General Data Protection Regulations

Implications for BCS

2016

What is the GDPR?

General Data Protection Regulations

- Ratified in May 2016, these regulations replace the old Data Protection Directive and associated European instruments around data protection and personal data
- Comes into effect on May 23rd 2018
- Builds upon 20 years of work in improving rights over personal data and setting standards for processing data for organisations
- Supersedes and replaces the Data Protection Act 1998

But what about Brexit?

- As Article 50 (Treaty on the European Union) has not been triggered yet, and with the anticipated two year negotiation period for departure, the regulations will take effect automatically on May 23rd 2018 regardless of our plans to leave and will take effect as worded
- The government confirmed on 24th October 2016 that the UK will be implementing GDPR as stated.

The Eight Principles of Data Protection

At all times data must be:

1. Processed fairly and lawfully
2. Processed for limited purposes and in an appropriate way
3. Adequate, relevant and not excessive for the purpose
4. Accurate
5. Not kept longer than necessary for the purpose
6. Processed in line with data subjects' rights
7. Secure
8. Not transferred to people or organisations situated in countries without adequate protection

So what is changing?

Key Changes summary

- Increased rights and control of personal data for the individual
- Increased oversight by the ICO over practices of organisations
- Stricter controls over data processing as a whole
- Increased sanctions for breaches
- Requirement for provable consent
- Data Protection by Design and Default
- Increased record keeping requirements

Data Protection Act vs GDPR
Consent

Current Law

- Consent required from individuals to process their data.
- Individuals must signify their agreement to processing through direct agreement, by an action or inaction (failing to tick a “do not contact” box in a web-form).
- Consent must specify what an individual agrees to and data can only be used for that purpose.

GDPR

- Consent must be an unambiguous affirmative action i.e. “I agree to BCS to process my data for the purpose of…”
- Consent must be fully informed, specifying exactly how data will be processed and the legal basis for doing so.
- Consent must be gained for each individual processing purpose and recorded for the purposes of audit by the ICO. Systems must have a way to record consent.
- Can be revoked at any time by an individual (this must be notified to them at receipt of consent).
- The requirement for specific consent does not apply to data already in our possession prior to May 23rd 2018 but expectation is that we will need to confirm consent upon the next contact with them after that date.

Data Protection Act vs GDPR:
Notification

Current Law

- Under current Data Protection law, we have no obligation to notify the ICO of breaches (loss, unauthorised release or corruption of personal data) unless of a serious nature.
- Serious nature is not defined by the ICO but it recommends that notifications are made where a breach could cause detriment to data subjects or is of a sensitive enough nature that it would be damaging.

GDPR

- Organisations are under an obligation to notify the ICO within 72 hours of a breach unless it is unlikely to result in a risk to individuals.
- If a breach is serious and could cause harm to individuals, it must be reported without “undue delay”
- Processors must notify the data controllers (owners of the data) when there is a breach and do so “without undue delay” if they will be impacted by it in a negative way.

Data Protection Act vs GDPR

Legal Basis and Legitimate Interest to Process Data

Current Law

- Require a legitimate interest – i.e. administering sales and marketing as part of business operations or administering exams
- Has to have either consent or a contractual or legal obligation to perform the processing

GDPR

- Consent alone is no longer enough to process data, there must be a specific additional reason for doing so which can be justified against the Data Protection law.
- Requires a specific reason for the processing of special categories of data (formerly known as sensitive personal data)
- For BCS, these would fall under processing by a not-for-profit body with a…philosophical aim…provided the processing relates only to members or former members and provided there is no disclosure to a third party without consent.
- Contract agreement can not be conditional on permitting processing of data except where the processing is necessary for the contract to be functional. We cannot therefore include “marketing” clauses in contracts.

Data Protection Act vs GDPR
Individual Rights

Current Law

- Right to request to access information that is held by a company about you (for a fee of up to £10) – known as a Subject Access Request
- Right to know what your information is being used for, how it is treated, which third parties have access to it
- Right to prevent data being processed for direct marketing
- Right to object to processing that is likely to cause or is causing distress or damage
- Right to object to automated decision making (using data or statistics through a computer system to make a decision about someone i.e. application for loans online with a credit check automatically performed by the system)
- Right to claim compensation for damages for breaches of the Data Protection Act

Data Protection Act vs GDPR
Individual Rights (continued)

GDPR

- Right to know if any information is being processed and for what purpose. Majority of people have information in the hands of a company that they are not aware of (see: PPI, Personal Injury nuisance calls)
- Builds upon the right to rectification, providing the subject with the ability to enforce corrections to data held by a controller or processor
- **The Right to be Forgotten:** Enshrines the right to have personal data removed from all systems unless there is a legitimate interest or reason that we cannot do this. This reason must be provable and agreeable with the ICO
- There are exceptions where legal obligations will override this such as for the purposes of employee taxation
- The right to data portability means that a data subject can request that their data can be moved from one controller to another in a machine-readable format without delay. Such situations may be where changing utility provider, instead of having to give all information again, you can request that your outgoing supplier can do this instead

Data Protection Act vs GDPR
Individual Rights (continued)

GDPR Continued

- Subject Access Requests can no longer be charged for unless it is a repeated request for the same information or is deemed unreasonable (rationale must be explainable to ICO)
- We must provide specific information to them under the expanded regulation:
  - Contact Details and Identity of the controller
  - Purpose and legal basis for the processing
  - Legitimate interests of the controller, processor or third party,
  - Any recipients of that data (third parties)
  - Details of international data transfers and safeguards to protect that data
  - Retention policy and how long their data is being retained for
  - The right to withdraw consent at any time
  - The right to complain to the ICO
  - If it was subject to automated decision making i.e. tracking or profiling

  This information regarding retention policies, decision making and rights to consent and complain must be present in our privacy notices and made clear at receipt of data or within 30 days if received from another source.

Data Protection Act vs GDPR
Security

Current Law

- Appropriate technical and organisational measures need to be taken against unauthorised or unlawful processing of personal data and against loss or destruction of data.

GDPR

- Have to ensure a level of security that is tailored and appropriate for each risk
- It sets out specific requirements for security measures that it would expect to be in place
- These include:
  - Pseudonymisation and encryption of personal data
  - The ability to ensure ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data
  - Ability to restore availability and access to data in a timely manner in the event of incident
  - Process for regular testing, assessment and evaluation of technical and organisational measures for ensuring security of the data and processing

Data Protection Act vs GDPR
Processor Obligations

Current Law

- Processor's obligations flow from the controller of the data to the processor, they are only obligated to comply with Data Protection law by virtue of being in contract with the controller
- Illegal to process data on behalf of another without a contract as these obligations must be passed on

GDPR

- Processors will now have to directly comply with Data Protection law regardless of contractual status with a controller
- Cannot sub-contract processing activities
- Must maintain full records of processing carried out on behalf of controllers, including contact details of relevant Data Protection Officer employed by the controller(s), categories of processing, where data is transferred to within or outside of the EEA
- Sanctions only apply where a processor fails to meet the processor-specific obligations in GDPR or controllers instructions

Data Protection Act vs GDPR
Record Keeping

Current Law

- Have to make an annual notification to the ICO on the processing undertaken by the company and that may be undertaken by the company as part of its daily business activities

GDPR

- No longer need to make annual notifications to ICO
- However, an extensive requirement for record keeping is introduced
- Must be able to demonstrate, on audit, compliance with the eight Data Protection principles
- Must also be able to demonstrate organisational and technical measures to ensure compliance including systems, training and internal data protection policies.
- Must retain written records of all processing activities and related information

Data Protection Act vs GDPR
Record Keeping (continued)

Record Keeping Requirements

- Names and contact details for any processors
- Details of controllers and their data protection officers where data is processed on contract
- Types of processing carried out
- Purposes and categories of processing
- Categories of data subjects
- Categories of recipients of personal data including overseas
- Details of transfers outside the EEA including documentation of any safeguards in place for that data
- Data retention periods
- General description of technical and organisational security measures

Data Protection Act vs GDPR
Privacy by Design and Default

GDPR

- Not previously a legal requirement under current Data Protection law
- The GDPR introduces requirements to include Data Protection in project planning, decision making and product design from the outset and throughout the processing.
- Systems and processes need to be designed to ensure that only data necessary for each specific purpose is processed and is not accessible to everyone – only those who need to participate in processing
- Privacy Impact Assessments will be required ahead of processing activities not previously undertaken or where new technology is involved.
- If there is a potential risk to the rights or freedoms of a data subject, these PIAs must be taken in consultation with the subjects of the processing and with the ICO prior to activities taking place.
- Data Protection must be a key consideration at every stage of our business activities

Data Protection Act vs GDPR:
Sanctions

Current Law

- Under current law, the maximum imposable fine for a business in breach of the Data Protection act is **£500,000**
- This covers all types of breaches, including lost or stolen data, misusing data, marketing to “opted-out” individuals, international data transfers etc.

GDPR

- GDPR will introduce two different limits for fines dependent on the violation:
  - **€10,000,000** or **2% of annual global turnover** (whichever is greater) for violations relating to record keeping, data processor contracts, data security and breach notification and data protection by default and design
  - **€20,000,000** or **4% of annual global turnover** (whichever is greater) for violations relating to breaches of the data protection principles, conditions for consent, data subject rights and international data transfers
  - Fines are applied for each individual breach so a set of breaches would have a cumulative financial impact.

How will it impact us?
Data Retention and Necessity

- We hold a huge amount of data across our business and we will need to ensure that we only retain the data that we absolutely need to keep and get rid of any which is outdated or no longer needed.
- We will no longer allow for large amounts of data to be held by any function, business unit or member group without justification.
- Before any large data collection activity, you will need to engage in a privacy impact assessment as directed by Legal Services and Compliance.
- All currently held data must be reviewed in line with the privacy impact assessment to ensure compliance.
- Data must be frequently reviewed and kept up-to-date or otherwise destroyed if it is not in use or has no justification for its continued possession.
- Audits will be performed to ensure that compliance with legislation and BCS policy is met.

Next steps

- Establish a cross-functional working group to establish how we can fully prepare the business for this legislation.
- Systems review to ensure we can meet the requirements for demonstrable consent and deletion of personal data on request.
- Define our retention policies across the business, establish the rationale behind existing retention policies and be able to explain them to the data subjects and ICO on request.
- Establish a way to centrally gather all information on our processing activities to meet the record keeping requirements.
- Review all of our contracts to ensure they meet the requirements and obligations on us and on our partners, clients and suppliers.
- Review our policies, procedures and privacy notices across a number of areas to ensure they are GDPR compliant.
- Train all employees to understand new obligations that they will be bound to while undergoing their work and in the new procedures that well need to abide by
- Review, expand and roll out breach notification policy across BCS

What we need from you

We need you to review your current data environment

- What data do you hold?
- What is the purpose of you having that data?
- Where is this data stored?
- Aside from the primary reasons, what other purposes is it used for?
- How long are you keeping it for and why?
- What happens with data that is no longer needed for the original purpose?
- What processes are in place for the deletion of unnecessary data?
- What protections are in place to protect held data?
- What risks beyond system intrusion are there on the data you hold?

Please email bcslegalteam@bcs.uk with detailed answers to these questions and the name of the Member Group you represent by January 13th 2017.

Other Business
Memorandums of Understanding

- We have reviewed our usage of MoUs against best practice direction and feel that they are not up to standard.
- This is because there is no legal backing for them, they are generally unenforceable and are very difficult to give effect to.
- From now on, non-disclosure agreements will be the preferred method of engagement where an MoU would normally have been used.
- This still allows for the same functionality as the MoU in providing scope for discussions but crucially allows those discussions to be protected as confidential until such time as a formal agreement happens or not.
- It is binding only on confidentiality, it is not binding on actions. This will allow you the freedom in your engagements to act in confidence until a full contract is created.

Any Questions?