Appendix A: the legal framework

Introduction

1. In this appendix we will describe at a high level the legislative and regulatory landscape relevant to the UK digital advertising market and platforms, as well as certain applicable aspects of self-regulation and standard setting.

2. This is intended to be a brief description of the applicable frameworks, and is not intended to assess the merits of the current system. For convenience, the appendix is structured in the following thematic way:

    - firstly, it describes the specific legislative and regulatory regime(s) for online activity;
    - secondly, it briefly addresses broadcasting and advertising standards;
    - thirdly, it briefly outlines generally applicable law of relevance, such as consumer, competition, data protection etc;
    - fourthly, it sets out the role of standard setting; and
    - lastly, it describes self-regulation.

3. Given the breath of potential coverage, it is not, and is not intended to be, comprehensive. Rather, it covers areas of the regulatory landscape of relevance, or potential relevance, to the scope of the market study.

Legislating for the internet – areas of specialised law

4. This section summarises sequentially some of the relevant specialist provisions which has been made in relation to online businesses,[1] although for consistency the Privacy and Electronic Communications (EC Directive) Regulations 2003, which transpose the 'ePrivacy Directive' in the UK, are covered in the subsequent section on data protection law.

[1] There are developments which are therefore not covered such as the 'Geo-blocking regulation – Regulation (EU) 2018/302', the recent 'Copyright Directive (EU) 2019/790' covering rights in the digital single market and the removal of 'eCommerce immunity' from certain content sharing service providers.

E-Commerce Directive

5. The Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013) (E-Commerce Regulations) implement the E-Commerce Directive (2000/31/EC) (E-Commerce Directive) in the UK.

6. The E-Commerce Directive provides the legal framework for online services and facilitates cross-border online services in the EU, with the providers of online services, in general, being subject to the law of the Member State in which they are established and not the law of the Member States where the service is accessible.[2] In relation to this study the E-Commerce Regulations, amongst other matters, make provision for:

   - requirements on mandatory consumer information;
   - steps to follow in online contracting; and
   - rules on commercial communications, such as online advertisement and unsolicited commercial communications, which require online advertisers to ensure that advertising is clearly identifiable as such, and provide certain information about themselves on their websites and adverts.

7. Since 2000, the European Commission ('the Commission') has brought forward various other legislative measures making provision for 'e-commerce' (some described below) and is reflecting on whether a new 'Digital Service Act' should be brought forward in this space.[3] On 2 June 2020 the Commission launched a consultation on elements of a new Digital Service Act Package. The Commission explains this new approach will have two main pillars involving, first clear rules for digital services, and secondly ex ante rules covering large online platforms acting as gatekeepers to ensure that those platforms behave fairly, supported by a system of cooperation for the supervision of platforms and effective enforcement.[4]

The 'Information Society Services' Directive

8. The 'Information Society Services' Directive (EU) 2015/1535 makes provision codifying the process for the development and implementation of new

---

[2] The e-Commerce Directive provides the legal framework concerning the (non)liability of intermediary providers of 'information society services'.
[3] Ursula von der Leyen - political guidelines for the next Commission.
[4] Commission Digital Services Act Package page and Consultation.

technical regulations and rules on Information Society services, ie, online businesses, by Member States in the EU.[5]

9. Essentially Member States are required to notify the Commission of any draft technical regulations that fall within scope of the Directive, and operate a 'standstill period' of at least 3 months before adopting the draft regulations. This process gives the Commission and other Member States an opportunity to consider and provide comments on the draft proposals.[6]

Payment Services Directive 2 (PSD2)

10. The Payment Services Directive (EU) 2015/2366,[7] is intended to promote competition in the payments market by allowing non-bank companies, Third Party Providers (TTPs), to offer new innovative services to their customers. It is of potential relevance to this study in relation to the concept of 'Open Banking'.

11. Banks that offer online access to accounts must cooperate with others providing such services, to allow certain regulated third parties providing payments-related services (TPPs) access to payment data, subject to the customer's explicit consent. In order to make that possible, banks must establish secure communication channels to transmit data and initiate payments, where customers give their consent to the access, use and processing of their data. The CMA facilitated the making of this access possible via its Open Banking remedy, which follows from the 2016 market investigation into competition in the UK's retail banking sector.

12. As an example of the standards that might be necessary to facilitate this, the **Commission Delegated Regulation (EU) 2018/389** makes detailed provision for the requirements for common and secure standards of communication.[8]

Audiovisual Media Services Directive (as amended)

13. Audiovisual Media Services Directive 2018/1808 makes additional EU-wide provision on audiovisual media, the AVMS Directive coordinates national legalisation on standards for TV and on-demand services. The most recent revisions to the AVMS Directive have not yet been transposed in the UK.

---

[5] Article 1 makes provision for the services covered by the Directive, *inter alia* services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
[6] Further detail is provided in guidance published by the UK Government, Technical standards and regulations - Government guidance.
[7] PSD2 is (largely) transposed in the UK via the Payment Services Regulations 2017.
[8] Article 30 to 36.

These changes extend certain audiovisual rules to video sharing platforms (eg YouTube) as well as certain audiovisual content shared on social media services (eg Facebook) in the scope of this study.[9] Of relevance to this study the AVMS Directive will be extending existing general principles governing advertising in linear broadcast to Video Sharing Platforms, like measures to protect children. The AVMS Directive also mandates that data collected to protect children may not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.[10] DCMS will take a variety of steps, some transitional, to transpose the AVMS Directive in advance of its 19 September 2020 deadline.[11]

Platform-to-Business Regulation (P2B Regulation)

14. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services to access consumers was adopted on 20 June 2019 and applies from 12 July 2020.[12] As a 'regulation' this has direct effect in the UK without the need for transposition, as opposed to the Directives described above, which generally require an implementing measure in each Member State. A regulation provides a harmonised approach across the Common Market.

15. The P2B Regulation applies to online intermediation service providers, that is services which connect businesses to their consumers, such as online search engines, consumer market places and social media platforms.[13] The P2B Regulation requires such service providers to comply with certain transparency obligations to their business customers. These include:

- clear terms and conditions;
- giving reasons for restriction, suspension or termination of accounts;
- explaining the basis for ranking;

[9] The directive also makes provision for a Country of Origin (COO) principle, under which audiovisual media service providers need to only abide by the rules of the Member State that has jurisdiction over them, which usually means the Member State in which they are established.
[10] DCMS have consulted on the transposition of the directive in the UK in 2020.
[11] DCMS's response to public consultations on the government's implementation proposals. As DCMS notes in the medium term the proposed Online Harms Framework, and the outputs of this market study and the Secretary of State's review of online advertising may make wider provision in this area.
[12] UK enforcement regulations have been laid, The Online Intermediation Services for Business Users (Enforcement) Regulations 2020, SI 2020/609.
[13] However, an 'ad exchange', ie a business selling to business, would not be within scope as it is not a platform which allows a business users to offer direct transactions to consumers.

- the reasons for any differentiated treatment between the business and the platforms own businesses;
- differences in access to data; and
- restrictions on offering other services or using other sales channels.

16. This is supported with mechanisms for dispute resolution. It aims to create a fair, transparent and predictable business environment for businesses and traders when using online platforms to offer services to consumers.

Advertising and Broadcasting Standards

17. This Appendix provides a very brief outline of the broader approach to the regulation of the **content** of certain advertising in the UK, which is controlled through a combination of self-regulation and legislation,[14] as this is largely outside the scope of the study.

Self-regulation and co-regulation by the advertising industry

18. The advertising industry operates an independent self-regulatory system, with the Advertising Standards Authority (ASA) responsible for enforcing the industry 'BCAP Code', for broadcast adverting, and the 'CAP Code' or non-broadcast advertisements, sales promotions and direct marketing communications (the Codes).

19. The Codes are written by the Broadcast Committee of Advertising Practice (BCAP), and Committee of Advertising Practice (CAP) respectively, who also issue guidance on the Codes. The members of CAP and BCAP are representatives of advertisers, agencies, media owners and other industry groups, with the system funded by a levy on advertising expenditure.

20. Whilst the content of the Codes is outside the scope of this appendix. The CAP Code contains the rules regulating non-broadcast advertising, including advertising which is sent by post or email or appears online, and the rules applicable to regulated video-on-demand services, eg ITV Hub. With the

[14] Including the Communications Act 2003 which prescribes certain standards objectives for broadcast advertising, including, preventing misleading, harmful or offensive advertising in television and radio services. BCAP takes these objectives into account when writing the BCAP Code. As well as the Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277) (CPUT) which transpose the Unfair Commercial Practices Directive (2005/29/EC) (UCPD), which prohibit misleading actions and omissions, aggressive practices, and commercial practices which contravene professional diligence. The *Business Protection from Misleading Marketing Regulations 2008 (SI 2008/1276)* (BPRs) which transpose the *Misleading and Comparative Advertising Directive (2006/114/EC*).

BCAP Code containing the rules regulating all adverts on radio and television services that are licensed by Ofcom, the UK telecommunications regulator.[15]

21. The ASA investigates complaints and rule on the Codes. If an advertiser fails to comply with an ASA ruling, the ASA may ultimately refer the issue to Trading Standards for non-compliance with the legislation which underlies the CAP Code,[16] or to Ofcom in relation to broadcast advertising.

General law

22. The appendix now provides a brief description of the legal framework of general application relevant to the study, with the fields of competition, consumer, and data protection law being addressed alphabetically rather than in term of importance or relevance to the study. It also identifies other areas of the general law which apply to digital platforms and online advertising.

Competition law

23. The appendix provides a brief description of the enforcement of the prohibitions against restrictions of competition or abuse of a dominant position; the review of mergers; and the market investigation regime.

24. The UK has an established set of rules to govern how the competitive process should operate to promote the economic benefits that competition between different businesses can bring for consumers, businesses and markets. In the UK these are set out in the Competition Act 1998, and the Enterprise Act 2002, with similar provision made at the EU level in the Treaty on the Functioning of the European Union in Article 101 and 102; Council Regulation (EC) No 1/2003; and the EU Merger Regulation 139/2004

25. Whilst these laws are of direct application, public enforcement is the responsibility of a designated competition authority, in the UK the CMA[17] and at an EU level the Directorate-General Competition of the European Commission.

[15] Broadcasters are required to comply with the BCAP Code under the terms of their licences from Ofcom, which retains overall sign-off on major changes to the BCAP Code.
[16] Trading Standards apply consumer law, eg in respect of misleading advertisements.
[17] With 'concurrent' regulators having authority for antitrust enforcement in specific sectors of the economy alongside the CMA. For simplicity, the appendix refers only to the CMA as the UK enforcer of competition but this should be taken to include the concurrent regulators, as appropriate.

Enforcement (antitrust)

26. Competition law protects businesses and consumers against anti-competitive agreements or behaviours. The enforcement of this body of law is sometimes described as antitrust, with enforcement and the imposition of penalties and remedies where businesses are found to have infringed the law, having an important role to deter anti-competitive behaviour.

Chapter I / Article 101

27. The Chapter I prohibition essentially prohibits anti-competitive agreements between businesses. Section 2 of the Competition Act 1998 (CA98) reflects the provisions of Article 101 of the TFEU,[18] and provides:

'… agreements between undertakings, decisions by associations of undertakings or concerted practices which—

(a) may affect trade within the United Kingdom, and

(b) have as their object or effect the prevention, restriction or distortion of competition within the United Kingdom,

are prohibited unless they are exempt in accordance with the provisions of this Part.'

28. With section 9 CA98 providing an 'exemption' analogous to Article 101(3) where efficiencies justify exempting a restriction from the prohibition.

29. Currently the Chapter I prohibition is interpreted consistently with the analogous provisions of EU law, having regard to any relevant differences between the provisions concerned.[19]

Chapter II / Article 102

30. The Chapter II prohibition is set out in section 18 of the Competition Act 1998 and reflects the provisions of Article 102 of the TFEU,[20] and provides:

[18] 'shall be prohibited as incompatible with the internal market: all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market…'
[19] S.60 CA98. Section 60A CA98 makes alternative provision for the UK leaving the EU.
[20] 'Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States.'

‘any conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market is prohibited if it may affect trade within the United Kingdom’

31. As an illustration of this prohibition, the European Commission has found a number of infringements in areas of relevance to this study (all of which are currently subject to an appeal):

- **39740 Google Search (Shopping)** – the Commission Decision finds that:

  ‘the more favourable positioning and display by Google Inc. (‘Google’), in its general search results pages, of its own comparison shopping service compared to competing comparison shopping services, infringes Article 102 TFEU’[21] because;

  ‘Google's conduct is abusive because it: (i) diverts traffic away from competing comparison shopping services to Google's own comparison shopping service, in the sense that it decreases traffic from Google's general results pages to competing comparison shopping services and increases traffic from Google's general search results pages to Google's own comparison shopping service; and (ii) is capable of having, or likely to have, anti-competitive effects in the national markets for comparison shopping services and general search services.’[22]

- **40099 Google Android** – the Commission decision finds,

  ‘that conduct by Google with regard to certain conditions in agreements associated with the use of Google's smart mobile operating system, Android, and certain proprietary mobile applications ("apps") and services constitutes a single and continuous infringement of Article 102 [and] constitutes four separate infringements of Article 102 … (1) tying the Google Search app with its smart mobile app store, the Play Store; (2) tying its mobile web browser, Google Chrome, with the Play Store and the Google Search app; (3) making the licensing of the Play Store and the Google Search app conditional on agreements that contain anti-fragmentation obligations, preventing hardware manufacturers from: (i) selling devices based on modified versions of Android ("Android forks"); (ii) taking actions that may cause or result in the fragmentation of Android; and (iii) distributing a software development kit (‘SDK’) derived from

[21] Summary of Commission decision, (2018/C 9/08), paragraph 1.
[22] Summary of Commission decision, (2018/C 9/08), paragraph 10.

Android; and (4) granting revenue share payments to original equipment manufacturers ("OEMs") and mobile network operators ('MNOs') on condition that they preinstall no competing general search service on any device within an agreed portfolio.'[23]

- **40411 Google Search (AdSense)** – the Commission press release explains it found:

  'Google 'misuse[d] … its dominant position in the market for the brokering of online search adverts. Google has cemented its dominance in online search adverts and shielded itself from competitive pressure by imposing anti-competitive contractual restrictions on third-party websites. This is illegal under EU antitrust rules. The misconduct lasted over 10 years and denied other companies the possibility to compete on the merits and to innovate – and consumers the benefits of competition'.[24]

Merger control

32. The UK merger regime is set out in Enterprise Act 2002 (EA02). UK merger control law does not require that a qualifying merger (ie, a relevant merger situation) be notified to the CMA, but the CMA may choose to review any qualifying merger. The assessment of mergers in the UK is conducted as a two-phase process, with both anticipated and completed mergers being covered by EA02.

33. The CMA assesses whether a merger will lead to a 'significant lessening of competition' (SLC). The CMA's Merger Assessment Guidelines provide that 'A merger gives rise to an SLC when it has a significant effect on rivalry over time, and therefore on the competitive pressure on firms to improve their offer to customers or become more efficient or innovative. A merger that gives rise to an SLC will be expected to lead to an adverse effect for customers.[25]'

34. Under the UK's two-phase merger control regime, the CMA applies different thresholds in its Phase 1 initial assessment, a 'realistic prospect' threshold for a SLC, and a 'balance of probabilities' threshold at Phase 2, ie, it addresses the question: is it more likely than not that an SLC will result due to the merger. If so, the CMA considers whether the SLC can be 'remedied', such as

[23] CASE AT.40099 Google Android, Brussels, 18.7.2018 C(2018) 4761 final, paragraphs 2 t0 4.
[24] Press release: Antitrust: Google fined €1.49 billion for online advertising abuse.
[25] Merger Assessment Guidelines, 4.1.3.

by a structural remedy (eg by a divestment) or behavioural remedy,[26] and if not, the merger is prohibited.

35. Mergers that have a 'Community dimension' under the EU Merger Regulation (ie mergers above certain thresholds) fall outside the scope of the jurisdiction of the EA02. Instead they must be notified in advance to the European Commission.[27] The underlying economic approach to assessment carried out by the CMA is generally similar to that carried out by the European Commission.

36. The CMA's approach to mergers is set out in guidance, 'Mergers – the CMA's jurisdiction and procedure: CMA2' and 'Merger assessment guidelines: CC2/OFT1254'.

37. Last year, the CMA conducted a call for views on our approach to the assessment of digital mergers,[28] to inform a review of our guidelines on how we assess merger cases. We also published an independent review of past digital mergers.[29] This includes a review of the mergers in Facebook/Instagram; Facebook/Instagram; Priceline/Kayak and Expedia/Trivago; and Amazon/The Book Depository.

Market investigation regime

38. A longstanding feature of the UK competition regime is the ability to investigate the operation of markets as a whole, as reflected in the work of this market study. The CMA may investigate to assess if a market operates in a manner which works well for consumers, and if not, may make proposals or adopt measures (remedies) so they might be made to work better.

39. Like the process described above for mergers, there is a two-phase process. First, the 'Phase 1' process is the market study, which determines whether there is a case for a more detailed examination during the 'Phase 2' process, which is the Market Investigation. This is achieved through a 'Market Investigation Reference' (MIR). The Market Investigation seeks to determine if features of the market have an adverse effect on competition (the 'AEC test'), and if so the CMA decides what remedial action, if any, is appropriate

[26] An example of, an exceptional, behavioural merger remedy, was Contract Rights Renewal remedy in Carlton/Granada ITV merger; where a remedy was put in place to protect the position of advertisers in respect of the combined entity with an adjudicator to determine disputes http://www.adjudicator-crr.org.uk/.
[27] Assessment of mergers can in certain circumstances be transferred between the UK and EU regime.
[28] CMA call for information: digital mergers, 3 June 2019.
[29] LEAR Report - Ex-post Assessment of Merger Control Decisions in Digital Markets, 9 May 2019.

for it using its own order making powers,[30] or for others to take following a CMA recommendation.

40. Like in mergers, markets remedies are conventionally classified as either structural or behavioural. Structural remedies are generally one-off measures that seek, in market investigations, to increase competition by altering the competitive structure of the market. Behavioural remedies are generally ongoing measures that are designed to regulate or constrain the behaviour of parties in a market and/or empower customers to make effective choices.

41. As the then Government observed when last significantly reforming the markets regime 'A distinctive feature of the [UK] regime is that where a market is found not to be working well, the firms might be prohibited from particular practices for the future, but they face no retrospective penalties nor do they face the prospect of third party actions for past abuses.'[31]

42. An example of a structural remedy occurred in the *BAA airports* market investigation, the CMA's predecessor required BAA divest Gatwick and Stansted airports and a Scottish airport as part of its package of remedies. An example of a behavioural remedy is the Groceries (Supply Chain Practices) Market Investigation Order, this required large UK grocers, to follow the Groceries Supply Code of Practice, with a recommendation to the Government to put in place a Groceries Code Adjudicator, which it did.

Consumer law

43. This Appendix provides a non-exhaustive description of the consumer law relevant to the study. The main focus is on Part 2 of the Consumer Rights Act 2015 and the Consumer Protection from Unfair Trading Regulations 2008, although other consumer protection legislation may apply to the activities of online platforms and across digital advertising.[32]

The Consumer Rights Act 2015 (CRA) – Part 2

44. Part 2 of the CRA implements the Unfair Contract Terms Directive 93/13/EEC into UK law.[33]

---

[30] The CMA may also accept binding undertakings from market participants.
[31] Paragraph 6.8, White paper – A World Class Competition Regime, DTI, 30 July 2001.
[32] In particular platforms may also need to comply with the requirements of other parts of the CRA or the Consumer Contracts (-Information, Cancellation and Additional Charges) Regulations 2013.
[33] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (The Unfair Contract Terms Directive, 93/13/EEC).

45. Part 2 of the CRA applies to both consumer contracts and consumer notices[34] and requires the terms in consumer contracts and consumer notices to be fair and, if written, transparent.

46. A term in a consumer contract or consumer notice is unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations under the contract, to the detriment of the consumer (the 'fairness test').

47. Generally, contract terms or notices are unfair if they put the consumer at an unfair disadvantage. The 'fairness test' starts by asking whether the wording used tilts the rights and responsibilities between the consumer and business too much in favour of the business. The test is applied by looking at the words and how they could be used. It takes into consideration what is being provided, how a term relates to other terms in the contract and all the circumstances at the time the term was agreed.

48. Some terms may be exempt from the 'fairness test' – namely those describing the main subject matter and setting the price – provided that they are transparent and prominent. There is also an exemption for wording that reflects mandatory legislative or regulatory provisions, for example, words that legally have to be used.

49. The CRA illustrates what 'unfairness' means by listing some types of terms that may be unfair in Schedule 2 to the CRA (known as the 'Grey List'). Terms like those included in the Grey List are not necessarily unfair, but concerns about the fairness of a term are likely to arise where it has the same purpose, or can produce the same result, as the types of terms listed in the Grey List. The Grey List is not exhaustive, which means that terms that do not appear on it may still be unfair.

50. Part 2 of the CRA includes a specific requirement that all written terms have to be transparent. This means they must be expressed in plain, intelligible language and be legible.

51. Transparency is also relevant to the 'fairness test'. The reference to good faith in the 'fairness test' relates to how contracts are drafted and presented and the way in which they are negotiated and carried out.

52. To achieve the openness required by good faith, terms should be expressed fully and clearly so consumers can make informed choices about whether or not to enter the contract. Terms that might disadvantage the consumer should

[34] A consumer notice is wording that may not form part of a contract but which relates to the same kind of issues that would be dealt with in a contract – for instance the rights or obligations between a business and a consumer.

be given appropriate prominence. Contracts should not contain concealed pitfalls or traps.

53. Examples of cases decided in relation to the Unfair Contract Terms Directive in relation to relevant digital services include:

- WhatsApp – in 2017 the Italian competition authority (the AGCM) found a number of WhatsApp's terms of use unfair. These included terms which gave WhatsApp the right to introduce changes without reason and without informing the consumer and the tacit approval to obtain consent through consumer inertia. [CV154, dated 11 May 2017]

- Facebook – in 2019 a French court fined Facebook €30,000 for using unfair terms. These included terms which allowed Facebook to retain, use and resell user's data, even after their account had been closed, and to unilaterally change the terms and conditions without informing users. [Paris TGI judgment. 9 April 2019]

The Consumer Protection from Unfair Trading Regulations 2008 (CPRs)

54. The Unfair Commercial Practices Directive[35] (UCPD) is implemented into UK law by the Consumer Protection from Unfair Trading Regulations (SI 2008/1277) (CPRs).

55. Broadly speaking, the CPRs prevent businesses (described as 'traders' in the CPRs) from treating consumers unfairly. Businesses are also responsible for the commercial practices of anyone who acts on their behalf or in their name. Both the business and those acting on their behalf may be held liable for breaches of the CPRs.

56. The CPRs apply to a wide range of commercial practices which might affect consumers. Commercial practices may include matters such as advertising, marketing, sales, supplies and after-sales services. A commercial practice is governed by the CPRs if it is directly connected with the promotion, sale or supply of goods or services (both described as 'products' in the CPRs) to consumers. This means that although a business may not be selling to consumers themselves, or advertising their own products, they may still have to comply with the CPRs.

57. There are 31 practices listed in Schedule 1 to the CPRs, which because of their inherently unfair nature, are prohibited in all circumstances.

---

[35] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business -to-consumer practices in the internal market.

58. Regulations 3, and 5 to 7 of the CPRs, also prohibit unfair practices; however, to be in breach of those Regulations the business must exhibit the conduct specified in the prohibition and the practice must have, or be likely to have, an effect on the transactional decisions of the average consumer.

59. The average consumer is generally assumed to be reasonably well informed and reasonably observant and circumspect. Average does not mean a statistically average consumer. Where a commercial practice is targeted at a particular group or it is reasonably foreseeable that a group of consumers will be particularly vulnerable to that practice, then the average consumer refers to the average member of that group.

60. The CPRs prohibit unfair practices which affect a wide range of decisions taken by consumers in relation to products before, during or after a commercial transaction (if any). This is not simply confined to a consumer's decision whether or not to purchase a particular product but could also include, for example, a consumer's decision to view a product, contact a business or visit a shop, as well as a decision not to purchase a particular product or to exercise a contractual right.

61. Regulation 3 contains a general prohibition on unfair commercial practices. This prohibits practices that contravene the requirements of professional diligence (meaning honest market practice and good faith) and materially distort or are likely to materially distort the economic behaviour of the average consumer.

62. Regulation 5 prohibits misleading actions, which occur when a business gives consumers false information (about a wide-range of things listed in the CPRs), or is deceptive in the presentation of that information even if it is factually correct, and causes or is likely to cause the average consumer to take a different decision.

63. Regulation 6 prohibits misleading omissions, which occur when businesses fail to give consumers the information that they need to make an informed choice in relation to a product. This includes practices which omit or hide ‘material information’, or provide it in an unclear, unintelligible, ambiguous or untimely manner, and the average consumer takes, or is likely to take, a different decision as a result.

64. Regulation 7 prohibits aggressive commercial practices. These are practices that, in the context of the particular circumstances, put unfair pressure on consumers, restricting their ability to make free or informed decisions.

65. Examples of cases decided in relation to the Unfair Commercial Practices Directive in relation to relevant digital services include:

- WhatsApp – in 2017 the AGCM fined WhatsApp €3,000,000 for the use of aggressive commercial practices, in particular putting unfair pressure on consumers to accept WhatsApp's new terms of use (which included pre-selected consent to share personal data with Facebook for commercial and advertising purposes). [PS10601, 11 May 2017]

- Facebook in 2018 the AGCM fined Facebook €5,000,000 for an unfair commercial practice, misleading consumers by emphasising the 'free' nature of the service but failing to properly inform consumers that their data would be used for commercial purposes, as well as failing to make a distinction between the personalisation of services for connecting with friends and the use of that data for targeted advertising. [PS11112, dated 29 November 2018]

- In 2018 the AGCM fined Facebook a further €5,000,000 for the use of aggressive commercial practices, in particular sharing existing user's data with third party websites and Apps for commercial practice without express and prior consent. [PS11112, dated 29 November 2018]

What about 'free' services?

66. The overarching intention of consumer law is to protect consumer's economic interests. However, that does not necessarily mean that contracts involving non-monetary consideration will fall outside its scope. Courts in various international jurisdictions have accepted that a consumer's personal data, preferences and user-generated content can have an economic value[36] and is a valid form of consideration in return for a service.

67. In principle, consumer law may apply to services provided by platforms to consumers in exchange for their personal data, just as it would if they paid a monetary price.

68. The European Commission (EC) guidance on the application of the UCPD[37] notes that:

> Products presented as 'free' are especially common in the online sector. However, many such services are only accessible for consumers on the condition that they provide personal data such as their identity and email address … The marketing of such products as 'free' without telling consumers

---

[36] The EU Commission stated: "*personal data, consumer preferences and other user generated content have a "de facto" economic value …"* European Commission, *Commission Staff Working Document: Guidance on the implementation / application of Directive 2005/29/EC on Unfair Commercial Practices*, p 25 (SWD(2016) 163 final)
[37] Ibid pg. 88 -89

how their preferences, personal data and user-generated content are going to be used could in some circumstances be considered a misleading practice.

69. The AGCM has successfully taken action in Italy, under its national equivalents of the CRA and CPRs, against WhatsApp and Facebook in relation to services which they provided in return for personal data as opposed to monetary consideration[38]. The UFC-Que Choisir has also successfully brought similar actions in France, relating to unfair terms, against Facebook, Twitter and Google. However, it should be noted that similar arguments about misleading practices were rejected by the German courts in an action brought by the VZBV against Facebook.[39]

Twitter, Google and Facebook

In a series of three cases brought by the French consumer association (UFC-Que Choisir) commencing in 2014 and heard separately by the Tribunal de Grande Instance in Paris between August 2018 and April 2019; the French Court found clauses within Twitter, Google and Facebook's terms of use unlawful and abusive In the main, these terms concerns the exploitation of user's personal data without appropriate consent. All three companies were separately fined €30,000.

Despite arguments that the free provision of the service meant the social networks fell outside consumer law, the French Court found consumer law applied to the as the companies acted for commercial purposes and profited from their activity exploiting and using personal data.

In assessing Twitter's clauses, the court was critical of default provisions that data was public, liability exclusions and heavy use of hyperlinks (making it impossible for the consumer to consider the information provided.)

The court was critical of Facebook's clauses allowing collection and exploitation of user data without consent, clauses concerning third party involvement in relation to data and use of vague and unclear terms.

Google's terms of use and privacy rules were also abusive and unlawful concerning transparency and consent of personal data. Clauses were insufficiently detailed information was provided to allow consumers to be aware of the real purpose.

[38] WhatsApp cases, case number PS10601 and CV154 dated 11 May 2017 and Facebook case number PS11112, dated 29 November 2018.
[39] Case No. 16 O 341/15, Berlin Regional Court case, Dated 16 January 2018

70. The 2019 Digital Contents Directive,[40] recognising such digital content and services are often not supplied for a monetary price, explicitly includes contracts to a consumer in exchange for the provision of personal data.

How does consumer law fit with the GDPR?

71. Consumer law and data protection law are generally complementary and, in many senses, pursue similar objectives, in particular promoting transparency and genuine, informed choices.

72. Although a breach of the GDPR will not automatically constitute a breach of consumer law, it is likely to be relevant to any assessment of a business' compliance.

73. To the extent that wording in a privacy notice or policy reflects wording legally required by the GDPR, then it may not be assessable for fairness under Part 2 of the CRA.

74. However, to benefit from this exemption it is not enough, for instance, for a term or notice merely to resemble what is provided for by law in a different context, or for wording merely to include some elements that reflect legal requirements. Similarly, the provisions' effects must be set out in a way that consumers can understand.[41]

75. In relation to the CPRs, the EC guidance on the UCPD says:

> '… data protection violations should be considered when assessing the overall unfairness of commercial practices under the UCPD, particularly in the situation where the trader processes consumer data in violation of data protection requirements, ie for direct marketing purposes or any other commercial purposes like profiling, personal pricing or big data applications.'[42]

76. For example, the prohibition in the CPRs on providing false or deceptive information extends to information about a consumer's rights, which could, for example, include their statutory rights under the GDPR.[43] Similarly, the

---

[40] See recital 24 of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (The Digital Contents Directive 2019/770)
[41] RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen e.V: C-92/11
[42] European Commission, Commission Staff Working Document: Guidance on the implementation / application of Directive 2005/29/EC on Unfair Commercial Practices, p 25 (SWD(2016) 163 final) pg. 24
[43] Reg. 5(4)(K)

prohibition on omitting or hiding important information includes any information required by European (EU) derived law, such as the GDPR.[44]

Data Protection Law

77. This appendix summarises aspects of the data protection framework of most relevance to the scope of market study. The Information Commissioner's Office (ICO) has published detailed guidance on the application of the GDPR and DPA18, which this note does not attempt to replicate.[45]

The General Data Protection Regulation 2016/679 (the 'GDPR')

78. The GDPR is a regulation which has direct effect in the UK, *sitting alongside* the Data Protection Act 2018 (the 'DPA18') which tailors how it applies in the UK. Together, this legislation provides the general framework for the protection of personal data that applies in the UK.[46]

79. The GDPR came into effect on 25 May 2018, and whilst it introduced important changes, it built upon similar principles derived from the Data Protection Directive 95/46/EC and the Data Protection Act 1998.

80. The ICO assisted the introduction of the GDPR in the UK by publishing extensive guidance on the interpretation of the GDPR, and this is in turn supported by a wider body of interpretive guidance from the European Data Protection Board (the EDPB).[47] Whilst not binding, this material is an important and useful aid to interpreting the principles in the GDPR and applying them to relevant factual situations; practices that are not in line with the guidance provided by the expert regulator are likely to be non-compliant.[48]

81. The GDPR has been in effect for a little over two years, there has therefore been a limited period of time for an authoritative body of case law to develop in the domestic or European appellate courts to assist in clarifying the application of the general principles prescribed by the GDPR to particular sets of factual circumstances.[49] In the course of this study the CMA has

---

[44] Reg. 6(3)(b)
[45] Guide to the General Data Protection Regulation (GDPR), and Introduction to data protection
[46] The Privacy and Electronic Communications Regulations 2003 (PECR) are described in a subsequent section.
[47] Which adopted guidance prepared by its predecessor body under the Directive, the Article 29 working party, which had published guidance on the GDPR and published guidance on the similar principles under the Directive. In this Appendix the term EDPB is used to cover adopted Art.29 Working Party Guidance adopted by the EDPB.
[48] Advocate General Szpunar in his opinion for the CJEU in C-673/17, Planet49 GmbH v BVV, EU:C:2019:246, when considering the proper interpretation of the relevant provision in relation to 'Cookies' had regard to 'the non-binding but nevertheless enlightening work of the 'Article 29' Data Protection Working Party ('the "Article 29" Working Party')' [81].
[49] In relation to decisional practice by independent supervisory authorities, in February 2020, in its Annual Report on data protection, the DPC reported on its 21 open investigations into 'Multinational Technology Companies'

encountered disparate interpretations of the application of the GDPR to the matters in scope of this study.[50] This appendix describes the GDPR and the interpretations taken by the ICO and the EDPB on issues of relevance to this study.

Harmonisation

82. As an EU regulation the purpose of the GDPR is to produce, as appropriate, a consistent European wide regime for the protection and processing of personal data, as recital 10 provides:

> to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.
>
> As the recital also provides
>
> Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

Definitions

83. Article 4 of the GDPR is makes provision for several important definitions:

- 'Personal data' is a wide concept and 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

---

which it is progressing. In late May 2020, the DPC announced that it had progressed a number of its 'big tech' investigations towards conclusion, including having 'completed the investigation phase of a complaint-based inquiry which focuses on Facebook Ireland's obligations to establish a lawful basis for personal data processing. This inquiry is now in the decision-making phase at the DPC.'

[50] This experience is consistent with that of the ICO which found it 'become apparent during our work that there are substantially different levels of engagement and understanding of how data protection law applies, and the issues that arise'

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.[51]

- 'Processing' is also a very wide concept, and means any operation performed on personal data including collection, storage, alteration, use, dissemination and erasure.

Who's who in the GDPR:

- A 'controller' is 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.

- A 'processor' is a natural or legal person, which processes personal data on behalf of the controller.

- Independent supervisory authorities[52] – monitor and enforce compliance with the GDPR. Where a controller/processor carries out cross-border processing the GDPR makes provision for a lead supervisory authority, which is the authority of the controller/processor's main or single establishment. The UK's independent supervisory authority is the Information Commissioner's Office; others include the Irish Data Protection Commission.[53]

- European Data Protection Board[54] – seeks to achieve consistency in the application of the GDPR by providing opinions and resolving disputes between independent supervisory authorities.[55]

Principles relating to the processing of personal data – Article 5 GDPR

84. To comply with the GDPR processing of personal data must meet the following principles:

---

[51] Art.4(1) GDPR, ICO general guide to the GDPR - what is personal data.
[52] The GDPR provides for the existence of independent supervisory authorities (Article 51), and Article 52 provides that they must 'act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation' and provides that they must 'in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody'.
[53] This is relevant to this market study as a number of the companies' in this market have their main EU establishment in Ireland, and as such the DPC is their lead supervisory authority (Art.56).
[54] Whilst not directly part of the GDPR regime, the European Data Protection Supervisor, the EU (institutions) independent data protection authority, also adopts a wider policy role on interpreting data protection law, and sits on the EDPB Board, as well as providing its secretariat.
[55] Note the EDPB in its first plenary meeting endorsed a number of the GDPR related 'WP29 Guidelines' adopted by the Article 29 Working Party under the previous Directive.

- Principle A: ‘lawfulness, fairness and transparency’ – data must be processed lawfully, fairly and in a transparent manner in relation to the data subject

- Principle B: ‘purpose limitation’ – collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…

- Principle C: ‘data minimisation’ – adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- Principle D: ‘accuracy’ – 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

- Principle E: ‘storage limitation’ 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…

- Principle F: ‘integrity and confidentiality’ – processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- Accountability principle: ‘the controller shall be responsible for, and be able to demonstrate, compliance with’ (the above principles)

85. Principles of particular relevance to this study include:

- ‘lawfulness, fairness, and transparency’.

86. Personal data in addition to being processed lawfully, must be used in a way that is fair, ie is not unduly detrimental, unexpected or misleading to the individuals concerned, and must be done in a way which is clear, open and honest – transparency is an overarching principle with detailed provision on the ‘right to be informed’ and its modalities provided for in Articles 12 to 14).[56]

- ‘purpose limitation’.

87. The GDPR requires controllers to collect personal data for specified, explicit and legitimate purposes and not further process that data in a manner

[56] The detail of the requirements of the right to be informed are not covered in this interim report appendix.

incompatible with those purposes. The GDPR also limits the processing of personal data a new purpose other than that for which the data was collected, where this is not based on consent or on a clear obligation or function set out in law; in these cases the controller must assess whether processing for the new purpose is compatible with the original purpose.

- ‘data minimisation’ – adequate, relevant and limited.

88. The data minimisation principle requires controllers to identify the minimum amount of personal data they need to fulfil their purpose.

- Accountability.

89. Article 5(2) provides the data controller is responsible for, and must be able to demonstrate, compliance with these principles. This is underpinned by Article 24 of the GDPR which requires the controller to implement appropriate technical and organisational measures to ensure, and demonstrate, compliance with the GDPR. The controller must take into account the nature, scope, context and purposes of the processing as well as the risks it poses to the rights and freedoms of individuals. The measures they implement should therefore be risk-based and proportionate; and should be reviewed and updated as necessary.

- Lawful basis for processing – Art. 6.

90. For the processing of personal data to be lawful, at least one of the following lawful bases needs to apply:

- ‘consent’ – the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

- ‘contract’ – processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

- ‘legal obligation’ – processing is necessary for compliance with a legal obligation to which the controller is subject;

- ‘vital interests’ processing is necessary in order to protect the vital interests of the data subject or of another natural person;

- ‘public task’ – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- ‘legitimate interests’ – processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

91. This appendix focuses on ‘consent’, ‘contract’ and ‘legitimate interests’ as these are the principle basis on which we have been told processing takes place in the digital advertising market.

92. The appropriateness and validity of a lawful basis for processing needs to be considered in the context of the GDPR as a whole, including controllers’ duty to process personal data in compliance with the data protection principles in Art. 5. This includes processing personal data in a fair and transparent manner and in line with the purpose limitation and data minimisation obligations.

93. The ICO has previously noted that ‘The lawful bases for processing personal data that different organisations operating in the adtech ecosystem currently rely upon are apparently inconsistent. There seem to be several schools of thought around the suitability of various bases for processing personal data – we would like to understand why the differences exist.’[57] The has ICO expressed doubt that, for the purposes for which personal data is processed in the current real time bidding ecosystem and the means by which that data is processed, whether any basis other than consent is practically available where PECR applies, and has identified that there is an issue with the extent to which consent will be ‘fully informed’ in an environment where data is being shared with potentially hundreds of organisations (some of which are controllers, some processors, and other joint controllers).

94. Processing without a valid legal basis is an infringement of the fundamental data protection principles in Article 5, and therefore risks substantial fines under the GDPR. Article 83(5)(a) provides that infringements of the basic principles for processing personal data, including the conditions for consent, contract and legitimate interests, are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of total worldwide annual turnover, whichever is higher.

[57] ICO blog: advancing the adtech debate from a data protection perspective.

Consent

95. Consent is defined as being 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.[58]

96. As such the GDPR sets a high standard for what constitutes positively giving consent to processing, it must be freely given, specific, informed, and there must be an indication signifying agreement.

97. Article 7 sets out further provision for consent covering:

- keeping records to demonstrate consent;
- prominence and clarity of consent requests;
- the right to withdraw consent easily and at any time;[59] and
- freely given consent if a contract is conditional on consent.

98. The rest of this sub-section considers some of these factors.

'Freely given'

99. The GDPR recitals provide helpful elucidation,[60] with recital 42 providing:

'…Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.'

100. The ICO explain:[61]

Consent means giving people genuine choice and control over how you use their data. If the individual has no real choice, consent is not freely given and it will be invalid.

---

[58] Article 4 (11), see also Articles 6(1)(a), 7, 8, 9(2)(a) and Recitals 32, 38, 40, 42, 43, 171
[59] Processing based on consent is a dynamic process, and '*must be as easy to withdraw as give consent*' Article 7(3).
[60] In his *Opinion* in *Planet49,* AG Szpunar provided a helpful reminder of the role of the recitals specifically in the context of the GDPR '*Because I shall make extensive reference to the recitals, I feel compelled to recall that they obviously do not have any independent legal value, but that the Court frequently resorts to them in interpreting provisions of an EU legal act. In the EU legal order they are descriptive and not prescriptive in nature. Indeed, the question of their legal value does not normally arise for the simple reason that, typically, the recitals are reflected in the legal provisions of a directive. Good legislative practice by the political institutions of the EU tends to aim at a situation in which the recitals provide a useful background to the provisions of a legal text.*', and the CJEU in giving its subsequent judgment indeed placed reliance on the GDPR's recitals in respect of consent.
[61] ICO detailed guidance: consent.

This means people must be able to refuse consent without detriment, and must be able to withdraw consent easily at any time. It also means consent should be unbundled from other terms and conditions (including giving separate granular consent options for different types of processing) wherever possible.

101. There is a real question about the extent to which consent can be genuinely freely given if consent is a precondition of being able to use a service. Art. 7(4) provides

'When assessing whether consent is freely given, utmost account shall be taken of whether… the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'

Recital 43 provides

'Consent is presumed not to be freely given… if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.'

102. Recital 42 to the GDPR provides that:

'Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment'

103. The ICO guidance explains the GDPR is clear that consumers must be able to refuse to give their consent, or later withdraw the consent they have given without being penalised. We understand this is because, if consumers knew that they would suffer a detriment if they didn't give consent, consent given in that context would not be considered freely given, and so would not be valid. However, the ICO guidance goes on to explain that its 'view is that it may still be possible to incentivise consent to some extent', without creating a detriment for those who do not consent.

104. The ICO's guidance notes that there will usually be some benefit to consenting to processing data. Where the processing of the consumers data provides them a benefit, the consumer is therefore incentivised to choose to consent so they can have that benefit. The ICO give the example of a consumer who consents to receive a retailers marketing material as part of its loyalty scheme. In the promotional material the retailer sends the consumer money-off vouchers to incentivise them to return to the retailer's store (rather than its competitors). As such there is an incentive to consent to the processing of their data so the consumer can be sent the discount vouchers.

The fact that consumers who choose not to sign up to the newsletter don't get sent promotional vouchers, and so don't benefit from the discounts, does not constitute a detriment for deciding not to sign-up (they can still freely access the retailer's services if they choose). However, having explained why it considers it is possible to incentivise consent to some extent, it cautions data controllers 'must be careful not to cross the line and unfairly penalise those who refuse consent', that is creating a detriment for consumers.

105. In relation to 'cookies' and so called 'cookie walls', which purport to require a consumer to 'agree' or 'accept' the setting of cookies before they can access an online service's content, whilst there are specific rules governing the use of cookies in PECR, it takes the GDPR's definition of consent as the applicable standard. In relation to 'cookie walls', the ICO's guidance on the use of cookies caution against this approach by reflecting its core guidance on consent, stating that they may be inappropriate where the consumer has no genuine choice but to sign up for general access, explaining 'The key is that individuals are provided with a genuine free choice; consent should not be bundled up as a condition of the service unless it is necessary for that service.' The ICO cautions:

'If your use of a cookie wall is intended to require, or influence, users to agree to their personal data being used by you or any third parties as a condition of accessing your service, then it is unlikely that user consent is considered valid.'[62]

106. The concept of freely given also needs to have regard to the potential imbalance of power between parties, the 'particular' example given in the GDPR are those between an employer of public authority, but as the ICO guidance provides 'Freely given consent will also be more difficult to obtain in the context of a relationship where there is an imbalance of power'.[63]

'Specific and informed'

107. Consent requires a clear and specific affirmative action, ie an opt-in,[64] to constitute consent, this will require a level of 'granularity' about the processing

---

[62] ICO guidance on the use of cookies and similar technologies. See also EDPB statement on ePrivacy Regulation, '*the necessity to obtain a freely-given consent will prevent service providers from including cookie walls for their users*' EDPB - statement on ePrivacy.

[63] See Recital 43 '*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation…*'

[64] 'Opt out', ie pre-ticked boxes, are not acceptable for consent. Recital 32.

(which will need to be balanced against clarity and being concise). This will involve it being:

- Granular: giving distinct options to consent separately to different types of processing wherever appropriate (this might be achieved through a layered approach).[65] Recital 43 provides:

  'Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case,[66] or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.'

- Active opt-in: pre-ticked opt-in boxes are invalid –unticked opt-in boxes or similar active opt-in methods (eg a binary choice given equal prominence).[67]

- Easy to withdraw: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you need to have simple and effective withdrawal mechanisms in place.

108. This needs to be done in a way which is prominent, concise, separate from other terms and conditions,[68] and in plain language. Whilst not being unnecessarily disruptive to users (eg using layered information and just-in-time consents).[69] The ICO explain:

'You must clearly explain to people what they are consenting to in a way they can easily understand. The request for consent needs to be prominent, concise, separate from other terms and conditions, and in plain language.[70]

If the request for consent is vague, sweeping or difficult to understand, then it will be invalid. In particular, language likely to confuse – for example, the use of double negatives or inconsistent language – will invalidate consent.'

---

[65] Recital 43.
[66] A coronally to the concept that consent is invalid where aggregation of different processing operations is inappropriate, ie the control is insufficiently granular, is that an appropriate aggregation of processing operations may be valid when seeking consent.
[67] The requirement to be 'a clear affirmative act' is, according to the Ar.29 WG, will not be met be satisfied by the user continuing to scroll down or swiping as that is not sufficiently unambiguous from normal use.
[68] Art.7(2) 'If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.'
[69] Recital 32.
[70] ICO general GDPR guidance.

109. In relation to digital services the Recital 32 expressly provides in relation to consent:

'This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.'

110. However, the ICO Guidance explains that recitals observation that electronic consent requests must not be unnecessarily disruptive to users for example, by developing user-friendly layered information and just-in-time consents 'is not an exemption and avoiding disruption does not override the need to ensure that consent requests are clear and specific. Some level of disruption may be necessary to obtain valid consent.'[71]

111. The ICO guidance acknowledges 'There is a tension between ensuring that consent is specific enough and making it concise and easy to understand.' and suggest that 'In practice this means you may not be able to get blanket consent for a large number of controllers, purposes or processes. This is because you won't be able to provide prominent, concise and readable information that is also specific and granular enough.'[72]

112. Consent is an area where the ICO have published 'detailed guidance' as a supplement to its general guidance on the GDPR,[73] and the EDPB have adopted guidance on consent.[74]

***Contract** – Art. 6(b) – processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract*

113. The GDPR recognises that some specific processing is part and parcel of delivery of the service requested by the data subject, and it is in the interests

---

[71] ICO general GDPR guidance
[72] ICO general GDPR guidance.
[73] ICO detailed guidance - consent.
74 Guidelines on Consent under Regulation 2016/679 (wp259rev.01), updated in May 2020, Guidelines 05/2020 on consent under Regulation 2016/679 (Version 1.1).

of both parties to process that data, as otherwise the service could not be provided, and the contract could not be performed.[75]

114. There are essentially two limbs available, processing must be necessary:

- for the performance of a contract to which the data subject is party; or
- in order to take steps at the request of the data subject prior to entering into a contract.

115. The ICO explain, 'necessary for the performance of a contract' does not simply mean what is in the terms of the contract.[76] Assessing what is 'necessary' is a question of fact in each case. To take an example from the ICO guidance, where a customer makes an online purchase which they want delivered to their home, the processing of their home address will be necessary (as would a pre-contract check to see if delivery is possible to that address). However if the retailer wants to use the purchasing behaviour to build a profile of the consumer's interests and preferences to better advertise to them, it cannot rely on the contract as the lawful basis for this processing as this is not necessary for the performance of the contract (which is to deliver the purchase product). The ICO explain this applies 'even if this type of targeted advertising is a useful part of [the retailer's] customer relationship and is a necessary part of [its] business model, it is not necessary to perform the contract itself.' The ICO explain 'This does not mean that processing which is not necessary for the contract is automatically unlawful, but rather that you need to look for a different lawful basis (and other safeguards such as the right to object may come into play).'

116. The EDPB have recently published, following consultation, specific 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects'.[77] Particular use cases explored include:

---

[75] See recital 40, 'the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'. The EDPB have published 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects'. The EDPB's predecessor the Article 29 Working Party previously expressed views on the contractual necessity basis under Directive 95/46/EC in its 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217)'.

[76] ICO general GDPR guidance. For a more detailed exposition of the concept of 'objective necessity' see the EDPB Guidance on contract in the provision of online referred to below.

[77] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subject.

- *Processing for personalisation of content*

117. The EDPB observes that 'personalisation of content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases.' It explains it 'will depend on the nature of the service provided, the expectations of the average data subject in light not only of the terms of service but also the way the service is promoted to users, and whether the service can be provided without personalisation.' The EDPB considers that 'where personalised content delivery is intended to increase user engagement with a service but is not an integral part of using the service' it will not be objectively necessary for the purpose of the underlying contract.[78]

- *Processing for online behavioural advertising*

118. Whilst the EDPB observes that 'online behavioural advertising, and associated tracking and profiling of data subjects is often used to finance online services', it considers that as 'a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services'. Although such processing for advertising may fund the delivery of a service, is not sufficient to establish that it is necessary for the performance of the contract at issue'. Advertising is likely to be separate from the objective purpose of the contract, and so not necessary for the performance of the contract from the consumer's perspective. Few consumers will feel they did not get the contractual service if they were not served behavioural advertising.

119. The EDPB observes this view is supported by the fact Article 21 provides an absolute right to object to processing of your personal data for direct marketing purposes, ie that freestanding 'right' and the idea of advertising being necessary to a contract are incompatible.

- *Trading of a fundamental right*

120. The EDPB provided in relation to processing for behavioural advertising its view that[79]

Considering that data protection is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights, and taking into account that one of the

[78] Paragraph 57.
[79] Paragraph 54.

main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity.[80] Even if the data subject can agree to the processing of personal data, they cannot trade away their fundamental rights through this agreement.[81] (*footnotes in original*)

121. The scope of this section of the EDPB's view is not clear in this context. If the meaning is that a consumer can never provide valid consent to processing of their personal data for the purposes of advertising, if that consent is linked to receipt of a service (or if it ever did constitute a necessary part of a contract), the Opinion of AG Szpunar, C-673/17 Planet49, EU:C:2019:246, provides a different view. The AG observes that when having regard to Article 7(4) ('When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'); 'as transpires from the terms 'utmost account shall be taken of', the prohibition on bundling is not absolute in nature.' In other words, the express terms of the GDPR make clear that, exceptionally, 'unnecessary' terms might be freely consented to alongside a contract. The AG observed:

Here, it will be for the competent court to assess whether the consent to the processing of personal data is necessary for the participation in the lottery [to win a mac book]. In this respect it should be kept in mind that the underlying purpose in the participation in the lottery is the 'selling' of personal data (ie, agreeing to be contacted by so-called 'sponsors' for promotional offers). In other words, it is the providing of personal data which constitutes the main obligation of the user in order to participate in the lottery. In such a situation it appears to me that the processing of this personal data is necessary for the participation in the lottery.

122. It was ultimately not necessary for the CJEU to answer this question as it was not part of the reference question from the German court.

'Legitimate interests' – *Art.6(1)(f) – processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or*

---

[80] See Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

[81] Besides the fact that the use of personal data is regulated by the GDPR, there are additional reasons why processing of personal data is conceptually different from monetary payments. For example, money is countable, meaning that prices can be compared in a competitive market, and monetary payments can normally only be made with the data subject's involvement. Furthermore, personal data can be exploited by several services at the same time. Once control over one's personal data has been lost, that control may not necessarily be regained.

fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

123. The ICO observes that 'Legitimate interests', can appear to be a more 'flexible' lawful basis, but involves a careful three part balancing test whereby the controller assessed the interests, rights and freedoms of the data subject against their own interest. As per the accountability principle it is for the controller to demonstrate that they can meet the requirements of the legitimate interests tests.

124. The ICO explains[82] that the case law of the CJEU clarifies that the legitimate interests test breaks down into three parts:[83][84]

- Purpose test – is there a legitimate interest behind the processing?
- Necessity test – is the processing necessary for that purpose?
- Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms?

125. The ICO's guidance on legitimate interests[85] and its Update Report into Adtech and RTB[86] reflects these points of law.

- *Purpose*

126. The GDPR does not define legitimate interest, although some examples of processing that can constitute such an interest are present in its Recitals, for example recital 47 the GDPR provides that 'The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest'.[87] ICO guidance also provides further examples, such as business purposes.[88]

- *Necessity*

127. The ICO guidance provides[89] 'need to demonstrate that the processing is necessary for the purposes of the legitimate interests you have identified. This

---

[82] ICO General GDPR Guidance.
[83] *Rigas* EU:C:2017:336.
[84] The wider GDPR requirements require that this contemporaneous decision making/reasoning is documented.
[85] ICO Legitimate interests: detailed guidance.
[86] ICO Update Report into Adtech and RTB.
[87] The recitals give wider examples of fraud prevention, ensuring network and information security or indicating possible criminal acts or threats to public security. ICO observes anything illegitimate, unethical or unlawful is not a legitimate interest.
[88] ICO Legitimate interests: detailed guidance.
[89] ICO general GDPR guidance.

doesn't mean that it has to be absolutely essential, but it must be a targeted and proportionate way of achieving your purpose. You need to decide on the facts of each case whether the processing is proportionate and adequately targeted to meet its objectives, and whether there is any less intrusive alternative, ie can you achieve your purpose by some other reasonable means without processing the data in this way? If you could achieve your purpose in a less invasive way, then the more invasive way is not necessary.'

- *Balancing – 'interests, rights and freedoms'*

128. This 'balancing' is an objective test – the interests of the individual could override legitimate interests if personal data was to be processed in ways the individual does not reasonably expect. This is because if processing is unexpected, individuals lose control over the use of their data, and may not be in an informed position to exercise their rights.[90]

  - *Reasonable expectations*

129. The required balancing will be informed by what an objective individual would reasonably expect in the particular circumstances, which will in turn be influenced what they have been told, ie information is provided in the controllers' privacy information. If an intended purpose or method is not obvious or widely understood or is new or innovative it may not be expected. The nature of the organisations relationship with the consumer will also be relevant, the ICO explain that legitimate interests is more likely to apply where a business and consumer 'have a 'relevant and appropriate relationship', for example, because they are your client or employee. If you don't have a pre-existing relationship, it is harder to demonstrate that the processing can be reasonably expected'.[91]

130. This is an objective test, what a reasonable person would expect the processing in light of the particular circumstances. However, this may be informed by evidence about expectations, eg from market research, focus groups or other forms of consultation.

  - *Impact and safeguards*

131. Part of balancing involves considering the potential impact on individuals and any damage that the processing might cause. The ICO guidance[92] provides

---

[90] Recital 47.
[91] ICO Legitimate interests: detailed guidance.
[92] ICO Legitimate interests: detailed guidance.

factors which should be considered include whether processing might contribute to:

- a barrier to individuals exercising their rights (including but not limited to privacy rights);
- a barrier to individuals accessing services or opportunities;
- any loss of control over the further use of personal data;
- physical harm;
- financial loss, identity theft or fraud; or
- any other significant economic or social disadvantage (such as discrimination, loss of confidentiality or reputational damage).

132. The adoption of safeguards to reduce or mitigate these risks, such as collecting less data, or providing data subjects with an opt-out, will be of relevance to the balance.[93]

133. Article 24(1) GDPR explicitly emphasises that the controller is obliged to demonstrate that processing is performed pursuant to the GDPR. Art. 30 GDPR says that the controller must maintain a record of processing activities under its responsibility in order to prove compliance with the provisions set forth in the GDPR. The controller himself must therefore not only ensure that the processing complies with the GDPR, he must also be in a position to prove that he has undertaken everything necessary to achieve the objective and has taken suitable measures accordingly.

134. The ICO explains in its adtech real time bidding interim report, that in its view that the nature of the processing within the current RTB market makes it impossible to meet the legitimate interests lawful basis requirements.[94]

[93] ICO Legitimate interests: detailed guidance.
[94] 'Reliance on legitimate interests for marketing activities is possible only if organisations don't need consent under PECR and are also able to show that their use of personal data is proportionate, has a minimal privacy impact, and individuals would not be surprised or likely to object. We believe that the nature of the processing within RTB makes it impossible to meet the legitimate interests lawful basis requirements. This means that legitimate interests cannot be used for the main bid request processing.' ICO adtech and RTB interim report.

Special categories of personal data

135. Processing of 'special category' personal data is further restricted by the GDPR,[95] and is prohibited unless a condition within Article 9 applies. 'Special category data' is 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.

136. For the purpose of this study into digital advertising the only applicable legal basis likely to apply is Art.9(2)(a) the explicit consent of the data subject.[96]

137. The ICO explain in its update report into adtech and real time bidding, the concerns it has about the presence of special category data in the RTB ecosystem without evidence that explicit consent has been given for its processing. The concern being that the consent mechanisms adopted to date for compliance with PECR are not designed to collect the explicit consent required for the Article 9 processing.[97]

'Right to be informed'

138. Whilst the detail is outside the scope of this appendix, these principles are supported by the right to be informed. The GDPR, principally in Articles 13 and 14, but also throughout, sets out the information that must be given to data subjects about the processing of their personal data and their rights and

[95] Schedule 1 of the DPA also makes further provision.
[96] Albeit in the wider processing of personal data by certain platforms it is possible other basis may apply such are Art.9(e) information made manifestly public by the data subject, eg a consumer posting information about themselves on a public forum.
[97] ICO adtech and RTB interim report..

access to it. This is an area where the ICO have produced 'detailed guidance'.[98]

Right to erasure ('right to be forgotten')

139. The GDPR give data subjects a right, in most of the circumstances of relevance to this study, to have their data erased, eg if the data is no longer necessary, if consent is withdrawn, where legitimate interest is being relied upon as the legal basis or the data is being used for direct marketing . However, the 'right to be forgotten' is not absolute.[99]

Right to data portability

140. The GDPR gives data subjects an express right to 'data portability', which allows individuals to obtain and reuse their personal data processed based on their consent or a contract, for their own purposes across different services and to have that data transmitted to a new controller.[100]

141. This right applies to information an individual has provided to a data controller. This means that not all data which is processed by a data controller about a data subject may be subject to this right. The ICO observes that sometimes this distinction will be clear, other times less so. For example, information provided by the data subject includes such things as their address or the profile information they have populated, as well as data observed about their behaviour when using a device or service, eg their searches, location data, or self-generated data eg heart rate data from a wearable personal fitness device. The right does not include 'inferred data', eg a characterisation of the user inferred from that data, although the GDPR as a whole applies to this data where it is personal data. This does not prevent a data controller giving the consumer a wider class of personal data than the 'right' applies to, and indeed the ICO observes that the data subject may have other rights over such data, eg by means of the right to access.

142. This right includes that the data be provided;

- in a structured, commonly used and machine-readable format; and
- where technically feasible to have the personal data transmitted directly from one controller to another, 'without hinderance'.

---

[98] ICO general GDPR guidance.
[99] ICO general GDPR guidance provides more detail.
[100] ICO general GDPR guidance.

143. Recital 68 provides 'Data controllers should be encouraged to develop interoperable formats that enable data portability.' and this is an area covered in the ICO's general GDPR guidance, and the EDPB have adopted detailed Guidelines on the right to data portability.[101]

Right to object

144. Data subjects have a general right to object to processing carried out on the basis of the public interest or the controller or third party's legitimate interests. This is then subject to an individualised balancing exercise.[102]

145. In respect of 'direct marketing' there is an absolute right for a data subject to object at any time to the processing of their personal data marketing (including the use of a profile for the direct marketing). On receipt of such an objection the processing must stop.

146. These rights must be brought to the attention of the data subject and presented clearly and separately from any other information. This is another example of the right to be informed (in addition to the general provision in Articles 13 and 14).

147. This is also an area covered in the ICO's general GDPR guidance.

Profiling

148. Article 22 makes provision for the control of profiling, automated processing of personal data to evaluate certain things about an individual, which produces legal or similar effects. Limiting this to where there is explicit consent, it is necessary for a contract, or authorised by law.

149. This is again an area where the ICO has prepared 'detailed guidance' on automated decision-making and profiling,[103] and the EDPB have adopted guidance.[104]

Data protection by design and default

150. The GDPR imposes a general obligation on controllers to take appropriate measures to implement the data protection principles in an effective manner, integrate necessary safeguards into the processing and ensure that, by

---

[101] Guidelines on the right to data portability, WP 242 rev.01, as last Revised and adopted on 5 April 2017.
[102] ICO general GDPR guidance.
[103] ICO general GDPR guidance.
[104] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)

default, only the personal data necessary for each purpose are processed – this is data protection by design and by default.

151. Whilst 'privacy by design' has always been important as part of data protection, the GDPR makes this a legal requirement on data controllers. In practice this means incorporating appropriate technical and organisational measures to implement the data protection principles and integrating safeguards into processing to meet the GDPR's requirements and protect the individual rights. This ICO explain this is likely to include strong privacy defaults, user-friendly options and controls, and respecting user preferences.

152. The ICO covers these principles in its general GDPR guidance[105] and intends to publish further detailed guidance in due course. This subject is also addressed in the ICO's final Age Appropriate Design Code.[106] The EDPB have also consulted on Data protection by Design and by Default guidance.[107]

Codes of Conduct, monitoring, certification and certification bodies

153. The GDPR provides a framework for the adoption and approval of codes of conduct, and the establishment and monitoring of certification bodies.

154. Given the relatively recent introduction of the GDPR this infrastructure is not yet fully developed,[108] but as it is deployed it will be a potentially important mechanism for consumers to be able to make choices about which sort of organisations to share their personal data with, and for organisations which adhere to the highest standards of data protection to ensure consumers see that via adherence to a code or by display of a quality mark.

The Data Protection Act 2018 (DPA 2018)

155. The DPA 2018 makes UK specific GDPR provision and makes provision for certain ICO functions.[109]

156. Of relevance to the study, section 9 makes provision to allow a child, who is at least 13, to consent to the processing of their personal data for an 'information

---

[105] ICO general GDPR guidance.
[106] Published in January 2020. The code was introduced by the Data Protection Act 2018, and there is a process before the Code is laid in Parliament for approval, following which there is a transition period before it comes into force. The ICO expects it to be in force by Autumn 2021.
[107] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Consultation closed January 2020.
[108] Whilst at this time, there are no approved certification criteria or accredited certification bodies for issuing GDPR certificates, the ICO has now finalised its submission process for applicants, and in December 2019 its accreditation requirements for code monitoring bodes were approved by the EDPB (Opinion 17/2019). The ICO has also published extensive guidance including on guidance on codes of conduct, on accreditation requirements for GDPR code of conduct monitoring bodies, and on certification.
[109] As well as other matters outside the scope of this study, eg law enforcement processing.

society service', rather than 16 as provided for in the GDPR. The ICO has recently submitted its 'Age Appropriate Design Code of Practice' to the Government which the DPA 2018 required to be produced.[110]

The Privacy and Electronic Communications Regulations 2003 (PECR)

157. PECR transpose the 'ePrivacy Directive' (Directive 2002/58/EC as amended by Directive 2009/136/EC).

158. Due to the prevalence of 'cookies' and similar technologies in the digital advertising market,[111] the main relevance of PECR to this study is the requirement that the placing of non-essential[112] 'cookies' require user consent, which must be given to the GDPR standard.

159. The basic rules on non-essential cookies are provided for in regulation 6 of PECR, and require a 'clear and comprehensive' explanation which:

- tells users the cookies are there;
- explain what the cookies are doing and why; and
- get the user's consent to store a cookie on their device.

160. As 'consent' has the same meaning as the GDPR regime, to be valid, consent must be freely given, specific and informed. It must involve some form of unambiguous positive action.[113] As such, providing information about cookies as part of a privacy policy that is hard to find, difficult to understand, or rarely read, or relying on users continuing to use the website is not sufficient to meet these requirements. To ensure that consent is freely given, users should have the means to enable or disable non-essential cookies, and this should be done in such a way that consent is as easy to withdraw as it is to give.[114]

161. In addition to its general guidance on PECR, the ICO has produced 'detailed guidance' on both 'cookies' and 'consent'.

---

[110] The Age Appropriate Design Code of Practice was laid in Parliament on 11 June 2020.
[111] The ICO explain that PECR applies to 'similar technologies' which access information on a consumers device, eg 'device finger printing' techniques.
[112] Reg.6(2) requiring consent does not apply to essential cookies, that is cookies '*6(4)(a)for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (b)where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.*' The ICO explain the definition 'essential' is narrowly bound, eg adding a session cookie product to facilitate the use of a shopping 'basket', or for security purposes, eg logging into an internet banking session.
[113] As affirmed by the CJEU in *Planet49.*
[114] ICO guidance on the use of cookies and similar technologies.

162. The process of getting user consent to the placing of cookies can be disruptive to consumers online experience, and an update to the 2002 'ePrivacy Directive', an ePrivacy Regulation is being considered.[115] As originally drafted, this included enhanced mechanisms for consumers to express their consent 'using the appropriate technical settings of a software application enabling access to the internet' ie at browser, app, system or device level.

Wider general law and common law (criminal and civil)

163. Whilst the detail is necessarily outside the scope of this appendix to the interim report, the perception sometimes encountered that online services are not subject to the general law is misplaced, and the wider general law applies to digital platforms and digital advertising, including:

- Contract law – eg handling the arrangements between parties;
- Tort law – eg misrepresentation as to conduct;
- Criminal (fraud) – eg in relation to alleged 'ad fraud';
- Intellectual property and copyright – eg in relation to provision of consumer services.

Non-legislative framework(s)

164. The development of the internet and internet enabled businesses has been enabled by effective non-legislative standard setting, as has been the case in the wider information technology space. It is beyond the scope of this appendix to the interim report to cover this in detail.

Tech standards and standard setting bodies

165. The **Internet Society** (ISOC), is a supervisory organisation comprising individuals, corporations, non-profit organisations and government agencies from the internet community. It provides the administrative home for:

- **Internet Engineering Task Force** (IETF), is a loosely self-organised group, who contribute to the engineering and evolution of Internet technologies, via producing high quality, relevant technical and

[115] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final – 2017/03 (COD).

engineering documents, like include protocol standards and best current practices documents, that influence the way people design, use, and manage the Internet.[116] It aims to support the evolution of the internet and maintaining the smooth running of the internet as a whole, via developing and maintaining the Request For Comment (RFC) documents that define the open standards by which the internet is managed. These open standards are developed via rough consensus.

- **Internet Architecture Board** (IAB), responsible for defining the overall architecture of the internet, and providing advice, guidance and broad direction to the IETF. It also provides oversight of the:
    - **Internet Corporation for Assigned Names and Numbers** (ICANN), primarily responsible for assigning domain names and considering the introduction of new generic top level domains
    - **Internet Assigned Numbers Authority** (IANA), operated by ICANN and is primarily responsible for assigning IP addresses.

166. The **World Wide Web Consortium** (W3C)[117] develop Web standards via its international community of Member organizations, a full-time staff, and the public. W3C's primary activity is to develop protocols and guidelines that aim to ensure long-term growth for the Web. The W3C adopts a process[118] to get to a 'W3C Recommendation' or 'standard', via workshop, activity proposal, working group, by which specifications and guidelines are reviewed and revised.

167. There are also a wider range of more formal standard setting organisations which adopt relevant standards such as the International Telecommunication Union (ITU), International Electrotechnical Commission (IEC), IEEE (institute of electrical and electronics engineers).

Digital Advertising

168. There are a wide variety of digital advertising industry initiatives in the UK, Europe and worldwide, including the Institute of Practitioners in Advertising (IPA), Incorporated Society of British Advertisers (ISBA), the UK Association of Online Publishers (AOP) and the UK Internet Advertising Bureau (IAB UK), which is part of IAB Europe. Joint initiatives include the Joint Industry Committee for Web Standards (JICWEBS), aiming to achieve comparable

[116] RFC 3935, 4677 etc.
[117] http://www.w3.org.
[118] W3C Process.

standards, eg for advertising measurement and measures to address ad-fraud.

169. Other examples or industry initiatives we have been told about include:

AdChoices

170. In April 2011, the IAB Europe and its members[119] adopted the IAB Europe EU Framework for Online Behavioural Advertising ('the Framework') which set out good practice principles for all EU and EEA markets to enhance transparency and user control for targeted advertising which are binding upon the companies and associations who subscribe to it. The aim of the Framework is to increase transparency and choice for web users within the EU. The principles are:

i. **Notice** – transparency about data collection and use practices associated with targeted advertising, providing consumers with clear, prominent and contextual notice in or around advertisements, linked to further information and control mechanisms.

ii. **User choice** – greater consumer control over targeted advertising.

iii. **Data security** – appropriate data security and retention of data collected and used for targeted advertising purposes.

iv. **Sensitive segmentation** – limitations on the creation of 'interest segments' to specifically target children and on the collection of sensitive personal data collected and used for targeted advertising.

v. **Education** – for consumers and businesses about targeted advertising.

vi. **Compliance and enforcement** – mechanisms to ensure the effectiveness of the self-regulatory programme run under the Framework (see below).

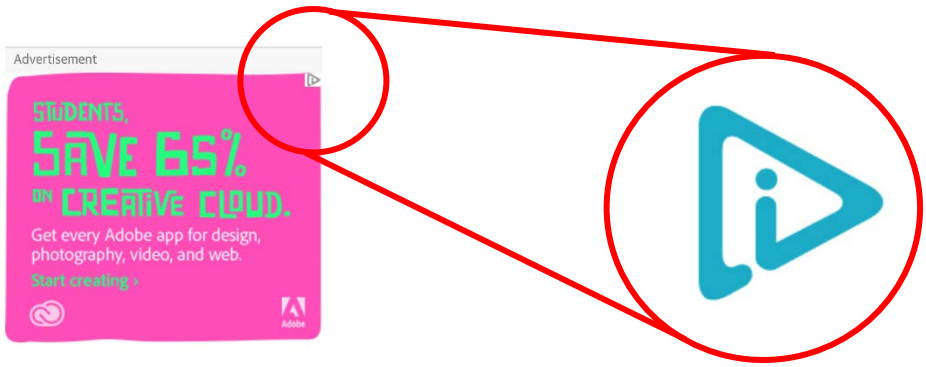
vii. **Review** – regular review (at least every three years) of the Framework in order to ensure that it evolves in line with developing technology and business practices.

Self-regulatory programme

[119] The IAB Europe's members include Google, Microsoft and IAB UK.

171. The European Advertising Standards Alliance (EASA)[120] developed its Best Practice Recommendation on Online Behavioural Advertising ('the BPR'), based on the Framework, which set out a harmonised, pan-European self-regulatory programme for online behavioural advertising. A second edition of the BPR was published in October 2016, to reflect the extension of the Framework to the mobile environment.[121]

172. The self-regulatory initiative is based upon the Framework and the BPR.[122] [123] The aim of the programme is to inform consumers clearly about businesses' data collection and use through enhanced notice, provided via the 'AdChoices' icon (illustrated below). Any company involved in targeted advertising, including first and third parties, may apply to start using the 'AdChoices' icon, which is then displayed by the company in its advertising.



173. When a user clicks on the 'AdChoices' icon, which is usually found in the top right corner of an online advertisement, they can learn more about the ad or a website's data collection practices, and be provided with the ability to opt-out of such targeting. For example, clicking on the 'AdChoices' icon in the corner of an advert placed by Oath brings up the following information and options:

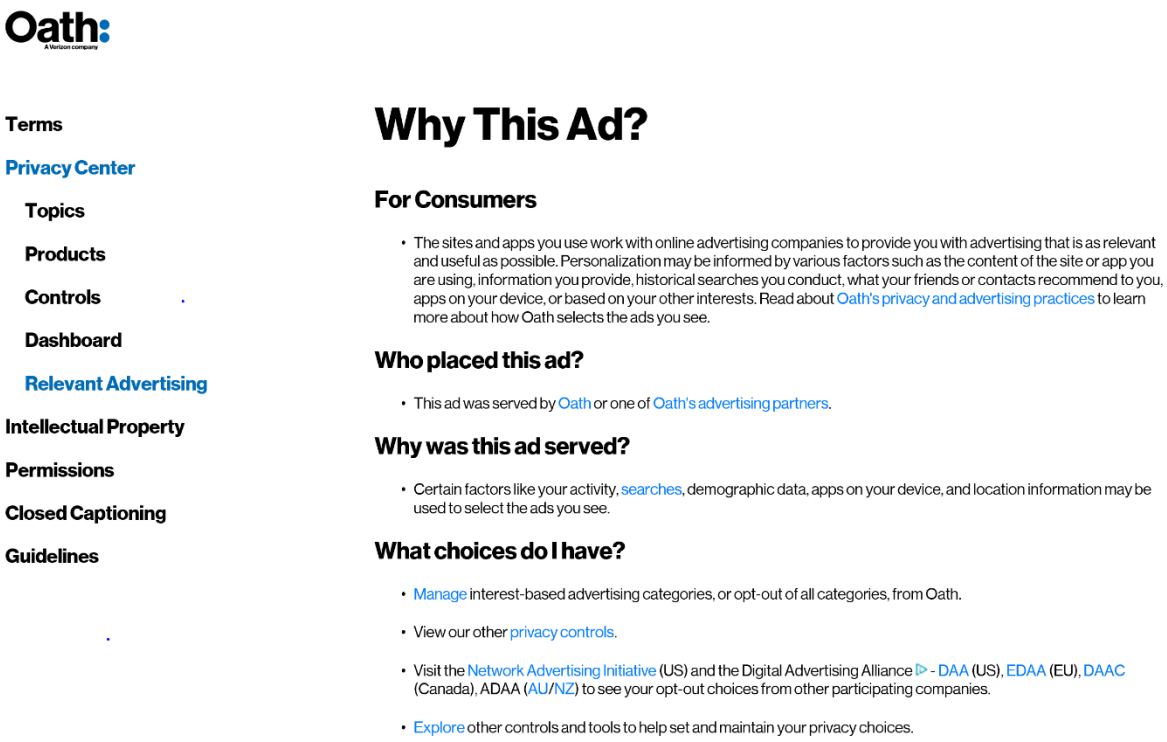
---

[120] The European Advertising Standards Alliance is a non-profit organisation based in Brussels, which brings together European national advertising self-regulatory organisations and other organisations representing the advertising industry (such as IAB Europe) to consider issues relating to advertising self-regulation

[121] The revised edition recognised that mobile devices had developed into 'essential marketing tools', and that this had created a global mobile advertising ecosystem which raised issues distinct to mobile devices, such as differences in expectations from a usability point of view due to smaller screen sizes and touchscreen functionality, and the fact that mobiles are the most personal devices owned by users and are normally always on. It set out, as an addendum to the Framework, a series of recommendations aimed at stakeholders operating in the mobile advertising ecosystem who may have been outside the scope of the Framework, such as app creators.

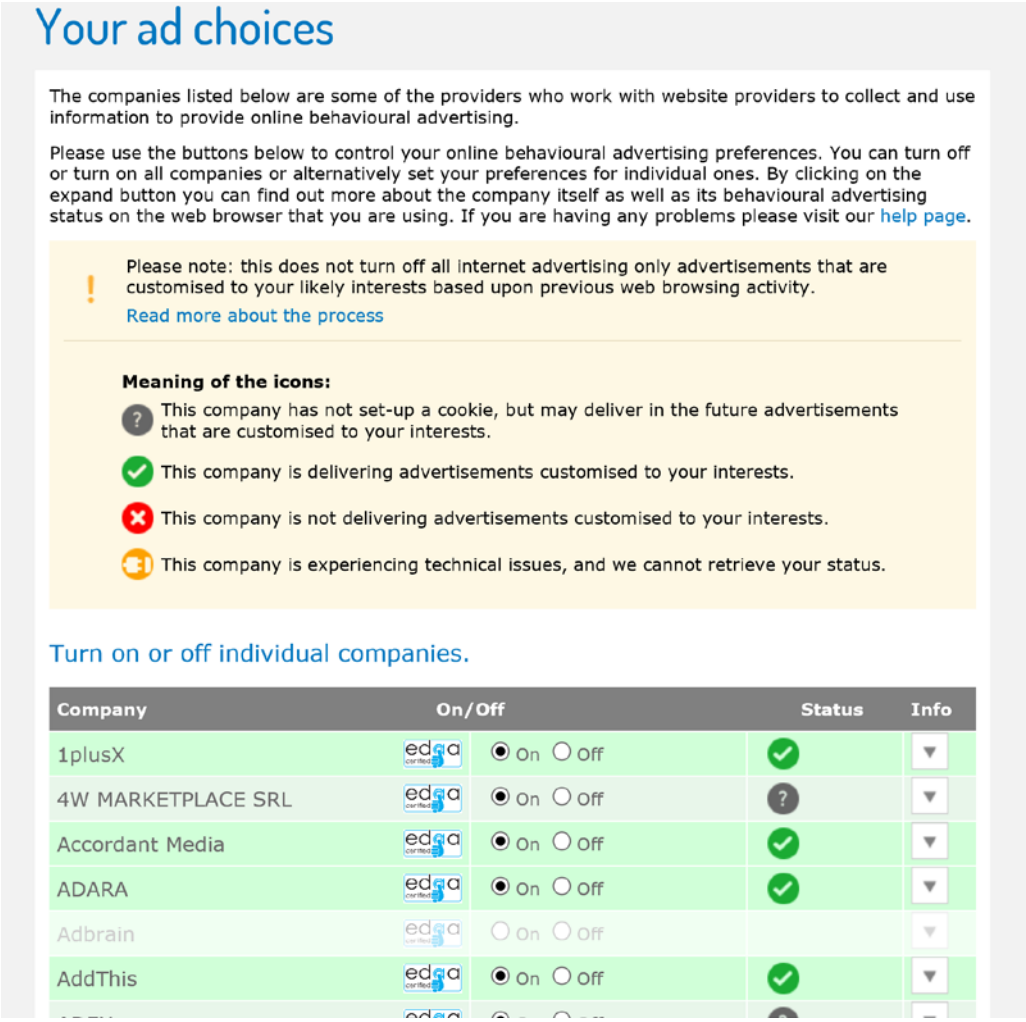
[122] Together, these constitute the Principles of the European Self-Regulatory Programme for Online Behavioural Advertising(the 'European Principles') referred to in the European Interactive Digital Advertising Alliance (EDAA)'s licence and certification processes.

[123] Compliance with the European Principles does not infer legal compliance (including with GDPR) for which businesses themselves are responsible.



174. The programme is managed by the European Interactive Digital Advertising Alliance (EDAA) which principally acts as the central licensing body for the 'AdChoices' icon,[124] as well as providing the means for consumers to exercise transparency and control over targeted advertising through an online 'Consumer Choice Platform'.[125] The platform brings together all of the businesses participating in the programme so that consumers can readily control the targeted advertising that they see: consumers are presented with a list of participating businesses and are able to set their preferences with regard to each of those businesses, as shown below:[126]

[124] Companies participating in the programme may use the AdChoices Icon with approved accompanying text for each European market, as set out in Annex A to the EDAA's technical specifications.
[125] www.youronlinechoices.com/uk
[126] Consumers can also continue to manage their privacy settings within their web browser.



175. Depending upon their business model, businesses involved in targeted advertising that wish to participate in the programme can do so in different ways: for example, those using consumer data to deliver or display adverts on websites that they do not own or control can apply to use the icon, while those that collect consumer data for targeted advertising purposes from websites that they do not own or control can apply to integrate with the Consumer Choice Platform.

176. The EDAA has created a comprehensive set of self-certification criteria, which align with the 'European Principles' set out in the Framework and BPR, for businesses participating in the programme.[127] These are set out below.

i. **Data security** – Businesses are required to maintain appropriate physical, electronic and administrative safeguards to protect the data collected and used for targeted advertising purposes. Data should be retained 'only for as long as necessary to fulfil a legitimate business need, or as required by law'; the criteria suggest that businesses might set a

[127] The criteria also include some 'best practice' recommendations for advertisers, agencies and publishers.

reasonable validity interval on any data collected for targeted advertising purposes and delete the data when the interval has been exceeded.[128]

ii. **Segmentation** – Businesses should not create segments for targeted advertising that are specifically designed to target children under 12 years of age or deliver adverts specifically targeted to age 12 or under.[129] Where businesses seek to create segments for targeted advertising purposes which rely on the use of sensitive personal data,[130] they are required to obtain consumers' explicit consent (see 'Explicit consent', below).

iii. **Education** – Businesses engaging in targeted advertising should provide information for consumers about targeted advertising, including 'easily accessible information' about how data is obtained and used, and how web user choice may be exercised'. The criteria suggest that this might also cover what targeted advertising means and how it works, and how data for targeted advertising purposes is collected, stored, processed and used, in language 'easily understood by the average Internet user'. [131]

iv. **Compliance and enforcement** – Businesses should ensure that, regardless of the various ways in which consumers might submit complaints, they have proper processes in place to resolve issues in a timely manner. [132]

v. **Criteria relating to third parties** – A business is defined as a third party to the extent that it engages in targeted advertising on a website other than a website that it owns or operates.[133] Third parties are required to give 'clear and comprehensible' notice of their collection and use of data for targeted advertising purposes on their own website; this should include a means for consumers to exercise choice over the collection and use of their data and over the transfer of that data to third parties for the purposes of targeted advertising (such as the Consumer Choice Platform). Third Parties are also required to provide enhanced notice of the collection and use of data for targeted advertising by means of the 'AdChoices' icon in or around their adverts, as outlined above. Third Parties are required to ensure that users are able to exercise their choices with respect to the collection and use of data for the purposes of targeted

---

[128] Self-Certification Criteria for companies participating in the European Self-Regulatory Programme on OBA, published 16 November 2012 by EDAA, paras 2.1.1, 2.1.2
[129] As above, paras 2.2.1 and 2.2.2
[130] Defined by Art 8.1 of Directive 95/46/EC as relating to racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, health and sex-life
[131] Self-Certification Criteria for companies participating in the European Self-Regulatory Programme on OBA, published 16 November 2012 by EDAA, para 2.3
[132] As above, para 2.4
[133] As above, paras 2.5, 2.6, 2.7

advertising (including the transfer of such data to Third Parties) and the criteria specify that the practice of using technologies to circumvent users' express choices should not be used (eg 're-spawning' deleted cookies). Third Parties be licensed by the EDAA to display the enhanced notice and must adhere to the EDAA's technical specifications.

vi. **Explicit consent** – businesses are required to obtain explicit consent[134] before collecting and using data via specific technologies or practices that are intended to harvest data from all or substantially all URLs traversed by a particular computer or device across multiple web domains and using such data for targeted advertising. As outlined above, explicit consent is also required under the criteria by any business seeking to create or use targeted advertising segments relying on use of sensitive personal data. In practical terms, the user must be informed that their browsing activity will be collected and stored; the consent must be specifically for the collection and use of data for targeted advertising purposes (with targeted advertising being specifically mentioned); it must also be freely-given, not be induced in any way (such as by suggesting that certain functionalities will not be available, or that their online experience might be impaired, by not consenting); users must also be informed that their explicit consent can be withdrawn at any time and provided with a straightforward mechanism for doing so. Once the explicit consent has been withdrawn, the collection and use of data for targeted advertising must obviously cease.

177. Within six months of either signing up to the Framework or entering into a licence agreement with EDAA, businesses must self-certify that they comply with the criteria by means of an online form available on the EDAA's website. Third Parties and companies that collect and use browsing data for the purposes of targeted advertising are required to submit to independent audits of their self-certification. Companies that are found to be fully compliant with the self-regulatory programme are granted a 'Trust Seal'.

[134] Explicit consent is defined by the Framework as 'an individual's freely-given specific and informed explicit action in response to a clear and comprehensible notice regarding the collection and use of data for [targeted advertising] purposes'.