40 years ago we did not have…….
Understand jurisdictional privacy frameworks

- Historical influences and empires
- English common law influences
- European civil law influences
- Convention 108 (1981)

Challenges and Process of Developing a Privacy Program -- Basic Thoughts

- Don’t Get Paralyzed – Waiting For Perfection Will Result In Nothing Getting Done
- It’s a Team Effort – Get the Right Stakeholders Involved
- Start With the Simple Things and Move On From There
- Don’t Forget It’s Not Just Digital Data
- Remember Your Third Parties / Processors
- Prepare for Crisis

Our roadmap approach to data privacy compliance

[Diagram showing the steps in the roadmap approach]

- Define the country and group of companies covered by the project
- Assess existing notifications/authorisations
- Assess specific client concerns
- Assess general existing policies and procedures
- Assess general existing processing operations
- Define the required compliance measures
- Implement the required compliance measures
- Include Compliance bundle
  - Data transfer agreements
  - Review of existing notifications/presenting new notifications
  - Implement/update existing training measures
  - Define security measures – coordinating with client’s IT/Facilities team
  - Including list of ongoing compliance requirements
  - Liaise with local counsel
Theoretically huge fines…

"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

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

Data Protection Principles
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)

Lawfulness of processing 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
- Consent 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
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 100 days to go!

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
-日讯
- DPIAs
- Privacy by Design
- Data Retention
- Breach Response

GDPR Compliance in Practice – Governance

- Implementing policies
- Training (on the policies themselves)
- DPO(s)
- Other roles/responsibilities
- DPIAs
- Record keeping (Art 30) (data inventory?)
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 individual rights: Rectification, Erasure, Restriction, Object, Data portability
- Record of consent
- Withdrawal of consent / Suppression

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

That dam breach or that damn breach?
What now?
Take a deep breath and ask............

Thank you

Bristows LLP
100 Victoria Embankment
London EC4Y 0DH
T +44(0)20 7400 8000
robert.bond@bristows.com

This document is for information purposes only and any statements or comments it contains relating to matters of law are not intended to be acted on, or relied upon, without specific legal advice on the matters concerned. To the fullest extent permitted by law, we disclaim all liability and responsibility for any reliance on the statements or comments contained in this document.