Online Targeting of Advertising and Prices – a market study

Annexe C - Regulatory Framework

May 2010

OFT1231c
## CONTENTS

*Chapter/Annexe* \hspace{1cm} *Page*

- Part 1 Data protection and privacy ................................................................. 4
- Part 2 Consumer Protection Legislation.......................................................... 15
PART 1 DATA PROTECTION AND PRIVACY

1.1 Part 1 provides a summary of existing regulatory protections in the UK and EU relating to privacy and data protection for consumers. It is not intended to act as a substitute for the substantive guidance provided by the Information Commissioner’s Office or the legislation itself.¹

1.2 Traders involved in the provision of online targeted advertising and customised pricing will be subject to requirements under the Data Protection Act 1998 (DPA) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (Privacy Regulations). Amongst other things, the function of the Information Commissioner’s Office (ICO) is to ensure compliance with these requirements and promote best practice concerning the collection, use and retention of personal information.² These requirements are set out in brief below.

DPA

Overview

1.3 The DPA implements the Data Protection Directive.³ The DPA’s purpose, reflecting that of the Directive, is to make provision for the regulation of the processing⁴ by data controllers⁵ of personal information relating to individuals,⁶ including the obtaining, holding,
use or disclosure of such information. It further provides that such data should not be kept in a form which permits identification of data subjects for longer than is necessary for the purpose for which the data was collected.

Personal data

1.4 'Personal data' is defined broadly. 'Data' can include information that is recorded or processed automatically by means of equipment in response to instructions given for that purpose. 'Personal data' is defined as information relating to an individual who can be identified from that data or from that data and other information which is in the possession of, or likely to come into the possession of, the data controller.

1.5 The Commissioner recognises that an individual may be identified without necessarily knowing the name and address of that particular individual. It would be sufficient if the data are capable of being processed by the data controller to enable them to distinguish the data subject from any other individual. This does not necessarily require that the data controller is in possession of traditional identifiers such as the name or address of an individual. It would also be sufficient for an individual to be identified from data together with information 'likely to come into possession' of the data controller.

1.6 The wide definition of personal information means that information about a particular web user which has been built up over a period of time, perhaps through the use of tracking technology, with the intention that it may later be linked to a name and address, is personal data. Similarly, information gathered with an intention to target a particular user with advertising or discounts when they revisit a particular site on the basis of the profile built up would still be regarded by the Commissioner as 'personal data'. That is, even

---

7 Personal information or data is defined in s.(1) of the DPA. See also ICO’s DPA Legal Guidance (DPA Legal Guidance) at paragraph 2.2.3 on the meaning of identification
8 Principle 5 of the fair processing requirements (Schedule 1, Part II, paragraphs 1 to 4 DPA)
9 s.1(1) DPA
10 S.1(1) DPA
11 See DPA Legal Guidance at 2.2.3.
12 DPA Legal Guidance at paragraph 2.2.3
where there is no such intention by the trader(s) of locating an individual within the physical world or to link them with a name and address or e-mail address.\textsuperscript{13} In its Personal Information Online Code of Practice Consultation Document (draft PIO Code) the Information Commissioner has proposed that data (personal or not) that is processed for profiling purposes should be treated as if it were personal data.\textsuperscript{14}

Data controller

1.7 Data controllers must ensure that any processing of personal data for which they are responsible complies with the DPA. A data controller is defined as a (legal) person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed\textsuperscript{15}.

1.8 The Commissioner recognises that possession does not necessarily mean that the identifying data are in the physical control of the data controller or likely to come into his control.\textsuperscript{16} Further, the Commissioner’s view is that the determination of the purposes for which, and the manner in which, any personal data are, or are to be, processed does not need to be exclusive to one data controller. Determination may be shared with others jointly (where the determination is exercised by acting together equally) or in common (where the data controllers share a pool of personal data, each processing independently of the other).\textsuperscript{17}

1.9 The draft PIO Code recognises that a website publisher will often use a third party to carry out profiling and targeting for electronic marketing and advertising on its behalf.\textsuperscript{18} The Code notes that there

\textsuperscript{13} DPA Legal Guidance at paragraph 2.2.3
\textsuperscript{15} s.1(1) DPA.
\textsuperscript{16} For example, a data controller would be deemed to be in possession of personal data where it enters into a contract with a data processor for the processing of personal data but determines the purposes for which and the manner in which the personal data are to be processed by the data processor; that is even though it may not have sight of all or any of the information which identifies a living individual (DPA Legal Guidance at paragraph 2.2.4).

\textsuperscript{17} DPA Legal Guidance at paragraph 2.5
\textsuperscript{18} Draft PIO Code at page 10
may be confusion amongst the organisations involved about the respective responsibilities of website publishers, content providers, advertisers, advertising agencies, advertisement networks and technology companies. Where responsibilities overlap, it is good practice for all the organisations involved to work together to establish their respective responsibilities. In particular, they should determine who is the data controller, or controllers, in respect of any personal data being processed. Data controllers should, in turn, ensure that any third party contractors they use are aware of their contractual obligations in respect of the personal data they have been asked to process. Further, that it is good practice for the company with primary responsibility for the website to act as a single point of contact for the content displayed on its site, even if it is not legally responsible for third party content.19

Jurisdiction

1.10 The DPA applies to a data controller in respect of any data only if they are established in the UK and the data is processed in the context of that establishment.20 The DPA also applies where the data controller is established neither in the UK nor in any other EEA State but where it uses equipment in the UK for processing the data otherwise than for the purposes of transit through the UK.21 For the purposes of 'established' this comprises any individual ordinarily resident in the UK, a UK registered company, partnership or other unincorporated association and a person who maintains an office, branch or agency in the UK.

1.11 The DPA requires notification of every data controller that processes personal information,22 The ICO publishes certain details in the register of data controllers, which is available to the public for inspection.23

---

19 Draft PIO Code at page 17
20 s.5(1)(a) DPA
21 s.5(1)(b) DPA
22 s.18(1) DPA
23 s.19(1) DPA
Data protection principles

1.12 The DPA creates a duty on all data controllers to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.\(^\text{24}\) There are eight data protection principles. These are set out in Part I of Schedule 1 DPA. The DPA makes provision for the principles to be interpreted in accordance with Part II of Schedule 1 DPA.

Processed fairly and lawfully

1.13 The first data protection principle requires that personal data should be processed fairly and lawfully and should not be processed unless at least one of the conditions in Schedule 2 is met and, in the case of sensitive personal information, at least one of the conditions in Schedule 3 is also met.\(^\text{25}\) As noted by the Commissioner, meeting a Schedule 2 and Schedule 3 condition will not, on its own, guarantee that processing is fair and lawful.\(^\text{26}\) The general requirement that data be processed fairly and lawfully must be satisfied in addition to meeting the conditions.

1.14 For the purposes of the first data protection principle, personal data are not to be treated as processed fairly unless the data controller ensures so far as practicable that the data subject has, is provided with or has made readily available to him the identity of the data controller (or a nominated representative if that is the case), the purpose for which the data are to be processed, and any further information necessary to enable the processing to be fair.\(^\text{27}\)

1.15 In the context of personal information collected on websites, the Commissioner states\(^\text{28}\) that in order to meet this requirement, website operators who collect personal information directly from

---

\(^{24}\) s.4(4) DPA

\(^{25}\) The DPA defines categories of ‘sensitive personal information’ as consisting of that information relating to the racial or ethnic origin of the data subject, his political opinions, religious beliefs, membership of a trade union, physical or mental health or condition, sexual life, commission or alleged commission of any offence or any proceedings for any offence committed.

\(^{26}\) DPA Legal Guidance at paragraph 3.1

\(^{27}\) DPA Schedule 1 Part II 2 (1) –(3).

\(^{28}\) Data Protection Good Practice Note - Collecting personal information using websites 05.06.07 (DPA Good Practice Note) at page 1
individuals must always make sure that those individuals are aware of:

- The identity of the person or organisation responsible for operating the website and of anyone else who collects personal information through the site. So, for example, third parties operating a secure payment mechanism or placing banner ads which collect personal data on the site may also need to be identified to users of a website.

- What the data controller will process the information for.

- Any other information needed to make sure the processing is fair to individuals, taking account of the specific circumstances of the processing. This will include telling individuals if the data controller will disclose any information about them to third parties, including to other companies within the group.

1.16 Unless the intended use of the personal information is obvious, website operators must give this information to consumers before they collect any personal information from them. This should also take into account the fact that visitors may not arrive at a site via the home page and so should ensure that all pages capable of being visited indirectly reproduce this information. This information is often included as part of a privacy notice or statement.29

1.17 Where personal information is collected from a website, the ICO Good Practice Note states that it is not enough to simply say, 'click here to see our privacy statement'. A basic description of the intended use of an individual’s personal information wherever personal information is collected should be provided; that is even where more detailed information is provided elsewhere. The Commissioner recommends a layered notice as the best means of making individuals aware of how they will use their information.30 This can consist of three linked notices of increasing concision, such notices being clear, easy to read and understand.

29 DPA Good Practice Note at page 1.
30 DPA Good Practice Note at page 2. For privacy notices generally, see the ICOs’ Privacy Notices code of practice at www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf
Consent

1.18 As outlined above, the DPA requires that, in addition to the requirement that personal data shall be processed fairly and lawfully, at least one of the conditions in Schedule 2 must be met. The first condition in Schedule 2 is that the data subject has given consent to the processing. This is not defined in the DPA. However, the Directive\(^\text{31}\) refers to the data subject’s consent in terms of 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.' Further, Recital 17 of the Directive clarifies that consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting a website.

1.19 The Commissioner’s view is that consent is not easy to achieve and that data controllers should first consider other conditions in Schedule 2;\(^\text{32}\) that the existence or validity of consent will need to be assessed in light of the facts of the case; and that a reading of the Directive suggests that 'signify' means that there must be some active communication between the parties. The Commissioner’s view is that, whilst this may be inferred from a means other than in writing, data controllers cannot infer consent from non-response to a communication.\(^\text{33}\)

Other principles

1.20 All the data protection principles apply to the processing of personal data. These include the second principle that states that personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. The third principle provides that personal data shall be adequate, relevant and not excessive in relation to the purpose of purposes for which they

31 Article 2(h)

32 And Schedule 3 if processing sensitive personal data.

33 DPA Legal Guidance at 3.1.5.
are processed. The fourth and fifth principles provide that personal data shall be accurate, and where necessary, kept up to date. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.

**Privacy Regulations**

1.21 The Privacy Regulations implement certain articles of the Directive on privacy and electronic communications.34

Existing requirement

1.22 Regulation 6 of the Privacy Regulations concerns the confidentiality of information.35 This provides that subject to an exemption set out in Regulation 6(4), a person shall not use an electronic communications network to store information, or to gain information stored, in the terminal equipment of a subscriber or user unless certain requirements are met.36 These requirements are that the subscriber or user of that terminal equipment is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information and that they are given the opportunity to refuse the storage of or access to that information.37

---

34 Articles 2, 4, 5(3), 6 to 13, 15 and 16 of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. Note Regulation 4 makes clear that nothing in the Privacy Regulations shall relieve a person of his obligations under the DPA in relation to the processing of personal data.

35 This reflects the wording of Article 5(3) of the Directive which provides: 'Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or use concerned is provided with clear and comprehensive information in accordance with Directive 94/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.'

36 Regulation 6(1) of the Privacy Regulations

37 Regulation 6(2) of the Privacy Regulations
1.23 In its Privacy Regulations Guidance, the Commissioner notes that the Privacy Regulations are not prescriptive about the sort of information that should be provided, but the text should be sufficiently full and intelligible to allow individuals to clearly understand the potential consequences of allowing storage and access to the information collected by the device should they wish to do so.

1.24 Further, on the issue of interpretation of the requirement that the user or subscriber be ‘given the opportunity to refuse’ the use of technologies, such as cookies, the Commissioner has stated that they should be given a clear choice as to whether or not they wish to allow a service provider to **continue** to store information on the terminal in question. The Commissioner regards the provision of an ‘opportunity to refuse’ as creating a greater obligation on a person than simply making refusal a possibility. This means that where relevant information is included in a privacy policy, for example, the policy should be clearly signposted at least on the pages where a user may enter a website. Such relevant information should be presented in the policy in a suitable, prominent and accessible way that is worded to enable all users and subscribers to easily understand and act upon it.

1.25 The Privacy Regulations are also not prescriptive about the mechanism by which a user or subscriber should be able to refuse the use of a cookie type device. The Commissioner suggests that service providers can choose to make their own switch-off facilities available. The Commissioner notes that there is nothing to prevent service providers from requiring users to ‘opt in’ to receiving the cookie rather than providing them with the opportunity to ‘opt out’.

1.26 The Commissioner further recognises that tracking technologies may be utilised on websites by a third party, such as for the delivery of advertising. However, the organisation the site primarily

---

38 ICO Guidance on the Privacy and Electronic Communications (EC Directive) Regulations Part 2: Security, confidentiality, traffic and location data (Privacy Regulations Guidance at page 5)
39 Privacy Regulations Guidance at page 5
40 Privacy Regulations Guidance at page 5
41 Privacy Regulations Guidance at page 6.
refers to will be obliged to alert users to the fact that a third party advertiser operates cookies and will not be able to avoid responsibility with the use of caveats. The third party would also have a responsibility to provide the user with the information required to be given under Regulation 6.42

Amendments to legislation

1.27 In October and November 2009, the European Parliament and Council of the EU adopted a directive amending legislation in force on universal service ePrivacy and consumer protection.43

1.28 Recital 66 and Article 5(3) is relevant to cookies. Recital 66 of the amended Directive recognizes that information may be stored on a user’s computer for a number of purposes, ranging from legitimate (certain types of cookies) to unwarranted intrusion (spyware). It states that it is therefore important that users are clearly and comprehensively informed when engaging in activities which may lead to such information being stored.44

1.29 The key amendment to the substantive Directive was to Article 5(3). This added text to the effect that the storing of information on a subscriber or user’s computer [such as a cookie] and any subsequent access to this is only allowed on the condition that the subscriber or user concerned has given their consent having been provided with clear and comprehensive information about the purposes of the processing.

1.30 Recital 66 sets out that the methods of providing information and offering the right to refuse should be as user-friendly as possible. In particular, it states that ‘where it is technically possible and effective, in accordance with the relevant provisions of Directive

---

42 Privacy Regulations Guidance at page 6.
A copy of the Press Release may be found at the following link: www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/.../110776.pdf
44 The exception to the obligation to provide information and offer the right to refuse is limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user
95/46/EC, the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application. 45

1.31 The Information Commissioner’s Code of Practice on Personal Information Online recommends as good practice offering individuals a simple means of disabling the process by which a record of their online behaviour may be created. Also to provide individuals with advice about how to use their browser settings or choices on the website to preserve their online anonymity as far as possible or to ensure information identifying them is erased at the end of a session.46

---

45 In its Opinion on the amendments to the Directive (Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications adopted on 10 February 2009), the Article 29 Data Protection Working Party strongly objected to the proposal that default browser settings would be a means to provide prior consent. Amongst other things, the Working Party expressed concern about what it regarded as the erosion of the definition of consent and a subsequent lack of transparency. In particular it stated: ’Most browsers use default settings that do not allow the users to be informed about any tentative storage or access to their terminal equipment. Therefore, default browser settings should be ’privacy friendly’ but cannot be a means to collect free, specific and informed consent of the users, as required in Article 2(h) of the Data Protection Directive’…’With regard to cookies, the Working Party is of the opinion that the controller of the cookies should inform its users in its privacy statement and may not rely on (default) browser settings. Also the chosen wording is not limited to the current issue of cookies, but implies any other new technology that could be used to track the users’ behaviour using their browser’

46 Draft PIO Code at page 11
Part 2 Consumer Protection Legislation

Consumer Protection from Unfair Trading Regulations 2008 (CPRs)

Introduction

2.1 The analysis set out below explains the OFT’s view that the CPRs may apply to targeted advertising and personalised pricing. However, the final decision on whether a breach of the CPRs has taken place rests with the courts.

Overview

2.2 The CPRs came into force on 26 May 2008, and implemented the Unfair Commercial Practices Directive47 (UCPD) into UK law. Essentially the CPRs apply to unfair business practices that may affect consumers.

2.3 The CPRs sit alongside the other protections for consumers. In particular, the existing system of contract law, including the law on unfair contract terms, remains unchanged by the CPRs. Broadly speaking, traders that treat consumers fairly are likely to be complying with the CPRs and do not have to make major changes to their practices. However, if a trader misleads, behaves aggressively, or otherwise acts unfairly towards consumers, then the trader is likely to be in breach of the CPRs and may face action by enforcement authorities.

2.4 The CPRs prohibit traders from engaging in unfair commercial practices which have or are likely to have an effect on the behaviour of the average consumer. They achieve this by creating a prohibition for failing to comply with the requirements of professional diligence (the general prohibition)48 and/or for engaging in practices which are misleading49 or aggressive.50 The CPRs also

---

47 Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market
48 Regulation 3
49 Such as the provision of false or misleading information (Regulation 5) or the omission of certain material information (Regulation 6).
50 Regulation 7.
create an outright ban on a list of 31 commercial practices which are prohibited in all circumstances (set out in Schedule 1).51

2.5 Breach of some of the provisions can also be an offence under Part 3 of the CPRs52. Breaches of the CPRs may also be enforced civilly under the Enterprise Act 2002 as Community Infringements. Every enforcement authority including the OFT and local trading standards authorities are under a duty under Part 4 of the CPRs to enforce these. Part 4 also confers certain powers on these bodies to investigate whether there has been a breach of the CPRs.

Key definitions

2.6 The CPRs is a comparatively new though not entirely untested legislation. The CPRs are principles-based and have broad scope.

Commercial practices

2.7 The CPRs apply to 'commercial practices'. This is defined widely to mean any act, omission, course of conduct, representation or commercial communication (including advertising and marketing) by a trader, which is directly connected with the promotion, sale or supply of a product to or from consumers, whether occurring before, during or after a commercial transaction (if any) in relation to a product.53

2.8 In the context of an online environment, the OFT is of the view that commercial practices may include behavioural (targeted) advertising, both first and third party as well as retargeting, personalised pricing, and explanations provided by traders to consumers relating to these practices.54

51 Because of their inherently unfair nature, evidence of their effect, or likely effect, on the average consumer is not required to establish a breach. They are not reproduced here.
52 Further information on the offences and defences is set out in OFT Guidance 1008 paragraphs 12.1-12.15
53 Regulation 2(1) of the CPRs
54 The adequacy of such an explanation is considered below in the sections on misleading and insufficient
Transactional decision

2.9 A ‘transactional decision’ means any decision taken by a consumer, whether it is to act or to refrain from acting, concerning – (a) whether, how and on what terms to purchase, make payment in whole or in part for, retain or dispose of a product; (b) whether how and on what terms to exercise a contractual right in relation to a product.

2.10 Transactional decisions may include actions which have no legal consequences under national contract law and may be taken at any time between the moment the consumer is initially exposed to the marketing and the end of a product’s life or the final use of a service. As recognised by the Commission, most common activities which consumers carry out in a 'pre-purchase' stage are to be considered transactional decisions.

2.11 Accordingly, in an online environment, transactional decisions may potentially include a consumer’s browsing behaviour, for example a decision to remain on a particular trader’s website as opposed to that of its competitors, or the decision to click through to another page on a site, such as part of a booking process.

Average consumer

2.12 A key concept is that of the 'average' consumer. Breaches of the regulations are assessed by reference to different types of consumer (which, for convenience, are referred to collectively as 'the average consumer' in this annex): the 'average consumer', the

---

55 Regulation 2(1) of the CPRs
57 Commission Guidance at page 23: ‘National enforcers should therefore investigate the facts and circumstances of an individual case (i.e. in concreto), but assess only the ‘likelihood’ of the impact of the practice on the transactional decision of the average consumer (i.e. in abstracto). For example, the fact that there is no evidence that a misleading commercial communication has actually induced consumers to make a further click to proceed with an online booking does not prevent a national authorities from considering the transactional decision test as fulfilled if the likelihood of that happening (i.e. the risk) is real.
'average member’ of a targeted group of consumers and the 'average member' of a vulnerable group of consumers.⁵⁸

2.13 Whether a commercial practice breaches the general prohibition and the prohibitions relating to misleading and aggressive practices will be judged by reference to its affect on the 'average' consumer.

2.14 The 'average consumer' is the notional average consumer whom the commercial practice reaches or to whom it is addressed. The concept of the average consumer has been developed in the case law of the European Court of Justice. In determining the effect of the commercial practice on the average consumer, he or she should generally be assumed to be reasonably well informed and reasonably observant and circumspect, taking into account social, cultural and linguistic factors.⁵⁹

2.15 The 'average targeted consumer' is relevant where a commercial practice is directed to a particular group of consumers. If a practice is so targeted then it is the average member of that group and that member’s characteristics which are relevant.

2.16 The 'average member' of a vulnerable group of consumers is relevant where a clearly identifiable group of consumers is particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could be reasonably expected to foresee.

2.17 In particular, the average consumer under the regulations is not somebody who needs little protection because he/she is always in a position to acquire available information and act wisely on it.⁶⁰ On the contrary, the definition of a misleading action in the Directive is intended to take into account the current state of knowledge of how consumers take decisions in the market space, including the insights from behavioural economics.⁶¹

---

⁵⁸ Regulation 2(1) and Regulations 2(2) to (6) CPRs. For a detailed discussion, see OFT Guidance 1008 paragraph 14.28ff.
⁵⁹ Regulation 2(2).
⁶⁰ Commission Guidance at page 25.
⁶¹ Commission Guidance at page 32.
2.18 In an online environment, depending on the particular circumstances of the case, the average consumer may not necessarily be expected to be technically proficient in understanding how the internet works, including the use of profiling/tracking technologies and how to prevent their use if they do not consent to the use of such technologies in the course of a session that visits sites that utilise these.

Prohibitions

i) General Prohibition

(a) Regulation 3 contains a general prohibition of unfair commercial practices. A commercial practice is considered to be unfair if:

- it is not professionally diligent, and
- it materially distorts, or is likely to materially distort the economic behaviour of the average consumer.

(b) The first test requires that the trader’s practice must be unacceptable when measured against an objective standard. In the OFT’s view, this may include a failure by a trader to comply with applicable regulations, such as the information requirements relating to cookies and similar devices under the Privacy Regulations (as outlined above) is likely to be contrary to the requirements of professional diligence. Depending on the particular circumstances of the case, such a practice may be likely to materially distort the economic behaviour of the average consumer.

---

62 Regulation 3(1) of the CPRs.
63 Regulation 3(3)(a) of the CPRs 'Professional diligence' means the standard of special skill and care which a trader may reasonably be expected to exercise towards consumers which is commensurate with either - (a) honest market practice in the trader’s field of activity or (b) the general principle of good faith in the trader’s field of activity (as defined in Regulation 2(1) of the CPRs).
64 Regulation 3(3)(b) of the CPRs 'Materially distort the economic behaviour' means in relation to an average consumer, appreciably to impair the average consumer’s ability to make an informed decision thereby causing him to take a transactional decision that he would not have taken otherwise (as defined in Regulation 2(1) of the CPRs).
ii) Misleading actions

(a) Regulation 3(4)(a) of the CPRs provides that a commercial practice is unfair if it is a misleading action under the provisions of Regulation 5. Amongst other things, for the purposes of Regulation 5(2) of the CPRs, a commercial practice is a misleading action:

- if it contains false information and is therefore untruthful in relation to any of the matters set out in paragraph (4)\(^{65}\) or if its overall presentation in any way deceives or is likely to deceive the average consumer in relation to any of the matters in that paragraph, even if the information is factually correct, and

- it causes or is likely to cause the average consumer to take a transactional decision he would not have taken otherwise.

iii) Misleading omissions

(a) Regulation 3(4)(b) of the CPRs provides that a commercial practice is unfair if it is a misleading omission under the provisions of Regulation 6.

(b) A commercial practice is a misleading omission\(^{66}\) if, in its factual context, taking account of the matters in paragraph (2):\(^{67}\)

\(^{65}\) The matters referred to in paragraph 5(2)(a) are: (a) the existence or nature of the product; the main characteristics of the product (as defined in paragraph 5); (c) the extent of the trader’s commitments; (d) the motives for the commercial practice; (e) the nature of the sales process; (f) any statement or symbol relating to direct or indirect sponsorship or approval of the trader or the product; (g) the price or the manner in which the price is calculated; (h) the existence of a specific price advantage; (j) the need for a service, part, replacement or repair; (k) the nature, attributes and rights of the trader (as defined in paragraph 6); (l) the consumer’s rights or the risks he may face.

\(^{66}\) Regulation 6(1) of the CPRs.

\(^{67}\) Regulation 6(2) clarifies that the matters referred to in paragraph (1) are: (a) all the features and circumstances of the commercial practice; (b) the limitations of the medium used to communicate the commercial practice (including limitations of space or time); (c) where the medium used to communicate the commercial practice imposes limitations of space or time, any measures taken by the trader to make the information available to consumers by other means.
• the commercial practice omits material information

• the commercial practice hides material information

• the commercial practice provides material information in a manner which is unclear, unintelligible, ambiguous or untimely or

• the commercial practice fails to identify its commercial intent, unless this is already apparent from the context.

and as a result it causes or is likely to cause the average consumer to take a transactional decision he would not have taken otherwise.

(c) 'Material information' in the above context means information which the average consumer needs, according to the context, to take an informed transactional decision.68

(d) Whether or not the commercial practice is unfair under the regulations in each case depends on whether it causes or is likely to cause the 'average consumer' to take a different transactional decision.

iv) Aggressive practices

(a) Regulation 7 sets out the concept of aggressive commercial practices. These are defined as where in its factual context, taking account of all its features and circumstances a commercial practice:

• significantly impairs or is likely to significantly impair the average consumer’s freedom, of choice or conduct in relation to the product concerned through the use of harassment, coercion or undue influence, and

• it thereby causes or is likely to cause the average consumer to take a transactional decision he would not have taken otherwise.

68 Regulation 6(3). It also means any information requirement which applies in relation to a commercial communication as a result of a Community obligation, for example under regulation 7 of the Electronic Commerce (EC Directive) Regulations 2002.
(b) As with Regulations 5 and 6 a list of circumstances are provided in Regulation 7(2) which must be taken into account to determine whether a commercial practice amounts to harassment, coercion or undue influence. These circumstances include:

- its timing, location, nature or persistence\(^{69}\)
- the use of threatening or abusive language or behaviour\(^{70}\)
- the exploitation by the trader of any specific misfortune or circumstances of such gravity as to impair the consumer’s judgment, of which the trader is aware\(^{71}\)
- any onerous or disproportionate non-contractual barrier imposed by the trader where a consumer wishes to exercise rights under the contract, including rights to terminate a contract or to switch to another product or another trader.\(^{72}\)

(c) Regulation 7(3)(b) states that ‘undue influence’ means ‘exploiting a position of power in relation to the consumer so as to apply pressure, even without using or threatening to use physical force, in a way which significantly limits the consumer’s ability to make an informed decision’.

---

\(^{69}\) Regulation 7(2)(a) CPRs
\(^{70}\) Regulation 7(2)(b) CPRs
\(^{71}\) Regulation 7(2)(c) CPRs
\(^{72}\) Regulation 7(2)(d) CPRs