Steeles Law
Solicitors

Are you ready for the GDPR?

12 December 2017

Nigel Lubbock
Senior Director
nlubbock@steeleslaw.co.uk

James Hopgood
Solicitor
jhopgood@steeleslaw.co.uk

What is the GDPR?

The **General Data Protection Regulation** is EU legislation that will replace the Data Protection Act 1998 (DPA):

- Takes effect from 25 May 2018
- Brexit unlikely to affect ongoing application. Data Protection Bill 2017 – 2019 will create a UK regime based on the GDPR
- Updates key concepts in light of technological changes
- It's about accountability and giving individuals more control
- Privacy by design
- Rules for data security and dealing with data breaches
- New regime for enforcement
  - Increased appetite for enforcement
  - "Draconian penalties"

Six questions

1. Are you dealing with personal data?
2. What are you doing and can you do it?
3. Is your storage secure enough?
4. Are you aware of the data subject's rights?
5. What if you get it wrong?
6. How do you get ready?

Think about: **Consent, accountability and risk**

Question 1: Are you dealing with personal data?

- “Information relating to an identified or identifiable natural person (“data subject”)”
- An individual “who can be identified directly or indirectly…by reference to an identifier”:
  - Name
  - Identification number
  - Location data
  - An online identifier (IP address)

Think about the impact on the individual:

- Special categories of personal data which are particularly sensitive
- Do you really need this?

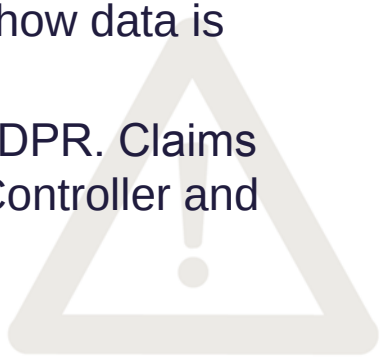
“Processing” personal data

The GDPR applies to personal data which is processed by automated means or which forms, or is intended to form, part of a filing system.

The fact that you have personal data most likely means you are “processing” it:

- Collection
- Storage
- Retrieval
- Use
- Erasure
- Destruction

- **Data processors:** Processing, dealing with, or using personal data
- **Data controllers:** The person or people who decide whether and how data is processed
- It is the Controller’s responsibility to ensure compliance with the GDPR. Claims for breaches of the GDPR may, however, be brought against the Controller and the Processor directly.



Question 2: What are you doing with personal data?

1. Use personal data lawfully and transparently
2. Collect only for specified, express and legitimate purposes. Further processing only allowed for purposes compatible with the original purpose
3. Adequate, relevant and limited
4. Accurate and kept up to date
5. Kept for no longer than necessary
6. Processed in accordance with the subject's rights
7. Ensure appropriate security
8. Not transferred to an organisation outside of the EEA without adequate protection measures

Fair and lawful processing

- Legitimate grounds for collecting and using the personal data
- Do not use personal data in ways that have unjustified adverse effects on the individuals concerned
- Be transparent about how you intend to use the data from the outset
- Handle personal data in ways the data subject would reasonably expect
- Do not use personal data for unlawful purposes
- Do not keep personal data for longer than necessary

Consent

- Data previously gathered without meeting the requirements of the GDPR should not be used
- Consent must be **freely given, specific, informed** and **unambiguous** indication of the individual's wishes
- There must be some form of **clear affirmative action**, a positive opt-in – consent **cannot be inferred from silence**, pre-ticked boxes or inactivity
- It must be **specific, clear, prominent, properly documented** and **not presumed**. The data subject should be able to **withdraw it at any time.**
- Ensure that consent is **evidenced** – record how, not just the fact
- Consent should only be sought to the **extent actually needed** – you are unlikely to be able to rely on a general "consent"

Other lawful purposes?

It's best to have consent if you can get it. In some cases this might not be possible.

Other lawful grounds for processing:

- Performance of a contract with the data subject
- Legal obligation to which the data controller is subject
- Protecting the vital interests of an individual
- To complete the performance of an activity which is in the public interest
- Necessary for the purposes of the legitimate interests pursued by the controller or by a third party

Marketing

“Soft opt-out”: Potential “legitimate interests” justification

Draft e-Privacy Regulations:

- Electronic contact details for electronic mail;
- Obtained from a customer in accordance with the GDPR;
- Use by that person only;
- Market similar products and services;
- Opportunity to object at the point of collection and each time a message is sent.

Accountability

It’s not enough to say you are compliant – demonstrate how.

- Keep records to show how and to what consent was given
- Use privacy notices
- Maintain records of activities related to higher risk processing.
- Implement appropriate technical and organisational measures
- Staff training, internal audits of processing activities and reviews of internal HR policies
- Policies are a good start but make sure that you comply with them.
- Implement data protection by design:
  - Data minimisation
  - Pseudonymisation
  - Transparency
  - Allowing individuals to monitor processing; and
  - Creating and improving security features on an ongoing basis

Sharing and transferring data

- Do you have consent or is there another justification?
- You are responsible for the actions of third parties with whom you share personal data
- Check third parties' privacy policies and procedures to ensure their compliance and use contracts to protect against risk
- The GDPR imposes strict restrictions on the transfer of personal data outside the EEA
- The transfer of personal data outside the EEA is permissible where:
  - Data is sent to a third country the subject of an "adequacy decision"; or
  - "Appropriate safeguards" are in place (e.g. standard contractual clauses); or
  - One of the limited exceptions apply

Question 3: Are you storing personal data securely?

Remember:

- Consent: **Should you still have this?**
- Accountability: **What are you doing to protect personal data?**
- Risk: **What are the consequences of a data breach for the data subject?**

Think about:

- Privacy by design. Set out to protect personal data and build in safeguards from the start.
- “State of the art technology”
- As technology moves on, the minimum measures you must employ will increase
- All information has value. Protect it even if it’s not personal data. **Consider your duty of confidentiality.**

Managing risk

Protect personal data by from the start by design

- Implement specific technical or organisational measures, such as encryption, to improve security; pseudonymisation or other steps to de-identify personal data or simply minimise the amount of personal data required.
- Three prong approach:
  - Identify any potential harms
  - Evaluate the severity of the harm
  - Consider the likelihood of the harm occurring
- This will allow you to think about what you can do to minimise and mitigate the risks to individuals

Data breaches

- “A breach of security leading to accidental or unlawful destruction, loss alteration unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed”
- The channel through which there is a breach does not matter.
- Think about malicious breaches (such as hacking) and passive breaches (such as documents left on a train)
- Clean desk policy & confidentiality agreements with service providers (such as cleaners)
- Limit access to personal data (particularly if high risk)

Data breaches: the notification regime

- Chain of notifications
- Data processors must inform the data controller
- Data controllers must report breaches to the ICO as soon as possible, within a maximum of 72 hours
- If dealing with **high risk data** the **data controller** must tell the **data subject** without undue delay
- There are only **limited exceptions**. If unsure whether or not to report, the presumption should be to report

Data breaches: Managing the risks

Be proactive:

- Identify weaknesses in security
- Have documented policies, audits, reviews, notices
- Avoid high risk data if possible: think minimisation & pseudonymisation

Be reactive:

- Keep records of breaches, the effects, and remedial steps that you take
- You may be required to make data processing records available to the relevant supervisory authority for purposes of an investigation

Question 4: Are you aware of the data subject's rights?

Similar rights as under the DPA but with some changes:

- The right to be informed (privacy notices)
- The right of access (subject access requests)
- The right to rectification
- "The right to be forgotten" (erasure)
- The right to restrict processing
- The right to data portability
- The right to object
- Further rights in relation to automated decision making and profiling

The right to be informed: Privacy notices

The information you supply must be:

- Concise, transparent, intelligible and easily accessible;
- Written in clear and plain language; and
- Free of charge

There are certain formal requirements, including:

- Identity and contact details for data controller
- Purpose of the processing
- Categories of personal data
- Recipients of personal data
- Details of transfers
- Retention periods
- Right to withdraw consent and right to complain

Right to be forgotten

- In fact a limited right to erasure.
- Not absolute.
- Individuals have a right to have personal data erased only in specific circumstances:
  - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
  - When the individual has withdrawn consent and there is no other lawful ground for processing
  - When the individual objects to the processing and there is no overriding legitimate interest
  - The personal data was unlawfully processed
  - The data has to be erased to comply with a legal obligation

Question 5: What if you get it wrong?

The maximum penalty for breaching the GDPR is €20,000,000 or 4% of turnover (whichever greater)

- Consider the seriousness of the breach from the data subject's perspective
- Compensation to the data subject for material and non-material damage (Vidal-Hall v Google Inc)
- Criminal liability
- Vicarious liability for employee's criminal acts (Various Claimants v WM Morrisons Supermarket PLC 16 October 2017)
- Future scope for directors' personal liability
- Reputational damage

Question 6: How do you get ready?

- Read the **ICO guidance**
- Awareness & Training
- Make sure you can evidence consent where possible
- Review and amend terms and conditions to incorporate a privacy notice
- Review contracts and include appropriate indemnities if possible
- Think about data breaches and review security: consider chain of custody and weak links
- Who in your organisation needs access to personal data?
- Put in place plans for review of data and routine destruction
- Consider how you might implement privacy by design

Data protection impact assessments (DPIA)

- The GDPR requires that an organisation must carry out a DPIA when:
  - Using new technologies; and
  - Processing is likely to result in a high risk to the rights and freedoms of individuals.
- A DPIA indicates best practice and may be helpful in demonstrating compliance with the principles of the GDPR even if no requirement to carry one out
- Allows organisations to identify and fix problems at an early stage, reducing costs and damage to reputation

Data protection officers (DPO)

The DPO will be in charge of ensuring that the business is compliant, putting in place the mechanisms and procedures, reporting a breach to their relevant authority and the point of contact to the business' regulatory authority

Businesses will need a DPO if they:

- Regularly and systematically monitor data subjects on a large scale; or
- Process special categories of (sensitive) data on a large scale; or
- Process data relating to criminal convictions

Steeles Law
Solicitors

Are you ready for the GDPR?

12 December 2017

Nigel Lubbock
Senior Director
nlubbock@steeleslaw.co.uk

James Hopgood
Solicitor
jhopgood@steeleslaw.co.uk