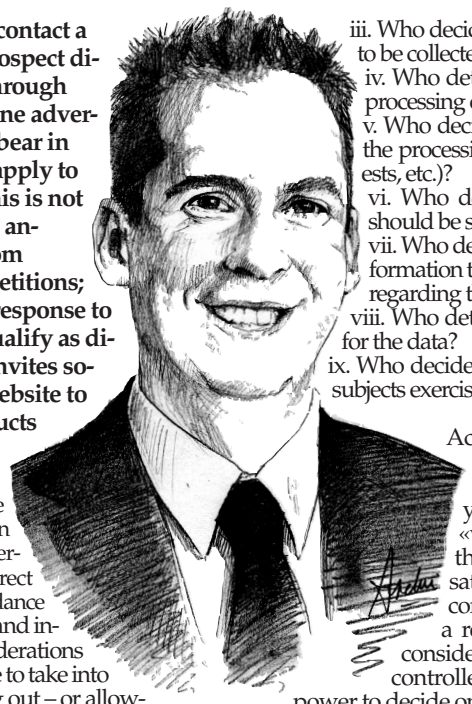
The Belgian data protection authority issues guidance on the processing of personal data for direct marketing purposes

Every time you contact a customer or prospect directly – even through certain forms of online advertising – you have to bear in mind the rules that apply to direct marketing. This is not only true for e-mails announcing rock-bottom prices or prize competitions; even an automated response to an enquiry might qualify as direct marketing if it invites someone to visit the website to see the newest products or services.



At least, that is how the Belgian Data Protection Authority (BDPA) interprets the concept of direct marketing The new guidance is nearly 80 pages long, and includes a range of considerations that organisations have to take into account when carrying out – or allowing – any direct marketing activity. From sections regarding an organisation's role (as controller, processor or joint controller) to sections on the legal grounds available under the GDPR (legitimate interests, consent etc.), it is a markedly different product compared to previous recommendations of the BDPA. In the absence of a similar extensive guide and taking into account that the guide is an interpretation of the EU data protection law which also is applicable in Luxembourg, the following is of relevance for the Luxembourg market as well.

What is direct marketing?

A range of scenarios are covered by the concept of direct marketing, based on the various illustrations the BDPA gives thereof:
- **Nature of recipient**: «direct marketing» covers both prospects and existing customers.
- **Activities covered**: the concept covers not only the actual commercial activity (e.g. the sale of products) but also the broader promotion of the organisation.
- **Nature of processing**: while the BDPA gave a definition of «direct marketing» that is squarely tied to a communication, it simultaneously suggests that «direct marketing» not only covers the communications themselves but also any processing activities carried out in the context of marketing operations, and it gives the example of automatic adaptations to the price of a product or service on the basis of a customer profile. We assume, however, that the BDPA intended for such operations to be tied to a communication.
- **Profit vs non-profit**: «direct marketing» does not require a «for profit» or commercial purpose; as a result, communications by a non-profit organisation can also fall within the scope of the direct marketing rules.
- **Solicited vs unsolicited**: both «solicited» and «unsolicited» commercial communications are covered.
- **Targeted online advertising & other means of communication**: the concept of «direct marketing» covers not only e-mail, SMS, direct messages on social media etc., but also targeted online advertising (based on e.g. IP address or other information linked to the recipient). Even advertising distributed by regular mail might be direct marketing if it is e.g. distributed only to non-clients.

Communications with customers and prospects will therefore often fall within the scope of the definition of «direct marketing».

In order to escape the classification as «direct marketing», it appears that communications must:
- not involve any processing of personal data (e.g. general publications on the organisation's website) or
- not have the intent of promoting anything (not even the brand), and be carried out solely for the relevant purpose (e.g. carrying out a customer satisfaction survey, without the aim of promoting products or services and without any collection of personal data for further use).

Controller vs processor, and reliance on social media terms of use

The guidance includes a reminder for organisations on how to determine whether they are controller or processor, with **nine** questions identified by the BDPA as relevant:
i. Who decides to collect personal data in the first place, and which type(s) of data to collect?
ii. Who determines the (categories of) persons targeted?
iii. Who decides on the (categories of) data to be collected?
iv. Who determines the purposes of the processing of the data?
v. Who decides on the legal grounds for the processing (consent, legitimate interests, etc.)?
vi. Who determines whether the data should be shared, and if so, with whom?
vii. Who decides on the content of the information to be provided to data subjects regarding the processing activity?
viii. Who determines the retention period for the data?
ix. Who decides on how to respond to data subjects exercising their rights?

According to the BDPA, **these decisions can only be taken by a controller**. As a result, if your organisation answers «we do» for even just one of those questions, your organisation will be «more than likely controller», says the BDPA. As a result, the BDPA is likely to consider two organisations as «joint controllers» if they each have the power to decide on at least one of those nine elements. The BDPA later states helpfully that the determination of the technical aspects of the processing, such as certain security measures, is not a decisive factor in the classification of a party as controller or processor. A processor can have greater expertise than the controller in relation to the technical measures to be taken, without this transforming the processor into a controller.

As a result, the processor can decide on secondary aspects related to the processing:
- the IT systems or other means to be used to collect personal data;
- the methods for storage of personal data;
- details regarding the security measures for the protection of personal data;
- the manner in which it will transfer personal data from one organisation to another;
- the manner in which it will collect personal data regarding certain individuals;
- the manner in which it will abide by the retention period;
- the manner in which it will delete or destroy the personal data in question.

However, the controller must remain free to refuse the processor's suggestions or at the very least to renegotiate the (framework) agreement between controller and processor.

The BDPA moreover notes that if an organisation processes personal data collected through social media platforms, the organisation itself must provide its own information to data subjects on how it processes the relevant personal data (Art. 13-14 GDPR). In other words, **the organisation cannot rely on the terms of use of the social media platform in question in relation to that information obligation** (also in relation to the sharing of personal data with the social media platform).

Using data brokers

The BDPA's guidance includes a section on data brokers, with specific instructions for organisations that might act as data broker. For organisations calling upon data brokers to enrich their datasets, the BDPA stresses the importance of providing information to data subjects in relation to the fact that the organisation itself has access to their (enriched) data, in accordance with Article 14 GDPR (and within the timeframe set out in that article).

Purposes of processing: «for direct marketing purposes» too vague?

The BDPA lists various examples of purposes of processing in the context of direct marketing, such as:
- Informing customers of the existence of new products or services;
- Creating a customer profile;
- Proposing personalised offers for customers' birthdays;
- etc.

According to the BDPA, this is the level of detail that has to be foreseen in the register of data processing activities and in the privacy statement. It states that in most cases, stating that *«we process your personal data for direct marketing purposes»* is insufficient to provide precise information, and that the level of detail required notably depends on the type of marketing communication (SMS, e-mail, telephone, etc.), its frequency (monthly, etc.), its content (newsletter, price reductions, etc.) or even the complexity of the processing (e.g. detailed profiling).

Right to object vs unsubscribe option

The BDPA makes an interesting comparison of the right to object under the GDPR and the «unsubscribe» option that is required for e-mail marketing under the e-Privacy anti-spam rules.

In this comparison, **the BDPA appears to suggest that an «unsubscribe» link might present «issues» for compliance with the GDPR requirements regarding the right to object**, notably for the following reasons:
- Unsubscribe links are typically in a small font size and easy to miss
- Wording such as «Unsubscribe» and «Do not contact me» *«does not imply that the processing of personal data for direct marketing purposes will end»*.

Instead of such a small «unsubscribe» link, the BDPA seems to suggest deploying a clearly marked «right to object» section in marketing e-mails, ideally located between the header elements (name of the organisation & title of the relevant offer) and the actual content (the offer itself), with even an integrated checkbox. From a functional perspective, though, the BDPA's recommendation to have a checkbox appears to ignore the vast discrepancies between e-mail clients and lack of uniform support for such functionality; it may have been more prudent to suggest having a link instead. More generally, the BDPA stresses that such right to object to processing for direct marketing purposes is in principle not limited to only direct marketing communications but also to direct marketing more broadly. As a result, if e.g. profiling activities were used in support of such direct marketing communications and were not used for any other purposes, they must cease as well.

Consent, transparency & new cookie guidance

A section on the conditions for consent includes various elements that refer to cookies, by virtue of which the direct marketing guidance also becomes a new form of cookie guidance by the BDPA. The BDPA thus illustrates **specific consent** by stating that in relation to cookies, this requires an indication of the precise purposes of cookie categories (e.g. distinction between first-party targeted advertising, third-party targeted advertising and audience metrics / analytics). It also stresses the fact that by default, intrusive and non-functional cookies must be inactive, and can only be placed after consent has been given.

On **unambiguous consent**, the BDPA uses cookies again as an illustration, stating that pre-ticked boxes will lead to invalid consent. In addition, the BDPA states that it is no longer possible to rely on further browsing as a basis for consent (i.e. informing a user that by continuing to browse on the website, he/she consents to the use of non-functional cookies). The BDPA suggests deploying alternatives to «Yes / No» buttons to combat so-called «cookie fatigue», such as consent sliders (sliding to one side to denote consent).

The BDPA stresses the need to be able to document consent, in particular in the case of orally given consent. On the duration of validity of consent, the BDPA merely states that comes down to common sense and that one must take into account the principle of proportionality. The BDPA examines also the issue of **withdrawal of consent**, with once more an illustration by way of cookies and more specifically third-party cookies. According to the BDPA, consent withdrawal for third-party cookies must be possible on the website itself, and consent will be invalid if the website merely refers to third-party websites on which the user must look for the manner of withdrawal of his consent.

Finally, the BDPA includes guidance on transparency (i.e. the obligation to inform data subjects regarding processing activities), and states that **privacy statements that are linked to in a website footer are inadequate** in its view. Instead, the BDPA wishes privacy statements to «*appear immediately on the screen, by inviting users of your website to read it*». In addition, the BDPA considers that the privacy statement **cannot be included in another document such as the terms & conditions of the organisation**.

The BDPA makes the same comment in relation to cookie policies, which must also be separate according to the BDPA.

Conclusion: changes afoot

The guidance introduces a range of new requirements, in particular as regards the contents and functionality of privacy statements (and links thereto), marketing e-mails (and «object» possibilities) and cookie banners & policies. In addition, the level of detail required in relation to the description of purposes suggests that registers of data processing activities will have to be revisited in many organisations. This guidance also comes at a time of heightened enforcement by the BDPA, with the most high-profile case being the recent cookie-related decision. While the fine it had imposed in that case (15.000 EUR) may appear small to some, it represented 1% of the turnover of the relevant company. But setting fines aside for a moment, it is useful to recall that the 2020s will be the decade of trust, and here transparency – that same transparency that underlies many of the BDPA's considerations in this guidance – plays a fundamental role.

Vincent WELLENS (picture),
Avocat à la Cour (Luxembourg) / Advocaat (Brussels),
Partner IP & Tech law | NautaDutilh
vincent.wellens@nautadutilh.com

Peter CRADDOCK,
Avocat (Brussels), Counsel Tech law | NautaDutilh
peter.craddock@nautadutilh.com