Information Commissioner's Office

Consultation:

Direct Marketing Code

Start date: 8 January 2020

End date: 4 March 2020

Introduction

The Information Commissioner is producing a direct marketing code of practice, as required by the Data Protection Act 2018. A draft of the code is now out for public consultation.

The draft code of practice aims to provide practical guidance and promote good practice in regard to processing for direct marketing purposes in compliance with data protection and e-privacy rules. The draft code takes a life-cycle approach to direct marketing. It starts with a section looking at the definition of direct marketing to help you decide if the code applies to you, before moving on to cover areas such as planning your marketing, collecting data, delivering your marketing messages and individuals rights.

The public consultation on the draft code will remain open until **4 March 2020**.The Information Commissioner welcomes feedback on the specific questions set out below.

You can email your response to directmarketingcode@ico.org.uk

Or print and post to:

Direct Marketing Code Consultation Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the consultation, please email the Direct Marketing Code team.

Privacy statement

For this consultation we will publish all responses received from organisations except for those where the response indicates that they are an individual acting in a private capacity (eg a member of the public). All responses from organisations and individuals acting in a professional capacity (eg sole traders, academics etc) will be published but any personal data will be removed before publication (including email addresses and telephone numbers).

For more information about what we do with personal data please see our privacy notice

Q1 Is the draft code clear and easy to understand?

☒ Yes

☐ No

If no please explain why and how we could improve this:

Q2 Does the draft code contain the right level of detail? (When answering please remember that the code does not seek to duplicate all our existing data protection and e-privacy guidance)

☐ Yes

☒ No

If no please explain what changes or improvements you would like to see?

In general the draft code does contain the right level of detail. However, there are some important points which have not been fully addressed. See for example paragraphs 4.1, 5.1, 9.2, 10.1, 14.1, 15.1, 16.2, 17.1, 18.2 and 18.3 of our attached response.

Q3 Does the draft code cover the right issues about direct marketing?

☒ Yes

☐ No

If no please outline what additional areas you would like to see covered:

Q4 Does the draft code address the areas of data protection and e-privacy that are having an impact on your organisation's direct marketing practices?

☐ Yes

☒ No

If no please outline what additional areas you would like to see covered

The draft code does address most areas of data protection that affect our direct marketing practices, but there are certain areas which have not been fully addressed and there are certain other areas which we consider go beyond what the code should be covering. See for example paragraphs 2.6, 3.2 and 7.1 of our attached response.

Q5 Is it easy to find information in the draft code?

- ☒ Yes
- ☐ No

If no, please provide your suggestions on how the structure could be improved:

Q6 Do you have any examples of direct marketing in practice, good or bad, that you think it would be useful to include in the code

- ☐ Yes
- ☒ No

If yes, please provide your direct marketing examples :

Q7 Do you have any other suggestions for the direct marketing code?

For reasons of practicality we have set out our additional comments in a separate document attached to this response. Please treat that document as if it were set out here.

About you

Q8 Are you answering as:

- ☐ An individual acting in a private capacity (eg someone providing their views as a member of the public)
- ☐ An individual acting in a professional capacity
- ☒ On behalf of an organisation
- ☐ Other

Please specify the name of your organisation:

TransUnion Information Group

If other please specify:

Q9 How did you find out about this survey?

- ☐ ICO Twitter account
- ☐ ICO Facebook account
- ☐ ICO LinkedIn account
- ☒ ICO website
- ☐ ICO newsletter
- ☐ ICO staff member
- ☐ Colleague
- ☐ Personal/work Twitter account
- ☐ Personal/work Facebook account
- ☐ Personal/work LinkedIn account
- ☐ Other

If other please specify:

Thank you for taking the time to complete the survey

TransUnion

Consultation response:

ICO draft direct marketing code of practice

TransUnion Information Group Limited

4 March 2020

1. Introduction

1.1. This is a response to the ICO's consultation on its draft direct marketing code of practice from TransUnion Information Group Limited and its subsidiaries ("**TransUnion**"). It accompanies a completed copy of the ICO's consultation response document.

1.2. TransUnion has a range of comments on the draft code of practice. These are set out under separate headings below, and paragraphs are numbered for ease of reference.

2. Broad definition of direct marketing purposes

2.1. In the draft code, the ICO has for the first time adopted a very broad definition of the meaning of "direct marketing purposes", to include all processing activities that lead up to, enable or support the sending of direct marketing communications. We consider that "direct marketing purposes" ought to be given a reasonably broad interpretation in order to ensure a high level of protection for data subjects, but believe that the ICO's definition extends too far and will lead to undesirable consequences for data subjects as well as businesses.

2.2. In particular, we do not agree that processing that is intended to exclude or prevent individuals from receiving direct marketing communications can be considered processing for "direct marketing purposes". This is because:

(a) Direct marketing is defined by statute as "*the communication (by whatever means) of advertising or marketing material which is directed to particular individuals*". Accordingly, "direct marketing purposes" means "*[the purposes of] the communication (by whatever means) of advertising or marketing material which is directed to particular individuals*". It is inherently illogical to consider that processing which aims to prevent the communication of marketing materials to particular individuals is performed for the purposes of communicating with those individuals. It is akin to saying that processing which aims to prevent (for example) tax evasion is processing for the purposes of committing tax evasion.

(b) Some businesses provide services which screen individuals out of their clients' marketing lists. For example, if a credit provider wishes to advertise a credit product, a data analysis company may be able to screen out of the provider's marketing list any individuals who would not be eligible for the product if they were to apply for it. This helps to ensure that people do not receive marketing which is inappropriate for them.

If that screening activity is considered to be processing for direct marketing purposes then the data analysis company would be prevented from applying it to individuals who have submitted objections to that company. This means that individuals who have objected to the processing of their personal data for direct marketing purposes may (counterintuitively) receive more direct marketing than they previously did. Given that most individuals who object to the processing of their personal data for direct marketing purposes typically do so because they do not want to receive direct marketing communications, this would be an unexpected and unwanted outcome.

Although in principle these issues could be resolved by discussing the consequences of the objection with the data subject, we understand that the ICO expects controllers to give effect to clear objections without further confirmation, and would not support anything that appears to be attempting to persuade the data subject not to object.

(c) More generally, the ICO's interpretation would result in undesirable outcomes. In particular, it would mean that controllers could no longer apply criteria designed to prevent inappropriate marketing to particular groups of individuals where those individuals have objected. This could, for example, result in the following consequences:

i. Individuals with a poor credit history may receive advertising for credit products for which they are not eligible or which would result in high interest payments if they do not repay the credit on time. These individuals could be in a vulnerable state and may find themselves in financial difficulty as a result of marketing activity which is inappropriate to their circumstances.

ii. Children may receive direct marketing for age-inappropriate products and services, such as gambling, alcohol and tobacco.

iii. Individuals with current or previous gambling addictions may receive advertising from gambling operators.

(d) Certain industry sectors have particular responsibilities to ensure that marketing is appropriate for the individuals to whom it is directed. For example:

i. The FCA Handbook requires FCA-regulated firms to take steps to ensure that their advertising activity is appropriate for the individuals to whom it is directed. See in particular sections CONC 2.2.2(1), 2.5.3(2), 2.5.8(10) and (18), 3.8.2(1) and (3) and (more generally) High Level Principles 6, 7 and 9. If firms are not able to take into account a person's financial status in order to exclude individuals from marketing which would be inappropriate to them, it will be difficult or impossible for them to comply with these requirements.

ii. Sections 5, 16, 18, 21 and 22 of the CAP Code (and similar provisions in the BCAP Code) recognise the need to protect children from certain kinds of advertising, such as advertising relating to gambling, alcohol and tobacco, and accordingly require that certain kinds of advertising are not directed at children. If processing cannot be performed to exclude children (or people who are likely to be children, or households thought likely to contain children) from such advertising, it will be more difficult for advertisers to comply with these requirements, and there may be significant negative consequences for these particularly vulnerable members of society.

2.3. We note the suggestion on page 35 that a potential significant negative impact may result from direct marketing where an individual in financial difficulties is targeted with marketing for high-interest loans, and the similar suggestion on page 59 that doing so may have a significant effect on them. We agree with that and, as explained above, some organisations provide screening

activities which aim to prevent individuals from being contacted with offers for inappropriate credit products. However, we consider that the broad definition of direct marketing purposes in the draft code would mean that such processing would not be permissible in respect of individuals who have objected to such organisations processing their data for direct marketing purposes.

2.4. For the above reasons, we suggest that a caveat should be added to the definition of "direct marketing purposes" in order to carve out processing which aims to prevent or exclude particular individuals from receiving marketing materials.

2.5. We note that at pages 110 and 113 the draft code suggests that applying a marketing suppression list (consisting of objections under Article 21) is considered to be processing for the purposes of complying with a legal obligation rather than processing for direct marketing purposes, but:

(a) This seems an artificial distinction. A particular processing operation can be carried out for more than one purpose at the same time, and so the fact that data is processed in order to comply with a legal obligation does not mean that the processing is not also being performed for direct marketing purposes. If "direct marketing purposes" is defined to include anything "*leading up to*" the sending of direct marketing communications, then we do not see why applying a suppression list consisting of objections does not amount to "direct marketing purposes" while screening individuals out of a marketing list for other reasons does.

(b) Applying TPS is a legal obligation whereas applying MPS is not. Following the logic of page 113, processing a file against TPS is not processing for direct marketing purposes, while processing against MPS is. Accordingly, an objection to direct marketing purposes would exclude a data subject from processing against the MPS but not against the TPS. This seems an odd result (which results directly from the ICO's position that excluding individuals from direct marketing is an activity performed for the purposes of direct marketing in relation to those individuals).

2.6. Even if "direct marketing purposes" is given a broad interpretation to include matters other than communicating with data subjects, this does not appear to be what Parliament intended the code of practice to cover. Under section 122 of the Data Protection Act 2018, the code of practice is to contain guidance on "*the carrying out of direct marketing*", and "*good practice in direct marketing*". "Direct marketing" is defined to mean communicating with data subjects, and accordingly section 122 requires the code of practice to contain guidance on best practice as to the carrying out of such communications. We question whether the ICO is acting properly and within its powers in extending the scope of the code of practice beyond its statutory parameters and, if it does so, whether the code (or particular parts of the code) can have the effects described in section 127.

3. Teleappending or tracing for direct marketing purposes

3.1. We note that the draft code suggests that buying additional telephone numbers or email addresses for existing customers, or tracing an individual to a new postal address in order to be able to send direct marketing to their new address, is likely to be unfair. We consider that it may in some circumstances be possible to be clear enough to the data subject about the processing activity such that a sufficient degree of fairness and transparency is achieved and the legitimate interests condition is satisfied. This would require the controller to ensure that the data subject has been given very prominent information, and additional safeguards may be required such as a simple mechanism to opt out (e.g. with a prominent checkbox). We do not

necessarily agree that the processing "*takes away control*" from the individual; they always have an unfettered, absolute right to object which the controller must comply with.

3.2. Page 62 makes the point that in a direct marketing context it is reasonable to expect individuals to inform controllers of changes in their contact details, and therefore tracing individuals to their new address is not necessary and is (in general) unjustified. However, we consider that the position may be different in other contexts. For example, while tracing for direct marketing purposes may be unjustified, it may be permissible for an organisation to obtain updated contact details for the purposes of:

(a) service provision – for example, where a bank traces a customer to a new address in order to continue to send account statements to the correct person;

(b) issuing a product safety warning or product recall message;

(c) contacting a person for asset reunification purposes (for example, if the individual has moved and need to be traced about a forgotten bank account or pension pot); or

(d) contacting a person for debt recovery purposes.

This means that an organisation may use tracing services to keep a customer database up to date for the above purposes but perhaps not for direct marketing purposes. In practice, an organisation will not maintain one database of customers for direct marketing purposes and a separate database of customers for other purposes such as those listed above. If it were to do so, then (a) it may be in breach of the data minimisation principle, and (b) it may be in breach of the accuracy principle if it keeps its non-marketing database(s) up to date by means of tracing services but fails to update its marketing database at the same time.

It would be helpful if the code could clarify how an organisation should manage this in practice. If an organisation has updated its database for non-marketing purposes, is it permissible to use that updated database (rather than another database, known to be out of date) for its direct marketing purposes too? Or does updating a database automatically preclude the use of that data for any subsequent marketing activity? Presumably the ICO would not expect an organisation to continuing using inaccurate data for marketing purposes when it has up to date data available for other purposes?

4. Privacy information

4.1. At various places (see for example pages 6, 46, 52, 54, 65, 91, 99, 100 and 102), the draft code indicates that controllers must inform data subjects about their processing activities. While this is generally true, it is not always true; for example, notice may not be required where either (a) the data subject already has the information; (b) the impossibility or disproportionate effort exception applies; or (c) a Data Protection Act 2018 exemption applies. On page 52 there is a paragraph which correctly recognises these exceptions and exemptions. We suggest that this wording is also used at the other places in the draft code where there is reference to the requirement to provide privacy notices to data subjects. If in some places the ICO is recommending that privacy information is provided irrespective of whether an exception or exemption applies, it should be clear that this is a matter of best practice.

4.2. Page 65 suggests that an organisation must provide privacy information to the data subject "*prior to contacting them*". In fact it is permissible to the provide the privacy information on first contact – see GDPR Article 14(3)(b).

5. Disproportionate effort

5.1. Page 49 refers to the need (when relying on the disproportionate effort exemption in GDPR Article 14(5)(b)) to assess the balance between the "*effort involved*" in giving privacy information and the effect of the processing on the individual. In this context, it would be helpful for the ICO to explain the factors that may be taken into account when assessing the amount of "effort" involved in providing privacy information. In particular, it would be useful to understand whether the costs of providing privacy notices (for example, the costs of sending privacy notices out by post) can be taken into account. This is an important point which any organisation will need to understand when considering the disproportionate effort exception, and it is therefore crucial that the ICO provides guidance on it if the code of practice is to be helpful in relation to this issue.

In our view it must be possible to take into account cost, given that any form of delivery mechanism could (and most likely would) be delegated to a service provider such as Royal Mail rather than being physically performed by the controller itself. If the cost of doing so cannot be taken into account, then nothing would ever satisfy the disproportionate effort exception because it would always be possible to pay another organisation to perform the notification task.

6. In-app advertising

6.1. On pages 16 and 72 the draft code suggests that PECR applies to "*in-app messaging*". We consider that only certain types of in-app messaging fall within the definition of direct marketing and therefore within the scope of PECR. Specifically, regulation 21 of PECR will only apply if the form of advertising amounts to the sending of "electronic mail", which depends on technical considerations such as whether the message is stored in the network or device until collected. This will not necessarily apply to all forms of in-app advertising.

7. Targeted postal marketing

7.1. Pages 16 and 66 contain sections explaining the meaning of "directed to" for the purposes of the definition of direct marketing. They indicate that:

(a) personally-addressed post is directed to particular individuals; but

(b) leaflets delivered to every house in an area are not directed to particular individuals.

There appears to be a middle ground which has not been considered here. An advertiser may wish to target advertisements on the basis of information about a property. For example, a company which installs conservatories may wish to direct its marketing to the occupants of houses rather than flats. It is not clear whether this is considered to constitute direct marketing where the marketing material has not been personally addressed and we suggest that the code is clarified to address this.

8. Possible sub-types of "direct marketing purposes"?

8.1. Page 26 suggests that a controller should ask itself "*What specified direct marketing purposes do you intend to collect this data for? (purpose limitation principle)*". This suggests that a controller needs to specify its purposes at a more granular level than "direct marketing purposes". While we would certainly agree that a controller needs to explain in its privacy notices what is involved in its "direct marketing purposes" (as suggested on page 50), we are not sure that there is merit in specifying purposes at a more granular level. This would be likely to cause confusion with the Article 21 right to object to processing for direct marketing purposes, and it also contradicts the approach taken in the examples found in the ICO's

template Article 30 records at https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx.

8.2. Similarly, on page 35, where the draft code says that a controller "*... may need to be more specific about [its] purposes ...*", we suggest that this might be better as "*... may need to be more specific about its processing activities ...*".

9. Examples

9.1. The examples on page 73 relate to situations in which there is a breach of PECR because of a lack of consent. However, the ICO appears to overlook the possibility that the relevant organisations are relying on the soft opt-in. If the ICO considers that the soft opt-in does not apply in these examples, it would be helpful for that to be made clear, and for the reason to be given.

9.2. Page 77 provides an example about an organisation which sends out a marketing email with an unsubscribe link at the bottom. It would be helpful for the code to include any requirements or best practice recommendations relating to that unsubscribe mechanism. For example:

(a) Must the unsubscribe link in the email immediately unsubscribe the individual, or can it take the person to an online preference centre or an "are you sure?" page?

(b) Is it permissible to require the individual to sign into an account in order to change their marketing preferences?

10. Requirement for "named" consent

10.1. One of the most important changes brought about by the GDPR in relation to marketing activity (particularly marketing which uses third party data) was the requirement that any controller relying on consent must have been specifically named at the time the consent was obtained. This requirement is highlighted several times in the ICO's separate guidance on consent. However, the draft code contains only two passing references to this important requirement – see pages 33 and 53. We suggest that the requirement that consent must "named" should be given much more prominence, including in particular on page 102, or else it is likely to be missed by advertisers who are not familiar with the ICO's other guidance.

11. Legitimate interests

11.1. Page 34 suggests that a controller "*might be able*" to rely on legitimate interests as its legal basis if it can show that the use of the data "*has a minimal privacy impact and is not a surprise to people or they are not likely to object to what you are doing*". We believe that this presents a distorted view of the legitimate interests condition. It is in principle possible for a controller to rely on legitimate interests even if its processing activity has a significant privacy impact and even if people would be likely to object to what the controller is doing, provided that the processing is necessary, the aims being pursued are sufficiently strong, and appropriate safeguards have been put in place.

Accordingly, we suggest that the wording on page 34 should be qualified, for example with words such as "*... especially if the use of the data has a minimal privacy impact ...*".

11.2. On page 35 the draft code quotes from GDPR recital 47 and then paraphrases it with "*... the GDPR says that direct marketing may be a legitimate interest. It does not say that it is always a legitimate interest ...*". In our view, the ICO places too much emphasis on the word "may" in recital 47 here. Firstly, recital 47 does not say that "*direct marketing may be a legitimate interest*"; it says that "*the processing of personal data for direct marketing purposes may be*

regarded as carried out for a legitimate interest". Secondly, it is not at all clear that "may" here means "might or might not"; it could well mean "it is permissible". Thirdly, as noted in the WP29 Opinion 06/2014 on legitimate interests, the question of whether a particular interest is "legitimate" is a low threshold to meet; it essentially includes any interest which is lawful and more than de minimis. The crucial question when relying on the legitimate interests legal basis is not whether the interests being pursued are legitimate but whether they override the potential impact on the data subjects.

12. Requirement of a DPIA for "wealth profiling"

12.1. Page 58 indicates that organisations performing "*wealth profiling*" must complete a DPIA. However, wealth profiling does not appear on the ICO's list of activities that require a mandatory DPIA. Does the ICO consider that wealth profiling will always involve "tracking" or "large-scale profiling", for example? If not, perhaps the ICO should make clear that DPIAs for wealth profiling are merely a best practice recommendation, or update its list of mandatory DPIA scenarios to include wealth screening in order to ensure consistency with the code.

13. Soft opt-in

13.1. Page 77 indicates that an organisation relying on the soft opt-in must give individuals the chance to "*opt out of every subsequent communication*" that it sends. This should read "*opt out of every subsequent direct marketing communication*" – individuals generally cannot opt out of being contacted for other purposes.

14. Marketing on social media

14.1. The bottom of page 89 lists three kinds of personal data that may be used in the context of social media advertising. We believe there is a fourth kind: personal data which the social media platform operator has purchased from a third party.

14.2. On page 90 there is a sentence reading "*This type of targeted advertising on social media does not fall within the definition of electronic mail in PECR.*" However, it is not clear from the context what type of advertising this is referring to or why it does not fall within the definition of electronic mail.

15. Reference to earlier WP29 guidance

15.1. Page 103 contains a box headed "*Example*", but it does not contain an example. It contains a quotation from an Article 29 Working Party Opinion dating from 2013 (reiterated in 2014) suggesting that consent should be required for (among other things) profiling and data broking. The draft code does not comment on the quotation except to say that it this was the "*view*" of the Working Party, and that "*this view is still relevant*". With respect, this is not helpful. There is little point in the ICO merely stating what the view of the Working Party was in 2013 and 2014. If the ICO believes that profiling and data broking can only be performed on the basis of consent, then it should say so clearly and explicitly in the code. If it does not agree then there is no point in including this quotation in the code. As it stands, this quotation will only cause confusion and uncertainty.

16. Individual rights

16.1. Page 107 makes clear that an organisation can ask for more information if it has doubts about the identity of the person making a request. It goes on to say, "*For example you may need to*

confirm what their email address or phone number is, in order to stop processing these details for direct marketing purposes." However, that example does not appear to relate to identity verification. It appears that the draft code is conflating the process of confirming that the data subject is who they say they are with the process of confirming which data the data subject wishes to exercise their rights over. In this scenario it appears that the individual's identity has already been accepted and the organisation is merely confirming what details the individual wishes to be suppressed.

16.2. Pages 112 and 114 contain brief references to Article 19 notifications. It would be helpful if the ICO could provide some practical guidance here on this subject – such as when it would and would not involve disproportionate effort to notify the onward recipients of the data. For example, we consider that disproportionate effort may arise where:

(a) an organisation has sold data to another organisation for a limited period of use, and that period has expired or is soon to expire; or

(b) the change in the data is trivial.

16.3. Page 53 suggests that a buyer of marketing data should ask whether the seller passes on individuals' objections. We note that GDPR Article 19 would require the seller to pass on erasures, rectifications and restrictions, but does not specifically require it to pass on objections. Perhaps the draft code should make clear that this is a best practice recommendation rather than a legal requirement.

17. Opt-outs / unsubscribes as distinct from withdrawals of consent and objections

17.1. At various places, the draft code appears to draw a distinction between (a) withdrawal of consent, (b) opt-out or unsubscribe, and (c) objections. This can be seen on pages 42, 73, 108 and 110 for example. While withdrawal of consent and objection have a clear basis in the GDPR (i.e. Articles 7(3) and 21(2)), we do not recognise opt-outs/ unsubscribes as a distinct concept within data protection law. Page 108 suggests that an unsubscribe has the effect of an Article 21 objection limited to a particular channel. It would be helpful to for the code to make clear:

(a) What is the basis of the ICO's statements relating to opt-outs/ unsubscribes, and are these legal concepts or best practice concepts?

(b) Does the ICO consider that an Article 21 objection can only apply to all processing for direct marketing purposes (creating the desire for a more granular "unsubscribe" mechanism), or can data subjects give Article 21 objections that relate only to specific processing activities that are carried on for direct marketing purposes?

18. Profiling and automated decision making

18.1. At various places in the section headed "*Profiling and data enrichment*", beginning on page 56, the draft code appears to conflate profiling with automated decision-making. These are two distinct concepts.

(a) **Profiling** involves processing personal data in order to "evaluate", "analyse" or "predict", for example by inferring new information about individuals.

(b) **Automated decision-making** involves using personal data to make decisions about individuals.

As is made clear in the ICO's separate guidance on automated decision-making and profiling, "*automated decision-making often involves profiling, but it does not have to*". They are

conceptually two different things. As a result, automated decision-making is subject to GDPR Article 22 and Articles 13(2)(f) and 14(2)(g), but profiling (per se) is not.

We suggest that this section of the code is reviewed to ensure that this distinction is clear throughout. This is particularly important for organisations such as TransUnion which often perform profiling activities for their clients but typically do not make decisions about data subjects themselves on the basis of that profiling.

18.2. Page 57 mentions some of the business benefits that can be produced as a result of profiling and data enrichment but does not mention any of the benefits to data subjects, such as the receipt of more relevant and interesting advertising materials. While we would not wish to overstate the extent of those benefits, this appears to be an obvious omission.

18.3. Page 58 suggests that a controller will be unable to rely on the legitimate interests legal basis in order to perform "*intrusive profiling*" for direct marketing purposes. In relation to this:

(a) Given the broad meaning that the ICO has given to "direct marketing purposes", this seems a rather sweeping statement. If "direct marketing purposes" can include anything that leads up to direct marketing, then it will include many activities that have negligible practical impact on data subjects. It seems odd to suggest that none of a very wide variety of potential activities can be justified on the basis of legitimate interests.

(b) It would be helpful if the ICO could clarify what it means by "*intrusive profiling*". Is it suggesting that all profiling is intrusive, or does it depend on the data which is used or inferred as a result of the profiling, or the subsequent uses of that data?

18.4. The final paragraph on page 58 refers to "*automated profiling*". Profiling is by definition always automated. Perhaps this means to refer to "automated decision making".