Data Protection Webinar

10th October 2023

Speaker: David Taylor, Data Protection Consultancy Limited

hospice UK

David Taylor

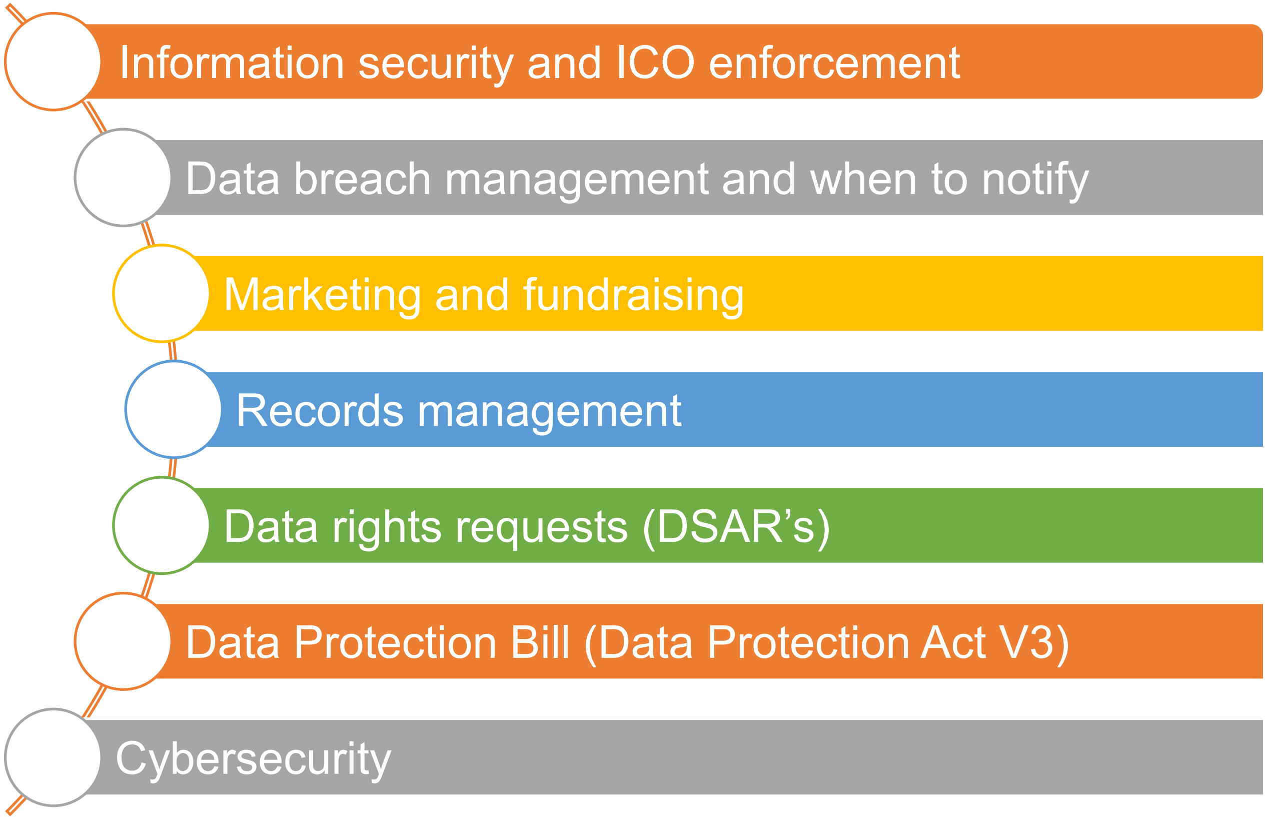
Hospice UK

October 2023

Data Protection Act 2018 (UK GDPR)

Please ask questions at any time

Some of what we will be covering



- Information security and ICO enforcement
- Data breach management and when to notify
- Marketing and fundraising
- Records management
- Data rights requests (DSAR's)
- Data Protection Bill (Data Protection Act V3)
- Cybersecurity

Quick update last 12 months

Data Protection Bill

Data Protection Act version 3 on its way maybe later this year. Is designed to remove red tape and make the life of data controllers and business easier

Breach reporting

Only significant breaches must be reported to the ICO, the ICO appear to be taking a sensible approach to what should be reported.

Fines

The ICO continue to focus on cybersecurity and marketing breaches these have accounted for most action in last few years

Data Controller

Hospice is the data controller of patient and staff data and ultimately responsible. However employees and volunteers can be held responsible if they use data in deliberately and malicious way.

Data rights

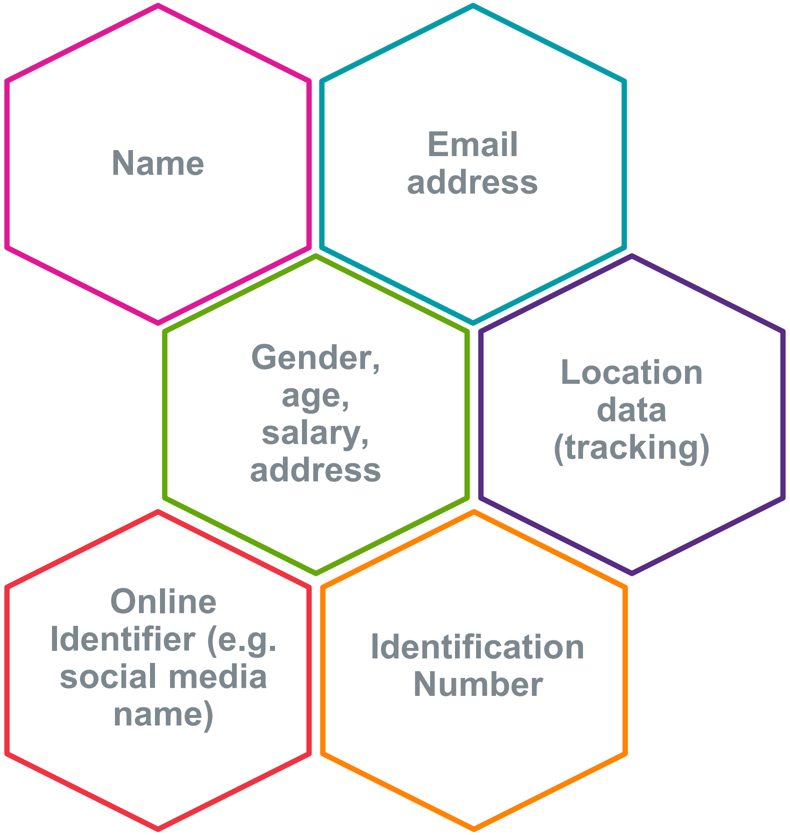
Steady increase in SAR's and deletion requests as was expected. The ICO are enforcing the 30/21 day rules and blocking charging for large requests

Codes of Practice

New statuary (enforceable) codes of practice written by the ICO for marketing, ePrivacy, data sharing, CCTV, children's data and HR with more on the way

What types of data are protected

Personal Data (includes "work" data)
Information from which a living person ('data subject') is identified or identifiable.



Name

Email address

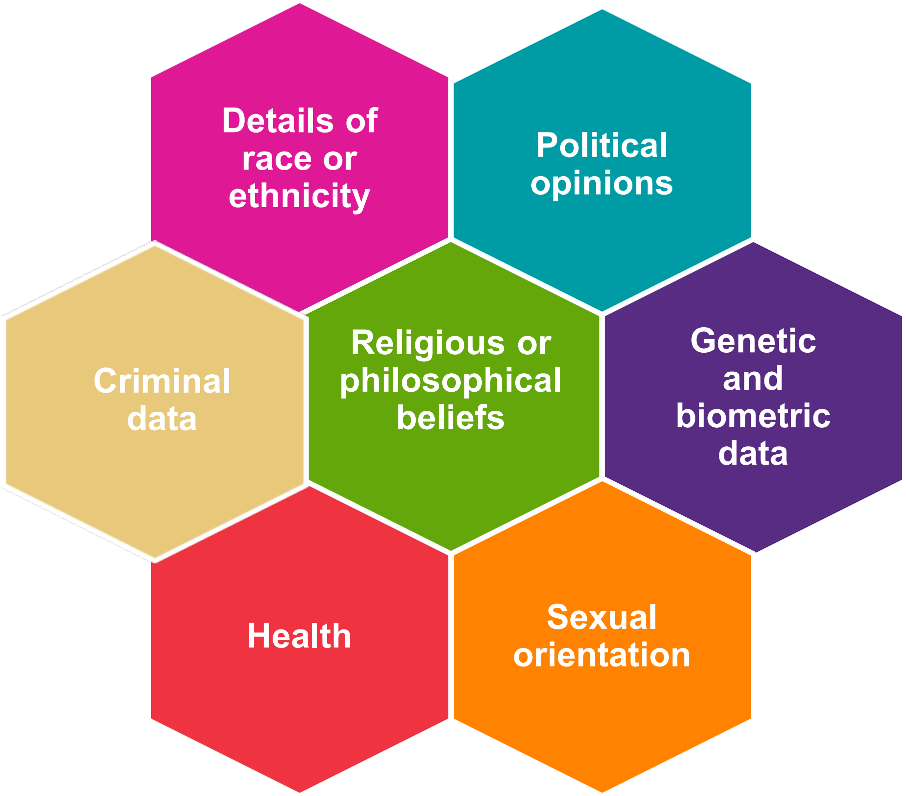
Gender, age, salary, address

Location data (tracking)

Online Identifier (e.g. social media name)

Identification Number

Special Categories of Personal Data
Personal Data that is particularly sensitive (e.g. health information)



Details of race or ethnicity

Political opinions

Criminal data

Religious or philosophical beliefs

Genetic and biometric data

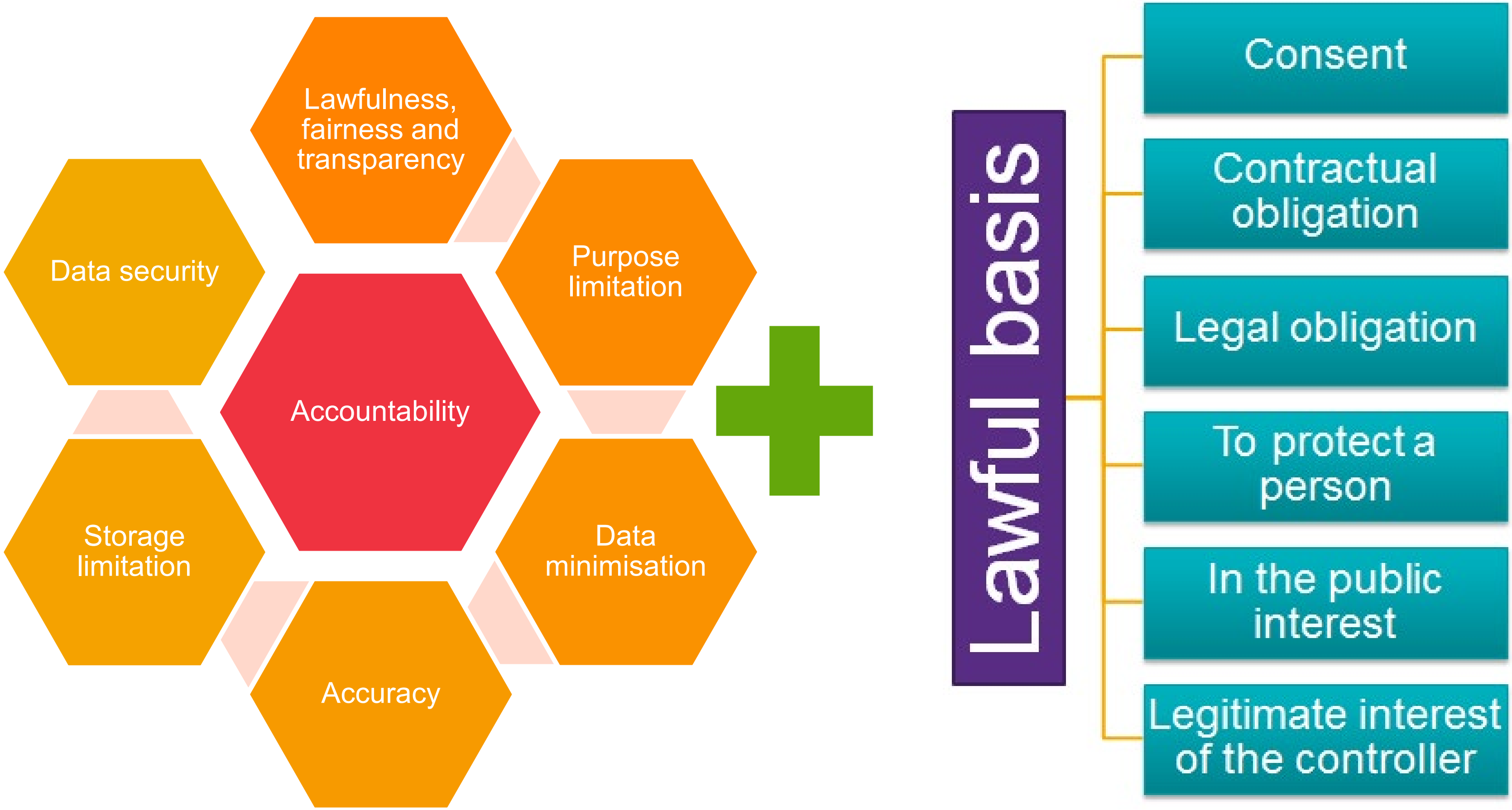
Health

Sexual orientation

Principles and lawful processing

Principles

Basis



Lawfulness, fairness and transparency

Purpose limitation

Data security

Accountability

Storage limitation

Data minimisation

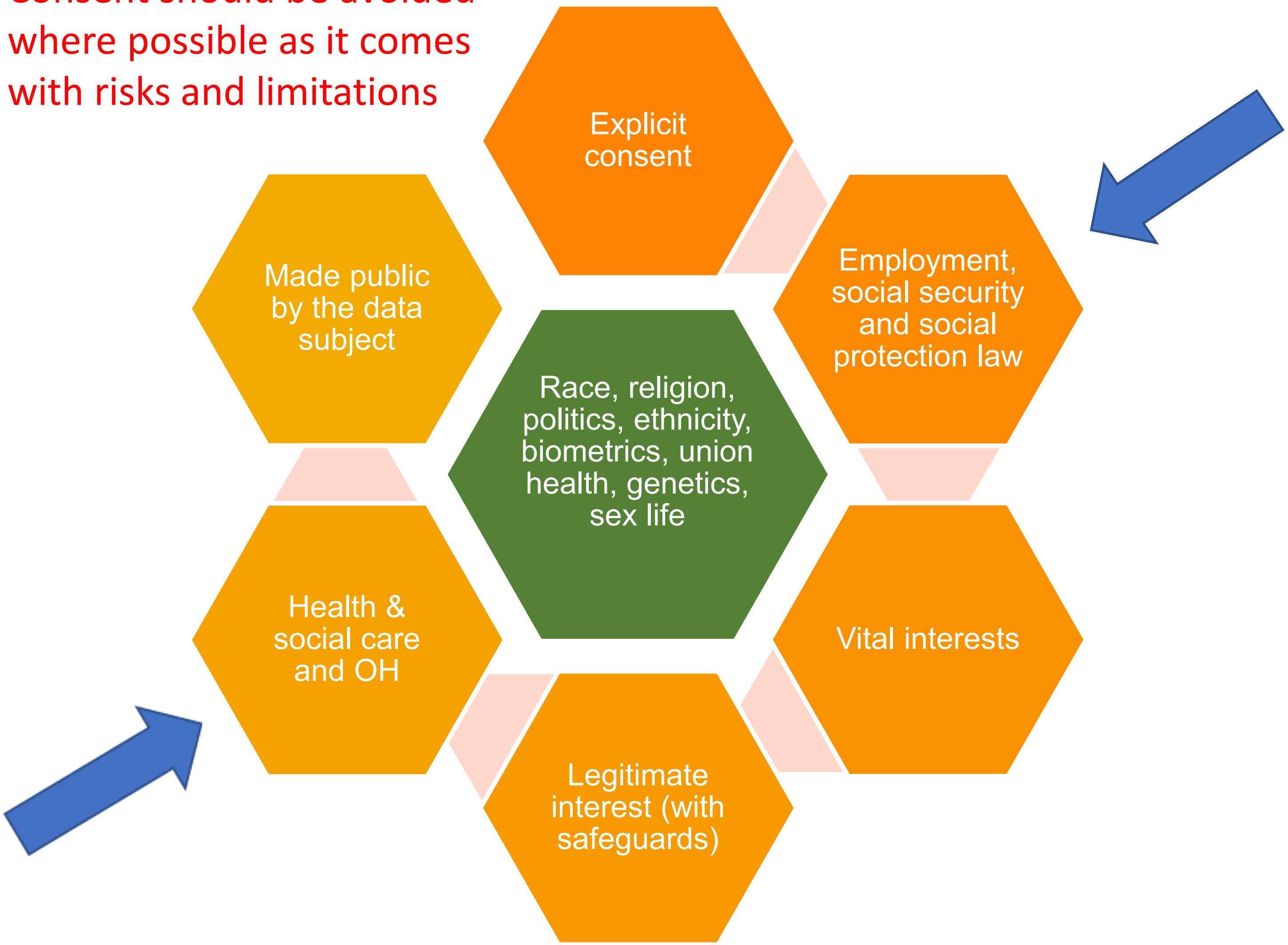
Accuracy

Lawful basis

- Consent
- Contractual obligation
- Legal obligation
- To protect a person
- In the public interest
- Legitimate interest of the controller

Processing special category data (sensitive)

Consent should be avoided where possible as it comes with risks and limitations



Explicit consent

Employment, social security and social protection law

Vital interests

Legitimate interest (with safeguards)

Health & social care and OH

Made public by the data subject

Race, religion, politics, ethnicity, biometrics, union health, genetics, sex life

Accountability – evidence how you comply

Accountability

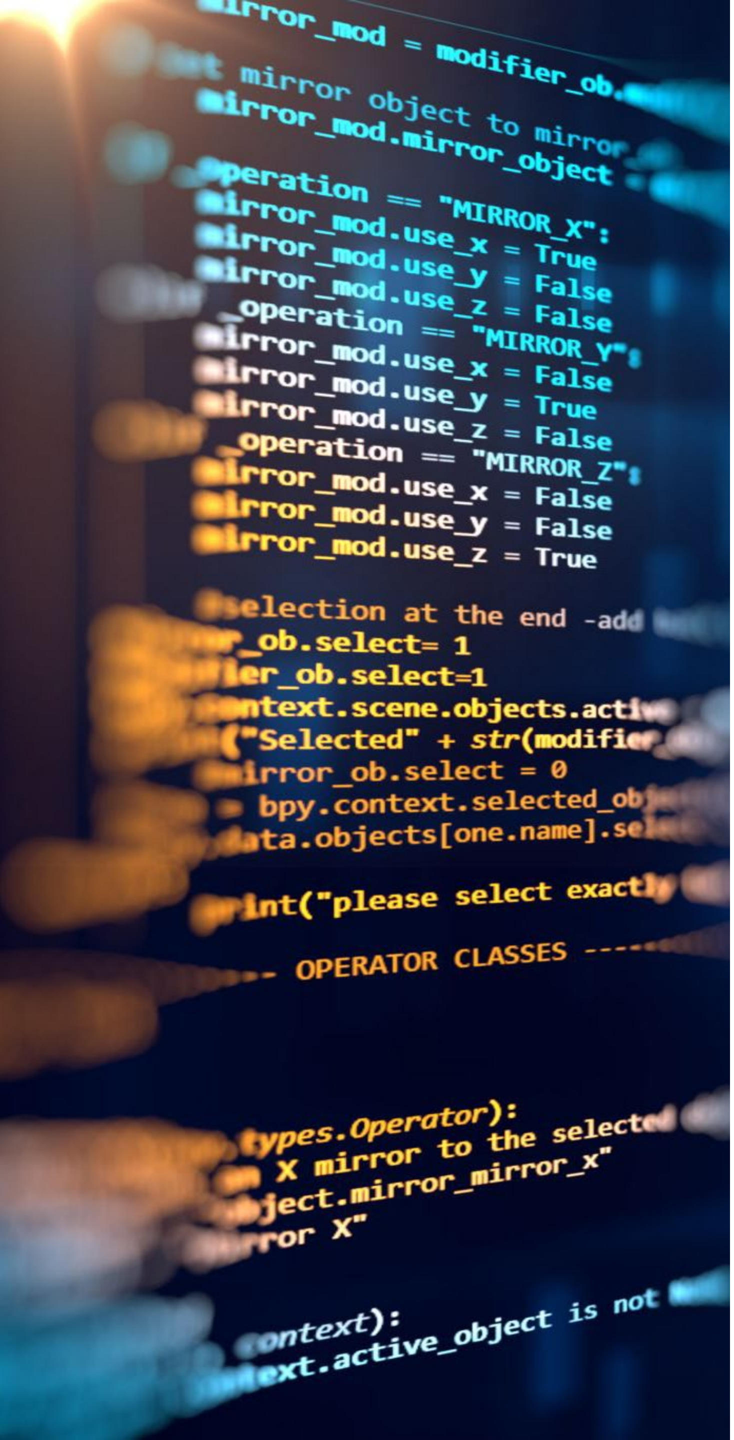
Just being compliant is no longer enough.

You must demonstrate how you comply by implementing:

- **Policies**
- **Operational procedures**
- **Training**
- **Audit of the above**

How to evidence accountability (compliance)

- Regular staff training (DP and Cyber Security every year) – include a quiz
- Policies and procedures (and make sure we all read them)
- Try and make systems disaster proof
- Use DPIA’s to show you are processing sensitive data responsibly
- Records management – keeping everything electronically is a good start
- Periodically review systems, policies and procedures (audit)
- Transparency (make sure data subjects can access privacy notices)
- Make sure we all know what to do in the event of a data breach
- Respect data subjects information rights



```
irror_mod = modifier_ob
 mirror object to mirror
irror_mod.mirror_object
operation == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
 operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
 operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
 _ob.select= 1
 er_ob.select=1
 ntext.scene.objects.active
 ("Selected" + str(modifier
 irror_ob.select = 0
 bpy.context.selected_obj
 ata.objects[one.name].se

 int("please select exactly

 -- OPERATOR CLASSES ----

 types.Operator):
  X mirror to the selected
 ject.mirror_mirror_x"
 ror X"

 context):
 ext.active_object is not
```

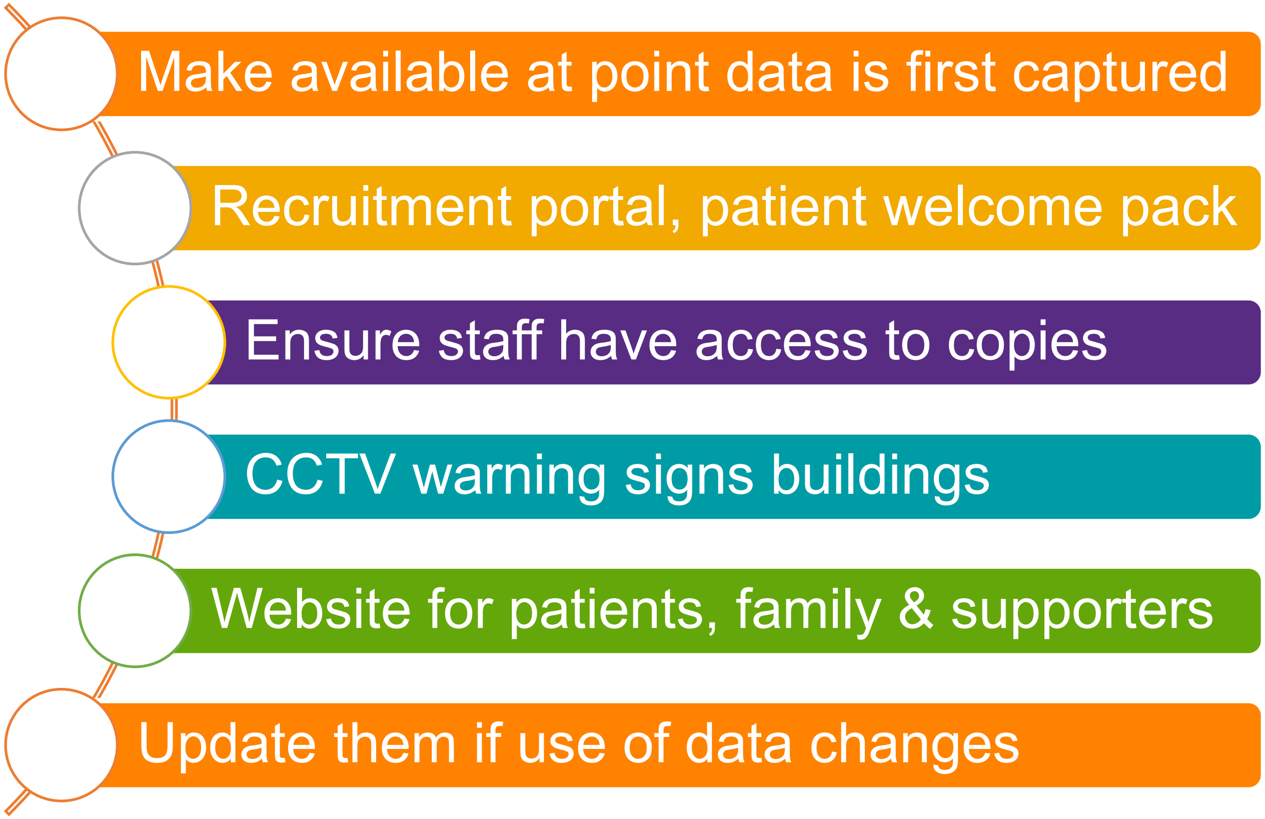
Data Protection and Information Security Policies

- **Data Protection and Information Security Policies**
  - Provide guidance on day-to-day management of data
  - **Essential that everyone reads them**
  - In the event of a data breach ICO will ask when you last read the policy
- **Data Retention Schedule**
  - Retention times for all categories of data
- **Other polices covering breach, rights requests etc**
- **Employee and patient privacy notices**
  - Detailed information on how the organisation uses employee and patient data. Everyone should familiarise themselves with them and notify the DPO if they feel they are no longer accurate. Note: - new projects using data may require privacy notices to be updated.

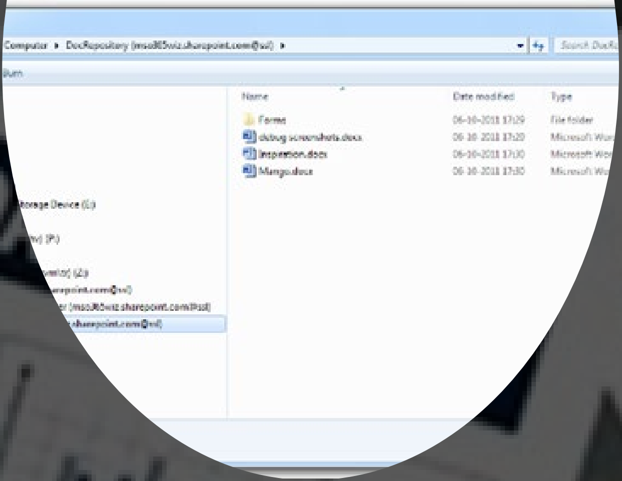
What must be included in a privacy notice

- Identity of the data controller
- Purpose of the processing and legal basis
- Categories of the personal data
- Any recipients including processors
- Retention period
- Data subjects rights
- Source you obtained data from (eg public domain)
- Any negative outcome by not consenting to the processing
- Any automated decision making

Use and publication of privacy notices



- Make available at point data is first captured
- Recruitment portal, patient welcome pack
- Ensure staff have access to copies
- CCTV warning signs buildings
- Website for patients, family & supporters
- Update them if use of data changes



```
Computer ▸ DocRepository (msoll05wiz.sharepoint.com@ssl) ▸                 Search DocR

Name                           Date modified       Type
Forms                          06-10-2018 17:29    File folder
debug screenshots.docx         06-10-2018 17:29    Microsoft Wor
Inspiration.docx               06-10-2018 17:30    Microsoft Wor
Mango.docx                     06-10-2018 17:30    Microsoft Wor

torage Device (G:)
ive) (P:)
ewstor) (Z:)
harepoint.com@ssl)
er (msoll05wiz.sharepoint.com@ssl)
.sharepoint.com@ssl)
```

Data security and enforcement

Information Security – on site

- Who can hear your phone call
- Who are you really talking to
- Do they really need to know
- Who can see your PC screen (privacy filter)
- Where does your waste paper end up
- What information is in on your desk or in-tray

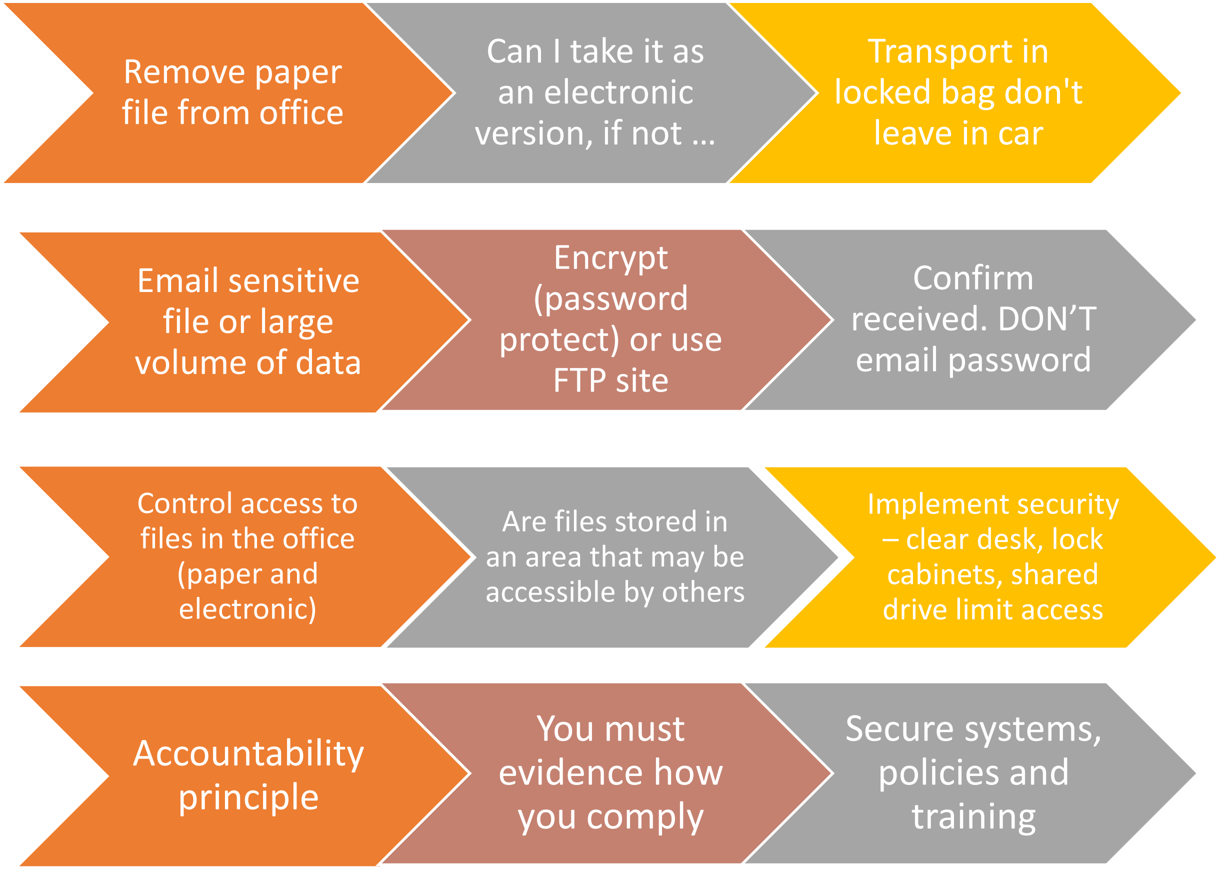
Information Security – on site

- Disable email address caching
- Lock filing cabinets – keep secure at home
- Punch code lock to ward office door
- Always screen lock PC - ALWAYS
- Use strong passwords and never share
- Working from home risks

Information Security – domiciliary services

- Paper records must be transported securely
- Use technology where at all possible
- Risks of staff using own phone (BYOD)
- Family access to electronic records
- Encrypt all technology including BYOD
- Policies and procedures to govern above

Data security



Remove paper file from office

Can I take it as an electronic version, if not …

Transport in locked bag don't leave in car

Email sensitive file or large volume of data

Encrypt (password protect) or use FTP site

Confirm received. DON’T email password

Control access to files in the office (paper and electronic)

Are files stored in an area that may be accessible by others

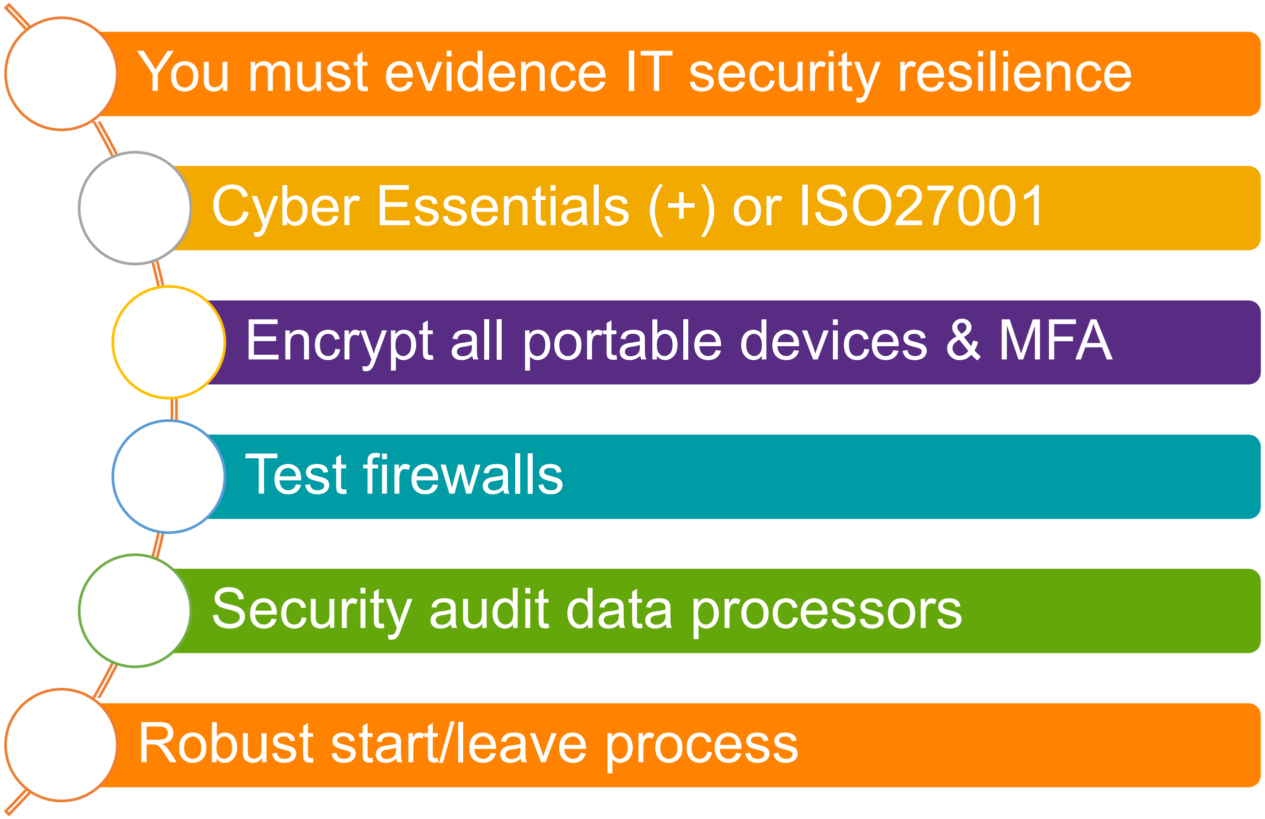
Implement security – clear desk, lock cabinets, shared drive limit access

Accountability principle

You must evidence how you comply

Secure systems, policies and training

Information Security – technology



You must evidence IT security resilience

Cyber Essentials (+) or ISO27001

Encrypt all portable devices & MFA

Test firewalls

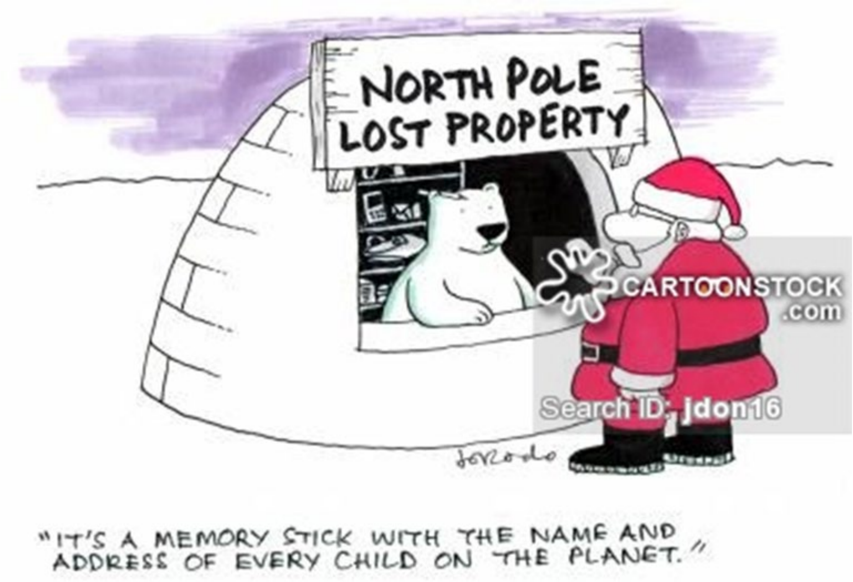
Security audit data processors

Robust start/leave process

Data breaches

Obligation to notify the ICO of a personal data breach

Fine: up to £17 million or 4 per cent of your global turnover

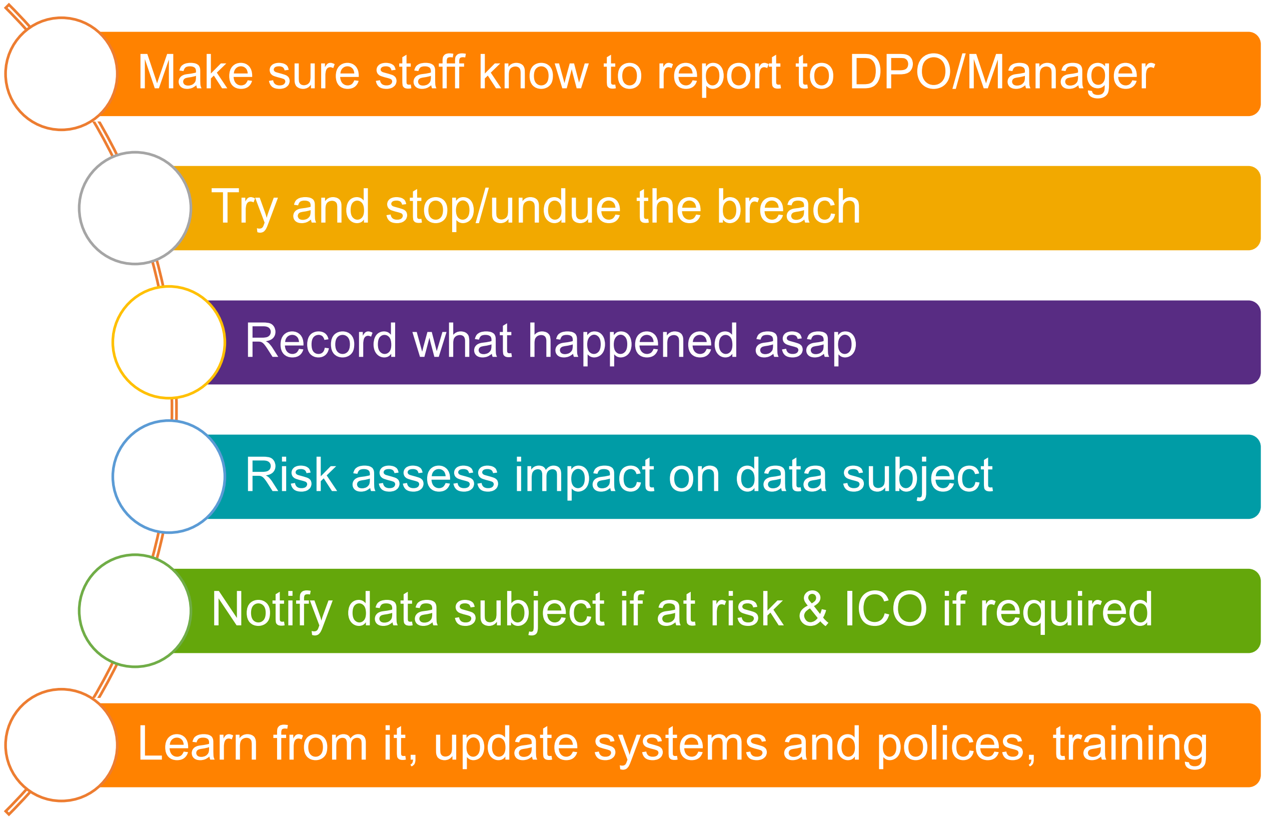

NORTH POLE
LOST PROPERTY
CARTOONSTOCK .com
Search ID: jdon16
"IT'S A MEMORY STICK WITH THE NAME AND ADDRESS OF EVERY CHILD ON THE PLANET."

Controller to notify:

- **The ICO** within 72 hours if it is likely to result in a risk to the rights and freedoms of individuals and significant detrimental effect on individuals e.g. potential for identity theft etc.
- **Affected individuals** without undue delay if it is likely to result in a high risk to the rights and freedoms of individuals.

In the event of any data breach where the Hospice is a joint data controller (commissioned services) there may be an obligation to notify the other party (NHS or local authority).

What to do if you have a breach



- Make sure staff know to report to DPO/Manager
- Try and stop/undue the breach
- Record what happened asap
- Risk assess impact on data subject
- Notify data subject if at risk & ICO if required
- Learn from it, update systems and polices, training

Disaster recovery (business continuity) plan – do you have one?

Covid was a good test of the ability to continue working in a disaster

What happens when the lights go off?

--- Do you have offline access to critical records

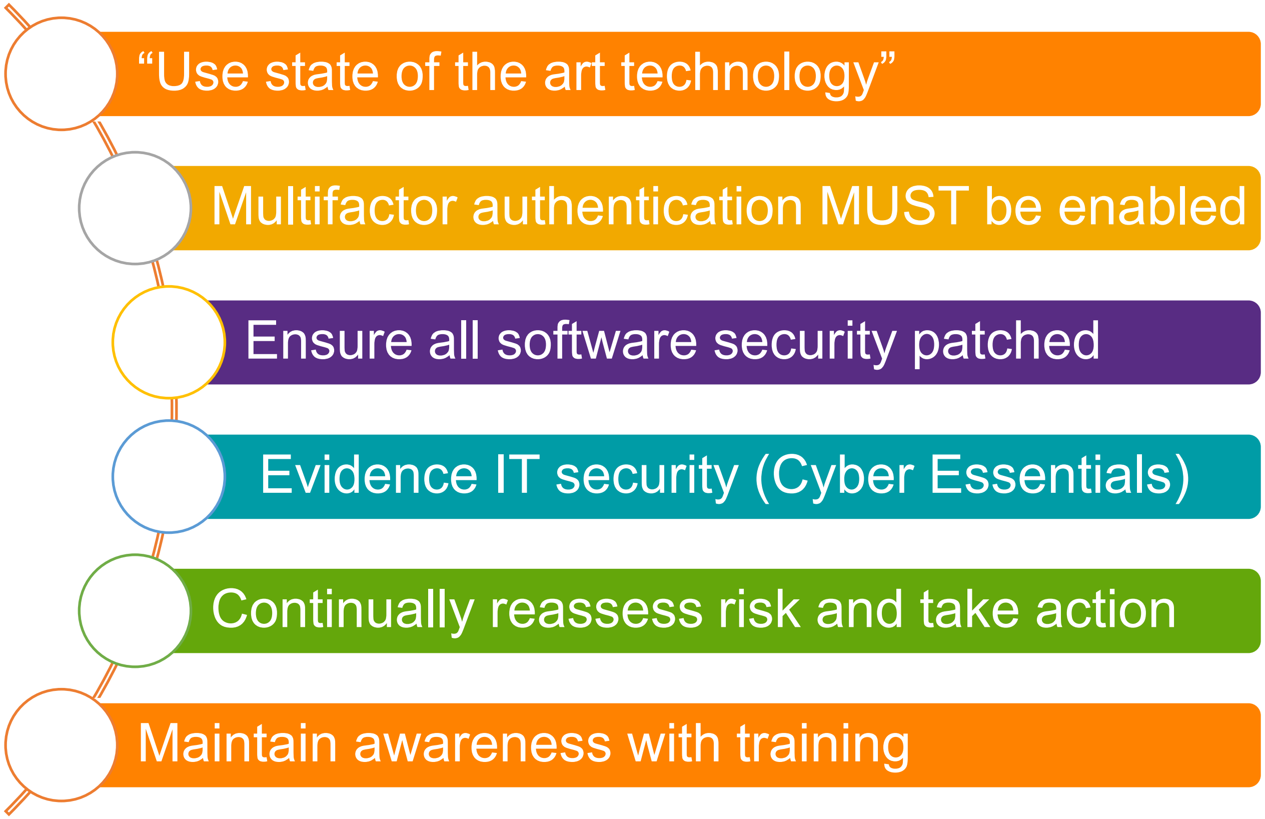
--- Can you run mission critical systems (patient records and payroll)

--- Our systems or the partner/processors systems failure (Access)

--- Security of paper records if we have to revert to paper

--- Don't use DR as an excuse to run a parallel filing system

Tuckers Solicitors – what this means for us



- “Use state of the art technology”
- Multifactor authentication MUST be enabled
- Ensure all software security patched
- Evidence IT security (Cyber Essentials)
- Continually reassess risk and take action
- Maintain awareness with training

Breaches that have resulted in substantial fines

- Tuckers Solicitors fined following Ransomware attack
- Accidently emailed sensitive document to the wrong colleague
- Unite Union £45K marketing breach – snarky with the ICO
- 13 charities fined for wealth screening and data sharing
- We Buy any Car £200K unsolicited marketing
- Marriot Hotels £18.4M - millions of customer records cyber attack
- Pharmacy £275K for leaving old prescriptions outside
- Kim Doyle (RAC) and William Shaw (CMC) – selling claims - Prison

Case Law Rolfe & Ors v Veale Wasbrough Vizards

The High Court has imposed indemnity costs on a family that claimed damages for distress after a law firm accidentally sent an email about outstanding school fees to the wrong person.

Describing the data breach as “trivial”, Master McCloud said the person who received the email, sent by a paralegal, was unknown and confirmed to Veale Wasbrough Vizards that the email had been deleted the following day.

According to the Rolfe family’s solicitor at North-West firm Forbes, they had “lost sleep worrying about the possible consequences of the data breach” and it had made them feel ill.”

The email did not contain any sensitive information or bank account details.

Master McCloud ordered the claimants to make an interim payment on account of costs of £11,000, which she described as a “conservative sum”.

https://www.bailii.org/ew/cases/EWHC/QB/2021/2809.html

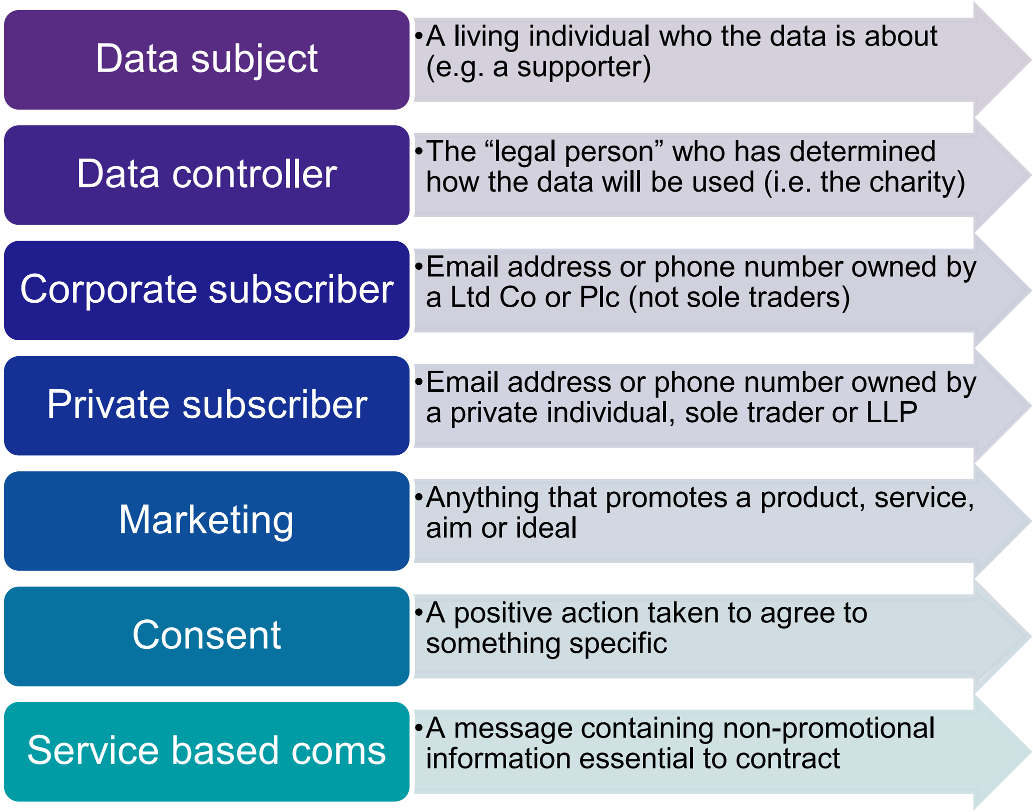
Marketing and Fundraising

- UK Data Protection Bill (DPA version 2)
- Which laws apply, and what do the specify
- In practice – email, SMS, calling and postal
- Is it marketing or a service communication
- Transparency and reducing risk
- ICO enforcement action

Which laws and regulations apply

- Privacy and Electronic Communications Regulations (PECR)
- UK GDPR & Data Protection Act 2018
- Telephone Preference Service ((B)TPS)
- Mail Preference Service (MPS)
- All regulated by the Information Commissioner
- Over the last 10 years more fines for marketing breaches than anything else

Definitions



Data subject

- A living individual who the data is about (e.g. a supporter)

Data controller

- The “legal person” who has determined how the data will be used (i.e. the charity)

Corporate subscriber

- Email address or phone number owned by a Ltd Co or Plc (not sole traders)

Private subscriber

- Email address or phone number owned by a private individual, sole trader or LLP

Marketing

- Anything that promotes a product, service, aim or ideal

Consent

- A positive action taken to agree to something specific

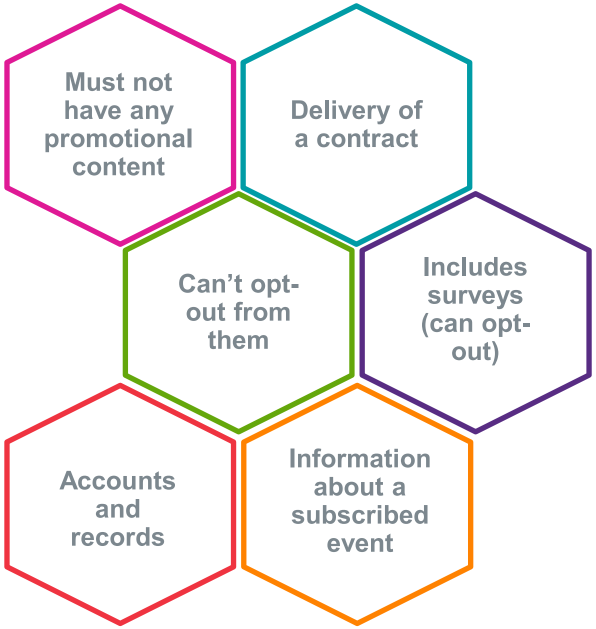
Service based coms

- A message containing non-promotional information essential to contract

Marketing – anything that promotes a product, service, aim or ideal

Service based

You must have told people how you will send service communications.



Must not have any promotional content

Delivery of a contract

Can't opt-out from them

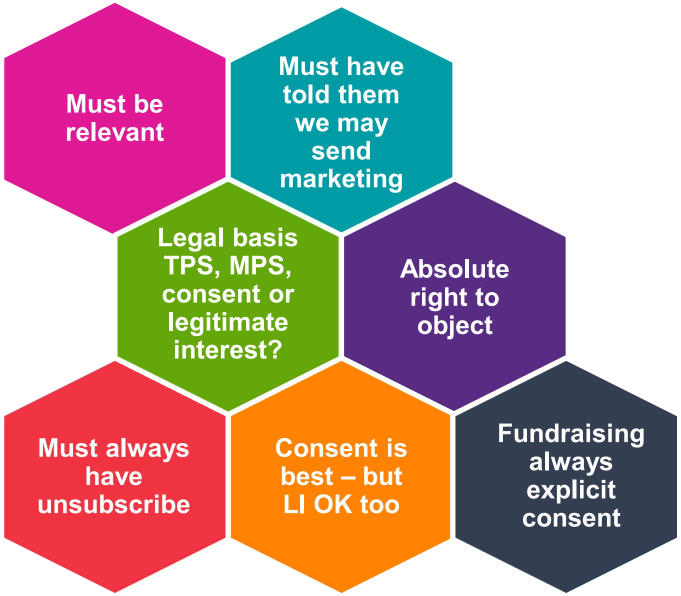
Includes surveys (can opt-out)

Accounts and records

Information about a subscribed event

Marketing

Should be no surprises!



Must be relevant

Must have told them we may send marketing

Legal basis TPS, MPS, consent or legitimate interest?

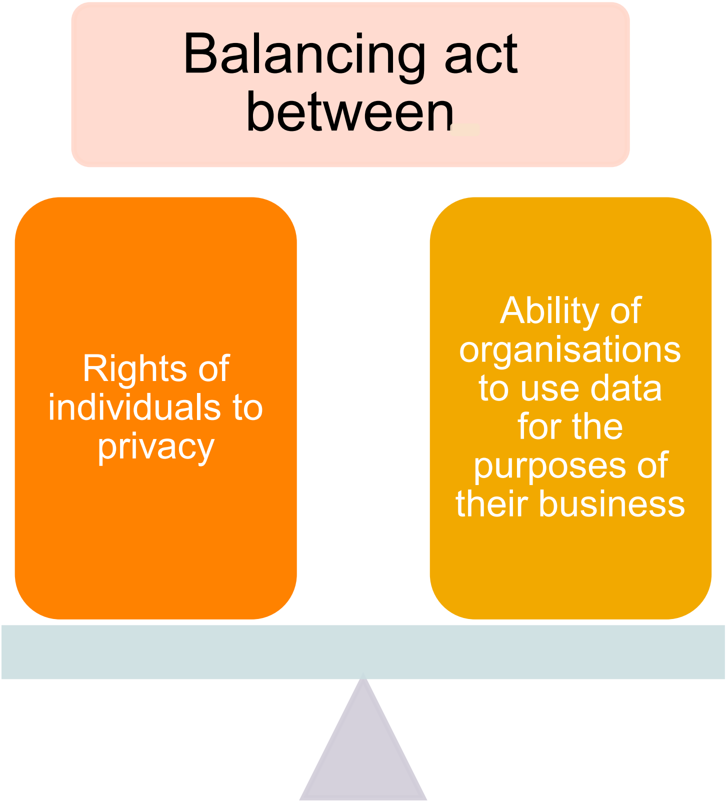
Absolute right to object

Must always have unsubscribe

Consent is best – but LI OK too

Fundraising always explicit consent

Electronic marketing without consent (legitimate interest) AKA soft opt-in


Balancing act between
Rights of individuals to privacy
Ability of organisations to use data for the purposes of their business

- ✓ You must either be in negotiations or a contract with the person
- ✓ Provided information on the type marketing you will send and how you will send it (email, sms)
- ✓ Have offered a clear opt-out at the point you captured the email address/mobile number

Legal basis and restrictions

Communication	Is consent required?	Further considerations
Postal	No	- Comply with data protection legislation - only process information for the purpose for which it was collected. - If an individual objects to, or opts-out of, the mailing they must be taken off the mailing list. - Must screen names against the Mail Preference System. - Provide the opportunity to opt-out at every communication.
Telesales	No (but consent to send further comms must be sought during the call)	- You can make unsolicited marketing calls so long as the individual has not told you that they do not want to receive its calls or has registered with TPS (unless they have specifically consented to your calls). However, beware of “fairness” first principle compliance - Always give the customer the opportunity to opt-out of further communications. Recording such consent is key. - Any voicemails left will be considered as “electronic mail” and can only be left if you has the customer’s consent, as detailed directly below.
Email/text	Yes	- Consent must be freely given, specific, informed, recorded, etc. - You must consider the customers’ capacity to provide “informed” consent. - May be able to use soft opt-in (legitimate interest) - Different rules for corporate & private subscribers

Do you still want to receive the ICO newsletter?

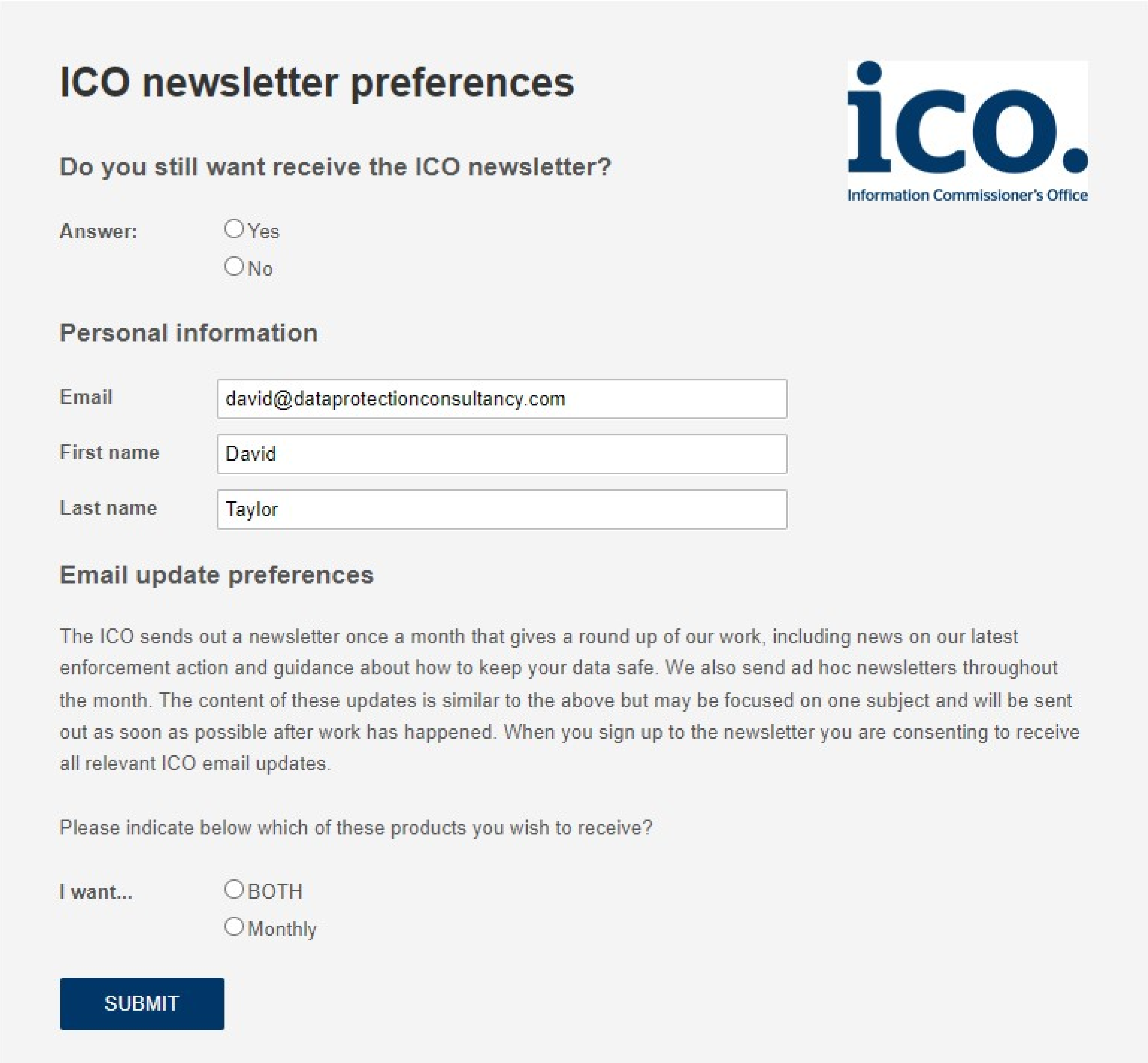
We want to be sure you only get email updates from us if you want to. We're asking all our newsletter subscribers to answer the question – "Do you still want to get the ICO newsletter?". **Those who answer no will be unsubscribed immediately. Those who do not answer before July 2022 will also be unsubscribed**.

So, if you wish to keep hearing from us, let us know now by visiting our new preference centre.

You can also let us know more about what subjects and sectors you are interested in hearing about – these can be changed at any time.

We have recently updated our privacy notice to reflect the creation of the preference centre.

Don't forget, if you want to keep hearing from the ICO, you must answer **YES** to the question "do you still want to receive the ICO newsletter?"



ICO newsletter preferences

Do you still want receive the ICO newsletter?

Answer: ○ Yes
○ No

Personal information

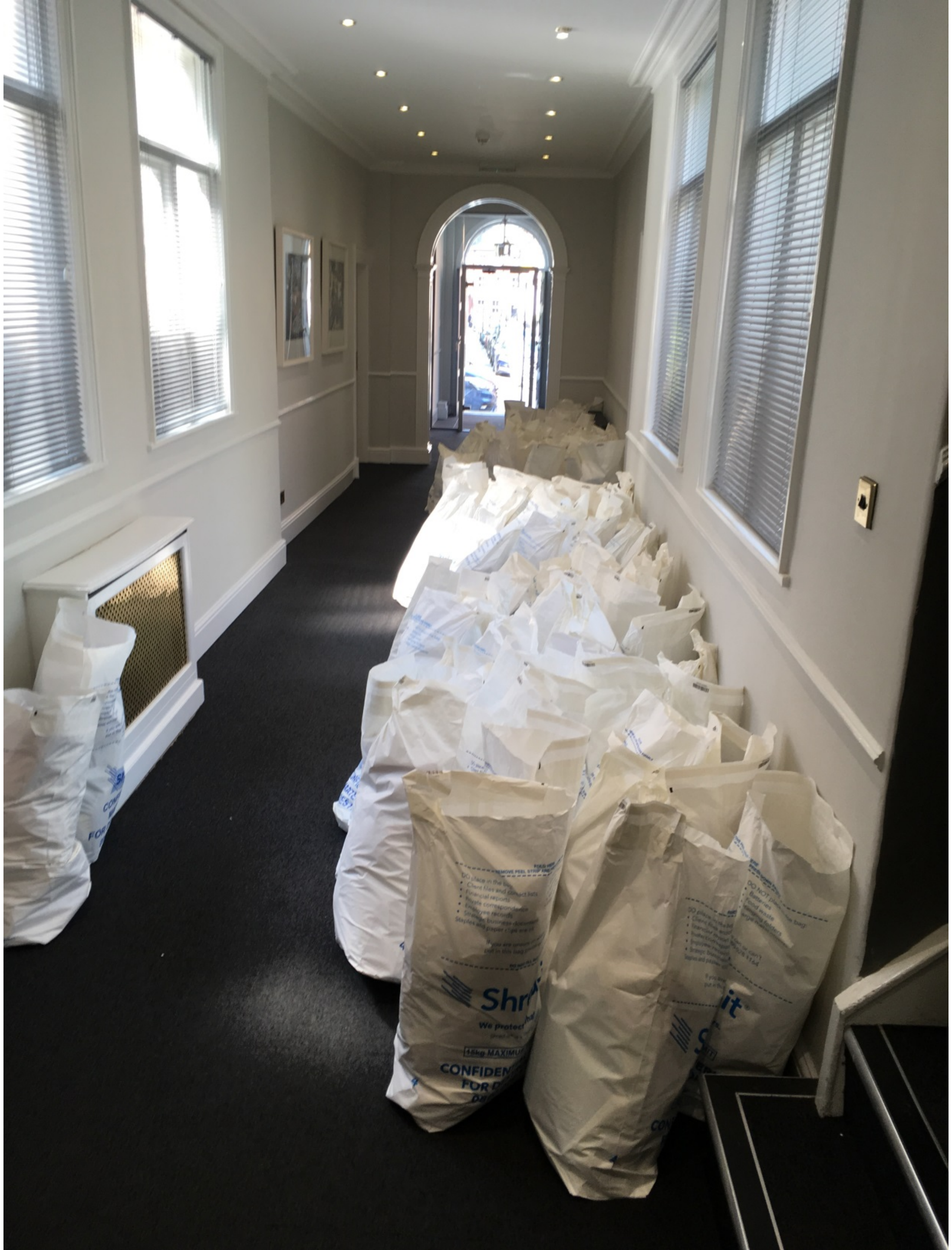
Email	david@dataprotectionconsultancy.com
First name	David
Last name	Taylor

Email update preferences

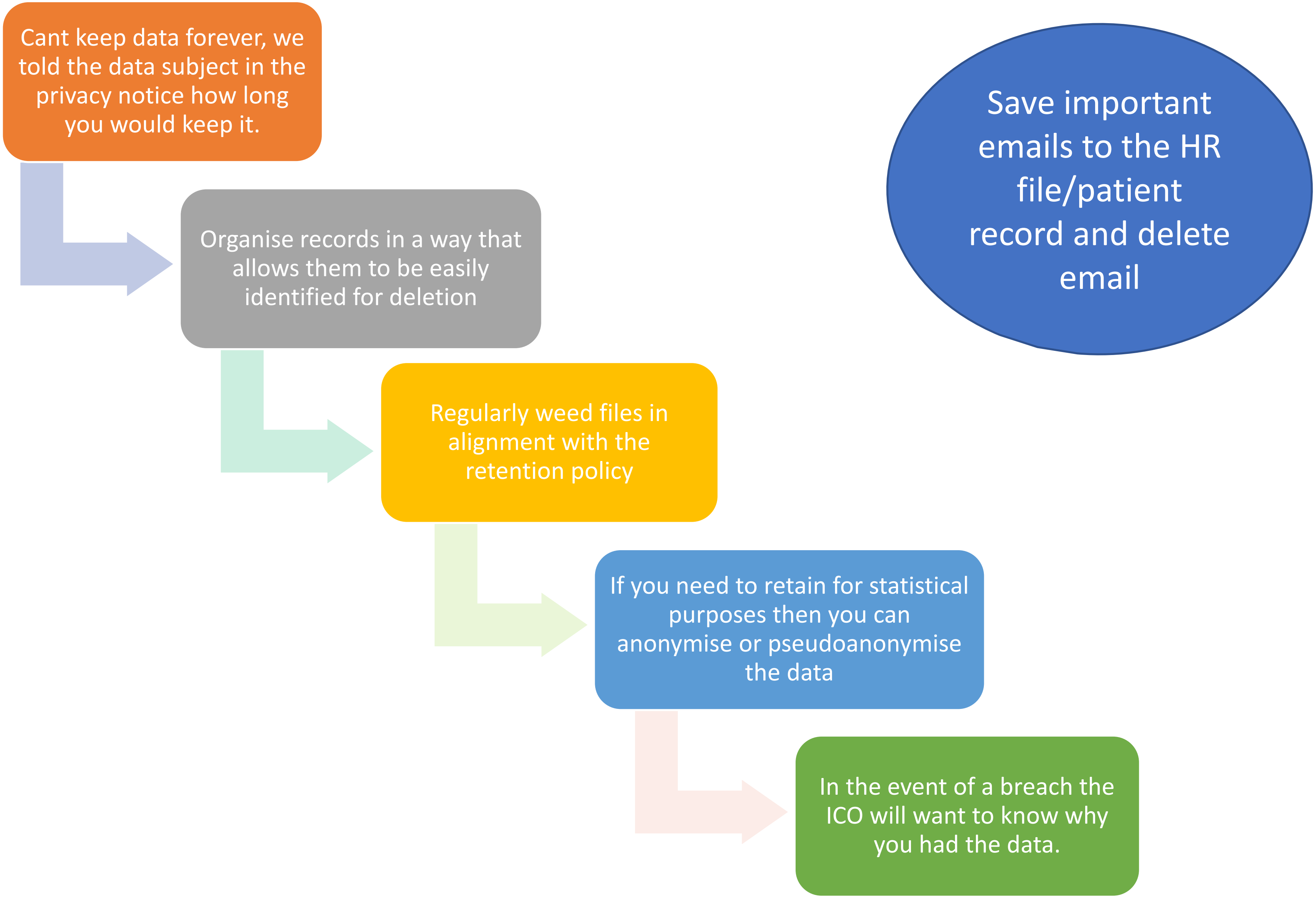
The ICO sends out a newsletter once a month that gives a round up of our work, including news on our latest enforcement action and guidance about how to keep your data safe. We also send ad hoc newsletters throughout the month. The content of these updates is similar to the above but may be focused on one subject and will be sent out as soon as possible after work has happened. When you sign up to the newsletter you are consenting to receive all relevant ICO email updates.

Please indicate below which of these products you wish to receive?

I want... ○ BOTH
○ Monthly


Shr
We protect
CONFIDEN
FOR D

Records management



Cant keep data forever, we told the data subject in the privacy notice how long you would keep it.

Organise records in a way that allows them to be easily identified for deletion

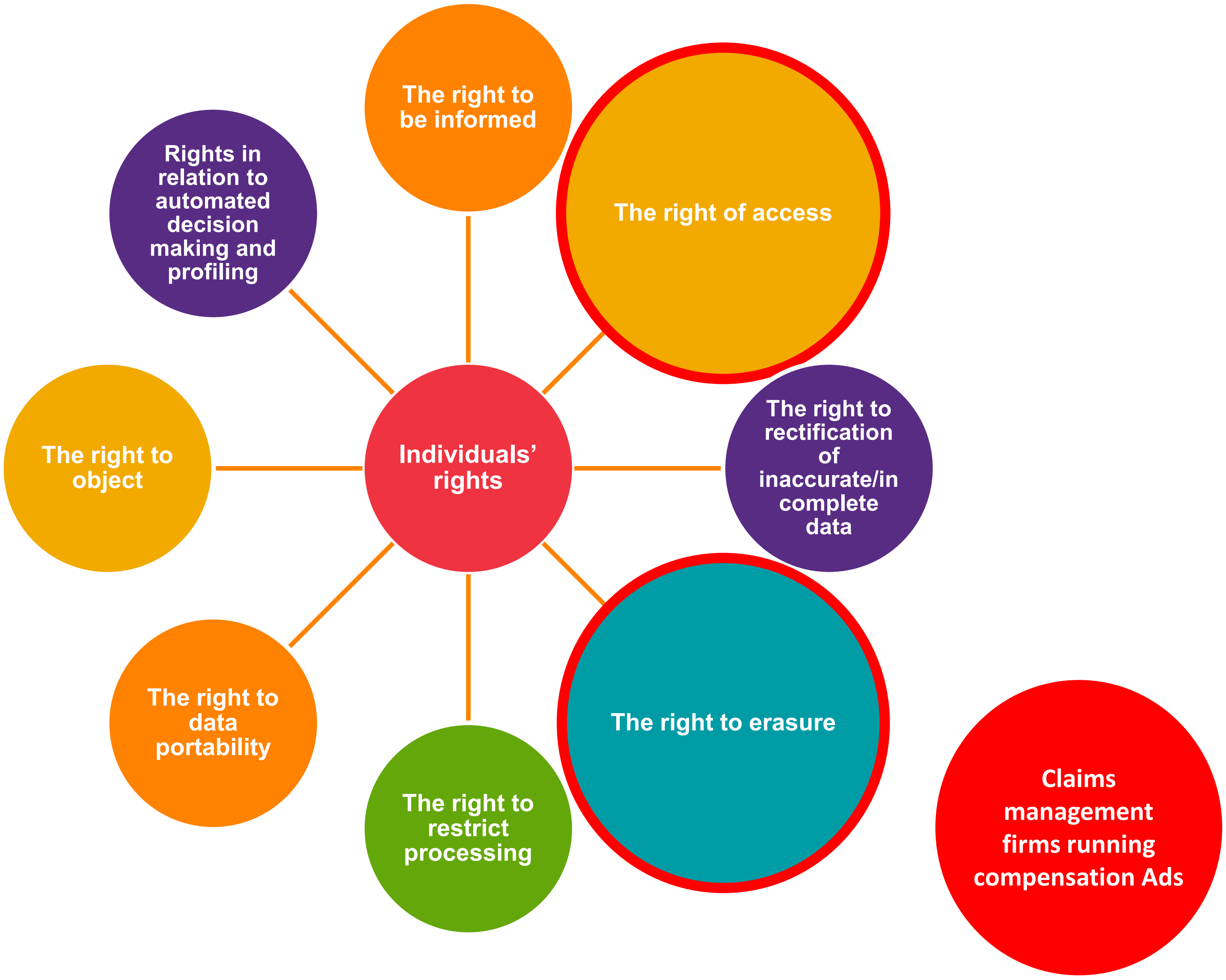
Regularly weed files in alignment with the retention policy

If you need to retain for statistical purposes then you can anonymise or pseudoanonymise the data

In the event of a breach the ICO will want to know why you had the data.

Save important emails to the HR file/patient record and delete email

Individuals’ rights



Individuals’ rights

The right to be informed

The right of access

The right to rectification of inaccurate/incomplete data

The right to erasure

The right to restrict processing

The right to data portability

The right to object

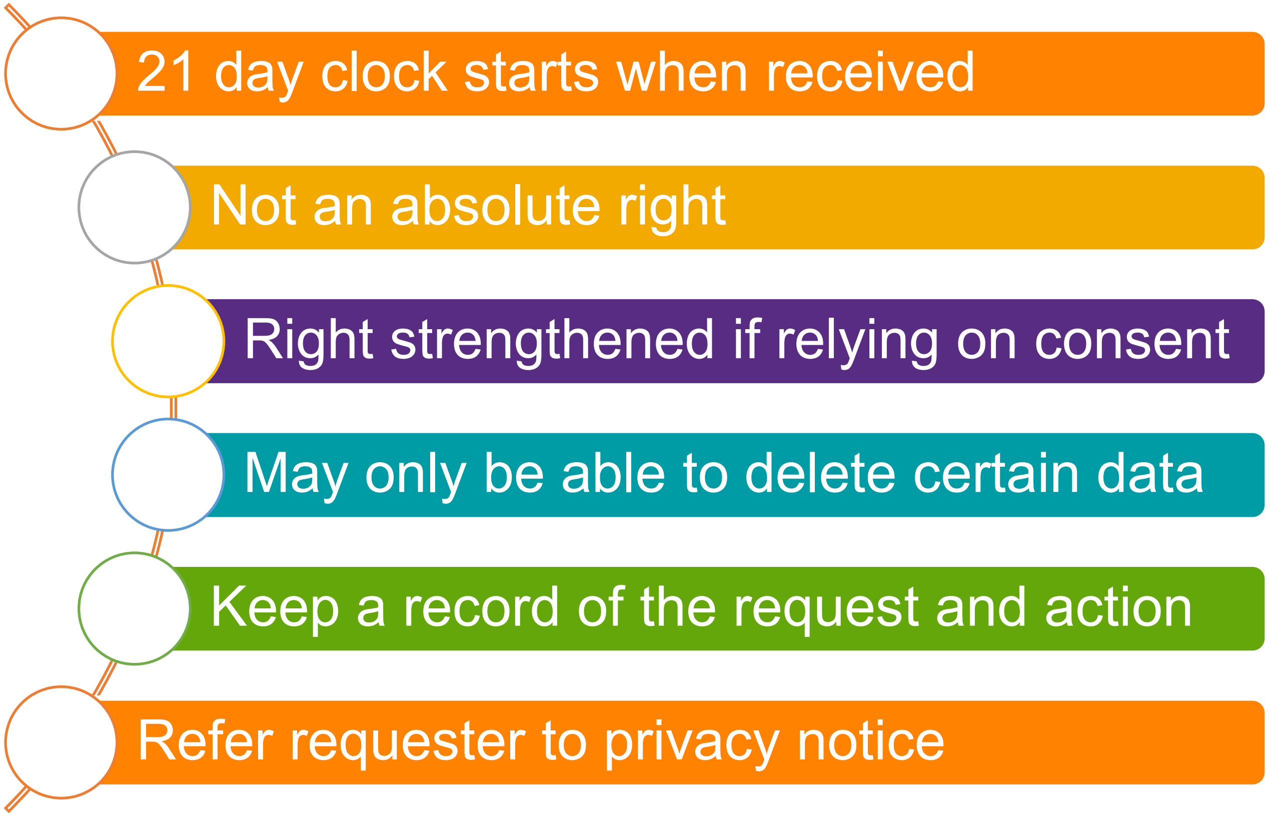
Rights in relation to automated decision making and profiling

Claims management firms running compensation Ads

Subject access requests

- 30 day clock starts when received
- Clock pauses if additional info required
- Can only extend time in exceptional cases
- Search **all** systems, can ask to narrow request
- Only entitled to their own data
- ICO prefer other data left in for clarity if possible
- Keep a record (redacted and unredacted)

Data deletion requests (right to be forgotten)



21 day clock starts when received

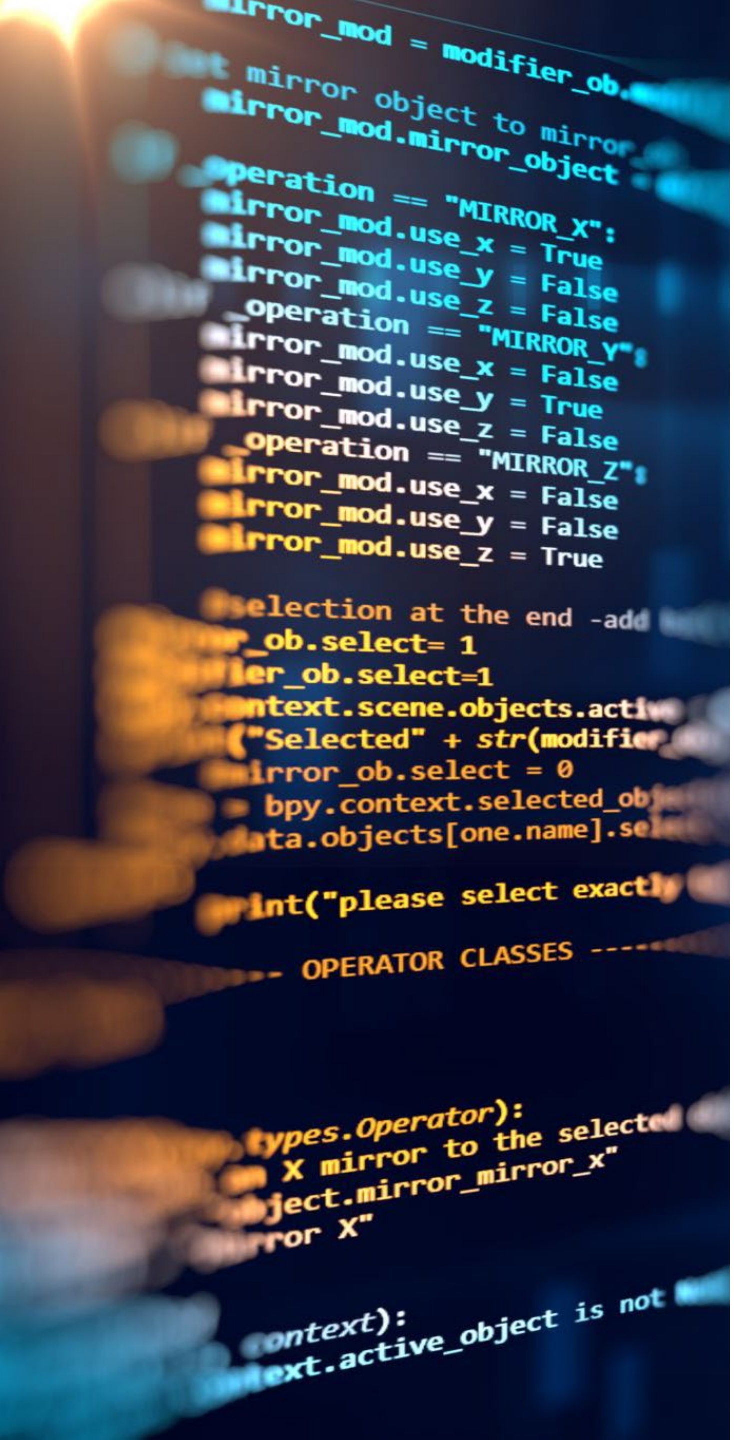
Not an absolute right

Right strengthened if relying on consent

May only be able to delete certain data

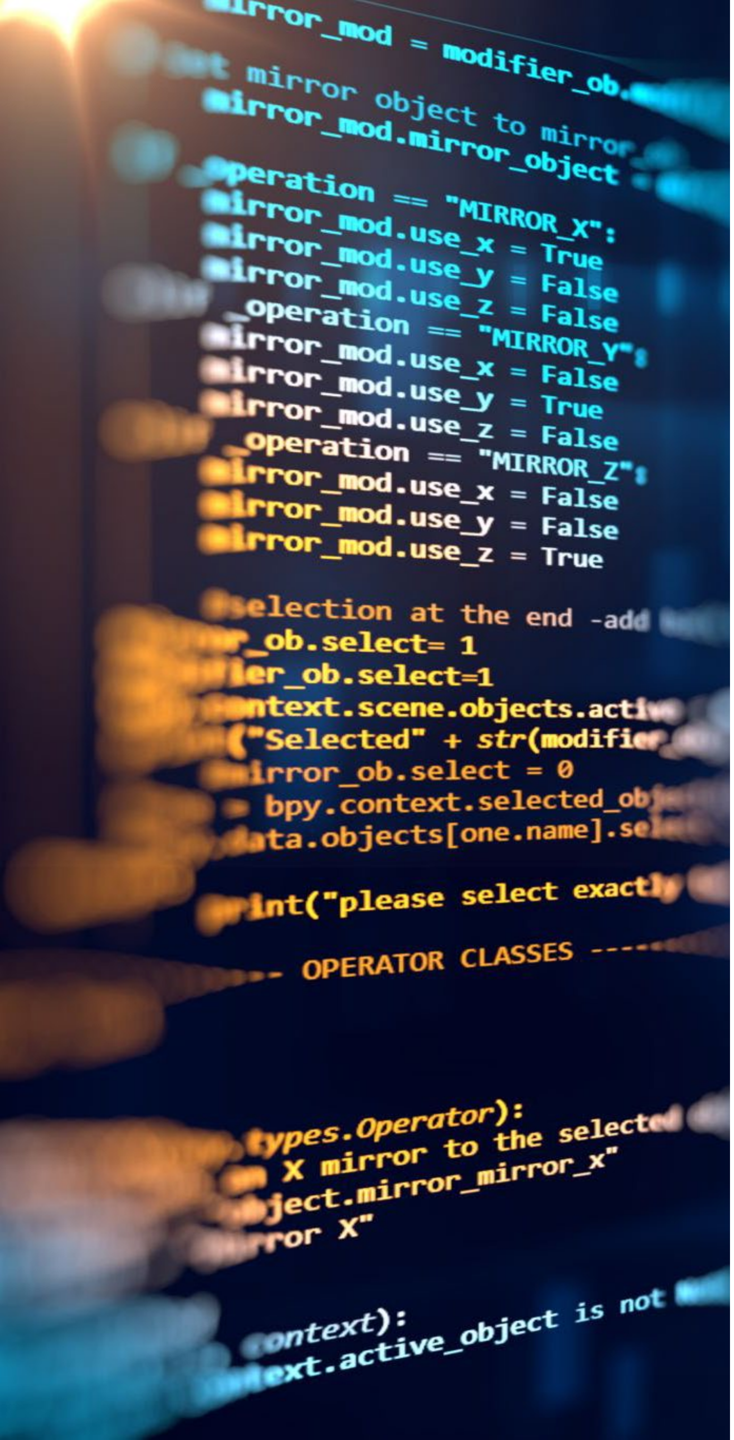
Keep a record of the request and action

Refer requester to privacy notice



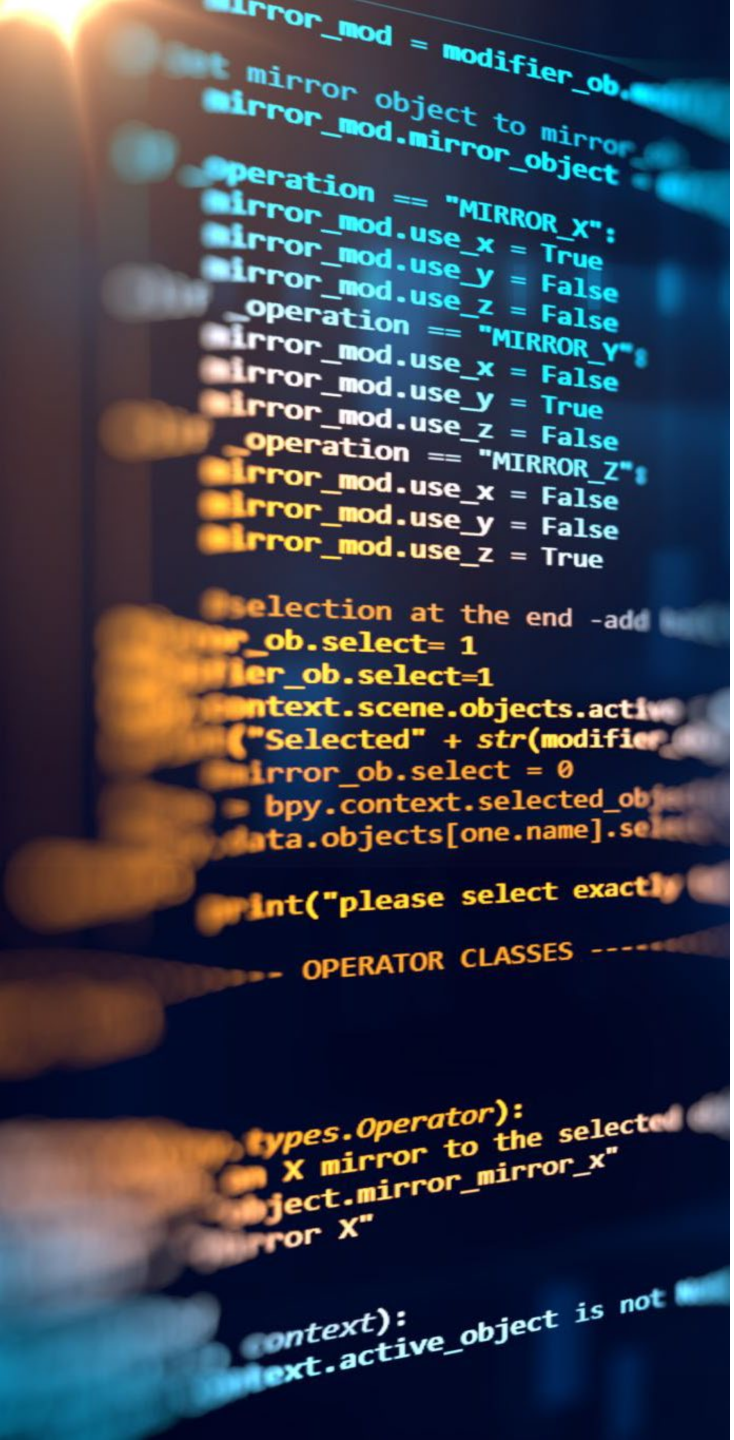
Data Protection Bill

- Lowering the standard on what defines anonymisation of data
- Data Protection Officers will no longer be required, with the statutory personal obligations. **BUT**, you will still require a senior responsible individual as a focal point for data protection who has all same responsibilities
- Article 30 register (ROPA) goes for all but those who process large volumes of SPD, with a simplified approach to records management
- The threshold for refusing to respond to a data subject access request has been lowered from “manifestly unfounded or excessive” to “vexatious or excessive”
- The requirement to obtain consent for cookies will be relaxed in relation to a broader class of purposes (but not for cross-site tracking).



Data Reform Bill

- No need to undertake legitimate interest assessments for approved purposes (safeguarding, public interest, HR, marketing etc)
- Article 30 register (ROPA) and DPIA's gone
- Lower threshold for rejecting a SAR with clarification on manifestly unfounded and excessive requests
- **Soft opt-in extended to fundraising**
- Raising (and clarifying) the threshold for breach reporting
- Can reuse data for a different purpose (different legal basis)
- Consent for scientific research can be less specific



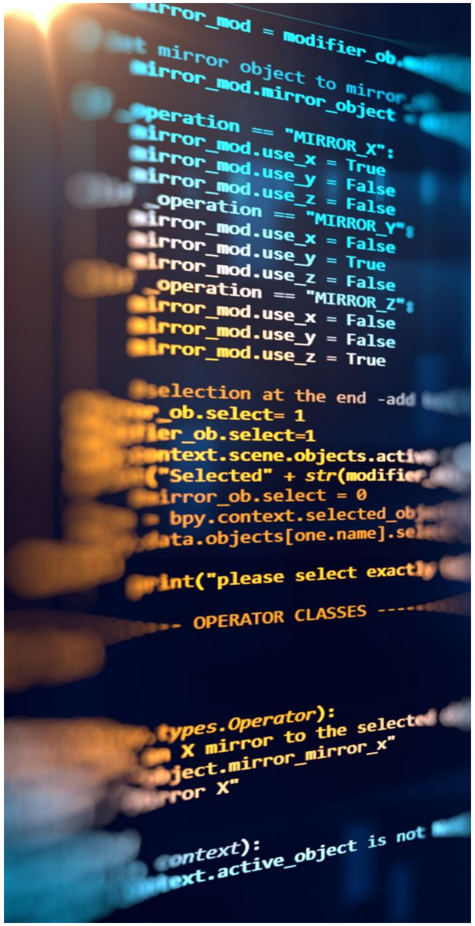
```
irror_mod = modifier_ob
 mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_obj
ata.objects[one.name].sel

int("please select exactly

-- OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
ror X"

ontext):
ext.active_object is not
```

Data Reform Bill

- A more logical and proportional approach to evidencing your compliance with the legislation. Low risk data controllers will not be expected to have the same level of compliance framework in place as a high risk controller
- Greater powers for the ICO to deal with nuisance callers and other spam marketing. Fines increasing from £500,000 to £20m
- Data subjects will have to attempt to resolve their complaints with the relevant data controller (who will be obliged to have a complaints handling process) before lodging a complaint with the ICO.
- A more logical risk based approach to international data transfers
- New measures to allow the easier sharing of data to protect vulnerable individuals

Cybersecurity

- **Largest fines issued by ICO are all for cybersecurity breaches**
  - Must have cybersecurity (IT) policy
  - Cybersecurity training for all staff
  - ICO stated in Tuckers Solicitors investigation report that you must evidence your IT security (Cyber Essentials, Cyber Essentials Plus or 27001)
  - Also stated that MFA must be enabled on all systems
- **Training and testing your people**
  - In addition to cybersecurity training you should also keep your staff on their toes. Implement social engineering testing (your own phishing emails) and leave USB memory stick lying around



```
irror_mod = modifier_ob.
t mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

selection at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.active
("Selected" + str(modifier
irror_ob.select = 0
bpy.context.selected_obj
ata.objects[one.name].sel

int("please select exactly

- OPERATOR CLASSES ----

types.Operator):
X mirror to the selected
ject.mirror_mirror_x"
ror X"

ontext):
ext.active_object is not
```

Cybersecurity threats

- Phishing Attacks
- Imposter Scams
- Ransomware
- Hacking

- Finance department always the highest risk department
- Be very suspicious of urgent requests with time deadlines
- Verify requests by phone calling the organization main number

Everyday Tips

- Be careful of email attachments, web links and voice calls from unknown numbers.
- Do not click on a link or open an attachment that you were not expecting.
- Use separate personal and business computers, mobile devices, and accounts.
- Use multi-factor authentication where offered.
- Do not download software from an unknown web page.
- Never give out your username or password.
- Consider using a password management application to store your passwords for you.

Top tips

- Security of electronic data – encrypt all electronic devices & privacy filters
- Security of paper data – lock and key, transport securely, don’t leave in car
- When you don’t need it anymore get rid of it – that includes email
- Be careful when working out of the office
- Records management, keep everything in one place (email, Word docs etc)
- Securely destroy paper and electronic data (certificate of destruction)
- Be careful when forwarding emails (email addresses) and reply all
- If you can show you were trying your best the ICO usually take no action
- And if goes horribly wrong call me before you speak to the ICO

Questions