[doc. web n. 4304228]

Guidelines on Marketing and against Spam - 4 July 2013

THE ITALIAN DATA PROTECTION AUTHORITY

Having convened today in the presence of Mr. Antonello Soro, President, Ms. Augusta Iannini, Vice-President, Ms. Giovanna Bianchi Clerici and Prof. Licia Califano, Members, and Mr. Giuseppe Busia, Secretary General;

Having regard to directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and to directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by directive 2009/136/EC;

Having regard to the Personal Data Protection Code (legislative decree No. 196 of 30 June 2003, hereinafter "Code");

Having regard to the DPA's decision of 29 May 2003 called "Spamming: Rules for the Appropriate Use of Automated Systems and for Sending Electronic Communications" (web doc. No. **29840**);

Having regard to the DPA's decision of 19 January 2011 laying down "Requirements Applying to the Processing of Personal Data for Marketing Purposes as Performed by Relying on Operator-Assisted Telephone Calls Following Establishment of the Public Opt-Out Register" (web doc. No. 1784528);
Having regard to the DPA's decision of 15 June 2011 concerning "Controllership of Processing as Vested in the Entities Outsourcing Promotional Activities" (web doc. No. **1821257**);

Having regard to the opinions rendered by the "Article 29" Working Party (Nos. 4/1997, 5/2004, 5/2009, 1/2010, 4/2010, 15/2011); to Recommendation No. 2/2001 by the said Working Party on certain minimum requirements for the online collection of personal data in the European Union; and to the Resolution on the use of personal data for political communication as adopted by the 27Th International Conference of data protection and privacy commissioners held in Montreaux on 14-16 September 2005 (web doc. No. **1170546**);

Having regard to the "Decision on Applicability of the Personal Data Protection Code to Legal Persons Following the Amendments Made by Decree No. 201/2011 of 20 September 2012" (web doc. No. **2094932**);

Having regard to official records and the considerations made by the Secretary General pursuant to Article 15 of the DPA's Rules of Procedure No. 1/2000;
Acting on the report submitted by Mr. Antonello Soro;

RESOLVES

a. To adopt the document containing the "Guidelines on Marketing and against Spam", which is annexed hereto and is an integral part hereof, pursuant to Section 154(1), letter h), of the Code (Annex 1);

b. To forward a copy of this resolution along with the said Annex to the Ministry of Justice in order for them to published in the Official Journal of the Italian Republic, pursuant to Section 143(2) of the Code.

Done in Rome, this 4th day of the month of July in the year 2013.

The President
Soro

The Rapporteur
Soro

The Secretary General
Busia

ANNEX 1

GUIDELINES ON MARKETING AND AGAINST SPAM

Table of Contents

1. Scope and Purposes

The "Rules for the Appropriate Use of Automated Systems and for Sending Electronic Communications" were issued by the Italian DPA on 29 May 2003 to address spamming issues (i.e. the unsolicited sending of promotional messages and advertising materials); they were based on the legislation then in force, in particular on the DP Act No. 675 of 31 December 1996.

Following entry into force of the Code, the above Act was repealed along with other data protection legislative instruments, whilst the relevant principles were reaffirmed against a different regulatory backdrop. More recently, in particular from 2009 onwards, several amendments were made to the Code that also impacted on its scope of application as to the protection afforded to individual entities and the rights that are actionable by spam recipients. This makes it necessary for the DPA to reconsider the issue in question.

It should be noted that complaints and claims continue to be lodged with the DPA, albeit to a lesser degree than in the past, concerning the conventional types of spam as mentioned in the Code. Furthermore, new criticalities and new types of spam have been surfacing over the years such as to give rise to increasingly subtle intrusions into data subjects' private lives. They include viral marketing, marketing via technological platforms owned by third parties that are often established abroad (and are difficult to locate), "targeted marketing" based on user profiling mechanisms, and the so-called "social marketing". It should also be recalled that spam increasingly affects children, who are entitled to enhanced protection by the legal system and accordingly by this DPA as well.

As a consequence, this DPA considers it necessary to adopt the Guidelines below in order to

- Take account of the changes brought about in the relevant regulatory framework by the entry into force of the Code and the subsequent amendments thereof as well as by EU law (directives 2002/58/EC and 2009/136/EC), and also ensure uniform application of the said regulatory framework including compliance with the fundamental principle of the rule of law;

- Clarify some criticalities in connection with the different types of spam to ensure that industry operators are compliant with personal data protection legislation;

- Focus on some novel forms of spam to limit the risks arising from technological innovations whilst being fully aware that the law cannot but provide partial solutions vis-à-vis the unrelenting evolution of increasingly advanced, fast-uptake technologies.

2. The New Regulatory Framework Applying to Spam

2.1. Spam: Definition of Factual Scope

It is necessary in the first place to define what spam is. Under the terms of the Code, spam is any communication performed for the purposes of sending advertising materials, direct selling, carrying out market surveys or commercial communications where such communication takes place in breach of the Code via automated, operator-unassisted calling systems (i.e. via

pre-recorded calls) or via similar mechanisms (such as emails, faxes, SMS-texting, or MMS-messaging) - see Section 7(4), letter b), Section 130(1), and Section 140 of the Code.

For the purposes of applying the Code, the fact that communications are sent in bulk and/or simultaneously to multiple accounts or phone numbers is irrelevant, whilst it is only to be taken into account in order to class the processing at issue as systematic in nature and determine the applicable sanctions accordingly.

2.2. Spam: Entities Concerned and Actionable Remedies

Given the major regulatory innovations – of which more below -, it is also necessary to clarify the scope of application of the spam-related provisions in the Code as for the entities concerned along with the actionable remedies as afforded to the recipients of automated promotional communications. Whilst natural persons may exercise the rights set forth in Section 7 and ff. of the Code in order to protect their personal spheres against unlawful intrusions, legal persons are currently deprived of the opportunity to rely on these remedies.

Consideration should be given in this respect to Section 40(2) of decree No. 201 of 6 December 2011 – subsequently enacted as Act No. 214 of 22 December 2011 – whereby a few of the "General Provisions" in the Code were amended including, for instance, Section 4 thereof as for the definitions of "data subject" and "personal data". In particular, all references to legal persons or similar entities were removed from the scope of such definitions, which only encompass natural persons as of today.

Legislative decree No. 69 of 28 May 2012 was then adopted to transpose Directive 2009/136/EC by amending some provisions in Chapter 1 of Title X of the Code ("Electronic Communications – Electronic Communications Services") – which transpose and are modeled closely after Directive 2002/58/EC and apply to automated promotional communications. More specifically, the definition of "contracting party" was introduced to replace that of "subscriber", and such new definition applies unquestionably to legal persons as well.

Following the above regulatory amendments, interpretive issues arose and the DPA decided to shed light on such issues by way of a decision adopted on 20 September 2012 (web doc. No. 2094932) regarding applicability of the Code to legal persons, organizations and associations.

Based on the above interpretive clarification, it should be pointed out that as of 6 December 2011 legal persons and similar entities receiving spam may no longer lodge claims or complaints with the DPA or exercise the rights set forth in Section 7 and ff. of the Code – contrary to what is the case with natural persons – because they are no longer to be considered as "data subjects".

Still, legal persons and similar entities may rely on the standard remedies made available by our legal system insofar as they are "contracting parties" – that is, they may seize judicial authorities under civil law to e.g. apply for injunctive orders or claim damages; if the preconditions set forth in Section 167 of Italy's Criminal Code are fulfilled, they may also lodge a criminal report and initiate criminal proceedings to obtain imposition of the applicable penalties. Moreover, they may benefit from the remedies this DPA is empowered to afford of its own motion – via prohibitory or injunctive orders and/or via the imposition of sanctions – if there is reason to believe that a given data processing operation is in breach of the law.

Regarding e-mails, it may prove difficult to tell whether the recipients are natural or legal persons.

This may be the case of the employees at a given company where the latter has made available corporate email accounts that include the employees' names – such as firstname.lastname@company.com.

In line with the clarification provided by the "Article 29" Working Party via its Opinions No. 4/1997 and 5/2004 as well as based on the "contents", "purposes" and "outcome" criteria that are referred to therein in order to determine whether certain items of information on legal persons "relate" to natural persons, the above accounts should be regarded as "personal" email accounts and the respective holders as "data subjects"; accordingly, the Code is applicable along with all the rights and remedies provided for therein. This is without prejudice to the provisions already made concerning corporate emails via previous decisions of the DPA on the processing of employees' data – see, in particular, the "Guidelines on E-Mails and the Internet" of 1 March 2007, web doc. No. **1387522**.

2.3. Principles of Fairness, Purpose Limitation, Proportionality and Minimization of Data Processing. Technological Neutrality

As well as other provisions of the Code, Sections 3 and 11 apply to automated communications; accordingly, the personal data at issue – in particular phone numbers and email addresses – must be used and stored in compliance with fairness, purpose limitation, proportionality and data minimization principles and may not be used further if a breach of the Code is committed.

Regarding emailed promotional communications, this DPA emphasizes that email service providers should ensure mutual authentication of their servers in compliance with the technological neutrality principle so that users can be afforded the highest possible spam protection levels. This is all the more important if one considers the harm caused by activities like the so-called phishing – i.e., sending counterfeited emails that contain graphical information and logos identical to those of the genuine senders, including banks or post offices or public institutions. Phishing emails are used to urge recipients to provide their personal data on technical or business grounds whilst the underlying motives are actually unlawful – e.g. getting access to the password used for one's online bank account or credit card services and thus syphon off moneys or otherwise perform activities that can affect one's legal and business status.

In particular, providers should install ad-hoc filtering systems to detect spam with a reasonable degree of certainty; however, such systems should not be such as to violate data subjects' privacy.

2.4. The Obligation to Provide Information Clearly and Thoroughly under Section 13 of the Code

A key obligation applying to data controllers consists in informing the recipients of promotional communications beforehand under the terms of Section 13 of the Code. This is aimed to ensure, on the one hand, that the recipients are informed clearly and thoroughly, i.e. appropriately, on the processing of their data and, on the other hand, that the recipients' consent, if necessary, is based on their full information.

Accordingly, the data subject or the individual whose personal data are being collected must be provided beforehand, verbally or in writing, with a set of indispensable informational items – including what mechanisms are expected to be used in processing the data, with particular regard to those mentioned in Section 130(1) and (2), i.e. automated phone calls and similar arrangements such as faxes, emails, SMS-messaging and MMS-messaging, as well as to conventional mechanisms such as paper mailing and operator-assisted calls, along with the purposes served by the processing such as statistical research, marketing or profiling purposes.

It should also be recalled that the above requirements apply to any processing operation for promotional purposes where performed via automated or similar tools; therefore, if the recipients' personal data are not collected directly from them, the information in question – including the categories of processed data – must be provided when the data are recorded or no later than when they are first communicated if such communication is envisaged (see Section 13(4) of the Code).

2.5. The Obligation to Obtain Prior Consent (Opt-In Requirements)

Processing for promotional purposes where performed by way of automated or similar tools falls under the scope of application of Section 130(1) and (2) of the Code; accordingly, such tools may only be used for marketing purposes with the contracting party's or user's prior consent (opt-in requirement).

In terms of making sure that a promotional communication is sent legitimately, it is therefore unlawful to inform recipients that they can object to further communications at the time such a promotional communication is first sent or to request their consent to the processing of their personal data for promotional purposes jointly with such a communication.

As a consequence, it is not permitted to send promotional communications by way of the aforementioned tools without the recipients' prior consent – not even if the personal data have been taken from publicly available sources, directories, web sites, records or documents. This has been emphasized consistently by the DPA, starting from its decision on spamming of 29 May 2003 (web doc. No. 29840).

By the same token, the PEC [certified email] addresses contained in the "National Register of PEC addresses for companies and professionals" set up under decree No. 179 of 18 October 2012, which introduced Section 6a into legislative decree No. 82 of 7 March 2005 (the "Digital Administration Code"), may not be used to send promotional emails without the data subjects' prior consent; indeed, the Register in question was set up to foster the electronic lodging and handling of applications, statements and records along with the exchange of information and documents as part of the relationships between public administrative bodies and businesses or professionals. Conversely, the subscribers listed in telephone directories that have not signed up to the opt-out Public Register (set up under decree No. 135 of 25 September 2009, which then became Act No. 166 of 20 November 2009 including amendments thereof) may be contacted via operator-assisted phone calls to ask for the contracting parties' consent to receiving promotional communications by way of the mechanisms mentioned in Section 130(1) and (2) of the Code. This also applies to the telephone numbers contained in publicly available directories "in compliance with the limitations and arrangements set forth in laws, regulations or Community legislation as for disclosure and publicity of the data" – which include "the purpose limitation constraint, whereby all personal data must be collected and recorded for specific, explicit and legitimate purposes and may be used in other processing operations under terms that are compatible with such purposes (see Section 11(1), letter b), of the Code)" (see the DPA's decision of 19 January 2011, web doc. No. **1784528**).

It should be pointed out additionally that the principle of prior consent to data processing is also set forth in consumer protection laws regarding distance contracts – whereby the consumer's prior consent is required if a company plans to use telephone calls, emailing, faxes or automated operator-unassisted calling systems (see Section 58 of legislative decree No. 206/2005, i.e. the so-called Consumer Code).

2.6. Valid Consent to Send Promotional Communications

Consent obtained to send promotional communications must be free, informed, specific; it must relate to processing operations that should be set out clearly; there must be written proof of such consent (see Section 23(3) of the Code). Accordingly, consent is only valid if all the foregoing requirements are met.

Based on the considerations made, inter alia, in paragraph 2.4 above, data subjects must be enabled to signify their choices knowingly and freely as for the processing of their personal data (see the DPA's decision of 24 February 2005, paragraph 7 – web doc. No. 1103045). To that end, data subjects must be informed appropriately, i.e. clearly and thoroughly, as explained above.

A contracting party's consent to promotional activities can be regarded as freely given if it does not represent the default setting or if it does not translate – even only factually or implicitly – into a precondition to obtain the product or service being offered by the data controller.

For instance, consent is not free if a company makes signing up to its website and using the relevant services conditional upon giving one's consent to processing for promotional purposes. From this standpoint, the Italian DPA has already clarified that consent is not "free" and is turned unlawfully into a precondition if the data subject "must" consent to further processing operations in order to obtain the specific service of interest (see various decisions by the DPA: 22 February 2007, web doc. No. **1388590**; 12 October 2005, web doc. No. **1179604**; 3 November 2005, web doc. No. **1195215**; 10 May 2006, web doc. No. **1298709**; 15 July 2010, web doc. No. **1741998**; 11 October 2012, web doc. No. **2089777**).

By the same token, it is not acceptable that forms are made available where the consent checkbox is flagged by default – see the DPA's decision on "Consent to Processing on the Internet and Use of Data for Promotional Purposes" of 10 May 2006, web doc. No. 1298709.

The contracting party's consent must be given specifically for each purpose being sought and for each processing operation at issue – including, in particular, disclosure of one's personal data to third parties who will then be enabled to send their own promotional communications; the guidance and clarification provided in the paragraphs below should be taken into due account.

2.6.1. Purposes of Processing

As for the purposes for which personal data are processed, it is to be reiterated that a data controller should obtain a specific consent statement for each separate purpose such as marketing, profiling, disclosure of the data to third parties (see decision of 24 February 2005, paragraph 7 – web doc. No. **1103045**).

However, one of the peculiarities of processing operations for promotional purposes should be highlighted here. Under Section 7(4), letter b), Section 130(1) and Section 140 of the Code, marketing-related purposes are manifold as they include the delivery of advertising materials, direct selling, performance of market surveys, and commercial communications – see Opinion No. 4/2010 of the "Article 29" Working Party on FEDMA's European Code of Conduct for the use of personal data in online direct marketing. Thus, it should be clarified whether consent is to be given specifically for each of those purposes. This DPA is of the opinion that the activities in question are mostly instrumental to the achievement of a single purpose, i.e. broadly speaking the marketing purpose; accordingly, obtaining one consent statement for the relevant processing operations would appear, as a rule, to be justified – see, inter alia, the DPA's decisions of 9 March 2006, web doc. No. **1252220**; 24 May 2006, web doc. No. **1298784**; 15 November 2007, web doc. No. **1466985**.

This view has already been endorsed in other decisions – such as the one of 31 January 2008, web doc. No. **1490553** – as well as being grounded in the Opinion No. 15/2011 of the "Article 29" Working Party regarding the definition of "consent", whereby the need for obtaining consent should be evaluated by taking account of the purposes to be achieved and/or the recipients of the data at issue. The ultimate objective is preventing the needless multiplication of consent statements, which is actually in line with Section 2(2) of the Code – whereby the data simplification principle is also to be implemented in setting out the arrangements to meet the obligations imposed on data controllers.

The approach in question is consistent with the purpose specification principle, which requires data to be used in "other" processing operations in a manner that must be "compatible" with the purposes for which such data was collected initially (see Section 11(1)b) of the Code).

2.6.2. Consent for Marketing Purposes (including conventional marketing and marketing activities as per Section 130(1) and (2) of the Code)

In order to simplify the arrangements related to the processing of personal data, this DPA considers that the requirement of obtaining specific consent may be legitimately construed to entail – as regards the various marketing mechanisms - that two separate, specific consent statements be collected in respect of conventional marketing and marketing activities as per Section 130(1) and (2) of the Code, respectively; alternatively, a single consent statement may be obtained with regard to both types of marketing.

In the latter case, it has been already clarified (see paragraph 2.4 on information obligations) that the individual marketing mechanisms must be specified – i.e., it must be specified whether conventional marketing channels or the marketing methods mentioned in Section 130(1) and (2) are relied upon; at the same time, measures to safeguard the data subjects' right to the protection of their personal data will have to be taken. In particular:

The information notice and consent request must be such as to clarify that the consent provided for marketing and commercial communications under Section 130(1) and (2) of the Code also applies to the conventional marketing mechanisms specified in the information notice, such as mailings and/or operator-assisted phone calls;

The information notice must clarify that the data subject's right to object to processing of his/her personal data for the above purposes as performed via automated mechanisms also applies to conventional marketing and that the data subject may in any case exercise that right also partly, e.g. by objecting only to marketing communications via automated means (under Section 7(4)b) of the Code).

2.6.3. Specific Consent to Communicate and/or Transfer Data to Third Parties for Marketing Purposes

It has been found in handling cases submitted to this DPA that some data controllers obtain, by way of contractual forms or ad-hoc online forms, a general statement of consent to processing for marketing purposes whether pursued by them or by third parties they communicate (and/or transfer) the personal data to; in so doing, such data controllers do not specify

who such third parties may be either in the information notices or in the consent forms, nor do they specify the respective business or commodity categories.

This issue is clarified accordingly in the paragraphs below by having regard both to communications made generally to third parties for marketing purposes and to the specific cases where the third-party recipient of the data collected for marketing purposes is a subsidiary, parent or related company in respect of the entity that had collected the personal data initially.

As for the communications made generally to third parties for marketing purposes, it should be noted, in the first place, that it is not permitted to communicate or transfer personal data to third parties for marketing purposes based on a single, unspecific statement of consent obtained from data subjects for marketing purposes (see several decisions by the DPA: 11 October 2012, web doc. No. **2089777**; 19 May 2011, web doc. No. **1823148**; 12 May 2011, web doc. No. **1813953**; and many more).

Thus, a data controller planning to collect personal data also with a view to communicate (or transfer) such data to third parties for the third parties' marketing purposes must first inform data subjects appropriately under Section 13(1) of the Code; this means that, as well as the items mentioned therein, the information notice must specify the individual third parties or else the respective (business or commodity) categories – e.g. "financing", "publishing", "clothing", see letter d) of the aforementioned Section 13(1).

Furthermore, the data controller must obtain specific consent to communicate and/or transfer the personal data to third parties for marketing purposes; such consent must be obtained separately from the consent requested by the data controller in order to perform marketing activities of its own.

Where a data subject gives his/her consent to communicate the personal data to third parties, those third parties may use the data for marketing activities of the type mentioned in Section 130(1) and (2) of the Code vis-à-vis the data subject without obtaining an additional consent statement for such marketing purposes.

Under the terms of the Code, the third parties in question may belong to business or commodity categories other than the one applying to the data controller that collects the data from the data subject.

If the third parties are detailed individually and the information notice to the data subject includes the additional items mentioned in Section 13 of the Code as for the processing such third parties may carry out, there will be no need for the third parties in question to provide additional information notices to the data subject: under Section 13(2) of the Code, the notice "may fail to include information that is already known to the data subject."

Conversely, if the consent request is not supported by an information notice that meets the above requirements, the third parties may only send marketing materials to the data subjects after providing them with specific information notices of their own (under Section 13(4) of the Code); those information notices must include, on top of the items mentioned in Section 13(1), a reference to the source of the personal data disclosed to them, so that every data subject is enabled to apply to the entity that had collected and disclosed the data initially in order to object to such processing under Section 7(4)(b) of the Code.

In either case the third parties must provide the contact details mentioned in Section 130(5) of the Code to allow data subjects to exercise Section 7 rights (see decision of 7 April 2011, web doc. No. 1810207); data subjects must be in a position to rely for this purpose on the same communication channel used for sending them the marketing messages, or anyhow on tools that are as user-friendly, quick, inexpensive and effective as possible (see, in this regard, the Article 29 Working Party's Opinion No. 5/2004).

For instance, if a third party plans to email ads, the data subject must be enabled to object to this processing by emailing his/her objection to an email account specified in the information notice; the account might be created on purpose to handle data protection issues.

The above holds true if the third-party recipients of the data disclosed or transferred by the initial data controller are subsidiary, parent or related companies in respect of the latter.

Regarding consent, this DPA has already provided clarifications on several occasions (see decision of 23 November 2006 including Guidelines on processing employees' personal data to manage employment relationships in the private sector, web doc. No. 1364099, and many others). In particular, it is to be reiterated that the members of a corporate group should be considered, as a rule, to be separate data controllers for the purposes of obtaining data subjects' consent.

2.6.4. Written Proof of Consent

Written proof of consent is also required for marketing purposes.

It should be pointed out that directive 2002/58/EC does not lay down specific mechanisms to obtain such consent (see Recital 17: "(…) 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 an Internet website.")

Hence, the industry is free to select the method they consider to be most appropriate by taking account of the existing organizational structure. Moreover, there is no need for consent to be provided in writing, whilst it is necessary for the data controller to take suitable measures to provide proof of such consent by making available evidence that the consent had been obtained and detailing the circumstances under which it had been obtained. In particular, there must be documentary

proof – under whatever form – of the date when consent was given and the identity of the person obtaining such consent. Similar procedures should be in place to make sure that the data subject's wishes are respected in full if the latter decides to withdraw his/her consent (see decision of 30 May 2007, web doc. No. **1412598**).

Mechanisms may be usefully implemented to confirm the identity of a contracting party that has signed in to a website to receive promotional materials. For instance, one might email an ad-hoc message to the contracting party's account and ask him/her to confirm identity by clicking on a specific link.

2.7. Soft Spam as an Exception to the Rule Regarding Promotional Emails

It should be recalled that the consent exemption conditions mentioned in Section 24 of the Code do not apply to the communications referred to in Section 130(1) and (2).

However, the so-called "soft spam" exception may apply to emails as per Section 130(4) of the Code; that is to say, if the data controller uses, to directly sell own services or products, the email contact information that was made available by the data subject within the framework of the sale of a product or service, that controller may do without the data subject's consent - providing the product or service in question is similar to the one previously sold and the data subject does not object to the use of his/her data after being informed appropriately.

3. Data Controllership in Case of Spamming Via Agents and/or Other Third Parties

The Garante has found that, in some cases, marketing communications are not sent directly by the company marketing the given products/services, since agents or third parties acting on the company's behalf are relied upon. This makes it necessary to clarify whether data controllership under Section 28 of the Code lies with the marketing company or the third party agent so as to determine the respective obligations accordingly.

The Guidelines issued by the Garante on 15 June 2011 are relevant in this respect; such Guidelines addressed "Establishing data controllership if agents are relied upon for marketing purposes" (web doc. No. **1821257**) and can be usefully referred to here since part of the considerations and arguments made therein also apply to marketing performed in the manner described in Section 130(1) and (2).

Mention should also be made of the Article 29 Working Party's Opinion No. 1/2010, which further clarified that "other elements than the terms of a contract may be useful to find the controller, such as the degree of actual control exercised by a party, the image given to data subjects and reasonable expectations of data subjects on the basis of this visibility." The Opinion emphasized that a company outsourcing marketing campaigns to third parties should be regarded as the controller of the processing of the personal data relating to the recipients of such marketing communications, taking account that the third parties in question were given specific instructions and the company must verify compliance with such instructions and the contractual terms agreed upon. Accordingly, the third parties will have to be appointed as data processors under Section 29 of the Code, whilst the individual operators will have to be appointed as persons tasked with the processing of data under Section 30 thereof.

The above also applies if marketing communications are performed in the manner described beforehand, since the way marketing is performed is irrelevant in determining who the data controller is.

Indeed, this Authority already emphasized (see the decision of 16 February 2006, web doc. No. **1242592**) regarding unsolicited telephone services that sellers or agents marketing products or services on behalf of another company must be appointed as data processors if this is actually what they are in terms of their data processing status. Furthermore, in a decision of 29 April 2009 (web doc. No. **1617709**) addressing the actual relationship between a data controller and several operators tasked with supplying individual services, the Garante found that the circumstance whereby such operators acted on instructions and under the supervision by the outsourcing company was of paramount importance in establishing that the latter was the sole controller of the processing; accordingly, the company in question was required to appoint the contractors as data processors under Section 29 of the Code.

In the light of the above considerations and criteria, this Authority draws the following conclusions as for spamming activities performed via agents and/or other third parties. If the marketing company plays factually a leading role in processing recipients' personal data by deciding on purposes and mechanisms of the processing, providing instructions and binding directives, and performing checks and controls on the agent's activities, such company must be considered to be the data controller under Section 28 of the Code independently of contractual qualifications. Furthermore, the marketing company is required to appoint the agent or any other third party as a data processor, except for the natural persons that only process personal data under the marketing company's direct authority and on the basis of the company's instructions – who are to be appointed as persons tasked with the processing ("incaricati").

Additionally, the Garante considers it necessary for the marketing companies to implement suitable measures and procedures to establish whether a contractor tasked with processing data via automated means for marketing purposes relies, in turn, on sub-contractors or other third parties to carry out the processing in question, and to verify and make sure that such sub-contractors or other third parties are compliant with the Code. This requirement applies both if the marketing companies are factually to be regarded as the data controllers – in which case they will have to appoint the sub-contractors or other third parties involved in the processing "chain" as data processors or persons tasked with the processing ("incaricati"), as the case may be (see Sections 29-30 of the Code), and will be liable for any breaches of the Code committed by them – and if the sub-contractors or other third parties rely on their own databases for the marketing purposes – in which case they are to be considered separate data controllers. The latter requirement is grounded in the need to enable the marketing company receiving an access or similar request under Section 7 of the Code to clarify the role it plays

factually vis-à-vis sub-contractors and thus direct the applicant to the entity that is the actual data controller in the specific case.

4. Unsolicited Faxes Sent Via Platforms Owned by Companies Abroad

Several complaints continue to be lodged with the Garante, albeit to a lesser extent than in the past, against unsolicited faxes that are sent (or attempted to be sent) at all times in a day. The promotional messages received in this manner do not always specify who the data controllers are and how they may be contacted in order to object to further messages, nor is there adequate information on data processing operations.

Based on sometimes complex inquiries, the Garante could establish that spam faxes sent from abroad mostly come from companies that provide this fax delivery service to Italian customers (companies, etc.); to that end, two separate channels are used, i.e. the Internet to send the faxes from the fax server abroad to the fax gateway located in Italy, and the Italian public telephone network for transmitting the fax from the fax gateway to user terminals.

As already clarified in the aforementioned decision by the Garante of 7 April 2011, the processing in question falls under the scope of application of the Italian data protection Code – whose Section 5(2) provides that the Code applies to any entity that "…makes use in connection with the processing of equipment, whether electronic or otherwise, situated in the State's territory, unless such equipment is used only for purposes of transit through the territory of the European Union." Accordingly, the case at issue must be addressed by determining who the data controller is and what obligations apply.

Depending on the specificities of the case and, in particular, on the role played in selecting the recipients as well as the purposes and means of the processing, the data controller may be the company or entity relying on such platforms as owned by third parties or the entity owning any such platform if the latter is used to perform marketing activities for the entity's own purposes.

In particular, the Garante considers it necessary for the data controller to make available, on each outbound message, a box containing an appropriate information notice – without prejudice to obtaining the recipients' prior specific and informed consent under Sections 23 and 130 of the Code; furthermore, the data controller must enable exercise of the rights set forth in Section 7 of the Code via expeditious, user-friendly and effective mechanisms.

5. Lists Used to Send Multiple E-Mails or Text Messages

It is sometimes the case that lists containing email addresses and/or phone numbers are used to simultaneously send one marketing message to several recipients.

Whoever relies on this mechanism for marketing purposes much comply with the principles and rules mentioned above by having regard to the legislation in force – in particular to Sections 3, 11, 13, 23 and 130 of the Data Protection Code – for each of the email addresses being considered.

In fact, these marketing emails sometimes show the addresses of all the other recipients of the given message, who are enabled thereby to become apprised of this information and may use such addresses for the most diverse purposes – including for additional spamming.

Marketing performed via non-blinded email listings gives rise actually to the communication of personal data (i.e. the data coming from the other email addresses) to third parties, being the recipients of the marketing message.

Thus, the email addresses used to send promotional messages must be kept confidential – for instance by entering them in the "Bcc" (Blind carbon copy) field.

6. New Types of Spam

Against the legal background detailed in the foregoing paragraphs, the Garante is providing the necessary general guidance below to take account of some new spam types and mechanisms that are currently not regulated explicitly by law. This is aimed partly to prevent the huge potential of the Internet and IT in general from allowing, in factual terms, the blanket and/or illegitimate use of personal data.

6.1. Social Spam

The so-called social spam consists in several activities that allow a spammer to send messages and links via online social networks. This is part of the bigger issue of users' making use of their personal data recklessly and inadvertently on social networks – which is compounded if "open" user profiles are involved. This situation lends itself to marketing activities and/or other processing operations concerning personal data that are performed for marketing and profiling purposes by third parties, which may be commercial partners of the SNS companies and/or take advantage of the factual availability of such data on the Internet. Furthermore, SNS being social networks of real individuals, spammers can target the contact lists of certain users to enhance the viral potential of their messages.

The Garante would like to recall in this regard that the circumstance whereby personal data (such as phone numbers or email addresses) can be retrieved easily on the Internet does not allow using such data to send automated marketing messages without the recipients' consent.

Any marketing message sent to SNS users whether in private or via their public notice boards is subject to the provisions of the Code – in particular to Sections 3, 11, 13, 23 and 130 thereof.

The same applies to marketing messages that are sent via increasingly widespread services or tools such as Skype, WhatsApp, Viber, Messanger, etc.. Here one should be mindful of the spam proliferation risk, since these services/tools may entail the sharing of all the personal data on one's smartphone or tablet (addresses, contacts, text messages, browsing data) – which is actually referred to in the respective terms of service – or else may allow the service provider to access the contact lists and/or the address book on one's mobile phone in order to retrieve or store such personal data.

The risk of receiving spam, in particular "targeted spam", based on user profiles might be increased because of the preference shown by the providers of such platforms towards simplified privacy policies that allow merging profiles from different services on a given platform and therefore enable increasingly detailed information to be gathered on users – who may thus receive customized messages depending on their interests and preferences as retrieved from multiple applications.

This practice may, on the one hand, facilitate producer-to-consumer relations because it can reduce marketing costs for the former and product search costs for the latter; on the other hand, it may also reduce the recipient's freedom to make use of information society services (on top of receiving spam) since he/she is being profiled irrespective of his/her consent.

Having said that, one should point out that messages sent for exclusively personal purposes remain fully lawful; however, one may also highlight cases in need of clarification from a regulatory standpoint.

One such case is where the user receives a marketing message relating to a specific product or service from a company that obtained the user's personal data from the user's profile on a SN – irrespective of whether the message is sent privately, to the user's notice board or to the email account specified on the user's SN profile.

Another such case is where the user is a "fan" of a given company or has joined a "group" of followers of a given brand, personality, product or service – i.e., the user has decided to "follow" the relevant news, events or comments – and then receives marketing messages related to such brand, product, service or company.

In the former case, the processing shall be considered unlawful unless the sender can show proof of the recipient's prior, specific, and free consent under the terms of Section 130(1) and (2) of the Code.

In the latter case, marketing messages concerning a given brand, product or service as sent by the company managing the relevant page may be considered to be lawful if it can be inferred unambiguously from the context or the operational arrangements of the SNS, also based on the information provided, that the recipient did intend in this manner to also signify his/her intention to consent to receiving marketing messages from the given company. Conversely, if the recipient unsubscribes from the group or stops "following" the brand or personality, or objects to further marketing messages, any marketing message sent thereafter will be unlawful and may carry the applicable punishments. This is without prejudice to the option of blocking messages from specific contacts and/or reporting possible spammers that is offered to users by some SNS.

Regarding an user's "contacts" (i.e. the so-called "friends"), it is often the case that a SNS or a community can access all the phone numbers or email addresses pertaining to that user; marketing messages may only be sent lawfully to such "contacts" or "friends" if a specific (marketing-related) consent statement is obtained beforehand from each of them.

6.2. "Viral" Marketing

"Viral" marketing is a marketing mechanism exploiting the communication potential of a bunch of direct recipients to convey a message to a substantial number of end-users. It evolved from the "grapevine" approach, from which it differs because the marketers' intention to initiate a promotional campaign is unquestionable from the start. Like a virus, the message containing the concept, product or service that may prove interesting to a user is conveyed by that user to other contacts, who in turn pass it on to yet other contacts, and so on.

"Viral marketing" is usually referred to Internet users that suggest or recommend certain products or services to other users. Of late, this marketing technique is being used increasingly for products that are not directly related to the Internet; however, the channel used for conveying messages remains the web community where communication is fast, free and friendly.

To facilitate dissemination, marketers offer incentives, bonuses or other benefits to the recipients, who accept in exchange to forward (sometimes to email or text) the marketing message to other recipients.

Where the above activity is performed via automated tools for marketing purposes, it may be a type of spam if the principles and rules set out above fail to be complied with as part of the legislation in force – with particular regard to Sections 3, 11, 13, 23 and 130 of the Code.

At all events, the Code does not apply if a user, having received a marketing message, forwards such message on a purely personal basis – to recommend a given product or service to own friends - via automated tools. Conversely, the Code does apply to the processing of data performed by a user that forwards or discloses such a marketing message to multiple recipients after obtaining their personal data (phone numbers, email accounts) from either public directories or the Web.

7. Sanctions

It should be recalled here as regards the various types of spamming that the Garante, having established a breach of the provisions in the Code and subject to the adoption of prohibitory or injunctive measures, is empowered to apply

administrative sanctions including, in particular, those set out in Sections 161 and 162(2 a) of the Code in order to ensure compliance with the fundamental requirements of providing an information notice and obtaining consent, respectively.

Additionally, the Garante is required to inform judicial authorities of any facts that amount to criminal offences to be prosecuted ex officio if it has reason to believe that a data processing operation is unlawful and in breach of specific criminal law provisions; imposition of the criminal penalty set forth in Section 167 of the Code will be up to the judicial authority.