General Data Protection Regulation Overview

GGF Window & Door Group & Conservatory Association Joint Meeting

GDPR: Background & Definitions

Introduction to GDPR

- Came in to force on 24th May 2016 – applicable from 25th May 2018
- EU Regulation – has direct effect – no local legislation required
- Replaces the Data Protection Act 1998 (for context, Google founded 1998 & iPhone launched in 2007)
  - DPA 1998 followed Data Protection Directive 1995 – 'patchwork quilt' of data protection laws across EU
  - GDPR replaces this with a single, harmonised law across the 28 member states
  - Some derogations
- Guidance on interpretation and compliance still being developed:
  - Article 29 Working Party (Future European Data Protection Board - EDPB)
  - National Supervisory Authorities – ICO in the UK
- UK Government has confirmed applicability in UK notwithstanding Brexit (Data Protection Bill)
- Places considerable **obligations on Controllers & Processors** and gives **greater rights and remedies to Data Subjects,** backed by considerable administrative penalties
- Applies to **all organisations that Control or Process the Personal Data of Data Subjects in the EU irrespective of where the processing takes place** or whether the Controller or Processor is EU resident
- **Opportunity** to foster **digital trust**
- **99 Articles & 173 Recitals**

Key Definitions

Data Controller

- *"the natural or legal person… which … determines the purpose and means of the processing of personal data"*

Data Processor

- *"a natural or legal person… which processes personal data on behalf of the controller"*

Data Subject

- *"an identified or identifiable natural person"*

Personal Data

- *"any information relating to an identified or identifiable natural person ('data subject'); …..one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data…. One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that person. "*
- *Special Category : Race, Ethnicity, Religion, Sexual Orientation, Political Opinions, Trade Union Membership, Health Data, Genetic Data, Biometric Data, Sex Life Data*

Processing

- *"any operation or set of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as collection, recording, organisation, structuring, storage.. alteration…use….restriction, erasure or destruction."*

GDPR: Principles, Accountability, Data Subject Rights, International Transfers

GDPR Principles

- Six data protection principles – overview of your most important duties in complying with GDPR

Personal Data shall be:

1	processed **lawfully, fairly and transparently**	• One of the lawful purpose as set out in the GDPR (lawful) • Data subject must be told what processing will occur (transparent) • Processing must match this description (fair)

GDPR: Lawful Processing

CYBERCROWD

Six grounds for lawful processing:

- Data subject gives consent for one or more specific purposes
- Necessary to meet contractual obligations entered into by the data subject
- For purposes of the legitimate interests pursued by the controller
- Necessary to comply with legal obligations of the controller
- Necessary to protect the vital interests of the data subject
- Necessary for tasks in the public interest or exercise of authority vested in the controller

If you rely on consent:

- Controller must be able to demonstrate consent was given – records are required
- Consent must be clear, unambiguous, involve an affirmative action and be **freely given**
- Implicit, 'opt-out' consent (such as pre-ticked boxes) is not sufficient
- Consent must be 'unbundled' from other terms and conditions
- Consent should not be a precondition of signing up for a service
- Data subjects have right to withdraw consent at any time – you need to tell people this
- There should not be an imbalance in power, (e.g. **employment contracts**)
- Consent should not be used if you would process anyway (e.g. **employment contracts**)

GDPR Principles

- Six data protection principles – overview of your most important duties in complying with GDPR
- Introduces ‘accountability principle’ – Data Controllers responsible for being able to demonstrate compliance with the six principles

Personal Data shall be:

1	processed **lawfully, fairly and transparently**	• One of the lawful purpose as set out in the GDPR (lawful) • Data subject must be told what processing will occur (transparent) • Processing must match this description (fair)
2	collected for **specified, explicit & legitimate purposes**	• Define up front what the personal data will be used for • Limit the processing to only what is necessary for that purpose
3	**adequate, relevant & limited to what is necessary** for processing	• Hold & process no more personal data than is strictly required
4	**accurate and kept up to date**	• Build in processes to ensure ongoing accuracy of personal data
5	**kept only for as long as is necessary** for processing	• Do not retain the personal data longer than is necessary
6	processed in a manner that **ensures its security**	• Process in a manner that ensures appropriate security: o protection against unauthorised / unlawful processing; and o accidental loss, destruction or damage

ACCOUNTABILITY

GDPR & Accountability

- Data Controllers required to demonstrate compliance with the six principles and the governance obligations in GDPR.
- Obligation is on the Data Controller to demonstrate compliance, not on the ICO to demonstrate non-compliance.
- Demonstrating accountability:
  - Implement '**appropriate technical and organisational measures**' – information governance best practices: data protection policy and processes, HR policies and processes, employee awareness training, internal auditing, Security of Processing
  - Create and maintain relevant **documentation on your processing** activities.
  - Implement **Data Protection by Design and Default** e.g. data minimisation, pseudonymisation, technical security controls etc.
  - Appoint a **Data Protection Officer**, where appropriate
  - Apply a **risk based approach** to your personal data processing and use **Data Protection Impact Assessments**, where appropriate
  - Notify the required parties following a personal data breach, have procedures for doing so
  - Keep a comprehensive **record of data breaches**
  - **Document your governance activities**, showing how you comply with your obligations
  - **Controller/Processor Agreements** – instructions, sub-processing, assisting the ICO, Data Subject rights, International Transfers

GDPR: Data Subject Rights

- **Information: (Privacy Notices)**
  - Controller & DPO contact details, purpose of processing, legal basis, legitimate interests, recipients, transfers to 3rd countries
  - Retention periods, data subject rights, existence of automated decision making and profiling
- **Access: (Subject Access Requests)**
  - Told whether any personal data is being processed, given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
  - Given a copy of the information comprising the data; and given details of the source of the data (where this is available).
  - Right to charge £10 is removed, response period reduced from 40 days to 30 days
- **Object to Processing:**
  - Data subject can object to processing for direct marketing, profiling, automated decision making, scientific or historical purposes
  - Unless controller can show legitimate interests override the interests, rights and freedoms of the data subject, or processing carried out for reasons of public interest
- **Rectification**:
  - Rectify inaccurate data, complete incomplete data
- **Erasure**:
  - Be 'forgotten' where data no longer necessary for the purpose and other grounds
- **Restrict Processing:**
  - Accuracy is contested, processing unlawful, controller no longer requires data etc.
- **Data Portability**:
  - Move personal data to another data controller, controller must provide in machine-readable format

GDPR: International Transfers

- Transfers of personal data to recipients in “third countries” (outside of the EEA) are regulated and restricted.
- Personal data may only be transferred to “third countries” where certain conditions are met:

1. On the basis of **Adequacy**
    - Where European Commission has determined that the country ensures and adequate level of protection.
    - Presently Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay
2. Subject to **Appropriate Safeguards**:
    - Legally binding and enforceable instrument between public authorities / bodies
    - Standard data protection clauses adopted by the Commission (the ‘model clauses’)
    - Approved codes of conduct
    - Binding corporate rules in accordance with the GDPR
        - Between multinational companies – internal rules which define global policy relating to international transfers of personal data within the same corporate group
        - Need to be legally binding, and enforced by every member of the group & expressly confer enforceable rights on data subjects
        - Must meet specific requirements laid down in GDPR (includes info on group structure, contact details, categories of data and processing, more)
        - Require approval from a Supervisory Authority (e.g. ICO)
3. Subject to **International Cooperation Mechanisms**:
    - EU – US ‘Privacy Shield’ - personal data transfer mechanism between EU and USA

GDPR: Remedies & Liabilities

GDPR Remedies & Liabilities
Supervisory Authority (ICO) Powers

- **Investigative Powers**
  - to order the controller or processor to provide any information
  - **carry out compulsory data protection audits**
  - notify controller/processor of any alleged infringement of the GDPR
  - **obtain from controller/processor access to all personal data and all information**
  - **obtain access to any premises of controller and processor including data processing equipment**
  - review certifications

- **Corrective Powers**
  - Issue warnings to controller or processor of likely infringement
  - Issue reprimands to a controller or processor where processing has infringed the GDPR
  - **Order the controller or processor to bring processing into compliance (with specific direction and time period if appropriate)**
  - **Order the controller to communicate a personal data breach to the data subject**
  - **Impose a temporary or definitive limitation including a ban on processing**
  - Order the rectification, restriction or erasure of data or order a certification body not to issue a certificate
  - **Order the suspension of data flows to a recipient in a third country or to an international organisation**
  - Impose administrative fines

GDPR Remedies & Liabilities: Administrative Fines

CYBERCROWD

Lower Tier Fines

€ 10,000,000 or, in case of an undertaking, 2% total worldwide annual turnover in the preceding financial year (whichever is greater) for infringement of the following Articles:

- 8: Child's consent
- 11: Processing not requiring identification
- 25: Data protection by design and by default
- 26: Joint controllers
- 27: Representatives of controllers not established in EU
- 26 - 29 & 30: Processing
- 31: Cooperation with the supervisory authority
- 32: Data Security
- 33: Notification of breaches to supervisory authority
- 34: Communication of breaches to data subjects
- 35: Data protection impact assessment
- 36: Prior consultation
- 37 - 39: DPOs
- 41(4): Monitoring approved codes of conduct
- 42: Certification
- 43: Certification bodies

Upper Tier Fines

€ 20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year (whichever is greater) for infringement of the following Articles:

- 5: Principles relating to the processing of personal data
- 6: Lawfulness of processing
- 7: Conditions for consent
- 9: Processing special categories of personal data
- 12 - 22: Data subject rights to information, access, rectification, erasure, restriction of processing, data portability, object, profiling
- 44 - 49: Transfers to third countries
- 58(1): Requirement to provide access to supervisory authority
- 58(2): Orders/limitations on processing or the suspension of data flows

Data Subject Remedies against Controllers & Processors

- **Right to an effective judicial remedy against a Controller or Processor**
  - Right to judicial remedy where their rights have been infringed as a result of the processing of personal data

- **Right to compensation and liability**
  - **Right to judicial remedy where their rights have been infringed as a result of the processing of personal data**
  - **Any person who has suffered material, or non-material, damage shall have the right to receive compensation from the controller or processor**
  - Controller involved in processing shall be liable for damage caused by processing
  - Processor liable only for damage caused by processing or where it has acted contrary to lawful instructions of the controller
  - **Joint and several liability** to ensure effective compensation
  - **Collective claims are possible**

GDPR: Practical Steps

Some Practical Steps

1. **Understand Personal Data You Hold:**
    - Data audit – identify Personal Data held, how it was/is collected, data flows, who has access, where it is stored, Int. Transfers etc.
    - Apply the 6 Principles to the Personal Data you hold – Do you have Consent, have you held for only as long as necessary etc
    - Assess the risk to privacy of the Data – risk of harm to the Data Subject – undertake Data Protection Impact Assessments.

2. **Document your Processing Activities:**
    - Put the required documentation in place – including proof of Consent from Data Subjects, records of Processing activities etc.
    - Document how you comply with GDPR – demonstrate you are consistently applying best practice.
    - Document the basis for your decisions. Demonstrate accountability.

3. **Apply Technical and Organisational measures**
    - Implement data protection policies and supporting processes & procedures, including (without limitation):
        - Privacy Policy (covering the information required by Article 13)
        - Information Security Policies
        - Fair Processing Notice (in line with the 6 Principles)
        - Policy and procedures for Data Breach, Data Subject Rights
    - Consider implementing an ISMS / PIMS / Compliance Framework – apply best practice and certify where appropriate.
    - Adopt a 'Cyber Resilience' approach covering People, Process & Technology in line with best practice.

4. **Secure 3rd Party and employee agreements**
    - Identify 3rd parties used for Data Processing and review contracts, including your procurement and outsourcing processes
    - If acting as a Processor prepare for Data Controllers' requests for contractual guarantees
    - Consider your Cloud service providers – where does the Data reside?
    - Review employee contracts in line with requirements for Privacy Notices and lawful bases (e.g. consent to process data may not be appropriate)

Sources of assistance

- **The ICO (www.ICO.org.uk)**
  - 12 steps to take now
  - Overview guidance
  - Specific guidance e.g. Consent, Controller/Processor Agreements etc etc
  - Phone Line
  - Chat box

- **Cyber Crowd**
  - Awareness Workshops
  - Readiness Assessments
  - Compliance Design (including Preparation Plans)
  - On-going Data Protection as a Service

- **Data Protection Lawyers**

Marketing – GDPR, PECR and the E-Privacy Regulation

Data protection | Privacy and Electronic Communications

At-a-glance guide to the marketing rules

Method of communication	Individual consumers (plus sole traders and partnerships)	Business-to-business (companies and corporate bodies)
Live calls	☐ Screen against the Telephone Preference Service (TPS) ☐ Can opt out	☐ Screen against the Corporate Telephone Preference Service (CTPS) ☐ Can opt out
Recorded calls	☐ Consumer must have given caller specific consent to make recorded marketing calls.	☐ Consumer must have given caller specific consent to make recorded marketing calls.
Emails or texts	☐ Consumer must have given sender specific consent to send marketing emails/texts. ☐ Or soft opt-in (previous customer, our own similar product, had a chance to opt out)	☐ Can email or text corporate bodies ☐ Good practice to offer opt out ☐ Individual employees can opt out
Faxes	☐ Consumer must have given sender specific consent to send marketing faxes	☐ Screen against the Fax Preference Service (FPS) ☐ Can opt out
Mail	☐ Name and address obtained fairly ☐ Can opt out	☐ Can mail corporate bodies ☐ Individual employees can opt out

ico.

20160516
Version 2.0

Above rules derive based on PECR
GDPR standard for consent will apply from 25th May 2018
E-Privacy Regulation was scheduled to replace PECR on 25th May 2018, now uncertain when will be introduced

Questions

Important Notice

The guidance provided in this presentation does not constitute legal advice. Our observations and recommendations are based on data protection and privacy good practice and the practical, operational, implications of the GDPR as we interpret them.