1

To Do List

- ICO Register £55 data controller register.
- Also Add CCTV. #128443

- Need Rolling issue Check signs CCTV display at + visible. Doc id 1076
✓ Must be present - legal signs.
- need to be present on front of house/wH/ car park. called - CCTV rational.

- A ✓ Need rational as to why recording CCTV Statement needed. Proc id 7910 Written are add to issue. #128445

✓ ~~A~~ sensitive info - sick leave - calls etc. #128448

~~A~~ add Contract - no extra health, personal life, ethnic, trade union
X - includes pay levels etc. ✓ Don't do this

~~A~~ ✓ security of files personel files ~~including~~ + better cabinets. needed. add review. HC ordered new lock personal file.

~~A~~ is what we collect relevant + not excessive + accurate. Process ID 912

- SL if we doing credit check must tell customer??

~~A~~ CV take old + dispose of? (keep list of names poss).
put procedure in place / time scale 6 months cvs keep - No Longer
retain information.
different to employee Applicant different.

AIREDALE ENTERPRISE SERVICES

mod assessment ward.

Supporting Busine[sses] ... 1983
01535 607775

To do cont.

CCTV Issue
Rolling
task
need to
add lab
then do
staff file ave.

o 1a
Issue - paper work lying around.
personal information must be kept secure.
ORDs PORs ≡ put away not left on
desks etc.
#128567

8 review #128568

9 Doc in System Needed - saying legitimate
interests + why. company that supplies med Equip.
#128570

010 MUST - Privacy Notice check/DO. TO DO
tell
pl. the doc patient info in -doc good. V.

send privacy notice to trainer to proof it wait.

o11 MUST do on slides.

12 add statement to System re (h). Sensitive Data
as to why keeping health info - #128572

HR 7 years after last Action HMRC
CRM 20 years X check MHRA time #128573
attendance 2 years after action/left.
Use GDPR to remove rest Archiving.

may need lock on office door to secure #128574
files being worked on.

~~A Do~~ DL check.
Recording calls need to say on telephone. system.
telephone tells you its recording
add to privacy policy

* 12 c need to review list c/ check all policies
need Data policy compliance per GDPR + 7x
privacy

* training staff – use course cardinal.
annually.

* 13 review – Jean
#128576.
issue re sensitive Data sent
Derek to speak to her re security
to do.

* Marketing
#128577
ct = make sure ~~we~~ we add 'say no to contact ~~marketing~~ marketing at bottom of all ~~__~~ marketing emails.
* we can Market ~~to~~ Business to Business as long as we give right to say stop.
* can to people who bought from as long as opt out.
* there is a Business TPS.

– Can market until people say stop.
– Always option to unsubscribe.

4

AIREDALE ENTERPRISE SERVICES

Supporting Business & Enterprise since 1983
01535 607775

All personally liable for D.P. Dues + person in training

#128580

GGL USB encrypted personal info - if lost ICO will fine. tell DL + GGL. #128576

#128601

#15 Do make staff sign Doc saying must not copy take home Data etc.

#16 Data Protection Impact assessment — #128581
DL. Risk assessment for new systems Change
do #17 to do

Business Coaching, Advice, Support & Training For Prestart,
New Start & Existing Businesses
www.airedaleenterprise.org.uk

Overview of the 2018 Data Protection Act and the General Data Protection Regulation

Stay Compliant
(BLS Ltd)

Purpose

1. Understand the General Data Protection Regulation (GDPR) key changes for businesses
2. Have confidence in what compliance looks like
3. Promote questions and discussions

Agenda

- 10:00 Welcome and Introduction
- 10:10 What is the GDPR & Data Protection Act and how does it apply to my business
- 12:00 The Information Commissioners Office, their powers and mandatory registration process
- 12:30 Lunch
- 13:15 Rights of the individual, Subject Access Rights and how to respond and redact
- 14.15 Preventing and managing a data breach & case study on breach incident and outcome
- 15:00 Refreshment break
- 15:15 The 2018 Act and General Data Protection regulations & Steps you should be taking
- 16.00 Summary of the day and Q & A

Data protection – legal position

Data Protection Act 2018

Data Protection Act 1998

GDPR

Data Protection Act 2018

*1

General Data Protection Regulation is an EU Regulation (May 2018) intended to:

- Strengthen data protection for all individuals across the UK
- Control the export of personal data outside the UK
- Give control back to citizens and residents over their personal and sensitive data

7 must do

The DPA Principles

The Data Protection Principles: Common Sense Rules –

a. Fair and Lawful
b. A specific purpose
- Adequate, Accurate, not Excessive

c. Kept up to date
d. Kept only as long as necessary
e. Processed in accordance with the data subjects rights
f. Kept secure
g. Not transferred outside the EEA without adequate protections

No clear rules!

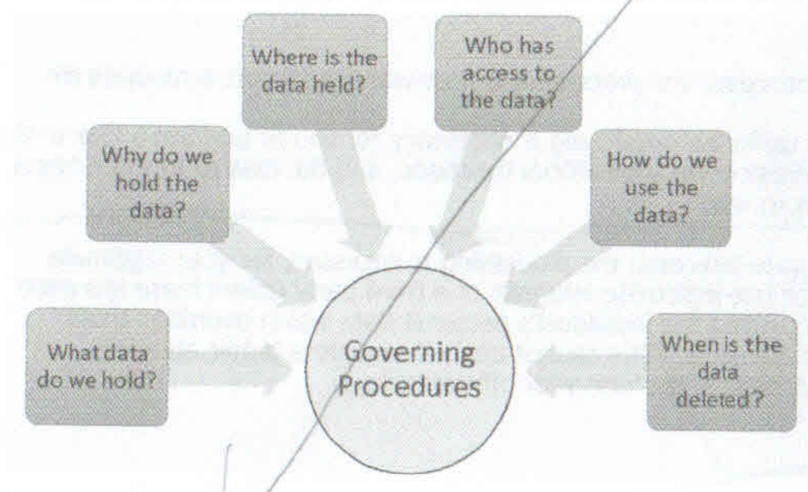
! QUIZ !

The Data Protection Principles: Common Sense Rules –

- Fair and Lawful
- A specific purpose
- Adequate, Accurate, not Excessive
- Kept up to date
- Kept only as long as necessary
- Processed in accordance with the data subjects rights
- Kept secure
- Not transferred outside the EEA without adequate protections

8

Understanding your position



9

Lawful basis:

You must have a valid lawful basis in order to process personal data.

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.

Lawful basis:

Most lawful bases require that processing is 'necessary'.

If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.

At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

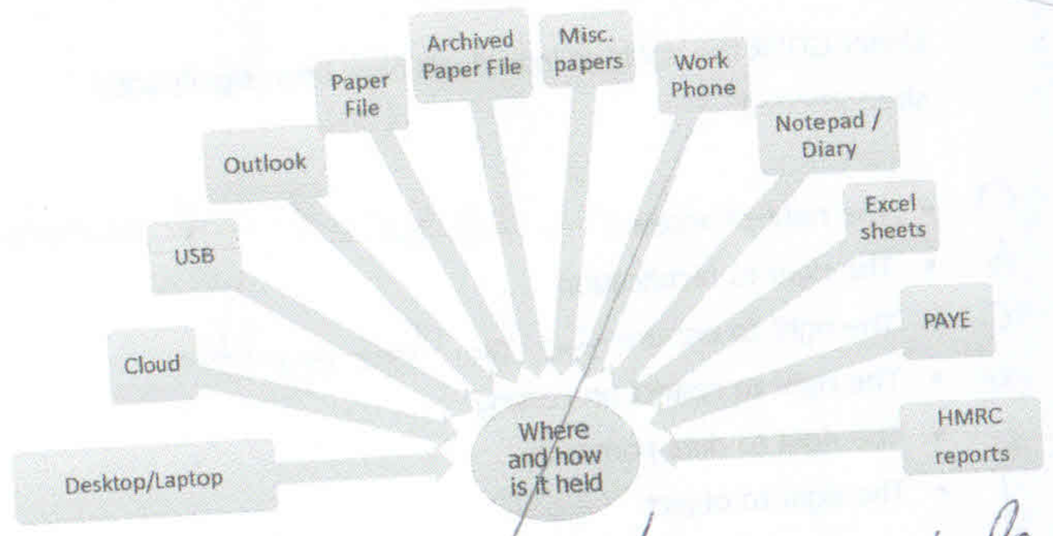
X 12

DPA: Not just your paper records

- **Physical security**: doors, windows, cupboards, locks and keys, CCTV.
- **Technical security**: firewalls, secure emailing systems, role based access, adequate password protocols.
- **Organisational security**: your information governance framework, policies, procedures, advice, guidance, training and sanctions.

13

Possible sources of data



Do you know where it all is.

If you carry out any telephone, email or other electronic marketing then you need to comply with the Privacy and Electronics Communications Regulations.

X 15

The PECR are concerned with the way organisations send marketing material by fax, text, email and telephone. Marketing can include the promotion of goods, services, aims or ideals.

The rules of the PECR only apply to email addresses owned by individual subscribers. Individual subscribers are likely to be domestic subscribers but also include sole traders and non-limited liability partnerships.

Business-to-business texts and emails

Corporate subscribers do not include sole traders and some partnerships who instead have the same protection as individual customers.

However individual employees using personal corporate email addresses (gary.baker@org.co.uk) have a right under the DPA to stop any marketing being sent to that type of email address.

X 14 5

DPA - Right to prevent processing for purposes of direct marketing.

(1)An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data in respect of which he is the data subject.

(2)If the court is satisfied, on the application of any person who has given a notice under subsection (1), that the data controller has failed to comply with the notice, the court may order him to take such steps for complying with the notice as the court thinks fit.

Timeframe to report a breach:

72 hours

"You are obliged to notify the ICO, within 72 hours, of a breach where it is likely to result in a risk to the rights and freedoms of individuals."

Breach of information –what now ?

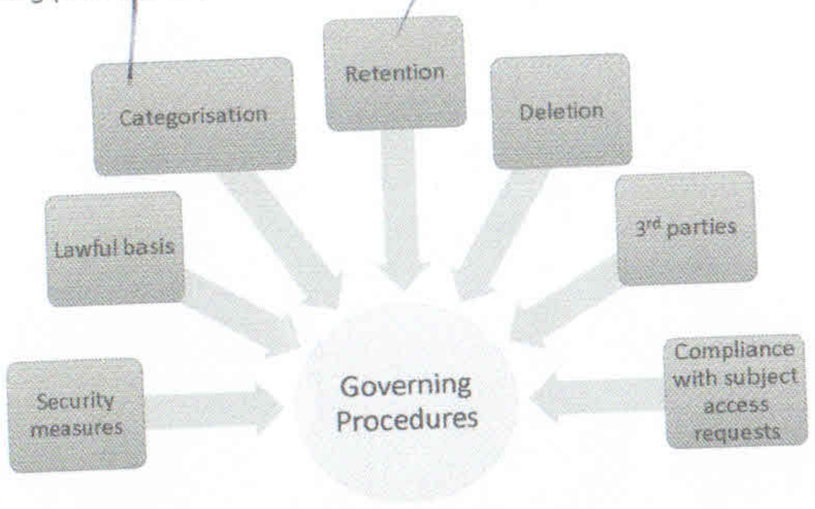
- What is your role? When are you informed?
- Are there procedures for recovering information, discovering the cause of the breach, mitigating any future risks
- Are both breaches and near misses logged?
- When would you inform the police or the ICO?
- Who would deal with the press?
- Does the data subject have the right to know their information has been compromised?

Make time for reflection and learn the lesson

Main Themes:

- Increased fines of :
  - - up to €20 million or 4% of international turnover for data controllers
  - - up to €10 million or 2% of international turnover for data processors
- 72 hour reporting to ICO (including legal requirement to report)
- Fairness - more control for data subjects including the ability to claim compensation for damages they suffer following a data breach
- A stricter view of consent (explicit)
- Age of data owner (child: under 13 years of age?)
- The right to be forgotten
- More emphasis on "proving" you are compliant
- Role of the Data Protection Officer
- Privacy by Design (Privacy Impact Assessment – can be fined)

Governing procedures you should consider



DPA 2018 – to do list

- ✓ Audit and comply across your business. Create a culture of transparency and accountability on how you use personal data –the public has a right to know what's happening with their information
- ✓ Understand what information you have – review what personal data you hold, where it came from and if you share it. Consider reviewing your contracts with 3rd party processors to ensure they are fit for GDPR.
- ✓ Record how you comply – who is your data protection lead, record lawful basis, review/write privacy notices, consider your response to a data breach incident & are you planning new projects that require a Data Protection Impact Assessment.
- ✓ Ensure appropriate security –identifying and taking appropriate steps to address security vulnerabilities and cyber risks is vital
- ✓ Train Staff – Staff are your best defence and greatest potential weakness – regular and refresher training is a must