General Data Protection Regulations: what you really need to know

9th March 2018

Stephen Thompson & Siobhan Williams

Clear Thinking. Smart Results.

What data does the GDPR apply to?

- The GDPR only applies to personal data
- 2 categories:
  - "personal data"
  - "sensitive personal data"

If data is completely anonymised, it will fall outside of the GDPR. However, beware that complete anonymisation can be difficult to achieve.

Clear Thinking. Smart Results.

DARWIN GRAY

Rights

The GDPR provides for:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automatic decision-making and profiling

Clear Thinking. Smart Results.

DARWIN GRAY

Legal basis for processing

There are six lawful bases set out in the GDPR:

1. Consent
2. Contract
3. Compliance with a legal obligation
4. Vital interests
5. Public interests
6. Legitimate interests

Legal basis for processing

Organisations are still entitled to deal with data providing they have a **legal basis** for doing so. What about consent?

Consent must be "freely given, specific, informed and unambiguous"

- ☐ We will contact you from time to time with marketing information about our services and events. If you do not wish to hear from us, please let us know by ticking this box.
- ☐ If you are happy for us to contact you from time to time by e-mail with marketing information about our services and events, please tick this box.

Clear Thinking. Smart Results.

DARWIN GRAY

Legal basis for processing

Legitimate Interests

- Three part test
  - Purpose
  - Necessity
  - Balancing
- Interests
- Document – the biggest change
- Use
  - Third parties
  - Marketing

Clear Thinking. Smart Results.

DARWIN GRAY

Legal basis for processing

- You need to think about what your justification for using data is:

  - Complying with a legal obligation will not give a blanket authorisation to use an individual's data for other purposes

  - You will be relying on different grounds to process data depending on your relationship with the individual

Documentation

- The GDPR contains explicit provisions about documenting your processing activities.
- You must maintain records on several things such as processing purposes, data sharing and retention.
- Records must be kept up to date and reflect your current processing activities.
- The ICO have produced some basic templates to help you document your processing activities which can be found on their website.

E-Privacy Regulation

- Includes specific provisions for electronic communications
- 05 December 2017 a consolidated version of the e-Privacy Regulation was released
- Missing the deadline of 25 May 2018 = a gap in the law

E-Privacy Regulation

Recommendations

1. Any processing of communications data must be based on a legal ground
2. Legal grounds must not include legitimate interest.
3. Confidentiality of communications data shall be ensured "at rest" and for machine-to-machine communications
4. Consent must have the same meaning as in the General Data Protection Regulation. Technical and privacy settings should support giving and withdrawing consent.
5. Weakening of confidentiality and integrity of communications should be prohibited
6. Protection against unsolicited communications should be comprehensive

Clear Thinking. Smart Results.

DARWIN GRAY

E-Privacy Regulation

Where a business has obtained an individual's electronic contact details in the context of the sale of a product or service, the business may send electronic direct marketing materials to that customer.

- Specific: in the context of the sale of a product or a service
- Right to object
- When? – at collection and every time a communication is sent

Clear Thinking. Smart Results.

DARWIN GRAY

Key changes to be aware of

1. Structural/cultural changes
    - “data impact assessments”
    - records of processing operations
    - appointment of a data protection officer
    - consent must be “freely given, specific, informed and unambiguous”
2. Additional individual rights
    - more transparency
    - a “right to be forgotten”

Clear Thinking. Smart Results.

DARWIN GRAY

Key changes to be aware of

3. Breaches and penalties

- “breach” is more than just loss of data
- “significant” breaches must be notified to the ICO within 72 hours
- Two tiers of potential fines:
  - the higher of €10million or 2% of your global turnover
  - the higher of €20million or 4% of your global turnover

Clear Thinking. Smart Results.

DARWIN GRAY

Issues

1. Information gathering

- Consider what information you need to fulfil your contractual and regulatory obligations. Are you currently collecting more information than you need?

2. Sharing information:

- who do you need to share information with and why?
- do you have data sharing agreements in place?
- have you informed individuals you will be sharing information?

Issues

3. Destruction timetable

Consider:

- Regulatory obligations
- Potential to use data in future
- Employee and recruitment information
- Information you have about third parties

4. Commercial or other activities

Think about what legal basis you have to use personal data for different activities:

- Commercial activities
- Marketing communications

Clear Thinking. Smart Results.

DARWIN GRAY

Employment issues

- Employment Data
  - CCTV film
  - lift or floor access information
  - internet records and email monitoring
  - sickness records
- Some employment data likely to be unstructured, more challenging for data controllers

What should you do to comply?

- Next few weeks
  - conduct an internal audit of your current policies & procedures
  - consider what data you actually need from individuals and what you need to do with it
  - educate / train your staff about the GDPR
  - Consider appointing a data protection officer

Clear Thinking. Smart Results.

DARWIN GRAY

What should you do to comply?

- March and April
  - review the contracts you have in place with third party suppliers
  - draft an internal strategy to deal with data
  - update your privacy policy and terms and conditions
  - review your contracts of employment and staff handbook
  - refresh your existing database for marketing communications

Clear Thinking. Smart Results.

DARWIN GRAY

What should you do to comply?

- May
  - ensure that updated policies and terms are finalised
  - conduct refresher training for staff
  - make sure all new employment contracts/consent forms are signed and returned to you, and staff have read your policies
  - ensure that your technology strategy is implemented and reviewed
  - documenting your processing activities

Clear Thinking. Smart Results.

DARWIN GRAY

Privacy Impact Assessments (PIA)

- A PIA enables an organisation to identify and minimise privacy risks
- A PIA will ensure that potential problems are identified at an early stage
- Conducting a PIA should enable an organisation to produce better policies and systems
- PIAs can be applied to new projects or existing systems

Clear Thinking. Smart Results.

DARWIN GRAY

Privacy Risk

- The risk of harm arising through an intrusion into privacy
- This may arise through personal information being:
  - Inaccurate, insufficient or out of date
  - Excessive or irrelevant
  - Kept for too long
  - Used in unacceptable ways
  - Not kept securely

Projects that might require a PIA

- New IT system
- Data sharing initiative
- Proposal to identify people in a particular demographic
- New surveillance system
- New database
- Legislation, policy or strategy changes

Clear Thinking. Smart Results.

DARWIN GRAY

The PIA Process

- A flexible and proportionate process
- Begin left early on in a project - screening questions
- Should incorporate the following steps:
  - Identify the need for a PIA
  - Describe the information flows
  - Identify the privacy and related risks
  - Identify the solutions
  - Sign off and record outcomes
  - Integrate and consult internally and externally

Identifying the need for a PIA and information flows

- Screening questions – keep simple
- Develop own questions or use ICO questions
- Not designed to be used by experts
- If not a PIA then at least a data legal compliance
- How is information collected, stored, used and deleted

Identifying privacy & related risks

- To individuals:
  - Inadequate disclosure controls
  - New surveillance methods means unjustified intrusion
  - Colleting a wider information set
  - Vulnerable people may be concerned
  - No longer collecting information anonymously
  - Collected and stored unnecessarily
  - Retained for longer than necessary

Identifying privacy & related risks

- Corporate:
  - Sanctions, fines and reputational damage
  - Expensive fixes for problems
  - Unnecessarily stored information less useful for business
  - Public distrust leads to reputational damage
  - Claims for compensation
  - Loss of business

Identifying & evaluating privacy solutions

- PIA should eliminate, reduce or accept risks
- Should be proportionate
- Possible steps
  - Decide not to collect or store certain information
  - Devising retention periods
  - Appropriate technological security measures
  - Staff training and guidance
  - Proper anonymising
  - Easy access to information if required
  - Care in selecting data processors
  - Data sharing agreements

Clear Thinking. Smart Results.

DARWIN GRAY

Sign off & recording outcomes

- Some risks may be acceptable
- Record details of decisions made
- Possibly publish a PIA report
- Integrate back into project plan

Possible Screening Questions (1)

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Clear Thinking. Smart Results.

DARWIN GRAY

Possible Screening Questions (2)

- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

Clear Thinking. Smart Results.

DARWIN GRAY

Further information

Lots of useful guidance and information on the ICO website. Their guidance is being updated all the time

www.ico.org.uk

Get in touch

If you would like advice or assistance with GDPR compliance please get in touch:

sthompson@darwingray.com

swilliams@darwingray.com

Clear Thinking. Smart Results.

DARWIN GRAY

Thank you for listening

@DarwinGrayLLP

Darwin Gray LLP

Clear Thinking. Smart Results.