The EU General Data Protection Regulation (GDPR)

It's never too late to get privacy compliant!

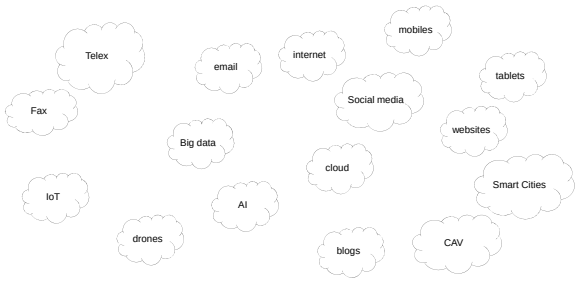
Maria Lancri, GGV Avocats, France

Axel von Walter, Beiten Burkhardt, Germany

Robert Bond, Bristows, UK

1

40 years ago we did not have…….



Quick recap

Key definitions

Term	Definition
Controller	A person who (either along or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed
Processor	Any person who (other than an employee of the data controller) who processes the data on behalf of the data controller
Personal data	Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller
Data Subject	An individual who is the subject of personal data

3

Quick recap

Key definitions

Term	Definition
Sensitive or special categories of personal data	Racial or ethnic origin, Political opinions, Religious beliefs Trade Union Membership, Physical or mental health condition, Sexual life, Criminal offences plus biometrics and genetic data
Processing	Recording or holding the information or data or carrying out any operation or set of operations on the information or data
Data Protection/Supervisory Authority	Tasked with the protection of personal data and privacy and take enforcement action against those who do not comply with the data protection law
Children's data	Personal data relating to a children - below the age of 13 then parental guardian consent is needed; above 13 and below 18 then a teenager can consent if privacy notices and in appropriate language

4

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

6

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)**

7

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

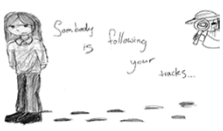
- More flexibility to rely on 'legitimate interests' as a lawful ground to process personal data where there is a **relevant and appropriate connection** between the data controller and data subject
- **Consent –** remains very high standard
- Must be **distinguishable from other matters** and provided 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

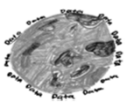
8

Data Protection – Preparing for GDPR
Information to be provided to individuals

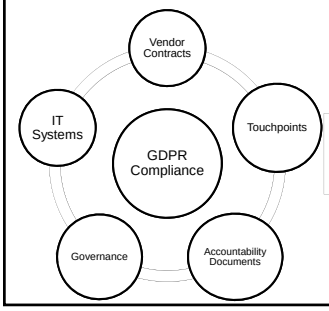
- Concise, transparent, intelligible and easily accessible form
- Clear plain language
- Iconography

Keep It Simple, Stupid!





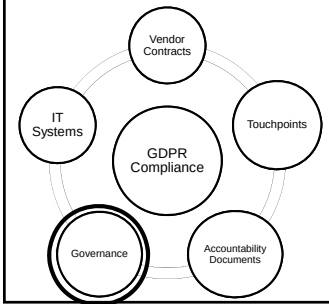
GDPR Compliance in Practice



Less than 100 days to go!

10

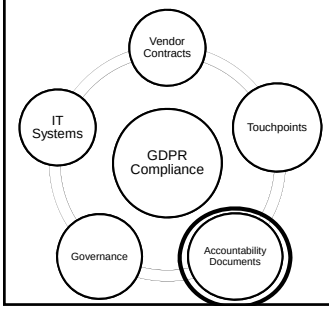
GDPR Compliance in Practice – Governance



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

11

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.*"

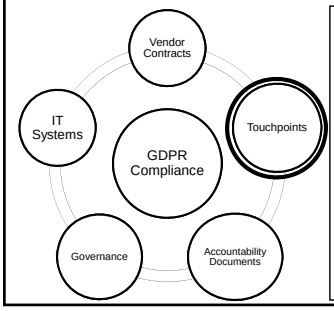
Overarching data privacy policy

Consumer Data | HR data

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

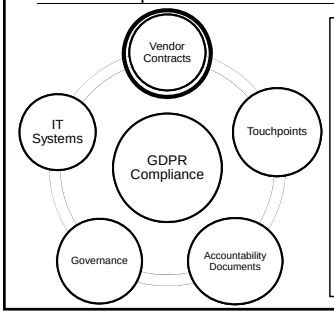
12

GDPR Compliance in Practice – Touchpoints



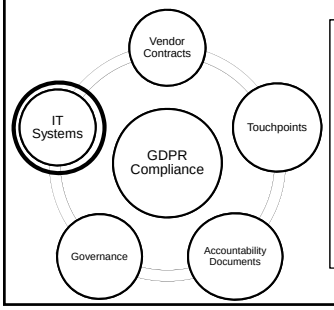
- All points at which data enters the business
- Update notices and consent statements
- Include within training and awareness
- **Website:** online privacy notice (layers?), cookie notice, marketing consent statements, just-in-time notices, privacy dashboard / preference centre
- **Apps:** Privacy notice, 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 – 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 – 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

15

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

16

That dam breach or that damn breach?

What now?

Take a deep breath and ask…….

What personal data do we process and why?

Where and how do we process personal data?

Do we comply with current law?

18

Thank you!

It's never too late to get privacy compliant!

lancri@gg-v.net

axel.walter@bblaw.com

robert.bond@bristows.com

19