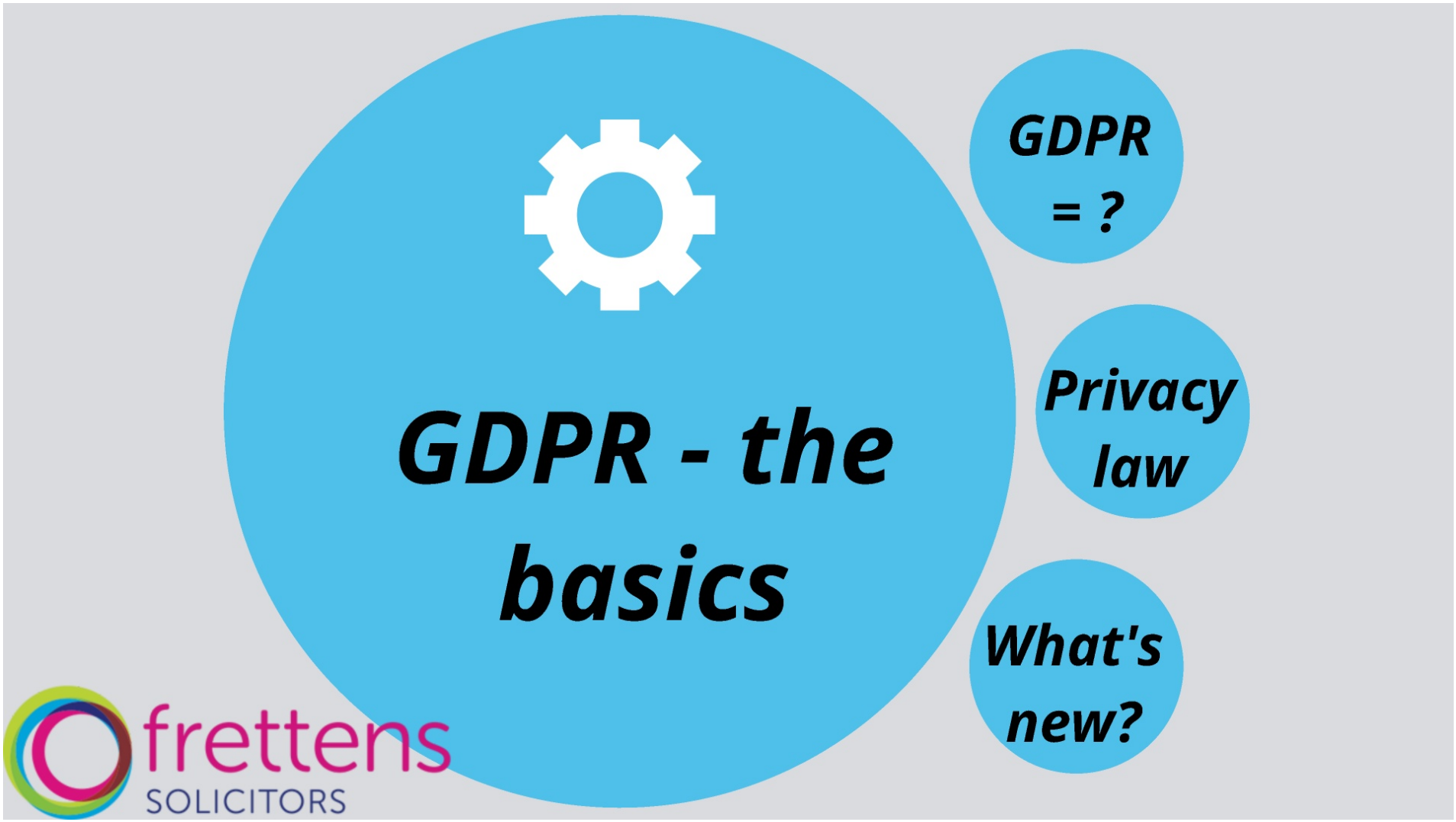
GDPR *refresher*


GDPR - the basics
GDPR = ?
Privacy law
What's new?
frettens
SOLICITORS

GDPR = General Data Protection Regulation

+

Data Protection Act 2018 (DPA'18)

+

The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (Brexit Regs)

We now have 'UK GDPR' and DPA'18

Brexit hasn't saved you...

The UK GDPR re-enacted GDPR with technical changes.

(They don't make it easier to understand.)

GDPR is developed from UK legislation. It provides international control over the activities of international tech companies.

frettens
SOLICITORS

A developing law of privacy

- The historical perspective
- The human rights perspective
- The golden rule

frettens
SOLICITORS

A developing law of privacy - the history

Common law

- No right of privacy
- A developing concept of implied confidentiality
- Contractual obligations of confidence (express and implied)
- Well-developed law of defamation (very effective tool to enrich lawyers)
- Difficult to assess compensation for breaches of privacy

Statute law

- Data Protection Act 1984
- Data Protection Directive 1995
- Data Protection Act 1998
- GDPR + DPA'18

frettens SOLICITORS

A developing law of privacy
Human rights at the core

Preamble to GDPR:

(1) *The protection of natural persons in relation to the processing of personal data is a fundamental right...*

(4) The processing of personal data should be designed to serve mankind...

(7) Natural persons should have control of their own personal data...

The golden rule

How would you like other organisations to treat you and the information about you they have?

Base your practices on that and you won't go far wrong!

frettens
SOLICITORS

What was new in GDPR?

Extra paperwork!

- Records about records - keeping a compliance record.

Better rights for people

- Better information about their rights.
- Better information about the stuff you've got about them.
- Why do you think you have a right to use information about someone? Record your reasons.

frettens
SOLICITORS


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner


Training
Who?
When?
What?

Your training programme.
For whom?

Your data protection partner

Everyone who handles 'personal data'

(Personal data = any information about an identifiable living person)

Your training programme. When to train?

GDPR came into force 25 May 2018.

Schedule a refresher?
(In the next 6-12 months, then every couple of years?)

New starters.

frettens SOLICITORS

Your training programme. The contents?

Basic principles:
- Take only what you need.
- Keep only what you're allowed to use.
- Record your right to use it.
- Consent is not the only way to authorise use.
- The golden rule

Your own policies, procedures and documents.

How to recognise sensitive ('special category') data.

frettens SOLICITORS

Categories of data

1 Anything that is not personal data

- *Remember professional and contractual duties of confidence may still apply*

2 Personal data

- *Information about an identifiable, living human*

3 Financial and identification data

- *This is not in a different category under GDPR or DPA. But you may want to put it in a higher category than other personal data.*

4 Sensitive ('special category') personal data

5 Criminal records

frettens SOLICITORS

Categories of data - 4 'special category'

GDPR contains tighter rules about when you can take, keep and use this.

Information about:

Health (physical or mental)
Sexual life (activity and preferences)
Religion; beliefs (or similar)
Political opinions
Racial and **ethnic** origins
Trade union membership
Biometric and genetic data (new to GDPR).

frettens SOLICITORS

Categories of data - 5 criminal records

GDPR contains even tighter rules about when you can take, keep and use this.

Information about **crimes** (alleged, prosecuted, convicted or sentenced)

- *CDDA offences*
- *Bankruptcy offences*
- *Allegations of fraud*

frettens SOLICITORS


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner


GDPR in a professional services firm
Marketing
HR
Clients

Marketing

- Don't use senstive data for marketing
  - (without explicit consent)
- Your 'legitimate interests' may permit marketing
  - (without consent - but you have to think about it)
- Make sure you understand PECR
  - (Privacy and Electronic Communications Regulations, as amended)
  - (PECR obstructs direct marketing to consumers)
  - (PECR is less obstructive of direct marketing to businesses)
  - (But make sure you know the rules)
- GDPR need not be much of an obstacle when marketing to businesses
  - (But there are rules to follow - mainly in PECR)

Managing your people

Your HR records include sensitive information:

- Health (checks when you took them on; sickness records; reasonable adjustments)
- Criminal records (allegations; disclosed convictions)
- Sexual life (family details; that disciplinary after the office party...)
- Religious beliefs (their name; requests for time off work)
- Political opinions (perhaps less likely?)
- Racial and ethnic origins (data collected for regulatory compliance)
- Trade union membership
- Biometric data (ID photographs; fingerprint and iris scans for security)

Keep HR records accessible on a 'need to know' basis

Client files

GDPR applies to people working for your clients (directors, etc)

You owe a duty of confidence to them, as well as the corporate client

Run your files to comply with GDPR

- Security of data
- Engagement letters (data consent letters)
- Privacy notices

frettens SOLICITORS


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner


Step-in GDPR issues
(GDPR & BustCo)
The IP's responsibility
Quick and dirty
Trading
Selling

The insolvency practitioner's responsibility

BustCo is the data controller - even after you're appointed

You are agent for BustCo - as liquidator or administrator

You may have responsibilities as data processor - a question of fact

frettens SOLICITORS

Do a 'quick and dirty' risk assessment

Your pre-appointment and 'Day One' checklists:

- Reliability of BustCo's existing systems - can we trust them?
- What sort of data does BustCo have?
- How will we need to use it?
- Suppose it goes wrong?
  - How many might be affected?
  - How bad might it be for them?
- What - if anything - do we need to change now?
- What - if anything - do we need to look into?

Trading review - data security

Trading issues to consider:

- What level of trading activity do you expect?
- How long will the business stay open?
- What is the risk (considering the same factors as the 'quick and dirty')?
- How often should you review this (each week?)?

Implement any changes required by the review

frettens
SOLICITORS

Realisation - data security review

Points to consider when selling assets include:

- TUPE transfer in a ToGC - the HR records - legal disclosure duties
- Issues on the sale of the customer database
- Issues on the sale of a marketing database

frettens SOLICITORS


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner


GDPR for the office holder
IP as data controller
Authority to use personal data
Authority to use sensitive data
Consent forms
Privacy notices
Third parties
Investigations

IP as data controller

You will be using personal data as office holder.

- Trustee in bankruptcy, nominee, supervisor
  - (information about the bankrupt, their family and associates)

- Liquidator, administrator, receiver, nominee, supervisor
  - (information about the directors, their family and associates)

Some of it will be sensitive.

frettens SOLICITORS

Authority to use personal data

Relevant bases for insolvency practitioners to use personal data:

- **Consent**
  - *(May be difficult in bankruptcies and some liquidations)*
- **Performance of a contract**
  - *(Useful for IVAs. Less useful for corporate appointments.)*
- **Legitimate interest**
  - *(This requires you to carry out - and record - a balance of interests)*
- To perform **legal obligations**
  - *(Not a catch-all, but very useful. Check the detail in DPA'18.)*
- If in the **public interest** or the exercise of **official authority**
  - *(Not a catch-all, but very useful. Check the detail in DPA'18.)*

You have to identify and record which you are using.

Authority to use sensitive data

You may sometimes need sensitive data on debtors and directors:

- Health
- Romantic affairs
- Family relationships
- Allegations of criminal activity
- (and the rest)

Your bases for being authorised to use it might be:

- Use in legal proceedings (criminal allegations)
- Substantial public interest - following your own policy document - for other sensitive data

frettens SOLICITORS

Consent forms - when and how to use them

You shouldn't ask for consent if there is a better basis for using the data.

Consent can be withdrawn at any time.

Consent forms are supposed to meet the requirements of GPDR (lots of detail)

Consent forms may be useful for:

- IVAs
- CVAs, MVLs, CVLs, administrations

And less useful for:

- Bankruptcies

frettens SOLICITORS

Privacy notices - how and when to use them

The general rule is that you should issue a privacy notice to everybody on whom you are collecting information.

There are set contents you must include. Which list? It depends:

- Are you collecting information from that person?
- Or are you collecting information about them from others?

You should issue the notice at the start.

frettens SOLICITORS

Privacy notices - how and when to use them

People to whom you issue privacy notices may include:

- The debtor (IVA or bankruptcy)
- The directors (all corporate procedures)
- The debtor's associates (family and business)
- The directors' associates (family and business)
- The shareholders

But, there are exemptions in DPA'18

frettens SOLICITORS

Privacy notices - how and when to use them

Exemptions for insolvency practitioners
(In DPA'18)

You may not need to issue privacy notices:

- For your file for investigating the bankrupt's conduct
- For your file for investigating the directors' conduct for CDDA
- For privileged information
- If doing so might prejudice negotiations with that person

The boundary of these exemptions is unclear. It may be easier (in routine cases) to issue privacy notices, rather than rely on these.

frettens
SOLICITORS

Third parties - their rights under GDPR

Remember that your file will often contain information on:

- The bankrupt's associates (business and family)
- The directors' associates (business and family)
- Other individuals (professional and other advisors)
- Creditors (individuals and individual representatives)

Each of them have their individual rights under GDPR

- Keep only the information you need.
- The right to receive a privacy notice
- etc

frettens
SOLICITORS

Investigations *(directors and bankrupts)*

Consider running these as self-contained files

Keep sensitive data on these files rather than the general file?

Issue privacy notices on these files

Consider relying on the exemptions for these files

This may be easier to manage if you receive a subject access request

frettens
SOLICITORS


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner


Subject access requests (SARs)
Right of access
Right to rectify
Right to be forgotten
Right to restrict processing
When you can deny access

Right of access

An individual has a right to know:

- Whether you have information about them
- Why you have it
- What sort of information it is
- Who you are sharing it with
- How long you will keep it
- Other information

They also have a right to a copy of it

You can't charge for replying to them
You have one month to comply

frettens SOLICITORS

Rectification rights

Inaccurate personal data?

The person affected has the right to insist:

- You correct mistakes
- You complete incomplete information

Right to be forgotten

There is a general duty to get rid of data that you no longer need

The person concerned can insist on that

Terms and conditions apply

For example, they may be able to insist that you delete your records if they take back their consent to you holding them.

Right to restrict processing

In some circumstances the individual affected may be able to insist that:

- You keep your records about them
- But you don't use them (except for specific limited purposes)

When you can deny access

You may be able to deny access to information:

- if you have it, as trustee, to investigate the bankrupt;
- if you have it as liquidator or administrator, to investigate the directors for CDDA;
- if it's protected by legal professional privilege;
- if releasing it might damage your negotiations with that person;

Consider ordering your files by these categories?
(For example, a privileged folder of everything passing between you and your solicitor)

frettens SOLICITORS


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner


Error reporting
What is an error?
Training and policies
Your legal duty

What is an error?

It's an error if:

- you lose any data
- your data passes into the wrong hands (accidentally or through malice)
- you receive any data (from a third party) you should not have
- you keep any data you don't need or should not have

Examples:

- a USB stick left on a train
- a stolen phone
- a letter - with an interesting enclosure - sent to you by mistake
- a lightning strike that corrupts your server and local back-up

Training and policies on dealing with errors

Your people need to know:

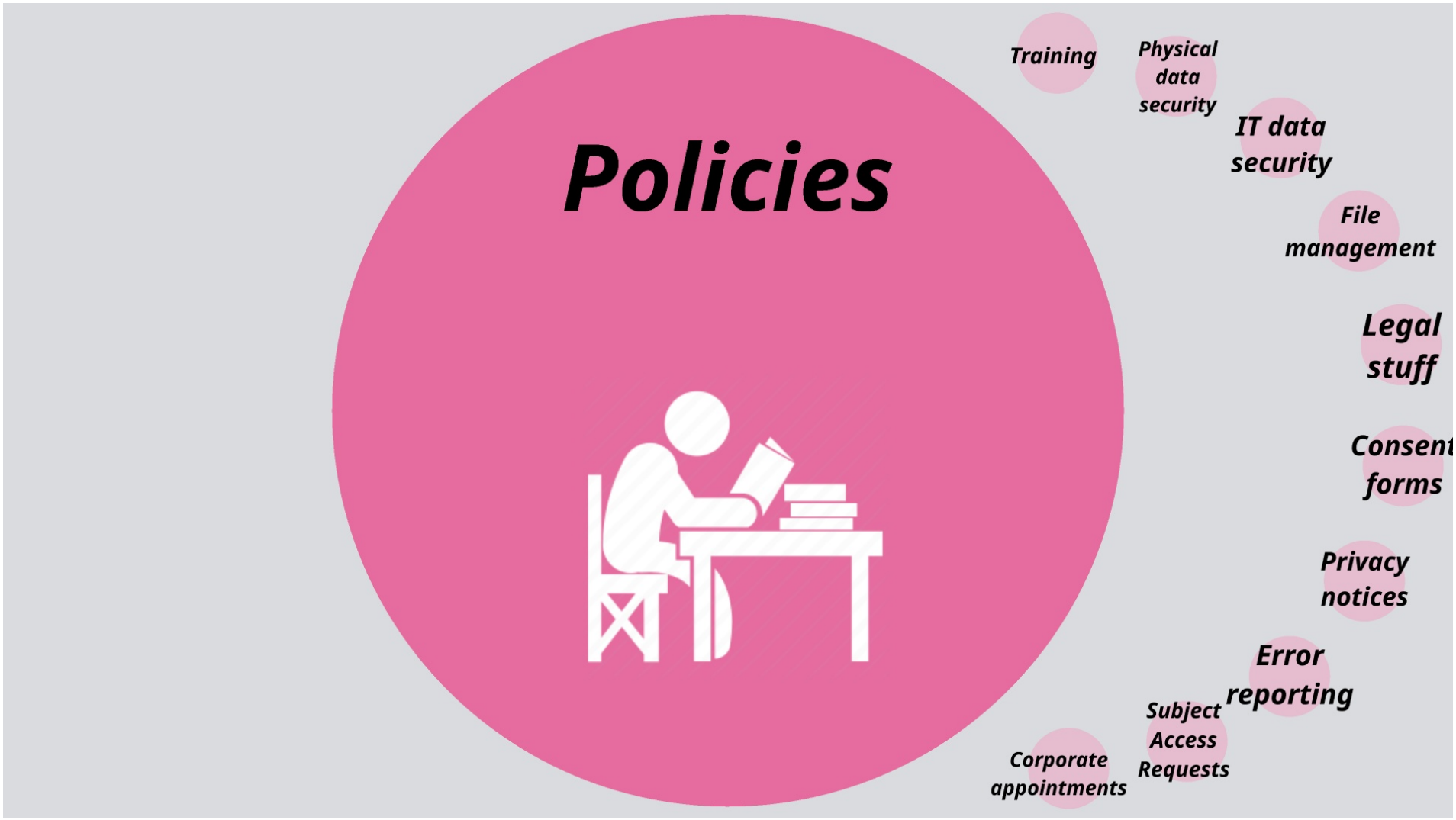
- What a data security error is
- That they won't be punished for honest mistakes
- That they ***must*** report it
- How to assess how serious it is
- How to minimise the damage (and how not to make it worse)

Your legal duty

As data controller, when an error occurs, you must

- assess the risk to those affected:
  - (consider the golden rule)
  - GDPR contains a hint on how to do this
- report it to the ICO:
  - within 72 hours, if possible
  - unless people's rights and freedoms are unlikely to be at risk
- tell the people affected:
  - but only if their rights and freedoms are likely to be at high risk; and
    - the data was not encrypted; or
    - you have not been able to mitigate the risk effectively; or
    - telling them individually involves disproportionate effort (in which case you must make a public announcement).


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner


Policies
Training
Physical data security
IT data security
File management
Legal stuff
Consent forms
Privacy notices
Error reporting
Subject Access Requests
Corporate appointments

Training

Make sure the data security director has the training they need

Set up a programme for all who deal with information about people:

- To bring in the changes
- With periodical refreshers
- To train new recruits

frettens SOLICITORS

Physical data security

Make sure that information on paper is safe

- Tighter rules for sensitive information?
- Limit access to sensitive files on a 'need to know' basis?
- Treat ID & financial information as sensitive?
- Who has keys to the office?
  - Are the cleaning contractors (for example) GDPR compliant?
- Lock cabinets?
- What do you do with the keys?
- (Limited) clear desk policy?
- Shredding policy?
- Off-site storage:
  - Transport arrangements?
  - Contractual arrangements?

IT data security

Make sure that digital data is safe

- Tighter rules for sensitive data?
- Where is your data kept?
  - Official copies
  - Unofficial copies
    - Laptops, tablets, phones, USB sticks, DVDs, etc
    - Personal email accounts, cloud accounts, home computers, private phones, etc

frettens SOLICITORS

IT data security

- Passwords. Are they secure? How often are they changed?
- Phishing attacks (on you, or on clients)
- Who has access, to which directories?
- How is your data backed up?
- Off-site back-ups; are they GDPR compliant?
- Encryption
  - (Some) files
  - Email attachments
  - Secure encrypted email (I have a Proton Mail account)
  - (Some) back-ups

File management

Working practices policies:

- Paper, or paperless files (or both)
- Emails and email attachments
- 'Follow me' printing
- Archiving dates
- Destruction of old files
- Destruction of back-ups
- Retention of minimal residual data files
- When to encrypt documents and emails

frettens SOLICITORS

Legal stuff

Recording the basis for taking and using personal data

- Manage files according to the type of data and the basis for using it
  - eg separate folder for CDDA investigation on each director
- Privacy notices for the folder

Consent forms

Identify the cases for which you may have to rely on consent

- IVAs (not the sole basis for using information about the debtor)?
- Other people mentioned in the IVA proposal (the spouse)?
- Corporate cases (particularly pre-appointment)?

Consent is not the best basis for using personal data in insolvency

But if you are not going to use consent, you need to identify another basis

frettens SOLICITORS

Privacy notices

Content - must comply with:

- GDPR requirements (which vary with the source of the information)
- The sort of information you are collecting
- The way you are using it
- The basis you are relying on to justify your use of it

Timing - you must send them out at the start

Who do you send them to?

- (This is a judgement for you, if you are not sending them to everyone)

Use a link in an email footer to comply?

frettens SOLICITORS

Error reporting

Establish clear reporting procedures for data security breaches

Subject access requests

Be prepared for them

Log the date of arrival and due date for supplying the information

Decide who would be the best people to deal with them

Organise file folders so information that needn't be disclosed is kept separate

Corporate appointments

Day one 'quick & dirty' data security review checklists

Trading - data security checklists

Asset realisations - data security checklists

HR records from BustCo - secure disposal policy

Other sensitive records - policies for identification, handling and disposal


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner


For the compliance director
Data protection officer?
The compliance role

Data protection officer?

IP's do not need to appoint a statutory data protection officer

(According to DPA'18)

The compliance role

Check that compliance matches the law. Review:

- the legislation (DPA'18 + UK GDPR)
- guidance
  - ICO
  - R3
  - your regulator
  - Solicitors

The compliance role

Register and pay the registration fee

- If already registered, your fee will carry forward
- The firm needs to pay a statutory fee to the ICO
- IP's also need to pay a statutory fee to the ICO
- The standard fee is £2,900.
    - Reducing to £40 (£35 by DD) for most firms

The compliance role

The task definition is likely to include responsibility for:

- Training
- Approving, implementing and monitoring compliance
- Reviewing and developing compliance
- Monitoring errors
- Reacting to serious errors
- Supervising subject access requests
- Keeping statutory records


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner

Any questions?

Disclaimer

Please treat this as entertainment, not compliance advice.

This presentation contains pointers towards the issues that you may need to consider to comply with the law.

It is not a comprehensive guide to the law.

Malcolm Niekirk

mniekirk@frettens.co.uk

07413 164814


The basics
Training
GDPR in a professional services firm
'Step-in' GDPR issues
GDPR for the office-holder
Error reporting
frettens
SOLICITORS
Subject access requests
Policies
For the compliance partner