betsson group

BETSSON COMMENTS ON THE ICO DRAFT CODE OF PRACTICE FOR DIRECT MARKETING

Dear Sir/Madam,

First, we would like to thank you for continuing work on this very important topic within this Code of conduct for marketing operations. We believe that this is one of the most controversial subjects in the privacy area, especially due to the fact that the new long-awaited e-Privacy regulation has not yet been adopted. For this reason, we appreciate these kinds of clarification since they are indispensable for every company. Also, we value the opportunity to be part of this dialogue by sending our comments on the text of the Code. As the idea behind these kinds of clarification is to see how to apply legal requirements in real life business scenarios, industry feedback is an important factor to attain a better understanding of the specific interpretations. Therefore, we hope you will find our comments useful and that you will take them into account when drafting the final version. Of course, we remain at your disposal for any further comments.

1. Interpretation of 'direct marketing'

The draft Code states that the concept of direct marketing purposes is wider than just sending direct marketing communications and includes not only the sending of the communications but also *all processing activities that lead up to, enable or support sending those communications* (Page 13,14). This means that a very wide scope of typical business activities used for other purposes, would potentially fall within the definition of marketing. As will be shown in more detail below, one needs to bear in mind that it is not always easy to make a clear distinction between different purposes of an activity. For example, sometimes some activities that were not initially intended for marketing, can be used by the company for marketing later on. Also, one cannot ignore the fact that the ultimate goal of every company is to maximise its revenue relying on different commercial and promotional activities. With this in mind, it becomes evident that with the Code's wide interpretation, any commercial activity (which includes practically all activities since all that companies do is commercially driven) in a company, would potentially fall within the promotional aspect.

As a result, we believe that this approach is impossible to follow due to several practical implications as follows:

1. The company would have to stop from carrying out any other activity such as market research (e.g. surveys), some form of BI, CRM and many other activities which traditionally did not fall within the same definition as 'direct marketing' and initially might not have been intended for marketing purposes, if an individual objects to direct marketing purposes;

2. If the company uses a different legal basis for email (legitimate interest) and calls (consent), this would mean that all activities related to these should follow the same legal basis. In that case if we use the same market research for both channels (email and calls), we cannot apply to the same activity (market research) a different legal basis for each channel. This broad approach would introduce a lot of uncertainty since as previously explained it is not always so clear whether some of the activities will be related to direct marketing;

3. The same is applicable for research activities. If one had to take into account the bigger picture that every activity in corporate entities is done for the commercial purpose (to maximise revenue, reach more customers or retain current ones) then every survey, in the end, can be related to the marketing activity or even used for marketing purposes. The idea behind every research activity in corporate entities is to get a better understanding of the market and where the company is on the market, so that it can use that information to better position in the future (which is ultimately related to marketing). Because of that we find it practically impossible to draw the line between commercial activities relating to direct marketing and the rest.

Finally, we need to bear in mind *ratio legis* behind provisions of unsolicited communication in the e-Privacy Directive; that is to protect customers from unsolicited communication that can bother them and be deemed intrusive. Therefore, the focus of direct marketing activities should be on the very contact with the customer, since without that contact (meaning the customer receiving the message) there is technically no 'direct marketing'. To this end we believe that it is crucial to narrow the scope of direct marketing to the very contact with the customer.

2. Roles of different parties in marketing activities

Nowadays, with development of technology and emergence of new online business models, there are many different and very complex structures of cooperation for the marketing purposes. For that reason, we find it essential to start any privacy analysis of marketing arrangements with an understanding of underlining principles of the GDPR.

The very idea behind the GDPR is that the entity that has decision making power – the data controller, should be responsible for complete compliance toward its customers (so customers can avoid situation where they need to impose claims against many entities involved in the processing operations, in a case of potential dispute). On the other hand, how these compliance obligations will be performed/achieved by other entities involved in the processing activities – data processors, is the matter of arrangements between the data controller and its data processors, of course following relevant provisions of the GDPR. Unlike in data controller – data processor relationship where a data controller should have control over processor's operations (governed in the respective data processing agreements), in situations where we have two independent controllers, one needs to understand that we have two parties with equal power, where each is responsible for separate processing activities. Therefore, each party in this relation should be solely responsible for its compliance obligations toward the data subjects and the 'other party' cannot be required to take on the burden of monitoring the compliance of the other independent controller (since these activities are completely out of the scope for the 'other party'). The maximum effort that the 'other party' can do in this situation is to inform its data subjects that for the purpose of specific cooperation, the sharing of data with other independent controllers will be necessary. However, for these purposes data subjects should reach out to these independent controllers for more information about their processing operations.

We believe that here one also needs to be pragmatical and understand limitation of companies in business to business relations. Processing of personal data is always integral part of the underlining business transaction and cannot be seen separately. Therefore, we have to examine how feasible it is for one company to control the other entity with equal power from a data privacy perspective (but possibly a higher power from a commercial perspective).

Therefore, in most of the marketing activities that the Code addressed we see the role of the companies and their marketing partners as separate and independent controllers, where each company is solely responsible for its compliance toward data subjects. Below we will elaborate on a few typical examples which were brought up in the Code:

- ***Advertisers and social media platforms are joint controllers***

The Code explains that the use of personal data for the creation of 'lookalike audience' on social media platforms renders the company and the social media platform 'joint controllers' for this activity. However, it is important to note that in this case the company has no real control over the activities of the platform and has no access to the data about these customers. In this specific case the social media platform offers this service as a standalone service. The social media platform is performing this service based on existing data that it has in its customer database (existing Facebook users). The company that uses this service is only requesting the specific service, that is to be performed completely and separately by the social media company from the existing data. Therefore, we believe that in this case social media platforms are separate and independent controllers since they solely decide which data they need to create lookalike segments and how they will process the data in order to perform the requested service1. The very fact that one company requested this service, does not mean that this company is responsible for the compliance of the social media platform.

In order to assess the relationship of the parties we need to understand who really has the decision-making power with respect to the personal data in this relation and how is the underlining commercial relationship is constructed. The very fact that these kinds of services are not subject to negotiations with platforms such as Facebook, but companies rather have to accept their terms and conditions to use them, is a testament of the roles of the parties and the fact that companies cannot really influence this kind of processing by social media platforms.

- ***Dual branding activities***

The Code states that in the event of a dual branding promotion, both parties need to comply with e-Privacy even if the company does not have access to the data that is used (Page 27). In this case it is very important to understand the previously explained relation of two separate controllers. In most of these cases the parties will be separate controllers, hence the party who sends the marketing material of the other party to its customer database should make sure that these activities are compliant with the relevant law (meaning that it has consent for marketing third party products/services). The other party (the one which has ordered these services) cannot be responsible for the activities of the other independent party and should neither have the obligation to reach the people who are not its customers (since that would require from this company to collect more information that is necessary for this purpose, thereby forgoing the principle of data minimisation).

However, even though we can find that in some of these activities, parties are together deciding about all important aspects of this activities and therefore should be classified as joint controllers, that does not mean that both parties need to fulfil the same obligations. In joint controller relations parties should be able to agree who will perform which obligations (for example, who will serve privacy notices, who will collect consents, etc. as defined in relevant

[1] The role of Facebook in these activities was already examined by relevant courts. See decision: https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-9586?AspxAutoDetectCookieSupport=1

provisions of the GDPR related to the joint controllers). The very type of the joint controller relation does not require that both parties need to fulfil all obligations toward the customers.

- ***Marketing via third parties***

Similar to the previous point, the Code also states that if companies use a third party to carry out marketing of services to third party's customers, the company also needs to collect consent from these third-party customers (Page 82, 83). The Code itself recognizes that this is a challenging exercise and for that reason it will be very difficult to be compliant in this respect. We find this approach practically impossible and not in line with the previously explained relation and roles of the parties. We consider important that any marketing activity is conducted in line with data minimization principle and for that purpose companies should not be obligated to collect more data than necessary, especially where it is clear that one of the companies is able to fulfil all obligations toward the customers. In these cases, it should be recognized that the third party, as a separate controller in its own right with separate legal responsibility, is responsible for its own operations and for ensuring it has adequate legal basis to advertise third party products/services. Different approach would make huge scope of marketing cooperation impossible and have severe consequences to whole the marketing industry.

- ***Due diligence checks***

The draft code states that organisations buying or renting direct marketing lists must conduct appropriate due diligence and must be able to demonstrate this compliance (Page 53, 63, 102). Although we recognize the idea behind this and we support the approach that in specific data buying/selling scenarios additional safeguards should be applied due to the sensitivity of situation, we also find it equally important to put this into the context of the underlining business relationship and roles of the parties. Companies that buy data should ask questions and get warranties from the other party (selling the data) that this is done in compliance with relevant data privacy laws. However, companies buying the data should not be put in a position to verify the compliance representations made by the company selling the data (for example, checking if consents are in fact collected, checking their privacy policy, etc.). The verification of the claims of the other party would require disproportionate effort and would be practically impossible. For example, in order to comprehensively assess whether a privacy policy is appropriate one should not only check if the mandatory legal requirements are contained in it but should also check if the privacy policy is explaining all processing activities, and whether they are clear enough. To do this, one needs to be aware of the entire processing activities of the company. In the end, as explained previously, this is the relationship of two independent controllers, where each party should separately fulfil its compliance obligations. Therefore, the buyer of data should be able to rely on guarantees provided by seller of data within the contract and that should be sufficient for this purpose.

3. B2B Marketing

The Code stipulates that GDPR will apply in the same way to processing of business contact data if they include personal data (Page 78). We believe that in this context it is essential to understand what kind of "personal data" are collected and for which purposes. The idea behind collecting contact information of business partners is to reach the company as the legal entity, and not the individuals working in that company. Therefore, the companies who are sending commercial offers to their corporate partners are not interested in persons working within the company or their personal characteristics. In fact, they are interested in getting a new client that is the business entity. The people who are working in the company are changing and they are not

relevant for the purpose of these activities. For example, if we want to make a specific offer to the company, we will do that based on the company's business needs, revenue etc. and not the personal characteristics of the person who is working in procurement department of that company.

Although we do understand the logic behind protecting companies from unsolicited marketing, we believe that the same goal can be reached without extending the interpretation of data protection scope to business relationships. The GDPR itself recognizes this by excluding from its scope processing of personal data that concerns legal persons. Therefore, we believe it should be made clear that business contact details are not personal data, but on the other hand businesses should also have option to unsubscribe from the commercial offers of other entities.

4. Regulatory communications

The Code states that direct marketing obligations also apply to communications which are sent by the company to comply with regulatory objectives, comply with licence conditions or meet a wider public policy objective (Page 21, 117). Although we are not aware of sectorial requirements that would request the companies to send marketing communication, we have to note that given the wide definition of the marketing activities in the Code, it could occur that from a privacy perspective some form of mandatory notifications are considered as marketing communications. The classification of regulatory communications as direct marketing puts companies in a dangerous position as they are expected to abide by possibly contradictory legal requirements. For example, if a customer has objected to the receipt of direct marketing communications, the company cannot reach out to that customer, thereby potentially breaching its regulatory obligations. In the end, as recognized by the GDPR, where there is a legal obligation defined by different law, companies should be able to rely on this legal basis as a ground for processing of personal data. The potential issue of inconsistencies of different laws, is not something that should be solved by corporate entities. Having a different approach would put companies in a 'nonsensical' position where they need to decide which law they will breach.

5. Contract as a lawful basis

On the page 29 of the Code states that if company have a contractual relationship with the individual it might be able to apply the contract as lawful basis to direct marketing, provided it is necessary for the performance of the contract. So far only legitimate interest and consent were deemed as appropriate legal bases for marketing activities. As a matter of fact, the Code explains that marketing activities cannot be a precondition for the provision of the service. Although we welcome and support this novel approach, given that this is a very important change in the current regime, we would appreciate more clarity (with practical examples) on this matter. We find it very important to understand when 'contract' would be deemed an appropriate legal basis for marketing and for which kind of marketing activities.

6. Advertising IDs are deemed personal data

The Code implies that advertising IDs are to be classified as personal data (Page 96). Although we recognize that this is a contextual question and depends of the scope of the information that can be linked with given ID, we believe it is important to clarify the following. From the advertiser's point of view, in most of the cases it cannot determine at all, or only with disproportionately high effort, which natural person is behind the online identifier in question. The identifier as such "may" leave such traces, however there may in fact be cases in which online identifiers do not leave such traces. The use of these kind of IDs is good way to reach the balance where we can avoid excessive use of personal data but in at the same time have enough data to

develop new innovative data driven methods in different industries. Therefore, we find it important assess this question in each case, rather than apply a blanket approach to these kinds of online identifiers.

7. Profiling that can have significant negative effect on the customer

When it comes to this matter, we have to note that we find important explanations provided and examples about profiling that can have significant effect to the data subjects (Page 59). However, we also believe it is important to be very precise when the examples are related to heavily regulated industries such as the gambling industry. One of these is the example of "*the profiling of individuals known as problem gamblers*". In that regard we need to mention that gambling regulations in the U.K. are very strict and clearly define when any kind of marketing activity is forbidden for specific types of customers. When it comes to the specific gambling issues, we recognize that this is definitely the case (such as self-excluded customers). However, we find it important to follow the approach from gambling regulations; meaning that we use definitions and regime from the relevant gambling regulations. Also, the criteria for exclusion of certain players, should be in line with relevant operator's polices about responsible gambling. Therefore, we find essential here to follow the approach already defined in relevant sectorial laws.

8. Data subject requests – right to access

The Code explains that in relation to the data subject access requests, individuals should have right to get *a copy of their data, including any assumptions, categories and segments you have assigned to them, etc*. (Page 114). We find that this approach is very extensive and not in the line with current case law on this matter. Data subject access requests presented to be one of the most challenging right to be fulfilled by the companies that hold huge amount of data. For that reason, this issue was subject of the interpretation by different courts, such as the one of the Cologne Regional Court Decision[2], where the Court confirmed that "*the right of access does not include: all internal processes, such as notes; all exchanged correspondence; legal evaluations or analyses are also not considered personal data in these terms; information such as ratings and private notes about employees' performance or appraisals should not necessarily be disclosed under a DSAR"*. Similar to that case, the ECJ explained[3] that *"extending the right of access of the applicant for a residence permit to that legal analysis would not in fact serve the directive's purpose"*. This position is reinstated by the Malmö Administrative Court's judgment of 28 February 2019 in case no. 12986-18.

Moreover, we find important to understand practical implications of this approach. For example, categories and segments are usually based on the generic and statistic information about customers, and sometimes company cannot recognize in which category each customer is. Although companies should aim to provide as much as possible information to data subjects, we find it important to limit this to the reasonable efforts that one company should invest in these requests.

Respectfully,

Data Privacy Team

[2] https://www.datenschutz.eu/urteile/Umfang-des-Auskunftsanspruchs-nach-Art-15-DSGVO-Landgericht-Köln-20190318/

[3] http://curia.europa.eu/juris/liste.jsf?num=141/12&language=en