BRISTOWS

Managing data transfers and preparing for GDPR

Robert Bond
Partner
Bristows LLP

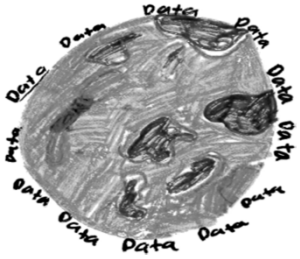
Topics

- Effective methods for data transfers
- Preparing for the General Data Protection Regulation
- Embedding ethics and trust into privacy practices

Data Protection – Preparing for GDPR

Data Transfers

- ~~Safe Harbor~~
- EU-US Privacy Shield
- EU approved third countries
- European Commission Standard Contractual Clauses
-
- Binding Corporate Rules
- Consent (although precarious to rely on)
- **Codes of Conduct (Article 38)**
- **Certifications / Seals (Article 39)**



Theoretically huge fines…

FINES FINES FINES!

ico. Information Commissioner's Office blog

Fake News

NEW LAWS TO THREATEN ORGANISATIONS

GDPR WILL LEAD TO HUGE FINES

Data Protection – Preparing for 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)**

5

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 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

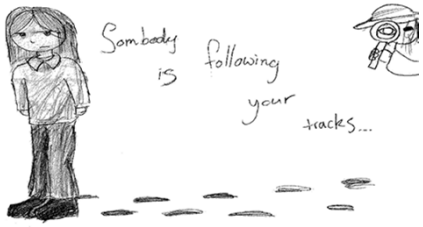
6

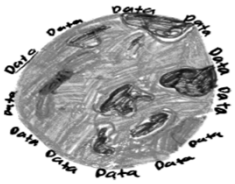
Data Protection – Preparing for GDPR

Information to be provided to individuals

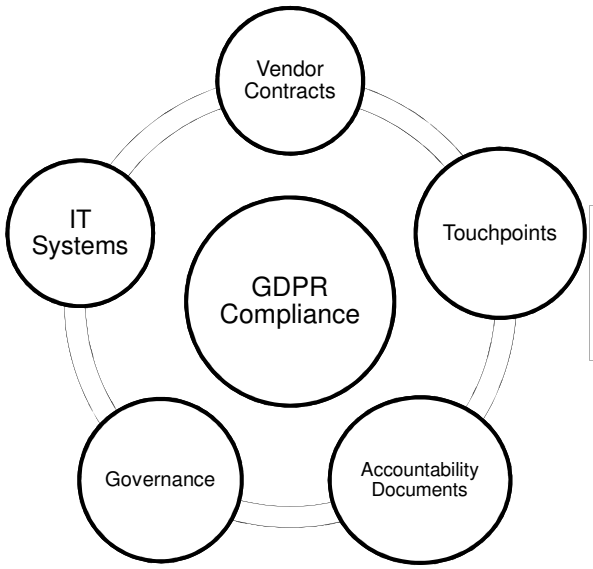
- Concise, transparent, intelligible and easily accessible form
- Clear plain language
- Iconography

Keep It Simple, Stupid!





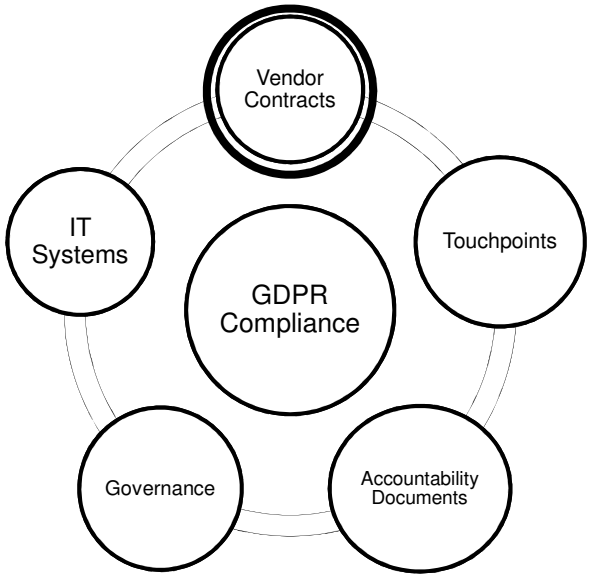
GDPR Compliance in Practice



Less than 70 days to go!

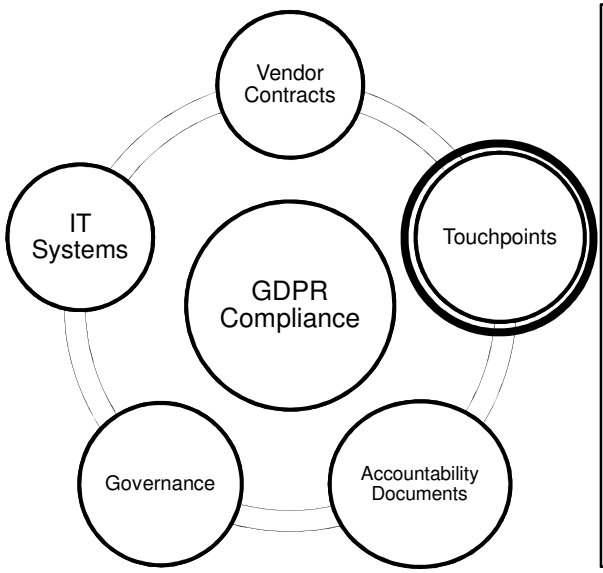
8

GDPR Compliance in Practice – Vendor Contracts



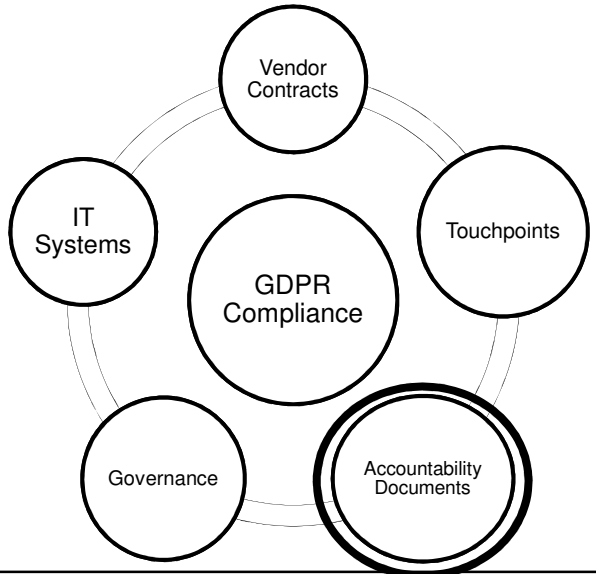
- Controller and processor both responsible for appropriate terms
- No transition period for updated terms. Review, prioritise and amend your existing contracts
- **De-scope** as many as you can: (i) expires pre-May (or 6 months post-May), (ii) no processing, (iii) vendor not a processor, (iv) MSA with 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 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.*"

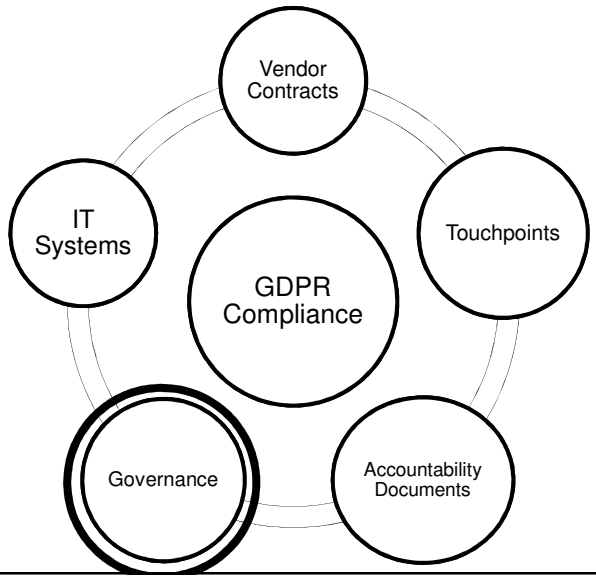
Overarching data privacy policy

Consumer Data | HR data

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

11

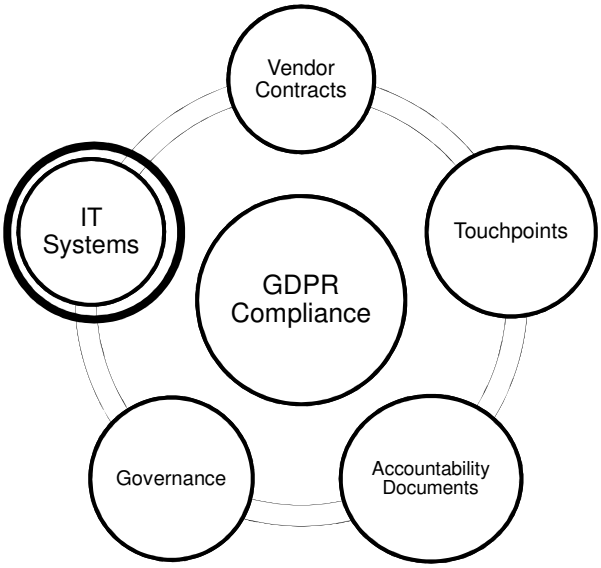
GDPR Compliance in Practice – Governance



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

12

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

13

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

14

That dam breach or that damn breach?

Why Ethics and Trust now?

- ✓ **Compliance with data protection law is mandatory**
- ✓ **Media attention on data breaches**
- ✓ **Consumer awareness of their privacy rights**
- ✓ **Risk of damage to brand and reputation**
- ✓ **Increased enforcements and fines**

16

What now?

Take a deep breath and ask…….

What personal data do we process and why?

Where and how do we process personal data?

Can we promote our compliance to build brand and trust?

Thank you

Bristows LLP
100 Victoria Embankment
London EC4Y 0DH
T +44(0)20 7400 8000

robert.bond@bristows.com