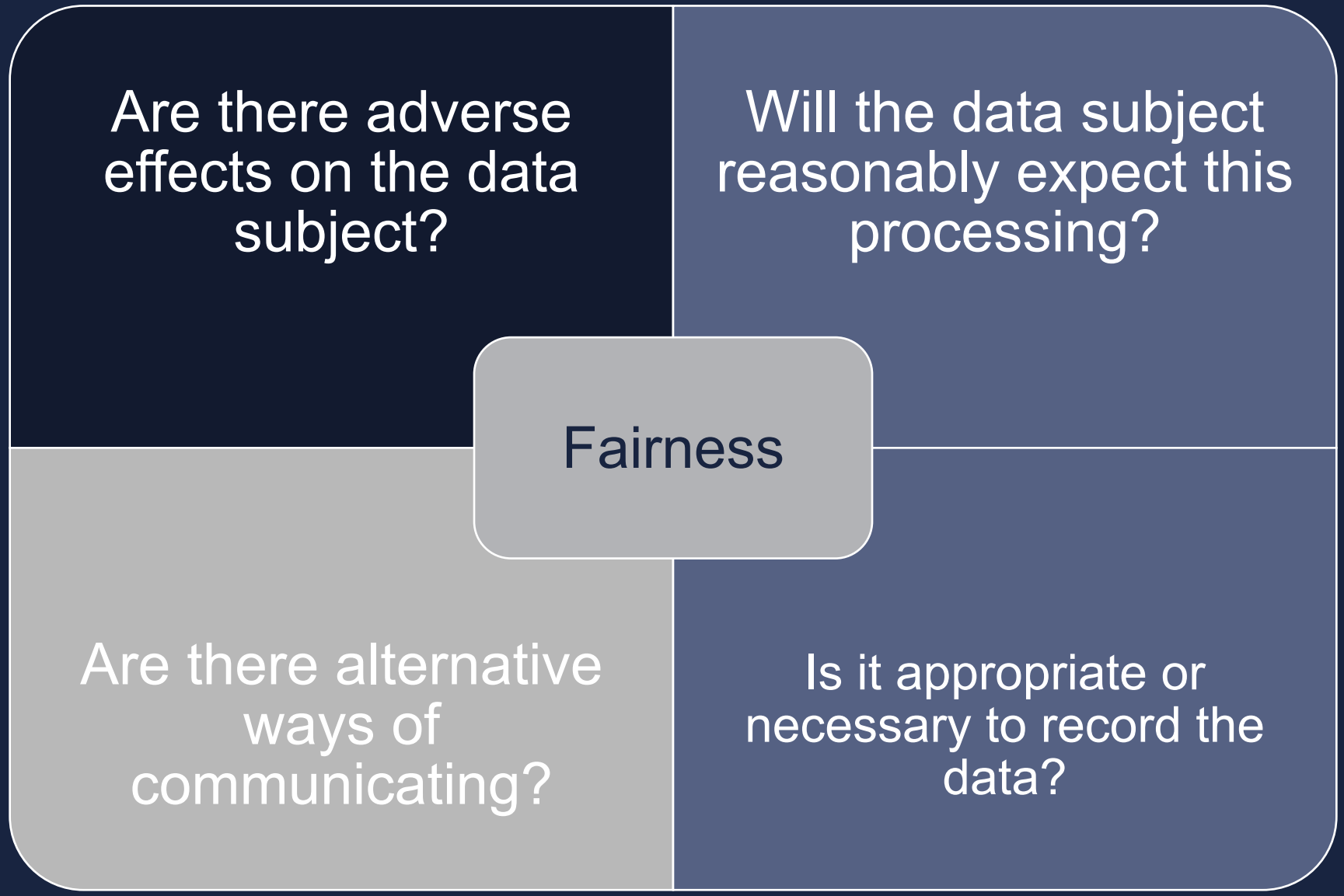
GDPR Principles

Recap

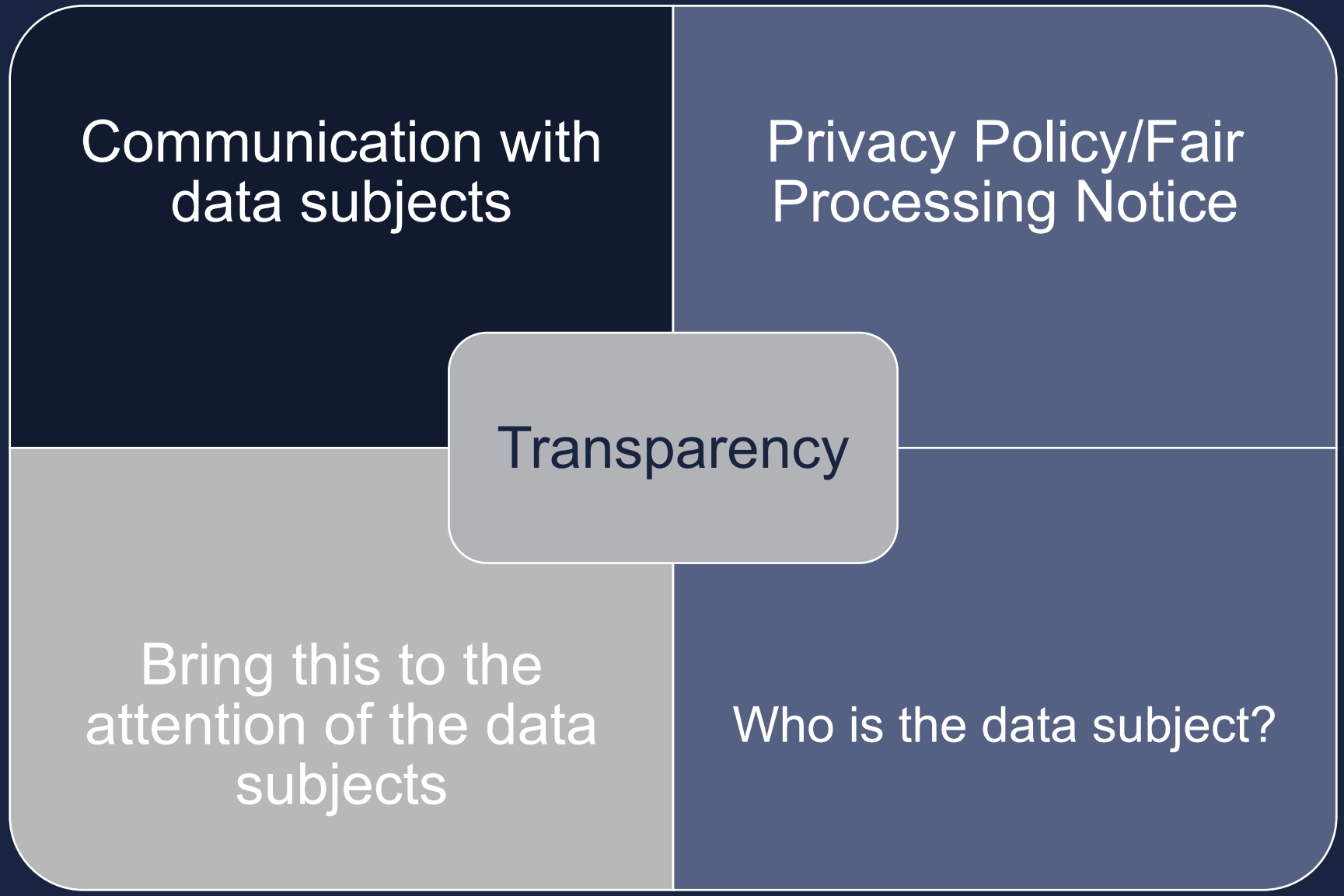
1. Lawfulness, Fairness and Transparency



1. Lawfulness, Fairness and Transparency



1. Lawfulness, Fairness and Transparency



2. Purpose Limitation

- Clearly identify the purpose or purposes for processing
- Any changes in the purposes will trigger an update to the records of processing and the privacy notices.

3. Data Minimisation

- What is the minimum amount of personal data you need to process to achieve your purpose?
- Hold that information, but no more.
- This links to necessity – what do you really need to collect and retain to achieve your purpose?

4. Accuracy

- Take reasonable steps to ensure the accuracy of any personal data which you collect.
- Record the source of the personal data – consider whether the source is reliable.
- Are there challenges to the accuracy of the personal information?
- Does the personal data require regular updating?

5. Storage Limitation

- Do you actually need to store the data?
- If so, how long are you storing it for?
- Regularly review data which you hold and assess whether it is still necessary to retain.
- Remember right of erasure.

6. Integrity and Confidentiality

- Key focus for remote working – building in security
- Where do the risks lie?
- What measures do you currently have in place to protect personal data?
- The chosen and implemented measures must ensure the confidentiality, integrity and availability of your systems and services and the personal data.

7. Accountability

- How can you demonstrate compliance?
- Agree a risk appetite and regularly review this. You must decide what risks are relevant and what measures are appropriate for the processing you undertake, then document and regularly review this.
- Document processing activities – have you considered the principles?

Coffee Break

Cyber Security and Remote Working – Practical Tips

What do the principles mean in practice?

1. Devices

Make sure to keep any work devices in a safe location, and ensure they are locked if unattended for any reason. Devices should be turned off when not in use.

Ensure all devices are password protected. Multifactor authentication is a good way of ensuring device security.

Identify a space to have confidential conversations /calls.

1. Devices

If you are living in shared accommodation, consider using a privacy screen if your laptop can be viewed by others while working.

Do not use social media for any official business. If using social media for any non-work reason, make sure work related information doesn't feature in any posts or message.

Make sure you know which devices are connected to your home network, and make sure each of them is secure by enabling automatic updates on them.

Where possible, carry out your work using your organisation's trusted network or cloud service.

Email

- Be extra vigilant when sending emails
- Ensure you do not overshare any personal information
- Do not attach extra or incorrect attachments
- Do you have the right recipient?

Phishing

If you receive an unusual or unexpected email or message, you should:

- **check the senders address/number;**
- **consider whether the sender is prompting you to click any links or attachments in the message/email;**
- **consider whether the content communicates a sense of urgency, prompting you to act irrationally;**
- **and be very suspicious of any phone call or message which purports to be from an official organisation, especially if it asks for your credentials**

This Photo

CC BY-SA

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

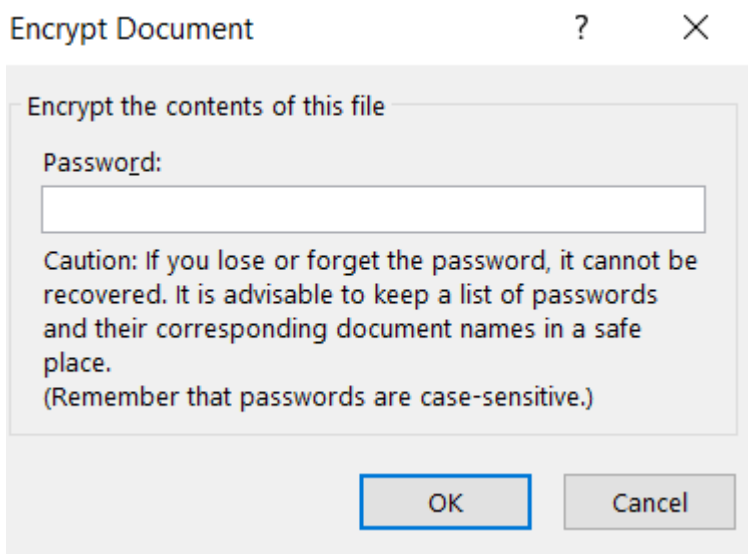
This Photo by Unknown Author CC BY-SA

Encryption

Password protect all documents which contain personal data/ sensitive advice.

You can add a password to any document by clicking file -> protect document.

Here, you can select access restrictions, encrypt the document with a password, or lock the document so that the details cannot be amended.



Video Conferencing – Practical tips

Where not all participants need to be recorded or use the video function, **limit the recording** or use of video function to only those participants for which it is necessary e.g. the presenter at an event.

In most cases, use of video conferencing tools for events or meetings should not adversely affect the data subject.

Where an **alternative e.g. audio option** is available and can serve the same purpose, this should be provided to the data subjects.

Necessity - aim to use the **least privacy-invasive methods by default.** Video functions on calls should be turned off by default, with the option of turning the camera on if desired.

Not every individual is comfortable with video conferencing and such **individuals should therefore be provided with options** that will be considered less intrusive.

Video Conferencing – Practical tips

If the **lawful basis** for processing the data is consent, you will need to reconsider your normal approach to obtaining this consent.

Default settings on devices and/or installation of software that facilitate the electronic personal data processing cannot qualify as consent, since consent requires an active expression of will.

If the individual needs to **download a tool or app f**or the video call, direct them to the relevant privacy notice (Zoom privacy policy, for example).

If you normally get a **consent** form signed you may now need to gain this over video conference.

Do not record individuals on videoconferences where they have not been informed that the conference would be recorded or that their participation would be recorded.

Instant Messaging

Do not use social media for communication. Where possible, avoid using instant messaging for communication.

This type of service is susceptible to cyber-attack and can be used for wholesale extraction of data and insertion of malware into targeted devices.

Data passing through these applications are vulnerable to surveillance and censorship, and there are risks involved with using them including ensuring that information in messages remains confidential.

Always consider whether there is an alternative way of communication – a phone call with note taking.

Questions

Resources

ICO Website - https://ico.org.uk/

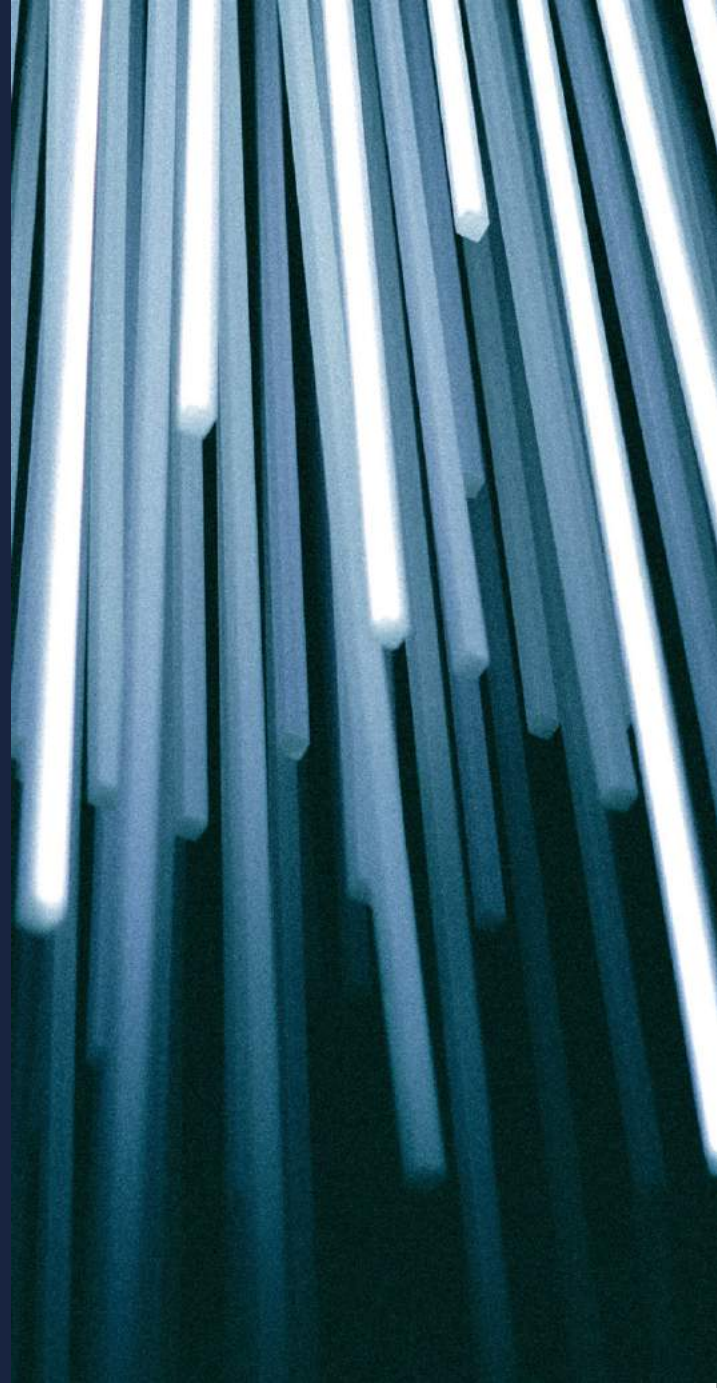
ICO – A Practical Guide to IT Security - https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

National Cyber Security Centre – Small Business Guide (includes tips on backups, protecting from malware, device security, passwords and phishing) https://www.ncsc.gov.uk/collection/small-business-guide

Guide to Encryption - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-is-encryption/

Templates

1. Records of Processing - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/
2. Privacy Notice - https://ico.org.uk/for-organisations/business/create-a-privacy-notice/



Thank you