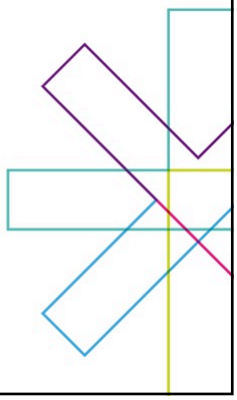
Taylor Vinters

The General Data Protection Regulation

12 October 2017



taylorvinters.com

The GDPR

- Talk about the GDPR in 30 - 40 minutes. (173 “recitals” and 99 “articles” long)
- * means the relevant paragraph has been simplified
- Red text means key change compared to the current law

Taylor Vinters

The GDPR

- European legislation which is largely replacing the Data Protection Act 1998
- Comes into force on 25 May 2018
- Applies throughout Europe
- Also applies to businesses outside the EU who are selling to, or monitoring the behaviour of, EU citizens
- Regulates “personal data”

Taylor Vinters

Section 1

Fundamentals

Taylor Vinters

Personal data

- Information relating to an identified or identifiable person
  - name, identification number, location data, or an online identifier (such as an IP address)
- Special categories: racial or ethnic origin, health data, genetic and biometric data.
  - Additional requirements apply!

Taylor Vinters

Controller or processor?

- Controller - decides why and how data is used:
  - Retailers
  - Online, consumer facing businesses
  - Employers
- Processor - does what its told with the data:
  - Cloud based service providers
  - Delivery companies
  - Outsourced payroll and IT

Taylor Vinters

The data protection principles

- Lawfulness, fairness & transparency*
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

- Accountability

Taylor Vinters*

Lawful, fair & transparent?*

Lawful: legal basis for processing

- Consent (freely given, specific, informed and unambiguous)

- Necessary for the performance of/enter into a contract with a data subject

- Necessary for the purposes of legitimate interests

Taylor Vinters*

Section 2

What does the GDPR mean for my privacy policies and contracts?

Taylor Vinters

GDPR: information requirements

- More information needs to be given to individuals by controllers:
  - Identity and contact details
  - Why they are processing their data
  - Which "legal basis" they are relying on
    - Consent, contract, legitimate interest, etc.

Taylor Vinters

GDPR: information requirements (cont)..

- Who they are sharing their data with
- Whether they will transfer the individual's data outside of the EEA (and if so, how they are protecting it)
- How long they will store it for
- A summary of individuals' rights under the legislation
- Meaningful information about any automated decision making (such as credit scoring)

Taylor Vinters

Privacy policies and notices

- Privacy policies are a convenient way of providing this information – but you don't have to use them
- You could provide the information on a "just in time" basis, with further detail set out elsewhere
- Policies and notices will need to be updated to comply: tweaks to business practices may be required to honour the new processes

Taylor Vinters

GDPR: contracting with others

- There must be a written contract in place where one party processes personal data on behalf of another.
  - Saying both parties will comply with the law is not enough!
- Current law has two requirements for processing contracts:
  - Processor will only act on the instructions of the controller
  - Processor will have technical and organisational measures in place to protect the personal data

Taylor Vinters

GDPR: contracting with others

- GDPR includes the current requirements, and adds:
  - contract must say what data is being processed, why and for how long
  - contract must make sure people carrying out the processing (think employees) are subject to confidentiality
  - only engage sub-processors with consent of the controller
  - assist the controller when dealing with breaches, audits and impact assessments
  - delete or return all personal data at the end of the services

Taylor Vinters

GDPR: contracting with others

- New rules apply to transfers of personal data outside of the EEA.
- Must have a formal mechanism in place to ensure the data is protected:
  - Model contract clauses
  - Certification scheme (such as EU-US Privacy Shield)
  - Code of conduct
  - Binding corporate rules

Taylor Vinters

Section 3

How to improve your personal data handling practices

Taylor Vinters

How to improve

- Look at the data protection principles!
- Review who has access to what data
- Secure devices and databases where you can
- Delete old data
- If relevant to you – when was the last time you reviewed when and how you use consent?
- Train your staff!

- Ask:
  - can we collect less data without compromising the project?
  - did we make it clear to individuals what we would be doing with their data?
  - do our contractors know about/respect data protection?
  - are we transferring data internationally? (additional rules apply)

Taylor Vinters

Section 4

Starting your own GDPR compliance project

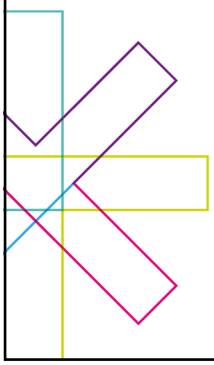
Taylor Vinters

GDPR compliance: getting started

1. Understand what data you hold, why, who you share it with and who has access to it.
2. Review data processing contracts and privacy notices (including what you tell your employees).
3. Do your answers to qs1 & 2 meet the lists set out in section 2? If not, update your documents/processes.
4. Review any transfers of data outside of the EEA.
5. Assess whether you need to appoint a DPO.

Taylor Vinters

Questions?



Taylor Vinters

Taylor Vinters LLP offices:
Tower 42, 33rd Floor
25 Old Broad Street
London
EC2N 1HQ
Tel: +44 (0)20 7382 8000

Merlin Place
Milton Road
Cambridge
CB4 0DP
Tel: +44 (0)1223 423444
DX: 724560 Cambridge 12

Taylor Vinters Via LLC
152 Beach Road
#10-08 Gateway East
Singapore
189721
Tel: +65 6299 0212

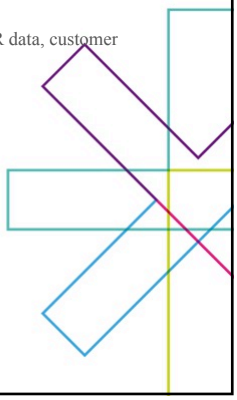
www.taylorvinters.com

GDPR: OUR SOLUTION Taylor Vinters

AUDIT | MAPPING | GAP ANALYSIS | REMEDIATION | GOVERNANCE | MAINTENANCE

Our solution works with you through the following 6 logical and sequential stages:

- **Audit and gap analysis**: review of an organisation's systems to determine their data protection compliance needs, and particularly what is required in order to become GDPR compliant
- **Mapping**: use of proven Data Flow technology to map their handling of personal data (internal HR data, customer and supplier personal data)
- **Remediation**: implementation of practical measures to achieve compliance, and to stay that way
- **Governance**: embedding data protection compliance within the fabric of their organisation
- **Maintenance**: ongoing support to maintain data protection and GDPR compliance



taylorvinters.com