MOORE STEPHENS

Data Privacy and Introduction to the EU General Data Protection Regulation

Chris Beveridge

Associate Director – Moore Stephens LLP, London

May 2017

What to expect from this session

- Introduction & background
- Privacy & data protection – “GDPR” specific
- What can you do now to best prepare?
- Can we help?
- The opportunity & conclusion
- Questions, concerns and AOB

Introduction & background

- Presenter introduction
- The last 18 months in London
- Where are we now?

What is data privacy and personal data?

Data privacy

"Information privacy, or data privacy (or data protection), is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them"

Definition of personal data

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Why is privacy important?

- Technological change – affecting customer experience more and more
- Individuals requiring more assurance that their personal data is secure
- Reputational damage
- Information held considered to be highly sensitive information

Regulatory requirements

In terms of data there are two regulatory requirements that UK organisations should be complying with:

- Current UK Data Protection Act 1998
- The European Union General Data Protection Regulation (“GDPR”)

Current UK Data Protection Act 1998

The UK Data Protection Act is currently governed by eight principles.

- **These principles will generally remain.**
- **Important to note that the EU General Data Protection Regulation will be an additional requirement.**
- **Principles that the current UK Data Protection Act is governed by:**

Data used fairly	**Specific purpose**	**Adequate**	**Accurate**
Retention	**Rights**	**Security**	**International**

The European General Data Protection Regulation (“GDPR”)

- Adopted by European Commission in April 2016
- Dubbed biggest shake up of data protection laws for 20 years
- Organisations around the globe will have until 25 May 2018 to fully comply with the new GDPR regulations
- Non compliance could result in considerable fines being issued
- Designed to strengthen and unify data protection for individuals within the EU. It’s primary objective is to give citizens back control of their personal data, along with simplifying the regulatory environment for international companies.

GDPR considerations

Increased territorial scope

- Captures all organisations processing or handing personal data residing inside the European Union.
- Applies to all organisations regardless of location.

Penalties

- Put simply if an organisation gets this wrong they could be fined up to 4% of their annual global turnover or €20 million – whichever is greater.
- Worst case scenario.
- Penalties can be issued to data controllers and data processors.

Data processors

- Data processors will also be liable to fines and will be asked to meet a number of obligations under GDPR.
- Data controllers need to be aware of any third party data processors in that process data on their behalf.

GDPR considerations (continued)

Consent

- Conditions surrounding consent have been strengthened.
- No longer allowed to use legal jargon – consents must be provided in an accessible form using clear and plain language.
- Consents must be as easy to withdraw as they were to give.

Breach notification

- Mandatory under GDPR.
- Breaches must be reported to regulatory authority and stakeholders within 72 hours of when the breach was discovered.
- Data processors must report to data controllers without ‘undue delay’.

GDPR considerations (continued)

Data portability

- Data subjects have right to request data held on them in a commonly used and machine readable format.
- Can now transfer to other “data controllers”.

Right to access

- Data subjects have right to confirmation from data controller that their personal data is being processed, where and for what purpose.
- Such requests must be provided free of charge.
- New timescales for such requests under GDPR.

Right to be forgotten

- Data subjects now have the right to be forgotten.
- Third party data processors need to be considered.
- Consent withdrawn or no longer holding data for specific purpose it was collected.
- Legal/public interest considerations.

GDPR considerations (continued)

Privacy by design

- Will be a legal requirement.
- Data protection must be considered at the design stage of a new system implementation.
- Not as an after-thought.
- Risks and controls need to be considered.
- Privacy impact assessments.

Data protection officers (“DPO’s”)

- Large jurisdictional organisations no longer required to notify local authorities of data activities.
- Internal record keeping requirement.
- Every organisation must have an individual designated with the responsibility of data.
- A DPO will become mandatory in some cases.
- A DPO is a role within itself.

What can you do now to best prepare?

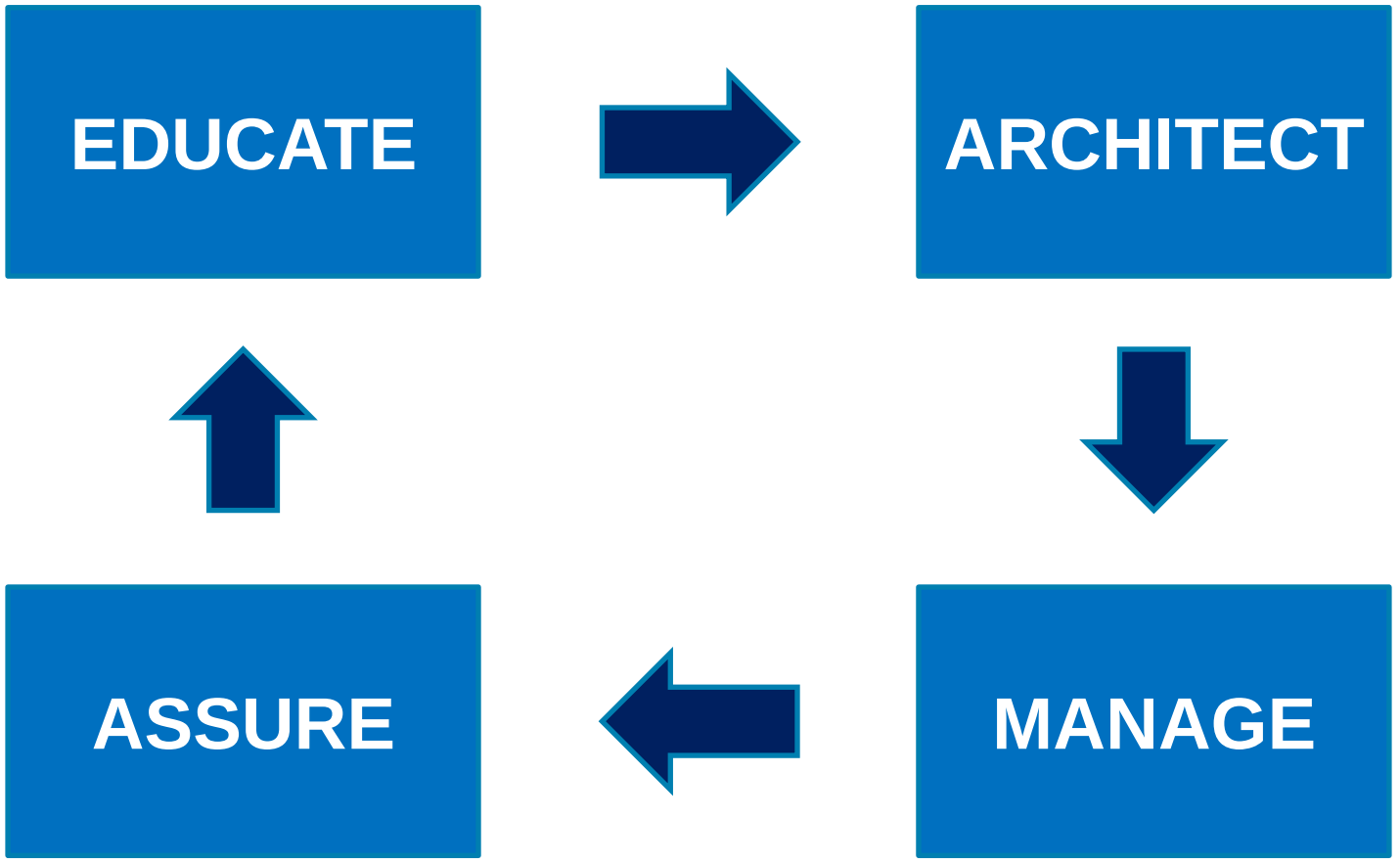
- Be aware.
- What personal information do you currently hold? Information audit?
- Review and ensure privacy notices are up to date.
- Individual’s rights – how would you deal with deletion and data portability requests?
- What procedures have you in place to handle subject access requests?
- Document the legal basis for processing the information you control.

What can you do now to best prepare? (continued)

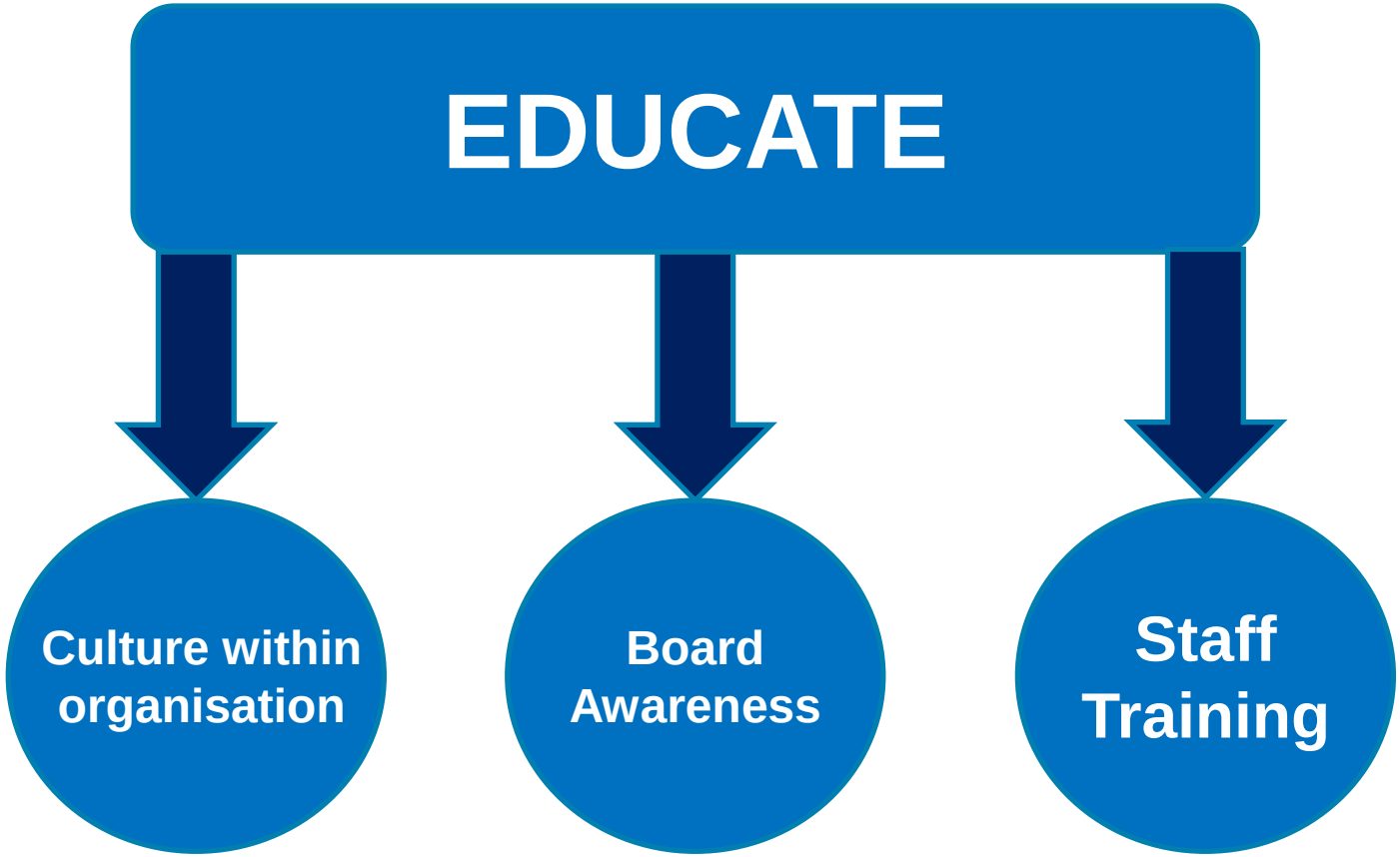
- Think about how you are requesting, obtaining and recording consents?
- Personal data held on children needs to be considered.
- Consider current procedures in place to detect, investigate and report data breaches.
- Undertake privacy impact assessments on any new systems planned.
- Ensure you have a DPO or designated data controller within your organisation that takes control of compliance issues.
- If you operate internationally need to consider data protection authority you may fall under in addition to GDPR requirements.

Can we help?

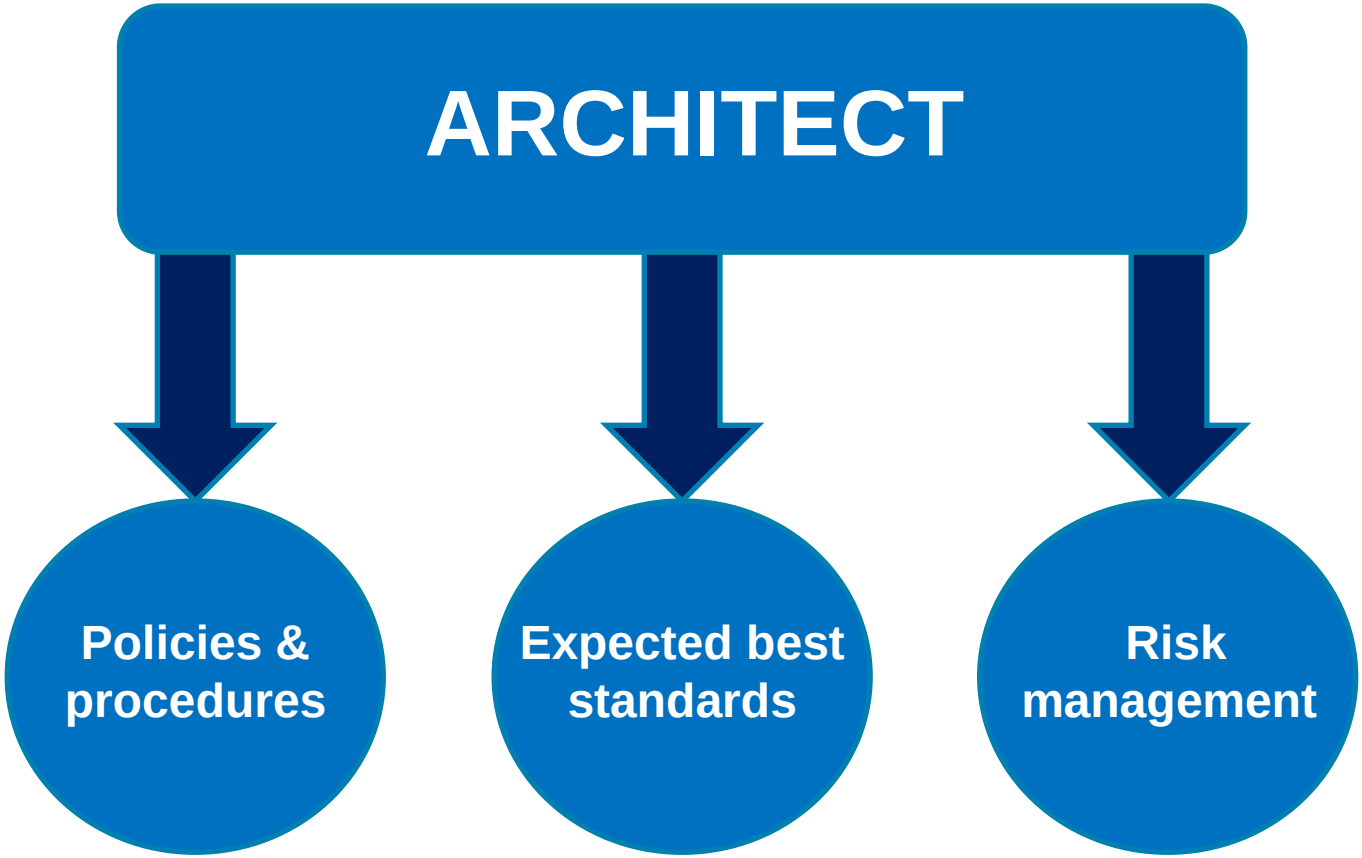
Split into four separate service areas:



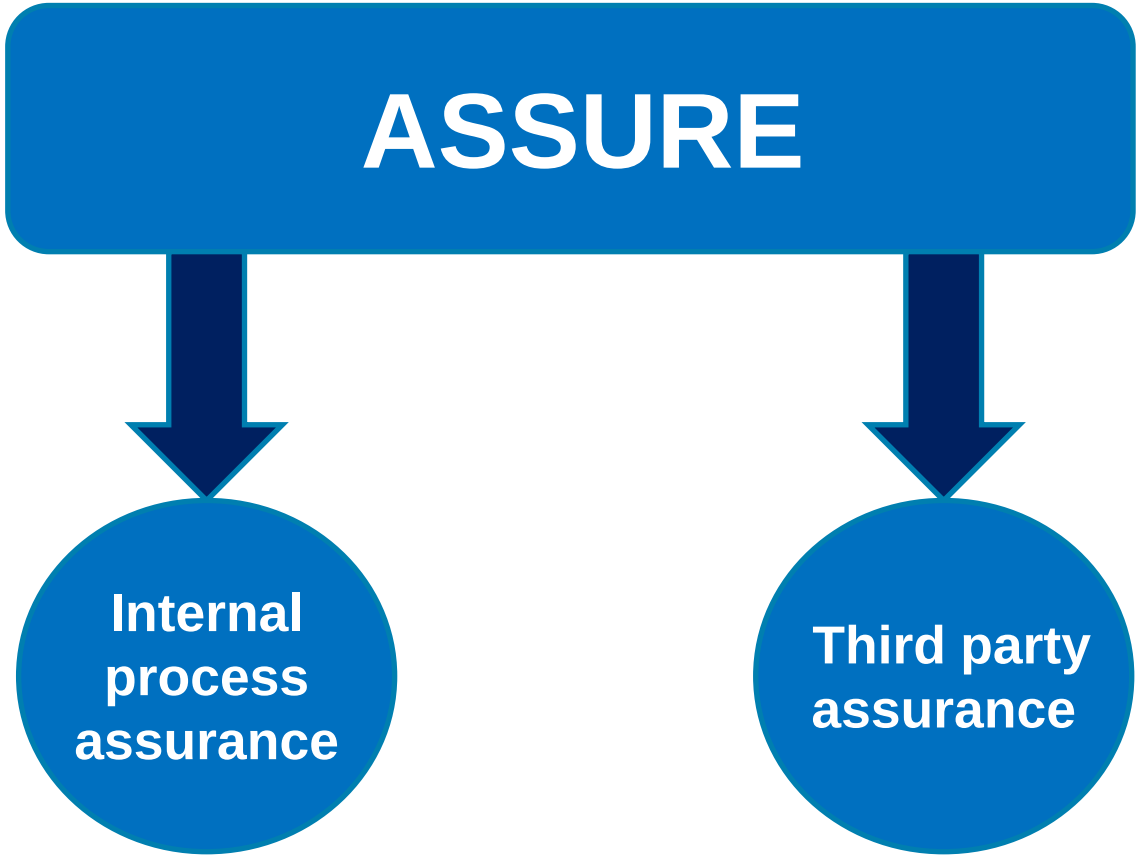
Can we help? (continued)



Can we help? (continued)



Can we help? (continued)



Can we help? (continued)

MANAGE

DPO outsourcing

Can we help? (continued)

Data Privacy Healthcheck

- Gap product
- Affordable & well received
- Bridging knowledge gap on what needs to be considered
- One stop shop on what is required before spending lots on legal and consultancy
- Interviews conducted with key individuals
- Report generated at end of healthcheck

Information you hold	Communicating privacy	Individuals rights	Subject access requests	Legal basis for processing personal data	Consent
Children	Data breaches	Data protection by design	Data protection officers	International	Information security

The opportunity & conclusion

- Probably viewed as a hindrance, however this is an OPPORTUNITY for you!
- Brexit has no effect on whether you need to comply or not!
- Please remember you should not ignore. Remember the size of the penalties earlier in the presentation on offer.
- Time is running out – only 1 year until enforcement date in May 2018.
- Failure to comply could have serious adverse affects on your organisation either financially through large penalties or from a trading perspective through loss of reputation.

Questions, concerns & AOB

MOORE STEPHENS

Christopher Beveridge

Associate Director

E christopher.beveridge@moorestephens.com

T +44 (0)20 7334 9191

www.moorestephens.co.uk

MOORE STEPHENS

Data Privacy and Introduction to the EU General Data Protection Regulation

Chris Beveridge

Associate Director – Moore Stephens LLP, London

May 2017