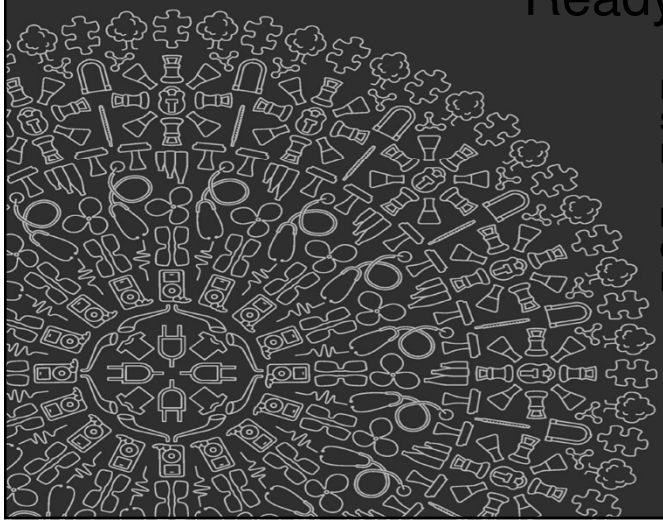
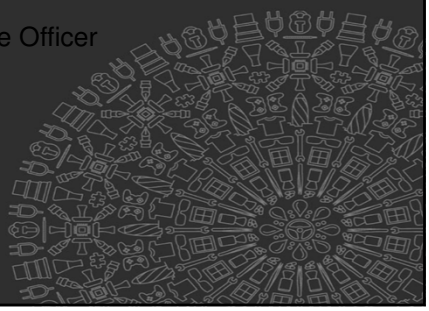
BRISTOWS

Ready or Not, GDPR is Here!



Robert Bond
Solicitor & Notary Public
Partner, Bristows LLP

Ken Liddle
Chief Compliance Officer
Rice University



40 YEARS AGO WE DIDN'T HAVE…

- Telex
- eMail
- Internet
- Mobiles
- Fax
- Big Data
- Social Media
- Tablets
- IoT
- AI
- Cloud
- Websites
- Drones
- Blogs
- CAV
- Smart Cities

Theoretically huge fines…

GDPR compliance is focused on a fixed point in time – it's like the Y2K Millennium Bug

"I'm still picking up a lot of concern from organisations about preparing for the GDPR by May.

Much of that is understandable – there's work required to get ready for the new legislation, and change often creates uncertainty.

However some of the fear is rooted in scaremongering because of misconceptions or in a bid to sell 'off the shelf' GDPR solutions.

I've even heard comparisons between the GDPR and the preparations for the Y2K Millennium Bug.

I want to reassure those that have GDPR preparations in train that there's no need for a Y2K level of fear"

Elizabeth Denham, Information Commissioner

4

Myth no.9

"We have to get fresh consent from our customers to comply with GDPR"

everything I do."

I can say categorically that these are wrong, but if misinformation is still being packaged as the truth, I need to bust another myth.

Myth #9 We have to get fresh consent from all our customers to comply with the GDPR.

You do not need to automatically refresh all existing consents in preparation for the new law. But the GDPR

31 May 2018

5

Data Protection under GDPR

Data Protection Principles

8 Key principles of DP law

Personal data must be…

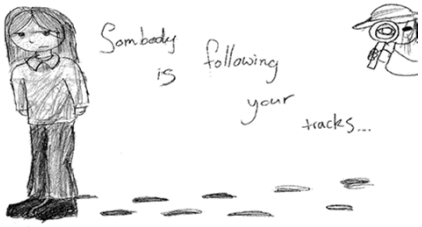
Processed fairly, lawfully and in a transparent manner **(lawfulness, fairness and transparency)**
Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes **(purpose limitation)**
Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **(data minimisation)**
Accurate and, where necessary, kept up to date **(accuracy)**
Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed **(storage limitation)**
In accordance with data subjects' rights **(rights of the data subject)**
Processed in a way that ensures appropriate security of the personal data **(integrity and confidentiality)**
Not be transferred to a third country or to an international organisation if the provisions of the Regulation are not complied with (**transfers)**

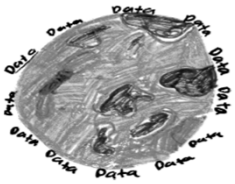
6

Data Protection under GDPR
Information to be provided to individuals

- Concise, transparent, intelligible and easily accessible form
- Clear plain language
- Iconography

Keep It Simple, Stupid!





Data Protection – Preparing for GDPR
Lawfulness of processing, legitimate interests and consent

- More flexibility to rely on 'legitimate interests' as a lawful ground to process personal data where there is a **relevant and appropriate connection** between the data controller and data subject
- **Consent –** remains a very high standard
- Must be **distinguishable from other matters** and provided in an intelligible and easily accessible form, using **clear and plain language**.
- It must be as easy to withdraw consent as it is to give it

8

How to make legitimate interests “legitimate”
Guidance on the use of Legitimate Interests under GDPR

- Processing needs a legal basis

✓ Consent

✓ Contractual

✓ Legal obligation

✓ Vital interests

✓ Public task

✓ Legitimate interests

◆ There is no hierarchy of grounds for lawful processing, but

◆ Different legal grounds carry different duties

◆ Controllers must be transparent about which basis they rely upon

9

How to make legitimate interests “legitimate”
Guidance on the use of Legitimate Interests under GDPR

Recitals 47 to 50 in the GDPR give some examples of when a Controller may be able to rely on Legitimate Interests:
1) DIRECT MARKETING - processing for direct marketing purposes under Legitimate Interests is specifically mentioned in the last sentence of Recital 47.
2) REASONABLE EXPECTATIONS - where individuals have a reasonable expectation that the Controller will process their Personal Data, subject to the balancing test.
3) RELEVANT & APPROPRIATE RELATIONSHIP - where there is a relevant and appropriate relationship between the individual and the Controller in situations where the individual is a client or in the service of the organisation. Examples of this would include (i) if an individual had recently (within the last 2 years) purchased goods or services from the Controller or donated to an organisation (ii) where the individual was a member of staff of the Controller.
4) STRICTLY NECESSARY FOR FRAUD PREVENTION - where the processing is strictly necessary for the purpose of preventing fraud. This could include verifying the registered address of the cardholder for a particular credit or debit card is the same as the cardholder’s normal place of residence or work.
5) ORGANISATIONAL - where Controllers that are part of an organisational group or institutions affiliated to a central body transmit Personal Data within that organisational group or to the central body. However, the rules on transferring Personal Data to a country outside Europe must be complied with if this is relevant.
6) NETWORK & INFORMATION SECURITY - where the processing of Personal Data is strictly necessary and proportionate for the purposes of ensuring network and information security. An example of this would include monitoring authorised users’ access to a Controller’s computer network for the purpose of preventing cyber-attacks.

10

How to make legitimate interests “legitimate”

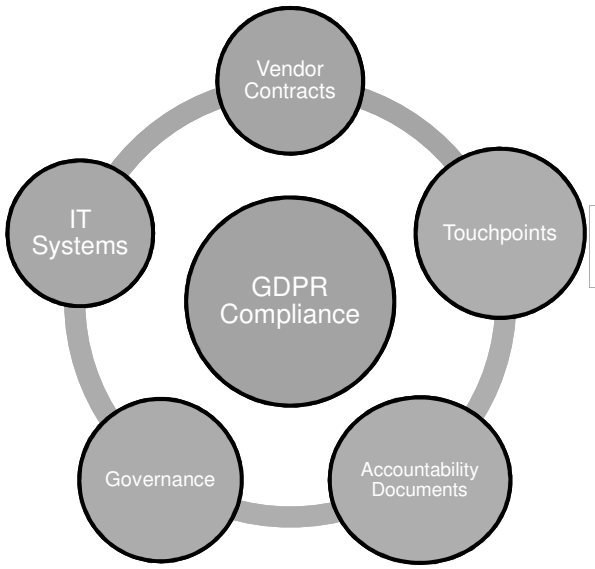
Guidance on the use of Legitimate Interests under GDPR

- Necessary
- Purposes
- Legitimate
- Interests
- Rights and freedoms
- Balancing test is needed or use of LIA

learn - apply - comply

11

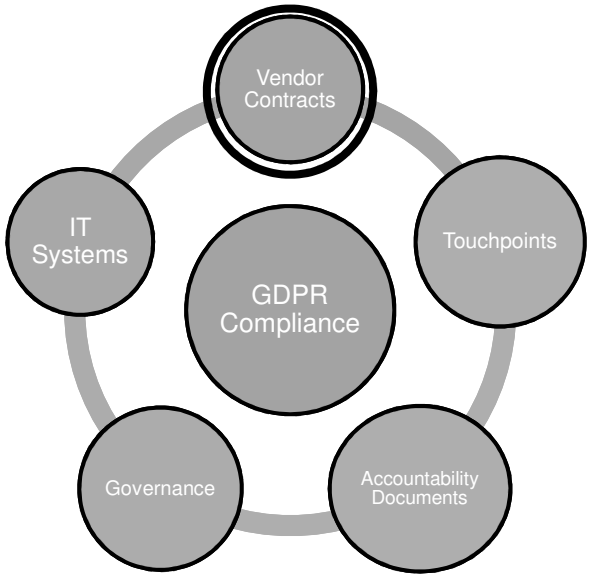
GDPR Compliance in Practice



Has time run out?

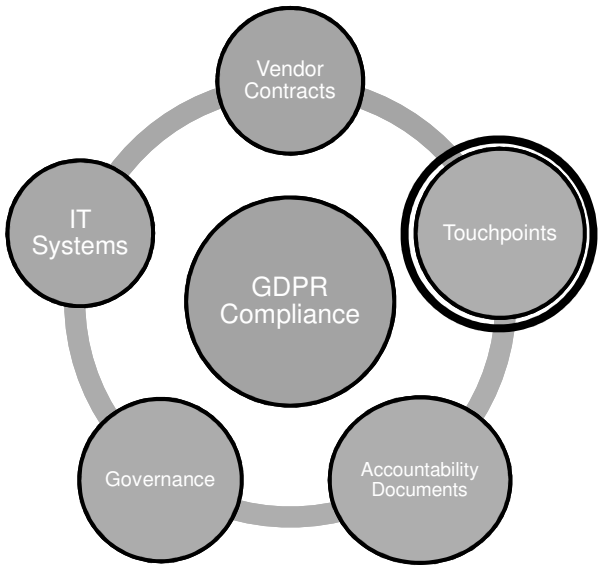
12

GDPR Compliance in Practice – Vendor Contracts



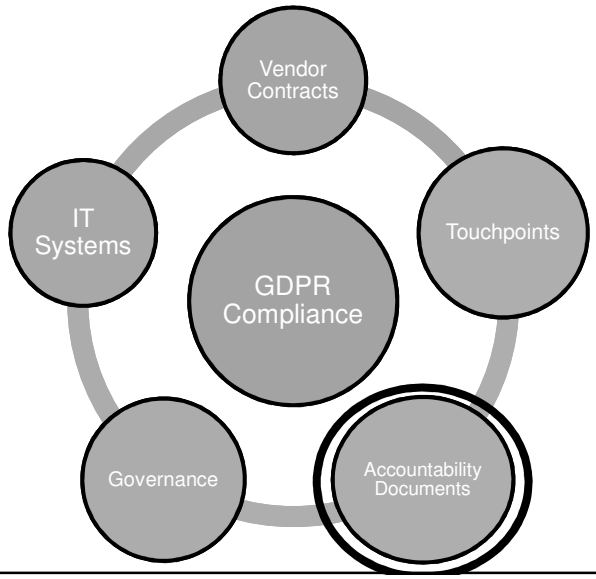
- Controller and processor both responsible for appropriate terms
- No transition period for updated terms. Review, prioritise based on risk and amend your existing contracts
- **De-scope** as many as you can: (i) expires pre-May (or 6 months post-May), (ii) no processing, (iii) vendor not a processor, (iv) MSA with no live SOWs, (v) large cloud vendors.
- **Prioritise**: volume/sensitivity of data, business criticality, service portability, duration, location.
- Remember to update templates too for new suppliers
- Send a standard processor addendum out?

GDPR Compliance in Practice – Touchpoints



- All points at which data enters the business
- Update notices and consent statements
- Include within training and awareness
- **Website:** online privacy notice (layers?), cookie notice, marketing consent statements, just-in-time notices, privacy dashboard / preference centre
- **Apps:** Privacy notice, modal windows, listing on app store
- Email: Link/footer to privacy notice
- Hard copy forms, Call centres (Pre-recorded messages, scripts)
- Don't forget Research, Development, Alumni Relations, Employees and Recruitment as well

GDPR Compliance in Practice – Accountability Documents



Art 24(2) GDPR: "*Where proportionate in relation to processing activities, the measures referred to in paragraph 1 [i.e. demonstrating compliance] shall include the implementation of appropriate data protection policies by the controller.*"

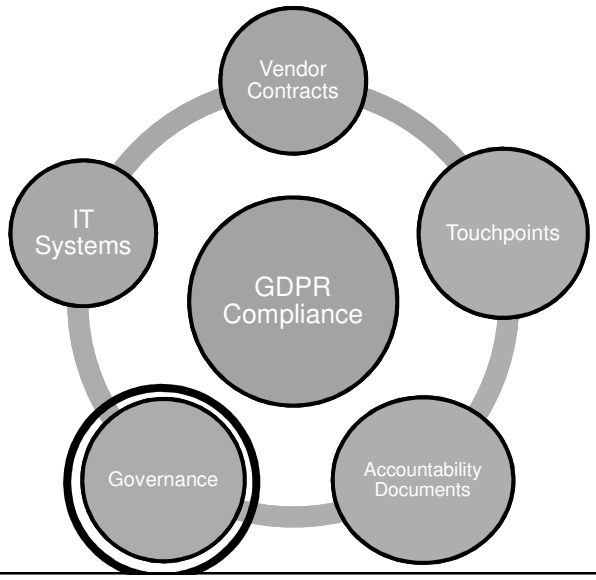
Overarching data privacy policy

Consumer Data | HR data

Vendors | DPIAs | Privacy by Design | Individual Rights | Data Retention | Breach Response

15

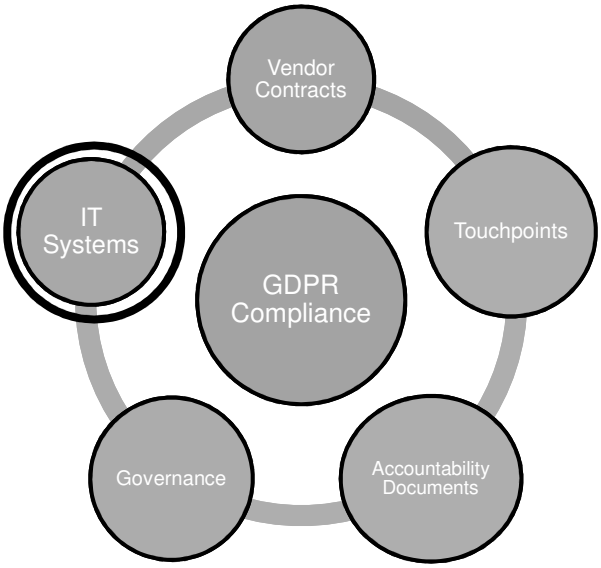
GDPR Compliance in Practice – Governance



- Implementing policies
- Training (on the policies themselves)
- DPO(s)
- Other roles/responsibilities
- DPIAs
- Record keeping (Art 30) (data 'inventory'?)

16

GDPR Compliance in Practice – IT Systems



- Review, prioritisation, remediation
- **Data security:** Appropriate to nature/risk of data
- **Data minimisation:** Remove unnecessary fields
- **Deletion/anonymization:** Automated process
- **Subject access:** Enable search/extraction
- **Other individuals rights:** Rectification, Erasure, Restriction, Objection, Data portability
- Record of consent
- Withdrawal of consent / Suppression

17

Data Protection – Preparing for GDPR

Sanctions for non-compliance are more than just for data breaches

Sanctions for non-compliance – two levels of fines…

➢Up to the greater of **2%** annual worldwide turnover of preceding financial year or **EUR 10 million** – for matters re internal record keeping, data processor contracts, data protection officers, data protection by design and default

➢Up to the greater of **4%** annual worldwide turnover of preceding financial year or **EUR 20 million** – for matters re breaching data protection principles, conditions for consent, data subjects' rights and international data transfers

18

Getting Started - The Big Four

1. Protect any personal data that you collect and use (including faculty!)
2. Update your Privacy Notice(s), and get it to touchpoints
3. Conduct departmental level data assessment
4. Have a breach notification plan to notify EU authorities within 72 hours of learning of a breach.

19

That dam breach or that damn breach?

GDPR Questions and Answers

Robert Bond
Solicitor & Notary Public
Partner, Bristows LLP
robert.bond@bristows.com

Ken Liddle
Chief Compliance Officer
Rice University
kliddle@rice.edu

21