

Data Protection

Key concepts, principles and approaches

Georgia Fishwick | Associate



Today's agenda and facilitators

Objectives

Understand the key concepts and principles of data protection

Apply the principles to typical commercial scenarios

What we'll cover

- Key concepts for data protection
 - Sources of law and guidance for data protection
 - How to analyse a data protection problem
 - The principles of GDPR
 - How to establish a legal basis for processing
 - Drafting privacy notices
 - Cookies
 - Email marketing
-

Georgia Fishwick

Associate

georgia.fishwick@cms-cmno.com

Key Concepts: What is personal data?



Article 4(1):

“**personal data**” means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person



Note:

- **Pseudonymised** data is still personal data (Article 4(5)):
 - ↳ ...in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately...
- **Anonymised** data is not personal data (but this is a high standard – Recital 26):
 - ↳ ...personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable...

Key Concepts: Special category personal data



Article 9(1):



personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation



Note:

- Defined list
- More robust basis for processing required, and more protections
- Additional definitions in Article 4
- sensitive personal data that is not Special Category Personal Data

Quiz Question

Which of the below are personal data?



payment details



sole trader's contact details



IP address



anonymous data



business email address



credit balance



Key Concepts: data processing



Article 4(2):



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**, adaptation or alteration, **retrieval**, consultation, use, disclosure by transmission, dissemination or otherwise **making available**, alignment or combination, restriction, erasure or **destruction**



Note:


Broad definition, includes not “doing anything” with personal data in the ordinary sense

Controllers and processors




Article 4(7) and 4(8)

Data Processor

 a natural or legal person, public authority, agency or other body which processes personal data **on behalf of** the controller

Data Controller

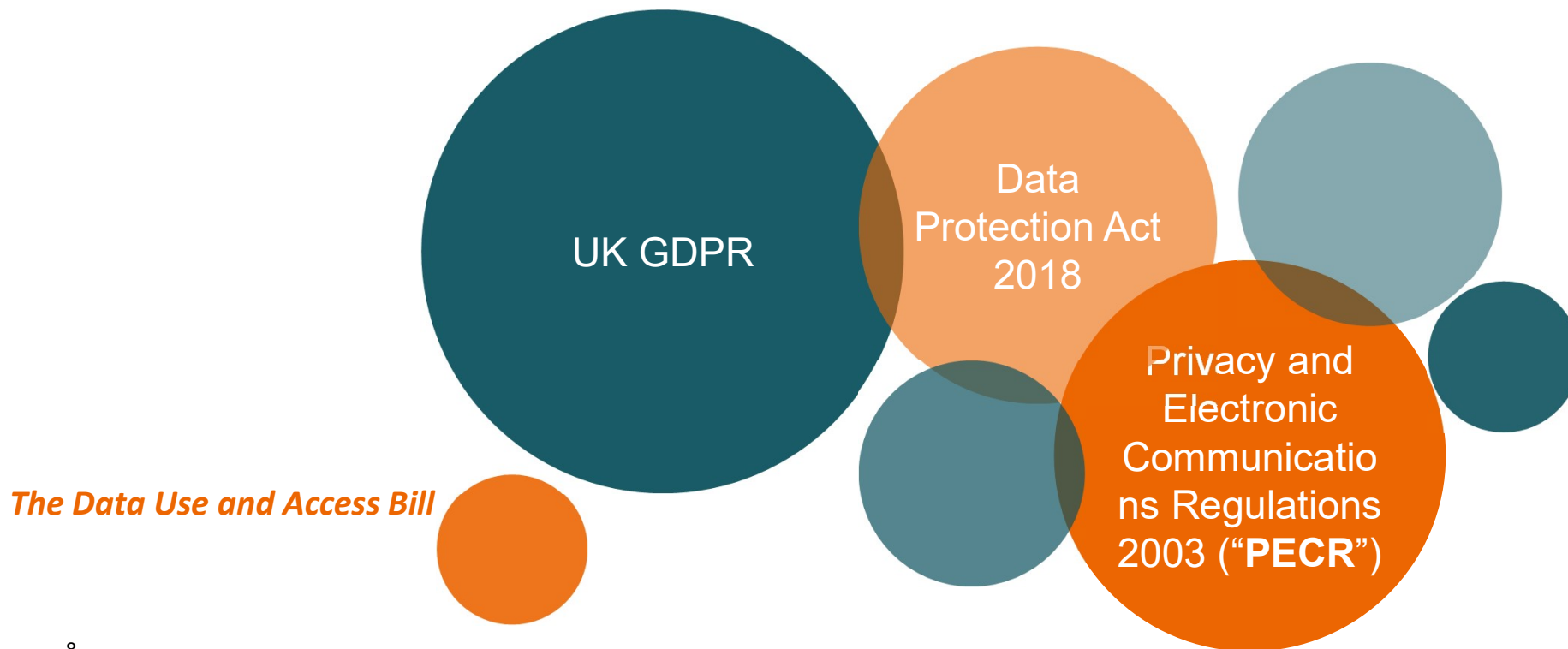
 ...the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means** of the processing of personal data

Note:

- Under GDPR, processors will be subject to various direct obligations and risk of sanctions
- GDPR specifies what must be in a controller – processor contract (Article 28)
- There may not be a data processor, but there will always be a data controller
- May be joint controllers / co-controllers

Current sources of law

Current sources of law



DP survival skills: navigation



STATUTE

- What does the UK GDPR say?
- What does UK Data Protection Act 2018 say?



CASE LAW

- Is there any CJEU or UK case law on point?
- Is it binding / non-binding?



GUIDANCE

- Is there any specific ICO guidance?
- Is there any specific EDPB guidance?

DP survival skills: analysis

How to analyse a DP question



DP survival skills: principles

Lawfulness Fairness and Transparency

- tell people what you are doing with their personal data and make sure you have a basis for processing in the first place

Purpose Limitation

- process personal data for clear purposes and don't then process it for new purposes

Data Minimisation

- don't process more personal data than you need to

Accuracy

- make sure personal data held is accurate and up to date

Storage Limitation

- don't hold personal data for longer than you need to

Integrity and confidentiality

- protect personal data

Accountability

- demonstrate compliance



DP survival skills: applying the principles

Principle 1 Lawfulness, fairness and transparency

Principle 1 = Transparency + a lawful basis for processing

Article 13 - Transparency

- being transparent about **identity** of data controller
- being transparent about **intended purposes** of processing
- other information (listed) e.g. **retention period, recipients, overseas transfers**
- have regard to **context** including **method by which data is obtained** and whether party disclosing data was misled as to purposes for which obtained

Lawful Basis for Processing

You must have a lawful basis for processing personal data!

- Data subject's **consent**
- Necessary for the **performance of a contract** to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract
- Necessary for **compliance with a legal obligation** to which the controller is subject
- Necessary in order to **protect the vital interests of the data subject** or of another natural person
- Necessary for the **performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller
- Necessary for the **purposes of the legitimate interests of the controller (or by a third party)** except where such interests are overridden by the right of data subject



Consent

Consent vs Notice

You must have a lawful basis for processing personal data!

Don't confuse "**consent**" with "**notice**" in DP advice.

- There is a fundamental difference between telling a person how you're going to use their personal information (i.e. **notice**) and getting their **consent**
- "**Consent**" = "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the processing..."
- "**Explicit consent**" (for use of sensitive personal data)
- Consent must be **demonstrable, granular, use clear and plain language**
- Data subject has the **right to withdraw consent**

Conditions for lawfulness of processing (Art 6) – stricter (e.g. standard for consent is higher). Fines of up to £17.5m / 4% of global annual turnover for breaching these provisions.

Know your purpose...

Principle 2 Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes

- specify your purpose(s) by giving notice to data subject
- if processing the data further, consider whether this is compatible with the intended purpose



Don't be greedy...

Principle 3 Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

What does it mean in practice?

- Avoid asking for superfluous data
 - E.g. “Nice to have” fields in a data collection form
 - Where the business doesn't have an immediate need for this information.

Keep it accurate...

Principle 4 Accuracy

Personal data shall be accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Previous guidance includes:

- data controller to take reasonable steps to ensure accuracy of data
- data should indicate if data subject has notified data controller of alleged inaccuracies

What does it mean in practice?

- e.g. good practice to make it easy for customers to update their details online
- Under GDPR data subjects have new rights of erasure/rectification

...but don't keep it for too long

Principle 5 Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

- Permissible retention period will depend case-by-case on purpose (how long is a piece of string...?)
- Important to have retention policies
- Must state retention periods or mechanisms in privacy notice



Keep it safe

Principle 6 Integrity and confidentiality

Personal data shall be processed in a manner that ensure appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

Note security obligations in Article 32; must take into account:

- state of the art
- costs of implementation
- nature, scope, context and purposes of processing
- risk of varying likelihood and severity for the rights and freedoms of natural persons

Possible measures (as appropriate):

- Pseudonymisation and encryption
- Ability to ensure ongoing confidentiality, integrity, availability and resilience
- Ability to restore availability and access in a timely manner following an incident
- Process for regular testing

Keep it safe

Principle 6 Integrity and confidentiality

Notification to regulator?



In the case of a personal data breach, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the regulator (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons).

Notification to data subjects?



When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

Demonstrate compliance

Principle 7 Accountability

Implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with [GDPR].

What should entities be doing?

- Implement data protection policies – that allow adherence to law and certifications
- Having records of processing: contact details, purposes for processing, description, recipients, transfers, time limits for erasure, technical and organisational measures. In writing. Can be made available to regulator on request.
- Undertaken Legitimate interest assessments
- Data protection impact assessment/prior consultation.
- Data processing agreements.

...and keep it near

BONUS Principle



any transfer of personal data which are undergoing processing or which are intended for processing after transfer to a third country or international organization shall take place only if...the conditions laid down in this Chapter are complied with...

(Article 44)

Respect data subjects' rights

BONUS Principle – Data Subject Rights

Data Subject Rights:

- Transparency and information – Articles 12-14
 - Right of access – Article 15
 - Right to rectification – Article 16
 - Right to erasure ("right to be forgotten") – Article 17
 - Right to restriction of processing – Article 18
 - Notification regarding rectification or erasure – Article 19
 - Right to data portability – Article 20
 - Right to object – Article 21
 - Right not to be subject to automated individual decision making including profiling – Article 22
- Data controller must action
 - Must be actioned within one month of receipt
 - May not charge a fee unless the request is manifestly unfounded or excessive (i.e. repeated)
 - Rights are not absolute – look back to the lawful basis for processing



Drafting privacy notices

What is a privacy notice?

- Specific, prescriptive requirements under GDPR:
- Article 5(1)(a) – transparency
- Article 5(1)(b) – purpose limitation
- Articles 13 and 14 – information to be provided



Drafting privacy notices: top tips

- There is no such thing as a “standard privacy notice”
- People use the phrase “privacy notice” to describe all kinds of things – make sure you are both talking about the same thing!
- Do you need more than one privacy notice?
- Increased importance placed on making privacy policies consumer friendly – think about your audience (e.g. age, accessibility etc.)
- Think about how you could present the information in an easy-to-understand way (images, videos etc.)
- Even if you are not consumer facing, privacy notice is still important
- Your survival kit:
 - ICO guidance
 - Articles 13 & 14 GDPR
 - EDPB guidance on transparency principle



Privacy notice requirements



Legal basis for processing



Details of 'legitimate interests' where relied on



Details of safeguards for overseas transfers and means to obtain copies



Period for which personal data will be stored



List of individual's rights including right to object, subject access right, right to be forgotten and data portability



Right to withdraw consent at any time



Right to lodge a complaint with supervisory authority



Whether provision of data is statutory or contractual requirement and consequences of not disclosing it



Details of automated decision making including profiling, along with details of the logic used and consequences



Source from which data originates and if it came from public sources



Cookies

Cookies: the legal requirements

- **What are cookies?** Small text files downloaded and stored on your device when website accessed
- PECR states that cookies or similar technology **must not be used unless** the subscriber or user of the relevant terminal equipment:
 - is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; **and**
 - has given his or her consent
- **If they process personal data GDPR also applies! Think about consent requirements and processing of special categories of personal data**

Example: cookie banner

By using our site, you acknowledge that you have read and understand our [Privacy Policy](#) and our [Disclaimer](#)

I agree

This website uses cookies

We use cookies to tailor the website based on the visitor's specified age level, as well as to ensure that you remain logged in and do not have to log in on every new page. Cookies are also used to conduct traffic measurements and customize our services, so that you receive relevant marketing. You can find more information about cookies under the [Details](#) and [About](#) tabs.

Show details

Deny


Customize

Allow all

Example: Compliant cookie banner

Cookies on the ICO website

We use some essential cookies to make this site work. We'd like to set analytics cookies to understand how you use this site. We may use services from Vimeo and YouTube that may also use cookies.

For more detailed information, see our [Cookies page](#). 

Accept non-essential cookies **Reject non-essential cookies**

Essential cookies

These cookies are necessary for core functionality, such as security and network management. They always need to be on.


Analytics cookies

We use Siltide to measure how you use the ICO website. These cookies collect information about how you got to the site, the pages you visit and how long you spend on each page, and what you click on.

Video player cookies

We use services from Vimeo and YouTube to show you embedded videos on the ICO website. Vimeo and Google may use cookies to receive information about the videos you watch for analytics and advertising purposes.

Save and close





E-Marketing

Marketing: the legal requirements

- **What are the requirements?** Regulation 22 of PECR
- PECR states that you can only send electronic mail marketing if:
 - **Consent** They have specifically consented
 - **Soft Opt In** Have bought or negotiated to buy a similar good or service in the past and you gave them a simple way to opt out.
- **Must meet GDPR requirements of consent - a pre ticked box is not sufficient**
- **Note rules for differ for different forms of communication such as text, calls, automated calls and post so check PECR and the ICO Guidance.**

Example: Marketing consents

Join CottonOn & Co. Perks and get a \$10 voucher!

✕

Get On The List!

Join our list for daily inspiration
& first access to global
fashion.

Enjoy 10% Off+ your first purchase
when you sign up now.

Womenswear Menswear

Already have an account? [Sign in](#)

To opt-out of email sharing or to view our [Privacy Policy](#), click here

* Terms and Conditions apply

Useful resources



[ICO Guidance – The Right to be Informed](#)



[ICO Guidance – The Right to Object](#)



[ICO Guidance – What is Valid Consent?](#)



[ICO Guidance on the rules on use of cookies and similar technologies](#)



[ICO Direct Marketing Checklist](#)

Any questions





Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices.

CMS locations:

Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Beirut, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sheffield, Singapore, Skopje, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

cms.law