SEE ALSO PRESS RELEASE OF 2 APRIL 2021

[doc. web no. 9570997]

Injunction against Fastweb S.p.A. - March 25, 2021

Register of measures

no. 112 of 25 March 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, prof.ssa Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, components and the cons. Fabio Mattei, general secretary;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46 /CE (General Data Protection Regulation, hereinafter "Regulation");

HAVING REGARD TO the Code regarding the protection of personal data (legislative decree 30 June 2003, n. 196), as amended by legislative decree 10 August 2018, n. 101, containing provisions for the adaptation of the national legal system to the aforementioned Regulation (hereinafter the "Code");

HAVING REGARD to the documentation in the deeds;

HAVING REGARD TO the observations made by the general secretary pursuant to art. 15 of the Guarantor's regulation n. 1/2000, adopted with resolution of 28 June 2000;

SPEAKER Dr. Agostino Ghiglia;

1. THE INVESTIGATION ACTIVITY CARRIED OUT

1.1. Premise

With deed no. 44174/20 of 20 November 2020 (notified on the same date by certified email), which must be understood here as reproduced in full, the Office has initiated, pursuant to art. 166, paragraph 5, of the Code, a procedure for the adoption of the provisions pursuant to art. 58, par. 2 of the Regulation against Fastweb S.p.A. (hereinafter "Fastweb" or "the Company"), in the person of its pro-tempore legal representative, with registered office in Milan, Piazza Adriano Olivetti 1, Tax Code and VAT number: 12878470157.

The proceeding originates from a complex investigation initiated by the Authority following the receipt of hundreds of reports

and complaints sent by interested parties who complained, and still complain today, of continuous unwanted telephone contacts made by Fastweb and its sales network to promote the services telephony and internet offered by the same.

The phenomenon of unwanted promotional calls and contacts is known to the Company, which, over the past ten years, has been the subject of various prescriptive and injunctive measures, as well as numerous administrative sanctions, most of which are defined in short terms. In particular, the provisions n. 300 of 18 October 2012 (in www.gpdp.it, web doc. n. 2368171), n. 235 of 18 April 2018 (in www.gpdp.it, web doc. n. 9358243) and n. 441 of 26 July 2018 (in www.gpdp.it, web doc. n. 9040267), which imposed prescriptions, treatment prohibitions and administrative sanctions in relation to millions of contacts by telephone and text message, which Fastweb and its sale have been put in place without acquiring a suitable consent from the subjects contacted.

Despite the extensive regulatory activity and the constant dialogue between the Guarantor and the telephone companies in the recent past, from December 2018 to February 2020, Fastweb was the recipient of four cumulative requests for information (prot. nos. 36218/18, 8975/ 19, 34440/19 and 5725/20), which examined 131 files, each of which referred to the receipt of one or more unwanted promotional telephone calls made on behalf of the Company, for a total of 236 reports. If we also consider the complaints presented pursuant to art. 77 of the Regulation, which the Guarantor treated, in the preliminary investigation phase, individually and the reports received after the last requests for information, the Office has opened, overall, over the last two years starting from the entry into force of the Regulation, 283 files against Fastweb, mostly concerning telemarketing activities and the sending of promotional messages by or on behalf of the Company. During the period in question, discussions with whistleblowers and complainants as well as with Fastweb itself led to the registration of 508 incoming letters in the Authority's protocol.

The above data testify to the strong impact that the marketing and teleselling practices carried out by Fastweb have on the Office's overall activity and confirm the Authority's judgment with respect to the methods of carrying out these practices conducted by the majority of telephone companies, expressed several times also in recent measures (see, inter alia, measures no. 232 of 11 December 2019, at www.gpdp.it, web doc. no. 9244365; no. 7 of 15 January 2020, at www .gpdp.it, web doc. n. 9256486; n. 143 of 9 July 2020, in www.gpdp.it, web doc. n. 9435753; and n. 224 of 12 November 2020, in www.gpdp.it, web doc. n. 9485681).

1.2. The request for information and presentation of documents, pursuant to art. 157 of the Code, of 23 September 2020, and

the feedback provided by Fastweb

1.2.1. The Office proceeded to identify the most recurring critical issues in Fastweb's findings and sent the Company, on 23 September 2020, a request for information and presentation of documents, pursuant to art. 157 of the Code, containing some questions relating to the methods of carrying out telemarketing activities.

Firstly, in relation to Fastweb's statements according to which promotion agencies, in order to increase their business, would assume "independent behavior[s]" with respect to the instructions on the treatments given by their clients, and promotional contacts would result from this towards interested parties who have not given their consent to the processing of their data for marketing purposes, the Company has been asked to specify such behaviours, indicating the agencies that have put them in place as well as the measures adopted by the Company to contrast such behaviours. Fastweb was therefore asked to provide a summary document of any penalties applied to the aforementioned promotion agencies and to describe, more generally, the remuneration system adopted by the Company as well as to provide a copy of the agency contracts signed with some of them.

Secondly, starting from the data emerging from the cumulative requests in relation to the considerable number of promotional calls (166 against 236 reports, equal to over 70% of the calls) which Fastweb declared were not made from numbers in its sale, the Company was asked to indicate what measures had been put in place in order to exclude that contracts or Fastweb utilities were then finalized from contacts originating from these numbers, as well as to indicate on the basis of which company procedures the Company had verified that each activation of a user or service, carried out directly or with the aid of the network of its partners, agents, call centres, dealers or telesellers, had taken place following a contact by the customer or potential customer made on the lists provided or authorized by Fastweb.

Thirdly, with regard to the use of lists of personal data to carry out promotional contact activities, it was requested to clarify the procedure adopted for the formation of lists of numbers that can potentially be contacted by Fastweb's partners, and to represent the methods of consultation and extraction of the data present in the lists, by the agencies, for the performance of promotional activities. It was also requested to indicate all the companies from which Fastweb acquires lists of personal data intended for promotional contacts, specifying, for each of them: whether it carries out the activity of list editor or list provider; any designation as data controller; and the legal form under which each company carries out the data processing.

With reference to the lists of personal data from third parties, it was asked to indicate the methods by which Fastweb verifies the correct acquisition, by the aforementioned subjects, of the consent of the interested parties for commercial purposes and

for communication to third parties as well as the distribution of responsibilities in the context of the related treatment. It was also requested to indicate the number of promotional contacts made, during 2019, through the use of these lists, as well as the number of contracts and activations made following the aforementioned contacts.

In addition, with reference to the contacts made for the management of the "Call me back" service (described in detail below), the Company was invited to provide information regarding the methods of re-contact and any recurrence of the contacts themselves.

Finally, the Company was asked to integrate, clarify and/or provide further documentation regarding some specific reports.

1.2.2. Fastweb replied to the Authority's request for information on 12 October 2020.

Firstly, the Company indicated the unlawful conduct detected by virtue of the checks it carried out on the work of its sales network and the agencies to which such conduct is attributable where it was possible to identify the perpetrator. These illicit activities have been grouped into the following categories: “calling a so-called contact Off List; use of unregistered caller numbers; use of the 'referee'; use of uncommunicated lists; use of lists that are no longer authorized; need to train collaborators".

The Company then indicated, in a summary document attached, the measures taken by the latter against the aforementioned agencies. Specifically, the Company highlighted that, in the reference two-year period (i.e. from October 2018 to 12 October 2020, hereinafter the "Two-year Period"), the latter sent: "14 massive communications"; "12 formal reminders"; "51 sales warnings"; and “44 requests for information”.

Furthermore, again in the two-year period, the Company: "imposed 33 penalties" in relation to "33 behaviors that did not comply with the provisions of the mandate, which resulted in the application of penalties of €125,000.00 to 26 commercial partners"; "from November 2018 to August 2020 [...] did not pay amounts for commissions and incentives for a total of approximately € 566,487.00"; it "disputed 3 contractual terminations for non-compliant conduct in carrying out telephone commercial contacts"; and it "interrupted the agency relationship" with "13 agencies subject to one or more of the previous measures - formal or criminal complaints".

Secondly, with regard to the measures adopted by the Company in order to exclude that contracts or activation of Fastweb users are then finalized from contacts originating from unknown numbers, the Company stated that the "telephone or data services [...] take on a real its character of public utility". Referring to the previous communications of 10 January 2019 and 8

April 2019, the Company declared that it had adopted "a mechanism" which allows for "not paying the amounts due for contracts originating from contacts not present in the authorized list" and "a process of analysis and report" of the calling numbers not recognized by Fastweb through the intervention of the judicial authority.

As for the first measure, i.e. the "non-payment of PDA [Purchase Proposals] off the list", the Company stated that it carries out "accurate analyzes on activation requests to verify that they match the contacts on the lists and, if case, not pay the amounts due for contracts originating from contacts not present in the authorized list". This system of checks and controls - noted the Company - "also includes the development of the newly developed log analysis tool" as well as "the implementation of a mechanism through which [...] to automatically and preventively inhibit even the uploading orders for new contracts where the contact numbers or other personal information do not match the data in the contact lists".

As for the "process for reporting unrecognized calling numbers", the latter provides that "interested prospects or existing customers can contact Fastweb to report and/or ask for clarification, regarding the receipt of unwanted promotional calls on behalf of Fastweb through various channels placed at his disposal". Subsequently, the numbers reported are checked by the Company and if they can be traced back to its authorized agencies, Fastweb will proceed with the provision of an order; otherwise, "the list of unrecognized caller numbers is prepared" and this list is then sent "for reporting". Fastweb stated that, as of 12 October 2020, it had reported "over 200 numbers".

Thirdly, with reference to the use of personal data lists to carry out promotional activities, Fastweb provided feedback by highlighting that the formation of a contact list involves the creation of a database made up of three repositories, based on the different sources from which records can be sent. The sources of input to the database consist of: i) the DBU numbers acquired from Fastweb; ii) from the mobile numbers that Fastweb acquires directly from third parties; and iii) from the fixed and mobile numbers that Fastweb acquires from its partners, who in turn acquire them from their suppliers. The validity of the lists is usually established in a calendar month (coinciding with the duration of a so-called "planning", i.e. a set of promotional campaigns all having the same start and end date), or in the shorter period envisaged by the legislation regarding the public register of oppositions.

As for the lists of personal data referred to in point ii), i.e. relating to the mobile telephone numbers that the Company acquires from third parties, Fastweb noted that "they all perform the activity of direct list editors, since they collect personal data independently from their sites". The companies therefore assume the legal status of "data controllers" who communicate the

data in their possession to Fastweb based on the specific consent that the interested parties have provided to them. As part of the data acquisition process, the latter requires the companies that they acquire consent for the transfer of data to third parties, as an optional option, and that Fastweb is indicated in the related information as the subject to whom the data can be given. Fastweb verifies that the data acquired directly from list editors comes from its own sites or from independent initiatives and not from the aggregation of different sources.

As for the master data lists referred to in point iii), i.e. relating to fixed and mobile telephone numbers that the Company acquires through partners, who in turn acquire them "independently from their own supplier", Fastweb noted that the agencies are required to request "authorisation" from the Company "before being able to use them", providing a series of elements: the contract signed between the parties with an indication of the time duration of the same; the information provided by the owner to the interested party; and an indication of the methods for collecting consent. In particular, Fastweb verifies that: the collection of consent for the transfer of data to third parties takes place through a separate box; the information is in any case accessible to the interested parties; and that this disclosure indicates the possible transfer of data to third parties with the express indication of Fastweb among these. In the event that the analyzes carried out by Fastweb provide a positive result, the partner is authorized to upload the personal data in his possession to carry out the comparison with the Fastweb black lists and with the public register of oppositions as well as for deduplication operations, so that they are used in planning for the current month. The list is also subjected to random checks based on a random extraction mechanism of names for which the partner is asked to provide evidence of the consents acquired. During each planning month, agencies can use telephone contact lists. Once a planning is completed, the lists used are archived in the Invoice system and are no longer accessible for commercial purposes. The Company specified that the number of promotional contacts made through these lists during the year 2019 "amounted to 7,542,000".

Finally, with reference to the contacts made for the management of the so-called "Call me back", Fastweb noted that this service allows customers and potential customers to be called back by a Fastweb operator, following a "click" on the "Call me back" button. The Company has specified that "the re-contacts that arise [...] are carried out on the basis of precise rules which establish the time intervals within which the system routes a subsequent call to the subject who has proved to be interested and, finally, they manage to close the contact in the event of reaching a limit of unanswered calls". For example – noted the Company – "it is foreseen that [...] if the number is busy for 20 calls it will be closed [...] As regards a free numbering, in a

scholastic hypothesis in which the CRM is not called to manage other calls as well, the user would be called back a maximum of 4 times in an hour at an interval of 15 minutes each for a total of maximum 20 attempts throughout the day". It was then added that "in the information sheet relating to consent for commercial purposes, there is a special link that refers to the privacy information [in which] all the essential information regarding the availability of the service is provided until consent is revoked and in any case for a maximum period of 24 months".

1.3. Claims filed individually

In addition to the reports referred to in the four cumulative requests indicated in the Introduction, the Authority has received further reports and numerous complaints against Fastweb, each subject to an independent investigation and subsequent joint treatment with the main proceeding, based on the provisions of articles . 10, paragraph 4, of the Regulation of the Guarantor's Office n. 1/2019 and 8, paragraph 2, of Regulation no. 2/2019.

The complaints and reports subject to joint treatment with the main proceedings can be divided into different groups on the basis of the issues and arguments raised.

1.3.1. A first group of complaints and reports pertains to Fastweb's management of data assets. In this context, the Authority noted the cases concerning a rather widespread phenomenon, reported by numerous whistleblowers and complainants, who, often following the reporting of a malfunction to Fastweb, complained of having been contacted by call centers offering alternative commercial offers on behalf of the latter or other telephone companies, and/or required customers to send a copy of an identity document via Whatsapp message. In particular: files no. 147286 and 154212, in which the whistleblowers complained that, following their request for assistance from Fastweb due to a "breakdown", they were contacted by a call center apparently attributable to other telephone companies, which proposed to the whistleblowers the migration of own user. In this regard, the Company declared the "total non-involvement of Fastweb" with respect to these calls, adding, in relation to file 154212, that this non-involvement would be confirmed "i) by the content of the same - undoubtedly aimed at obtaining the migration of the customer to another operator […]; ii) from the fact that on the customer's number [...], as emerges from Invoice, there are no contacts made by Fastweb or arranged by it and made by the sales network; iii) from calling numbers [...] not attributable to Fastweb or its structures"; files no. 146491, 146238, 146260 and 148138, in which the complainants complained that, following their request for assistance from Fastweb for problems with the Internet service, they were contacted by a call center operator apparently attributable to Fastweb, who invited them to send a double-sided copy of your

identity document for problem solving. In all cases, the complainants stated that they had sent copies of their identity documents believing that this request came from Fastweb's customer service, as the operators were "perfectly aware" of the "technical problems [...] of the time of the telephone appointment for the management of the technical notification" and of "technical details [...] that only the Fastweb service could know". In this regard, Fastweb provided similar feedback to the previous ones, reiterating, inter alia, that the reported contacts are "the work of unknown persons, who presumably act to the detriment of [the Company] as well, for possible purposes of stealing customers" and that "in any case, Fastweb does not in any way provide for the sending of its customers' identity documents in the circumstances described by you"; file no. 139824, in which the complainant complained that, following the stipulation of an "internet supply contract [...] with Fastweb", he was contacted by telephone by a call center operator who was aware of his "general information and 'supply address for which you had asked Fastweb to activate the internet", an address that does not correspond to "neither [your] residence nor domicile address'. The operator, after having feared possible problems with the activation of the contract due to alleged "problems with the exchanges", invited the complainant to stipulate an "internet supply through another operator" contract and to "send photos of the documents via whatsapp" . Not having received the requested documentation, the operator attempted twice more to get in touch with the complainant, using different numbers for calls.

With a letter dated February 10, 2020, with reference to the overall phenomenon mentioned above, Fastweb stated that it had "already filed several complaints against unknown persons to the Postal Police [...] and has launched a series of awareness and information activities towards and to protect its customers and the market". With these complaints, the first of which dates back to August 2019, "the more than 50 mobile numbers used for the request to send copies of identity documents were brought to the attention of the Judicial Authorities [...] on the whatsapp instant messaging system ” to the detriment of the Company and about 170 people contacted, who were “mainly Fastweb customers”. Furthermore, Fastweb highlighted that “the checks carried out on individual illicit contacts made it possible to identify a common trait. In particular, Fastweb noted that its customers, addressees of the aforementioned request for documents, all had an access technology for the use of fixed services which provides for the rental of part of the network [from another telephone company]. The [Company] therefore ascribed the conduct to a more complex illegal activity, probably aimed at distracting Fastweb S.p.a. customers. to another operator, an activity evidently carried out making use of the information which, due to the peculiar structure of the national network, is within the sphere of ownership of the infrastructure manager". The Company claimed to have "brought to the

attention of AGCOM as well countless evidences of illegitimate behavior attributable to the management of the main infrastructure both with periodic reports and [with other communications]". Fastweb has also started discussions with the AGCM.

1.3.2. A second group of complaints and reports pertains to the management of requests to exercise the rights guaranteed by articles 15-22 of the Regulation by Fastweb and to "manual errors", "system errors", delays in the realignment and correction of data by the Company. In particular: files no. 136409, and 146607 relate to reports and complaints with which customers have complained about receiving Fastweb communications presumably addressed to other customers. In both cases, the Company stated that the problems were generated by incorrect associations, even "manually", of the master data. In one of the two cases, the resolution of the problem occurred three years after the report; file no. 148287, in which the complainant complained that he had sent Fastweb, in November 2019, a request for the portability and deletion of his personal data to Fastweb, and that this request, as of March 2020, had not yet been satisfied. Fastweb found in August 2020, representing that "the technical times for remediation of the systems and the overlapping of a cancellation request did not however allow for the portability to be completed" and argued that "the portability requests entered by the whistleblower are not were successful due to a specific misalignment of the systems which precluded the receipt of the email containing the link to download one's data"; file no. 147619, in which the complainant represented that he had sent Fastweb, in September 2019, a request for rectification of his personal data incorrectly recorded in the MyFastweb personal area (i.e., the address of residence), and that "after more than a year of requests and reminders" despite Fastweb's reassurances, "wrong data was still present" with the "unacceptable" consequence that the correspondence addressed to him was "still sent to [another] address". In this regard, Fastweb stated that it had "managed to insert the modification of personal data internally on several occasions. These changes were successful, but due to a misalignment of the systems, they did not have a resolving effect, in some circumstances bringing back the pre-existing incorrect data"; file no. 152006, in which the complainant complained that she had "repeatedly tried" to "unsubscribe from the Fastweb mailing list", or "to request the cancellation of [her] data via [...] the form reserved for former customers". However, his request was not accepted due to a problem with his tax code. In this regard, the Company argued that "due to a misalignment [...] the objections filed were not correctly propagated on the systems"; file no. 137155, in which the whistleblower complained of receiving unwanted calls on his mobile phone. In this regard, Fastweb replied that this contact "happened erroneously" by one of its agencies, "due to a technical malfunction of the CRM managed by the same company,

which put the number back on call, despite having been inserted in black list".

1.3.3. A third group relates to complaints and reports concerning unwanted promotional contacts made on behalf of Fastweb, but not recognized by the latter. In particular, with regard to the unwanted contacts complained of (files nos. 117698, 144450, 152962, 138241, 151747, 154404, 144577, 149829, 150096, 150853, 151543, 152330, 152792, 152792 and 1541), the Company represented the caller numbers cited by the interested parties, would not be attributable to Fastweb, nor used by it and/or its partners for commercial purposes.

1.3.4. A fourth group pertains to complaints and reports concerning unwanted promotional contacts made on behalf of Fastweb on the basis of legitimate interest. In particular: files no. 149390 and 153360, in which the complainants complained of receiving unwanted promotional calls from some operators for "a discount on the Fastweb bill if [they had] signed a contract with Eni Gas e Luce", despite both having expressly denied their consent to receive promotional contacts. In this regard, the Company replied that the purpose of the contacts was "to submit a promotion that the [Company] dedicates to its customers, and which allows them to have a significant reduction in their telephone bill in the event of activation, under advantageous conditions, of a user with Eni. The call was made because, at that date, the reporting person had not objected to receiving contacts based on Fastweb's legitimate interest in proposing services similar to those already purchased, or promotions from us or from our partners that allow you to have discounts and other benefits on already active services".

1.4. The closure of the preliminary investigation and the start of the procedure for the adoption of corrective measures

Having examined the feedback provided by the Company, the Office, pursuant to art. 166, paragraph 5, of the Code, it adopted the act of initiation of the procedure referred to in the introduction, with which it charged Fastweb with the following violations:

1. violation of articles 5, par. 1 and 2, 6 par. 1, 7, 24 and 25, par. 1 of the Regulation, since Fastweb S.p.A. did not implement control systems of the personal data collection "chain" from the moment of the first contact of the potential customer, capable of excluding with certainty that illegal or unwanted promotional calls have led to the activation of services or the signing of contracts then merged into the Fastweb databases. The violation involves the entire customer base of the company and the complaints referred to in files 117698, 144450, 152962, 138241, 151747, 154404, 144577, 149829, 150096, 150853, 151543, 152330, 152792, and 154;

2. violation of the art. 5, par. 1 and 2, of the art. 6, par. 1, and of the art. 7 of the Regulation, since Fastweb S.p.A. acquired personal data lists from third parties (the partners of its sales network) who, in turn, had acquired them as independent data

controllers and who transferred them to Fastweb's systems. The transfer of data to Fastweb took place in the absence of the required consent for the communication of personal data between independent data controllers. The breach involved at least 7,542,000 data subjects in 2019;

3. violation of articles 5, 6, 7, 12, 13 and 21, in relation to the methods of activation, release of the information and revocation of the "Call me back" service;

4. violation of articles 24 and 32 of the Regulation, in relation to multiple and systematic accesses to corporate databases containing personal data, telephone numbers, telephone traffic and payment data, for having failed to implement proportionately effective measures to guarantee, and be able to demonstrate, that the processing is carried out in accordance with the Regulation, to ensure the confidentiality and integrity of the processing systems and services on a permanent basis and to regularly test, verify and evaluate the effectiveness of the technical and organizational measures in order to guarantee the security of the treatment (files 147286, 154212, 146491, 146238, 146260, 139824, 148138);

5. violation of the art. 33, par. 1, and 34 of the Regulation, for having failed to submit to the Guarantor and to the interested parties the notification of a violation of personal data, with reference to the multiple accesses referred to in the previous point;

6. violation of articles 5, par. 1, lit. d), with reference to the principle of "accuracy" of the data processed, in relation to articles 15-22 of the Regulation, in relation to the various requests to exercise the rights proposed by the interested parties for which system errors and delays in the realignment and correction of the data were found (files 136409, 146607, 148287, 147619, 152006, 137155);

7. violation of articles 5, par. 1 and 2, 6 and 7 of the Regulation, in relation to the processing of personal data carried out for promotional purposes of its products and services, carried out in the absence of the prescribed consent and awaiting the unsuitability of the legal basis of legitimate interest (files 149390, 153360) .

The disputes referred to above were formulated by the Office on the basis of the observations which are summarized below.

1.4.1. With reference to the objection referred to in point 1), the Company's failure to implement checks on the personal data chain acquired in the promotion phase of services suitable for "excluding that contacts from from [unknown] numbers contracts were then finalized or Fastweb users activated".

With regard to the controls described by the Company when replying to requests for information, it has been observed that these controls do not appear suitable for providing the guarantees that could instead be ensured if, at the time of activating the

services, they were indicated, for example , in addition to the contact list used (with time validity constraints consistent with the date of the first contact): i) the partner who made the first and subsequent contacts; ii) the calling telephone numbers (duly registered in the ROC, register of communication operators); and iii) the call script and information read by the call center operator.

As already observed by the Authority in previous provisions referred to in the introduction (see, inter alia, provision no. 224 of 12 November 2020, in www.gpdp.it, web doc. no. 9485681), the consequences connected to the failure to make use of the above information, (and of the others which, unequivocally, would allow the promotional contacts and the relative activation of services to be traced back to a correct telemarketing activity), cannot be substituted by the adoption of "dissuasive and sanctioning actions" , but they must be able to foresee, due to the potential illegality of the processing, the unusability of the data and therefore the impossibility of proceeding with the activation of the services and the registration of the contracts.

It was highlighted that the absence of initiatives as outlined above, especially in the presence of such a significant number of unacknowledged calls, reveals a serious flaw in Fastweb's accountability, as well as in some key elements of the privacy by design criterion (such as prevention, functionality, safety, transparency of the treatment and the centrality of the interested party), which can be wisely exploited by "unofficial" procurers to occupy market spaces by generating an induced without guarantees for users and suitable for determining further unlawful consequences (for example with regard to the labor and tax aspects of the sector).

It was then noted that, at the time of the conclusion of the preliminary investigations, at least 70% of the reports still resulted from commercial contacts resulting from an independent initiative not authorized by the Company.

As regards the measures adopted by Fastweb in relation to illicit commercial contacts carried out by the agencies belonging to its sales network, the inconsistency and inadequacy of the same was found to guarantee that the treatment is carried out in compliance with the Regulation as well as the lack of systematic in applying these measures.

Specifically: as regards the measure of the "exclusion of the fee", the latter appeared inadequate since it is undisputed that the Company proceeds with the loading of orders for new contracts also with respect to customers procured outside the customer list dedicated to an agency and/ or outside the area assigned to it, so that the Company would make a profit from the usability of data acquired on its behalf illicitly in violation of the relevant regulations on the protection of personal data; as for the "massive communications", the "formal reminders", the "sales warnings", being non-coercive in nature, it was considered that

they had a limited dissuasive effect; as regards the extent of the "penalties", an analysis of the documentation produced by Fastweb revealed the inadequacy of this measure both in that its application is not proportional to the number of abusive conduct identified by the documentation produced by the Company (not even the 1% of the illicit conducts were sanctioned through the application of a penalty) and because the amount of the sanction applied is negligible compared to the number of violations committed by an agency and/or compared to its turnover; as regards the measures of "contract termination" or "interruption of relations with the agencies", the inconsistency and contradictory nature of the Company was also found in the application of these measures.

1.4.2. With reference to the dispute referred to in point 2), in the act of initiating the procedure, some critical issues were highlighted regarding the process of acquiring the master data lists from suppliers or partners.

As a preliminary step, a survey was carried out of the contractual and operational conditions that bind the various commercial partners to Fastweb.

As regards the acquisition of the master data lists relating to the mobile telephone numbers that Fastweb acquires directly from list editors (who collect said master data from their sites), the Authority observed that overall the model followed appears correct: these companies assume the legal capacity of data controllers who communicate the data in their possession to Fastweb based on the specific consent that the interested parties have provided to them.

This model, however, does not appear to be correctly configured with reference to the eGentic "list editor", which would result in acquiring the data from the companies belonging to its business group, Naturvel Pte Ltd. and Tooleado Gmbh: in fact, eGentic's intermediation is not highlighted in the information provided by the aforementioned companies, neither among the subjects to whom the data may be communicated, nor among those who can become aware of it in the context of any intra-group communications.

As regards the personal data lists provided by Fastweb's sales network partners, following acquisitions made by them as independent data controllers, it has been found that these lists have merged into the circuit of treatments having promotional purposes for which the Company is owner, without the partners having acquired a free, specific and informed consent from the interested parties for the communication of their data, but only on the basis of the original consent that the same interested parties gave to the list editors.

1.4.3. With reference to the dispute referred to in point 3), relating to the methods for activating, issuing the information and

revoking the "Call me back" service, it was noted that, from the procedure described by Fastweb and from a check carried out on the website www.fastweb.it, some critical issues have emerged.

Firstly, the lack of ad hoc information was highlighted in relation to the above service, in which the functioning of the service, the methods of processing personal data and recontacting the user were explained. In particular, in the summary notice inserted near the service activation button, Fastweb merely informs the user that "by clicking on 'Call me back for free'", he gives his "consent to the processing of personal data to receive telephone contacts on Fastweb offers exclusively in the time slots [...] indicated", without providing any indication regarding the "recontacts that arise [...] after clicking on the 'call me back for free'" button if the first call is not successful (in this sense , the user is unaware, for example, of the fact that from his request to activate the service, if his numbering is then "free", there could potentially be "a total of 20 attempts [of calls] throughout the day" before "the contact [is] closed").

The privacy information available on the Fastweb website, regarding the consent given by the user for the processing of personal data in order to receive future telephone contacts for the proposition of commercial offers relating to Fastweb, also appeared to be deficient in this respect.

Secondly, the lack of a system that would allow the user to interrupt the flow of calls deriving from his "click" on the "Call me for free" button with equal simplicity was highlighted. Indeed, if to activate the service it is sufficient to "click" on the "Call me back for free" button, for its deactivation the user is invited to "send a communication" by e-mail.

1.4.4. With reference to the disputes referred to in points 4) and 5), in the act of initiating the proceeding it was noted that, in relation to the overall matter relating to contacts addressed to Fastweb customers aimed at acquiring identification documents or proposing migrations of telephone calls, during 2019 Fastweb received several notifications of "data breach" but none of them appears to be attributable to the specific violation, brought to the attention of the Authority by the Company with the note dated 10 February 2020.

The general vulnerability of the Fastweb systems in the light of the declarations of the complainants and also of what the Company itself reports, does not seem to have been addressed "taking into account the state of the art and implementation costs, as well as the nature, object, context and the purposes of the processing, as well as the risk of varying probability and severity for the rights and freedoms of natural persons" as provided for by art. 32, par. 1, of the Regulation. In particular, no proportionately effective measures have been implemented with reference to the ability to ensure the confidentiality and

integrity of the processing systems and services on a permanent basis (Article 32, paragraph 1, letter b) but , above all, to the procedures for regularly testing, verifying and evaluating the effectiveness of technical and organizational measures in order to guarantee the security of the processing (Article 32, paragraph 1, letter d) in view of the multiple accesses of partners' personnel commercial to company databases.

Furthermore, with reference to the circumstances indicated in the report of 10 February 2020, from the research carried out in the Office's protocol, the notification envisaged by art. 33, par. 1, of the Regulation.

1.4.5. With reference to the objection referred to in point 6), in the act of initiation of the procedure it was observed that the generic indication of generic errors at the basis of an undue contact or an unsuitable reply is not suitable for eliminating the responsibility of the Society, given that there is an adequate structuring of systems, organization and working cycles.

It should be added that, in some complaints and reports, even years have passed for the resolution of the issues raised (where they have been resolved), and only following multiple requests and/or reports from the complainants. As you know, a personal data breach may, if not addressed adequately and promptly, cause individuals to lose control over their personal data or limit their rights.

1.4.6. With reference to the objection referred to in point 7), in the act of initiation of the procedure it was observed that the legal basis of the legitimate interest, pursuant to art. 6, par. 1, lit. f), of the Regulation, cannot replace tout court that of consent in telemarketing.

The Regulation itself admits it only "provided that the interests or fundamental rights and freedoms of the data subject who require the protection of personal data do not prevail". The interests and fundamental rights of the data subject may in particular override the interests of the controller where personal data are processed in circumstances where data subjects cannot reasonably expect further processing of the personal data. The application of the legal basis of legitimate interest therefore presupposes the prevalence of the latter over the rights and freedoms of the interested parties (among which, in the case of marketing, the right to data protection and the right to individual tranquility of the interested), and it is also necessary, in compliance with the principles of responsibility and transparency, the concrete implementation of adequate measures to guarantee the rights of the interested parties, such as in particular that of opposition. Furthermore, the data controller cannot retroactively resort to the basis of legitimate interest in the event of problems with the validity of the consent. Since he has the obligation to communicate the legitimate basis at the time of collection of personal data in the information provided to the

interested party, the data controller must have decided on the legitimate basis before collecting the data.

For these reasons, it was considered that, in the cases subject to the complaint, the processing was carried out by Fastweb in the absence of a suitable legal basis, and this in particular, in violation of the provisions of articles 5, par. 2, 6 and 7 of the Regulation.

2. DEFENSIVE OBSERVATIONS AND ASSESSMENTS OF THE AUTHORITY

2.1 The defense brief and the hearing of Fastweb

On 20 December 2020, Fastweb sent the Authority the defense brief required by art. 166, paragraph 6, of the Code. Based on the same provision, on 21 January 2021, at the request of the party and by videoconference, the hearing was held for which a specific report was drawn up. Both documents are to be understood here as integrally referred to and reproduced.

2.1.1. On the checks carried out in the contract signing chain (see point 1 of the dispute), Fastweb represented the following. Firstly, the Company has strengthened controls on the external sales structures it uses to carry out telemarketing campaigns (also reducing the number of such structures by approximately 50%), and has introduced new sanctioning mechanisms. The Company, "confirming an ever greater accountability", has also signaled its intention to further expand the control system by: i) increasing the level of assessment of the structures; ii) the use of the control log tool; and iii) the new technology implementation on order blocking. In addition, during the hearing, the Company expressed its intention to proceed, in the next 12-18 months, with a tendential disposal of the outbound call channel of the agencies, possibly maintaining relations only with the more structured ones that provide suitable guarantees of compliance. The Company then noted that, in any case, in order to obtain the definitive interruption of this phenomenon "it is necessary to involve external actors" such as, for example, "the Judicial Authority".

Secondly, with regard to the obligation envisaged by the Authority not to proceed with the activation of contracts where the Company is unable to guarantee that customer data has been acquired lawfully, the Company argued that "the activation of voice or data services[s] [...] take on a real character of public utility" and that, also following the adoption of the automatic blocking system when entering contracts, "there will still be subjects who [...] they will receive unfair commercial contacts and that […] they will allow themselves to be persuaded by the callers to subscribe to a subscription with Fastweb. The latter, however, will not be able to be loaded on the company's systems due to the new technological implementation. The situation that arises from this is singular. Although the subject was contacted through an illicit promotional call, the same did not become

unwanted, so much so that it prompted him to sign a contract, which however will not be activated for him. In these cases, Fastweb will have to contact the subject to explain what happened and, if the will remains, proceed to the activation in any case".

The Company also observed that "on a civil and regulatory level [...] in the face of the persistent will of the interested party, Fastweb would have no right to refuse such activation. Nor would the principle of 'unusability' pursuant to art. 2-decies of Legislative Decree no. 196/2003". According to Fastweb, "this principle [...] undoubtedly concerns the data used for contact purposes but cannot extend to the same data that the interested party then asked to send to Fastweb through the contract proposal. The latter could not be said to be treated 'in violation' [...] as an expression of a request from the interested party and therefore covered by an independent legal basis pursuant to art. 6, par. 1, lit. b), of the regulation".

Fastweb then noted that "the complex system adopted to date has in any case contributed to significant reductions". According to the Company, given that the contract brokers who operate "in parallel" with the Fastweb sales network "are undoubtedly acting for the sake of profit, with the hope of being able to enter in one way or another the final section of the sales network and therefore indirectly receive a fee", Fastweb has envisaged "a first radical measure: that of not recognizing commissions for off-list contacts". It would be irrelevant that the Company then profits through the stipulation of contracts deriving from the illicit activity carried out by these brokers, since "the problem is to remove the incentives for these external parties, not for Fastweb". He then represented that, with reference to the amount of illicit contacts made on behalf of the Company by third parties or by its own sales agencies during the two-year period, these correspond to a small percentage compared to the tens of millions of promotional calls made.

Finally, on the Authority's objection regarding the vagueness, inconsistency and lack of systematic nature of the measures adopted by Fastweb, the latter replied that "differential treatments are proof of the proportionality, albeit perfectible, already in use".

The Company noted that on 11 November 2020 it had launched a working table with the main consumer associations (Altroconsumo, Udicon, Adocn, Federconsumatori) "for the implementation of a synergistic system to combat the phenomenon of unwanted calls" on whose progress the Guarantor will be kept updated.

2.1.2. On the purchase of personal data lists through partners of its sales network (see point 2 of the dispute), the Company represented the following.

Firstly, with regard to the lists independently acquired by the eGentic list editor which would, in turn, acquire the data from the companies belonging to its group (i.e. Naturvel Pte Ltd. and Tooleado Gmbh), the Company found that eGentic, as the holding company of the group, it would never acquire ownership of the data, but would limit itself to processing them "as a manager on behalf of Toleadoo and Nturvel with the purpose indicated by them". This would emerge from the information relating to the personal data of Toleadoo and Naturvel, which would expose "to the interested parties the very fact that their personal data may be processed 'on behalf of the Data Controller as External Data Processors'". Specifically, eGentic would have a "mere intermediary role". In Fastweb's opinion, "the transfer relevant to the GDPR takes place directly between Toleadoo and Naturvel, on the one hand, and Fastweb, on the other hand [...] As a result, the owner-owner relationship between Fastweb, Toleadoo and Naturvel is entirely legitimate and consequently it is structured in a manner compliant with the Regulations".

Secondly, with regard to the methods for acquiring the personal data lists autonomously by the partners of the Fastweb commercial network - according to the Company - "the subject who proceeds with the purchase does not do so as owner, but as data processor on behalf of Fastweb, the entity for which it is physically carrying out the activity". Indeed, "In the agency contract signed with its partners, Fastweb assigns them the task of promoting, without representation, business in its interest, expressly appointing them as responsible for the processing of personal data [who] receive detailed and complete indication of what tasks and activities they will have to carry out". In Fastweb's opinion, the agencies operate as "autonomous entrepreneurs on a statutory level", but in terms of data processing "the agencies do not have any space to autonomously decide the 'essential means' on which data, for how long and for which categories of interested parties". Therefore, "purchasing autonomy" would exist "on a purely commercial level" and not "from the point of view of the GDPR".

2.1.3. On the "Call me back" service (see point 3 of the dispute), the Company replied as follows.

Firstly - according to Fastweb - the disclosure "clarifies [it] that consent was given to the processing of personal data in order to receive telephone contacts on Fastweb offers exclusively in the time slots [...] indicated". The aspects relating to the "number of potentially feasible contacts or what would have happened in the case of free numbering [...] do not pertain to the purposes [...] but to the technical methods for their pursuit".

Secondly, Fastweb would have adopted "a simple and easy deactivation system" of the "Call me Back" service, whereby interested parties "can act by simply sending an email", or by "answering the call back request, to communicate that you are no longer interested in receiving support.

The Company deduced that "under both profiles" there would not have been an "injury to the consent of the interested parties", both because "pursuant to recital 42 - also referred to in par. 3.3.1. of the Guidelines on consent, WP259rev.01-, it was sufficient that the interested parties were informed of the 'purposes of the processing', which happened", and because "again pursuant to the aforementioned recital 42, it is not a condition for the validity of the consent that there are methods of revocation exactly mirroring those for the release". However, the Company, "as evidence of the constant search for improvement pursued", has made available "a new information [...] which illustrates the operating methods of the service, the related data processing and the re-contact policies as well as the revocation" .

Finally, with regard to the disputed files, Fastweb reports that it finds correspondence with management performed only for files 138241, 149829, 150096, 151543, 152330, 152792 and 154231, which in any case would not be evidence of the disputed.

2.1.4. On the security of Fastweb's databases and the declaration of data breach (see points 4 and 5 of the dispute), the Company represented the following.

Preliminarily, Fastweb deduced that it had not detected, "in the majority" of the disputed cases, unauthorized access or other anomalies on the systems and that "the reported cases mainly involved services provided pursuant to access and interconnection agreements by of third-party operators [...], to whom the data are legitimately communicated to allow the normal functioning of the network".

Specifically: in the cases referred to in files no. 154212, 146238, 139824, it was necessary to request an intervention from another telephone operator (in the first two, for the resolution of the disservices complained of by the customers, while in the last one, for the completion of the activation of the line requested by the customer) and all contacts complained of by customers - the Company reiterated - were made "only after the involvement of [this operator]".

As for the events referred to in files nos. 147286, 146260, 146491, and 148138, the events referred to in the first three files, were reported to the Postal Police. For files no. 147286 and 146260, moreover, the Company added that customer data and events occurring on the network were also visible to the "third party other than Fastweb who owns the network". Finally, in the cases referred to in files no. 146260, 146491, 148138, the Company found that "the analyzes did not lead to highlighting anomalies on the systems used for similar managements nor did it emerge that the data was subject to illegal extraction".

In light of the foregoing, "The Company [...] deemed it reasonable to assume that the data leakage was located outside the

systems of its pertinence".

In this regard, Fastweb referred to AGCOM resolution 321/17/CONS, noting that "the access and interconnection relationships between operators are subject to regulation by AGCOM and the existing contractual models, approved by AGCOM itself, lead to the conclusion each of the parties as 'independent controller' with reference to the related processing of personal data within its competence".

In the opinion of the Company, "in the presence of a distinct ownership of the processing, the communication of Data Breach [...] can only compete with the 'owner' stricto sensu in relation to the perimeter of processing that is his responsibility. This already results from the letter of these provisions and is consistent with the type of reactions that are required of the owner, who assume the direct governance of the treatment methods".

In any case - claimed the Company - Fastweb would not have overlooked the above phenomenon, "working [by] the AGCOM tables" and submitting "multiple complaints to the Judicial Authorities" as well as taking care of the relationship with its customers.

As regards the lack of security on Fastweb's systems in violation of articles 24 and 32 of the Regulations, the Company reiterated: that there would be no elements common to all reports of illegal calls; that compared to the hundreds of thousands of support requests that Fastweb receives every month, the reports received by the Authority correspond to a negligible percentage; and that it did not detect anomalies that could suggest unauthorized access.

Fastweb then illustrated the activities carried out to protect the security of the systems. In particular: "additional profile cleaning activity with elimination of the functionality [...] of massive download to customer care operators"; "for all those who still have the right to view and extract, the contact data from all reports have in any case been blocked"; "several dashboards managed on a single system have been implemented which allow for increasingly efficient monitoring of any accesses, views of customer files, use of reporting faculties and exports always referred to the CRM"; "masking when viewing contact data" and "training on the use of massive reporting and exports".

The Company also highlighted the "awareness-raising activity carried out also with respect to its customer network to [...] prevent fraud against Fastweb customers, protecting the security of their personal data, informing them on how to avoid handing over their documents to unauthorized persons, who unlawfully present themselves in the name or on behalf of Fastweb".

2.1.5. On system errors, delays in realigning and correcting data (see point 6 of the dispute), the Company represented the following.

Preliminarily, Fastweb argued that "by adhering to the accountability logic on which the new Regulation is structured - leaving aside the sanction system of the old Code based on the fact-penalty dichotomy - these events [...] represent isolated and evidently non-systematic cases which they can happen precisely because of manual input errors or communication difficulties between computers/systems". The few reports are to be considered an extremely small number compared to "an average of 40,000 requests for updating personal data, contact details and addresses" which are processed by the Company. There would have been no significant violations for the sanctioning purposes of Articles from 15 to 22 of the Regulation since the exercise of the rights would have "always been promptly guaranteed" to the interested parties and, where delays occurred, "the 'justifications' of the delay were used precisely as a possibility by the legislator himself" in articles 16 and 17.

As for the individual disputed reports, the Company recalled the answers already provided for each individual case and added, inter alia, the following: for file no. 147619, "Due to a misalignment of the systems, the management was only completed on 19.08 [...] the disservice is documented [...] The proof of the sporadic anomaly that occurred on the systems is given by the presence of [...] processing tickets"; and for file no. 152006, "the cause of the delay is proven by task 50897" relating to a problem with the tax code.

2.1.6. On the processing for promotional purposes carried out without consent or on the basis of legitimate interest (see point 7 of the dispute), Fastweb represented the following.

In general, the Company has observed that data collected for "specified, explicit and legitimate purposes" can also be processed for other purposes, if the processing is compatible with the purposes for which the personal data were initially collected. In that case, no separate legal basis would be required other than the one that allowed the personal data to be collected. Therefore, "the analysis of the legitimate interest as an autonomous basis of the processing - in particular for processing carried out in the context of a contractual relationship and for different purposes but connected to those of the execution of the contract and therefore 'reasonably foreseeable' by the interested party - it also absorbs the one on the compatibility of the new purpose".

As regards the contacts subject to complaints referred to in files nos. 153360 and 149390, on a preliminary basis, the contacts would have been made as the complainants had not expressed (file n. 153360) or had not "yet" expressed (file n. 149390) on

the day of the contact, "opt out on the legitimate interest ” and were directed “solely to Fastweb customers [...] in relation to partnership promotions that allow for discounts or other concrete advantages on services 'already active' with Fastweb”. Indeed, according to the Company "the circumstance that the interested parties had not given consent for commercial processing could not implicitly detect as an opposition to contacts based on legitimate interest".

With reference then to the information provided to both complainants at the time of the contract, the Company underlined that both the issue of legitimate interest and that relating to consent for commercial purposes are clearly indicated in the information itself. For these reasons, Fastweb noted that "the choice of the 'legitimate basis' had been made before the data was collected" and that "there is no overlap between the two types of legal bases, nor did Fastweb resort to legitimate interest to compensate lack of consent".

With regard to the right of opposition granted to data subjects, Fastweb noted that it "has ensured an easy right to exercise the right [...] in line with what is expressly reported in the information", where it is specified that the data subject will be able to manage his/her consents and oppositions "independently through the dedicated page within the [...] MyFastweb customer area", or can "call the Customer Service or go to the Fastweb Flagship Stores".

In support of its statements, the Company has reported a screenshot of the "consent and contact preferences" section available in the Myfastweb area of each customer, highlighting that "the customer can exercise his right to opt out by clicking on the 'I do not wish to receive information'".

At the conclusion of its defense brief, the Company recalled the previous arguments and communications, asking the Authority to "positively close the proceedings in its favour"; or, "subordinately", not to order "the application of sanctions pursuant to articles 58 and 83 of the Regulation”; or, "in a further alternative way" to "reduce [the sanction] to the applicable minimum and the generic and specific extenuating circumstances undoubtedly demonstrated are recognised".

2.2. Considerations in fact and in law

The above defensive arguments, together with what was represented by the Company during the preliminary investigation, do not allow Fastweb to be held liable for the alleged violations, the content of which is referred to in full, for the reasons set out below.

As a preliminary point, it should be noted that the telemarketing conduct described represents proof and confirmation of the alarming context in which the phenomenon of illicit contacts and unwanted promotional calls must take place. This

phenomenon, as already highlighted in the Authority's provisions referred to several times, also adopted in recent times, has been the subject of social alarm by citizens and attention by the legislator and the Guarantor for over fifteen years. There have been numerous regulatory interventions aimed at regulating the sector. These interventions were accompanied by constant control activities by the Authority regarding the various aspects of the phenomenon: from the relationships between the various subjects involved, to the correct acquisition of the lists of interested parties who can be contacted, from the management of telephone directories and the register of oppositions , to the use of call centres. The numerous provisions adopted on the subject by the Guarantor before the entry into force of the Regulation, the subject of debates among industry experts and attention from the press, have not resulted in a reduction of the phenomenon, so that the Authority, in April 2019, sent a general information to the Public Prosecutor's Office at the Court of Rome aimed at highlighting the criminal consequences of the telemarketing activities carried out in violation of the provisions on the protection of personal data. Also in the light of this context, it now appears necessary to make full reference to the new principles dictated by the Regulation, which frame the responsibilities of the data controller in a perspective of responsibility (accountability) and impose proactive behaviors on all players in the processing of personal data and consistent with the purpose of proving, at each stage, the legitimacy of the processing itself.

2.2.1. With reference to the dispute referred to in point 1), the existence of the disputed violation of articles 5, par. 1 and 2, 6 par. 1, 7, 24 and 25, par. 1, of the Regulation, in relation to the entire customer base of the Company, as well as the complaints referred to in files 117698, 144450, 152962, 138241, 151747, 154404, 144577, 149829, 150096, 150853, 151543, 152330, 15275942, 3 and 152759421. .

From the analysis of the reports and complaints received by the Authority as well as the related feedback provided by Fastweb, it emerged that for a considerable number of illegal promotional calls made on behalf of the Company (at least 70%) numbers not belonging to the Fastweb sales network and, in almost all circumstances, not registered in the ROC (i.e. in the Register of Communications Operators).

In general, it must be premised that the strengthening measures adopted by the Company and the further initiatives undertaken - among which there is also the intention to achieve a tendential divestment of the outbound call channel of the agencies and participation in the work table started with the main consumer associations - certainly demonstrate the latter's awareness of the seriousness of the phenomenon of illicit promotional calls, and the will to curb it.

However, the limitations and criticalities found with regard to some of the aforementioned measures cannot fail to be highlighted.

Firstly, with reference to the control mechanisms, in the act of initiating the procedure it was noted that the controls carried out by the Company on the numbers and on the results of the processed contacts uploaded by the partner on the Invoice portal (including the PDA result, as well as those ex post on traceability, even at different times, to contact lists authorized by Fastweb of the called numbers), do not provide any guarantee on the correct conduct of the promotional phase, as they limit themselves to verifying that the contact of the person called is included in a list authorized by Fastweb without however carrying out any checks on the calling number.

This may allow unknown subjects and in any case not attributable to the sales circuit officially recognized and authorized by Fastweb to make promotional calls on behalf of the Company using numbers that do not belong to the Fastweb sales network, in order to unlawfully collect users' personal data who, in the mistaken belief that they are talking to a Fastweb sales agent, in some cases give them by adhering to promotional offers. These personal data then flow into the company databases through subscription offers (the so-called "PDAs") which are loaded into the Company's systems and activated.

This phenomenon, as highlighted in the notice of dispute and in the aforementioned recent provisions of the Authority, can be stemmed or even radically eliminated by Fastweb, by configuring its systems in such a way as to be able to block the activation procedures for offers or services where the Company is unable to guarantee that the promotional activity was carried out in compliance with the rules and rights of the interested parties, from the moment of the first contact. In this sense, for each activation, the Company's systems, in addition to requesting the indication of the contact list used (with time validity constraints consistent with the date of the first contact), should require further elements necessary to determine the correctness of the performance of the promotional contact (e.g., indication of the partner who made the first and subsequent contacts; indication of the calling telephone numbers - duly registered in the ROC, register of communication operators; call script and information read by the call operator - center).

The consequences connected with the non-utilization of such information should in any case be able to foresee, due to the potential illegality of the processing, also the unusability of the data (pursuant to article 2-decies of the Code) or the "blocking" of the activation of contracts that do not meet certain requirements.

In this regard, we cannot agree with Fastweb's position according to which the latter "would have no right to refuse such

activation" even where the contracts originated from illicit promotional calls since "the activation of telephony services[s] or data [...] take on a real character of public utility".

In similar cases, the Authority clarified that "that of not proceeding with the activation of offers or services when there is no proof that they have been correctly offered to the user on the basis of the provisions governing the methods of carrying out of promotional contacts, does not constitute a mere faculty of the data controller but a precise obligation dictated by the combined provisions of the articles 5, par. 2, 6 and 7 of the Regulation and of the articles 2-decies and 130 of the Code. On the basis of the provisions of the Regulation, in fact, the owner is required to prove that the treatments carried out by him, also through managers, comply with the principles of lawfulness, transparency and correctness (in particular with reference to consent), principles which, in scope of promotional contacts are declined by art. 130 of the Code, and if this is not possible, the first effect deriving from it is the unusability of the data processed" (see provision no. 224 of 12 November 2020).

The same considerations can take place "on the civil law level", having to exclude that in the aforementioned cases a free and autonomous will has been formed by the parties to complete a contract: the same, in fact, would have been conveyed by a subject not provided with the essential requisites to be able to represent the Company (and, consequently, to collect the data of the other contracting party) and brought to the attention of a subject who expresses his/her consent to the subscription in the erroneous conviction of speaking with Fastweb.

The thesis put forward by the Company also appears without merit, according to which even after the adoption of the automatic blocking system in the insertion of new contracts, "in the face of the persistent will of the interested party, Fastweb would have no right to refuse such activation" .

As a preliminary point, it should be noted that Fastweb's thesis according to which there is a distinction between an "illegal" call and an "unwanted" call does not find any regulatory confirmation, since, obviously, the considerations are irrelevant for the Italian and European legislator regarding the "desirability" of a telephone contact. Conversely, promotional calls made without a suitable legal basis can be defined as unwanted (i.e. illicit) (article 130 of the Code and articles 6 and 7 of the Regulation).

Nor can the defensive thesis on the alleged "autonomous legal basis" be shared, given that the treatment of the Company would fall within the scope of the activity carried out by the unknown third party.

In this regard, it has already been highlighted that "the entire structure of the Regulation is based on the accountability of the data controller. Due to the fact that the personal data of the subjects contacted who have subscribed to the promotional offers

are destined to flow into the company databases, these should adopt special guarantee measures in order to prove that the contracts and activations registered in their systems originate from contacts made in full compliance with the provisions on the protection of personal data, in particular those referred to in articles 5, 6 and 7 of the Regulation relating to consent" (see the aforementioned provision n. 143 of 9 July 2020).

What is represented in the notice of dispute is confirmed in relation to the fact that the absence of initiatives as outlined above (i.e. systems that require further elements for each activation in addition to the indication of the contact list), in particular in the presence of so relevant in relation to unacknowledged calls, it has led to a serious flaw in Fastweb's accountability, as well as in some key elements of the privacy by design criterion.

As for the procedure that the Company intends to adopt following the implementation of the new technology, it should be noted that any "continuing willingness" of the interested party to subscribe to a subscription with Fastweb, in any case, could not be verified by the Company through a recontact user's phone. This operation would follow the illicit promotional activity initiated by the unauthorized third party, putting in place a further processing of data acquired illicitly in order to carry out promotional activities. To preserve the expression of will of the potential customer, it could possibly be considered the possibility of sending a short message to the same, informing him of the problems that prevent the registration of the contract and the activation of the service, with an invitation to recontact a specific articulation inbound of the Company in order to complete the contract itself: in this way the will of the interested party can be brought to the attention of the owner precisely on the impulse of the latter.

Secondly, also with reference to the new sanctioning mechanisms adopted by Fastweb, it was observed in the notice of dispute that the measures adopted by the Company, (including "non-payment of non-listed PDAs"), are not suitable for unhinging the phenomenon described above since they act exclusively on the "official" sales network and are not able to affect in any way what has been repeatedly defined as the "undergrowth" of telemarketing.

In particular, as regards the aforementioned "exclusion of compensation" measure, the latter appeared inadequate, first of all, because it allows in any case the loading of orders for new contracts also with respect to customers procured outside the customer list dedicated to an agency and/or outside the area assigned to it, thus determining the use of data acquired illicitly from unknown subjects in violation of the relevant regulations on the protection of personal data. Furthermore, since Fastweb would also make a profit from this use (the example of the 5543 contacts made to numbers outside the list was mentioned,

from which 5543 activation orders for Fastweb could potentially derive), the choices made by the same in order to exclude commissions and fees would be legally subject to attack by the agencies involved, as indeed highlighted by the Company during the hearing. Furthermore, the aforementioned measure does not appear to prevent remuneration from being paid to those who procure customers whose contacts are contained in lists authorized by Fastweb but who use unregistered calling numbers (activities which could potentially be carried out directly by an agent of the Fastweb sales network, or by the latter through the intermediation of an unknown third party).

As for the process for reporting unrecognized calling numbers implemented by Fastweb "to combat the use of illegal numbers", although useful in that it is aimed at blocking the numbers being reported, this mechanism also does not provide any guarantee that the promotional phase will run correctly . Indeed, it is a measure characterized by a very limited scope, given that it is activated only following the receipt of unwanted promotional calls by the interested party (therefore after the violation of his personal data), and only where the recipient of the call present a report to the Company or to the Authority (the measure, therefore, could, even not be activated or, in any case, would be activated only in relation to the limited number of promotional calls reported). In addition, the numberings subject to complaint may not be attributable to an identified contractor, resulting in substantial impunity for the authors of this measure.

As for the further measures adopted by the Company "in the event that it has been possible to identify the author" of illicit promotional calls, i.e. the application of "penalties", the "termination of the contract" and the "interruption of relations with the agencies" , what emerged in the notice of dispute regarding the non-systematic nature and inconsistency in the application of the measures with respect to similar situations is confirmed. With regard to the measure of the "penalties", the inadequacy of this measure was found in the notice of dispute both in that its application is not proportional to the number of abusive conduct detected by the documentation produced by the Company (less than 1% of the violations appear to have been sanctioned through the application of a penalty) and because the amount of the sanction applied is modest compared to the number of violations committed by an agency (as well as compared to its turnover). As regards the measures of "contractual termination" or "interruption of relations with agencies", the inconsistency and contradictory nature of the Company's conduct was found where the latter chose to terminate or interrupt relations with some agencies and to continue them with others, despite the fact that the latter had committed the same violations of the first, plus others.

Thirdly, with reference to the measures adopted by Fastweb which are currently under development, the following is noted.

Although Fastweb's intention to undertake a path that follows, at least partially, the indications of the Authority, both through the use of the "tool log" (which allows ex-post controls to be extended to the numbers callers and to all promotional calls made by agencies), and through the new technology implementation (which makes it possible to inhibit the possibility of loading orders referring to subjects not present in the authorized contact lists), both measures present the same criticalities where they do not envisage the exclusion of the contract proposals acquired illicitly from the information assets of the Company, as they would instead be required to provide for the reasons already amply illustrated above.

Lastly, the defensive arguments expressed by Fastweb relating to the limited number of reports and complaints, given the large number of promotional contacts made by the Company, are irrelevant. The Company is well aware that the 236 reports brought to the attention of the Guarantor correspond only to a minimal part of the illicit promotional activity that is carried out daily by the sales agencies (just consider that only with reference to "contacts made by the agencies towards unlisted numbers", the Company itself declared that 5,543 illicit contacts were made in less than two years). It is evident that the majority of users, victims of multiple illicit promotional calls, do not address the Authority with reports and complaints, despite the fact that telemarketing is often perceived as an invasive phenomenon, even beyond any tolerance limit. In addition to the number of cases reported, what is relevant is the degree of effectiveness of the responses provided by the Company to these reports and complaints, in order to prevent the activity carried out by the sales agencies on behalf of Fastweb from prevailing over the others confidentiality. Well, if in the case of Fastweb, out of 236 reports, the Company denied the origin of at least 166 telephone calls, thus providing the interested parties with a completely ineffective response to their requests. Therefore, it must be concluded that even from a numerical point of view, the problem brought to the attention of the Authority is extremely serious.

In the light of the above, it emerged that the Company, although it has "committed" and has "invested" in the phenomenon of unacknowledged calls, has not fully exercised its powers, which correspond to the duties of accountability and privacy by design identified by the 'art. 5, par. 2, and 25 of the Regulation, failing to introduce forms of control of the personal data acquisition "chain" that prevent the acquisition of new customers if it is not demonstrated that the same were initially contacted by a subject included in the chain of responsibility for processing the which has put in place all the precautions envisaged by the reference regulatory and ethical framework.

2.2.2. With reference to the dispute referred to in point 2), the outcome of the investigation revealed that Fastweb acquired lists

of personal data from third parties (the partners of its sales network) who, in turn, had acquired them as of independent data controllers and who have transferred them to Fastweb's systems. The transfer of data to Fastweb took place in the absence of the required consent for the communication of personal data between independent data controllers. Therefore, the disputed violation involving at least 7,542,000 data subjects in 2019 is confirmed.

Based on Fastweb's reconstruction, the personal data lists can be acquired, among others, from direct list editors (Chebuoni, Impiego24, ClickAdv, Bakeca and eGentic, which in turn acquires them from the subsidiaries Naturvel Pte Ltd. and Tooleado Gmbh), and by its partners who in turn acquire them autonomously from their suppliers and subsequently obtain authorization to use them from Fastweb.

With reference to the master data lists relating to the mobile telephone numbers that Fastweb acquires directly from the list editors, overall the model followed appears to be correct. It has been noted that, in the aforementioned case, the companies take on the legal role of data controllers who communicate the data in their possession to Fastweb based on the specific consent that the interested parties have provided to them. As part of the data acquisition process, Fastweb requires the companies that they acquire consent for the transfer of data to third parties, as an optional option and that Fastweb is indicated, in the related information, as the subject to whom the data can be transferred . Fastweb verifies that the data acquired directly from the list editors comes from its own sites or from independent initiatives and not from the aggregation of different sources. Therefore, the model provides for a communication of data from owner (list editor) to owner (Fastweb) supported by a specific and informed consent, suitable for allowing the interested party to exercise full control over the fate of the data that he has given to the original owner: this control can be easily exercised also through the indications that Fastweb provides when contacting the telephone.

Also with reference to the personal data lists that the Company acquires through the company eGentic, which in turn acquires the data from the companies belonging to its business group, Naturvel Pte Ltd. and Tooleado Gmbh, from the documentation produced by the Company and from the investigation carried out the Authority found that the data was processed correctly.

As regards the lists of personal data provided by Fastweb's sales network partners, following acquisitions made by them autonomously from one of their suppliers, the Company's thesis according to which the agencies act as data processors of personal data cannot be shared.

In fact, it has been noted that these lists are acquired by the agencies "independently", or "by themselves" and used "upon

request and authorization [...] by the Fastweb owner". In replying to the request for information, the Company highlighted that in order to be able to use these lists, the agency is required to request authorization from Fastweb by providing a series of elements which will be subject to verification by the latter. In the event that the analyzes carried out by Fastweb provide a positive result, the partner is authorized to upload the personal data in his possession so that they can be used in planning for the current month.

The preliminary investigation shows that the agencies acquire the personal data lists "independently", being able to abstractly use them not only for Fastweb promotional campaigns but also for other subjects. It follows that, at the time of acquiring the master data lists, they operate not as data processors (as Fastweb claims), but as independent data controllers.

It therefore emerges that the lists of personal data provided by the partners of the Fastweb sales network, following acquisitions made by them as independent data controllers, have merged into the circuit of treatments for promotional purposes of which the Company is the owner, through a transfer between independent owners. This transfer cannot be masked or circumvented by the subsequent designation of the partners themselves as Fastweb's data processors. The partners in question have therefore transferred these lists to Fastweb only on the basis of the original consent that the interested parties have given to the list editors, consent which however is unsuitable for allowing further data communications.

As observed in several recent provisions of the Authority (see, inter alia, provisions n. 232 of 11 December 2019, in www.gpdp.it, web doc. n. 9244365 and n. 224 of 12 November 2020 , in www.gpdp.it, web doc. No. 9485681), this method of data communication is unsuitable for allowing the interested party to exercise full control over them. Therefore, the business model adopted to allow partners to use their own personal data lists to carry out promotional activities on behalf of Fastweb violates the provisions of the Regulation on accountability and consent (art. 5, paragraphs 1 and 2, art. 6, paragraph 1 and art. 7).

2.2.3. With reference to the dispute referred to in point 3), it is confirmed that there is a violation of articles 5, 6, 7, 12, 13 and 21, in relation to the methods of activation, release of the information and revocation of the "Call me back" service.

It was noted that the "Call me back" service follows a well-defined procedure which allows for a planned recontact of the customer following his request.

However, from the investigation carried out by the Office, it emerged that the Company has not prepared ad hoc information in relation to this service, in which its functioning, the methods of processing personal data and recontacting the user are

explained . Indeed, the synthetic notice inserted near the service activation button merely warns the user that, by activating it, he gives his "consent to the processing of personal data to receive telephone contacts on Fastweb offers exclusively during the [...] indicated".

In this regard, the defensive arguments according to which "it was sufficient for the interested parties to be informed of the 'processing purposes', which happened", while "the number of potentially feasible contacts or what would have happened in the case of free numbering" do not appear acceptable they are "aspects that do not pertain to the purposes [...] but to the technical methods for their pursuit".

It should be noted that, when the "technical methods" are particularly invasive as in the present case, in which the user could potentially be "recalled [...] 4 times in an hour at a distance of 15 minutes each for a total of 20 attempts [...] throughout the day" before "the contact [is] closed", these become an integral part or rather a characteristic of the processing, of which the user must be informed in advance before giving his consent, precisely in reason for their particular pervasiveness. Consider, for example, the reports of users who have complained of "telephone persecution" following the activation of the service.

Even the new information prepared by Fastweb, although it explains how the service works by letting the user understand that following activation of the same, "subsequent attempts" to call will follow, it appears generic where it limits itself to stating that "in case of unsuccessful contact we will try to call you back in the following days until the expiry of the useful attempts which vary according to the impediment encountered (line busy, no answer) and the operators available. In any case, subsequent attempts to follow up on your request will be carried out in compliance with the originally chosen time slot".

We also note the lack of a system that allows the user to easily deactivate the service with the same simplicity with which it is possible to activate it. In this regard, Fastweb's arguments according to which, for the deactivation of the service, it would be sufficient for the interested parties to "respond[nde] to the requested recontact call" do not appear to have merit. Indeed, the object of the dispute is precisely the absence of a system that easily allows the interested party to interrupt the flow of calls if he is unable (or simply no longer willing) to answer the calls. Nor does the service deactivation procedure "by simply sending an email" appear to be a proportionate measure compared to the activation procedure which requires a simple "click". If it is true that "it is not a condition for the validity of the consent that there are methods of revocation exactly mirroring those for the release", it is equally true that it is the obligation of the data controller to "provide for methods aimed at facilitating the exercise, by of the interested party, of the rights referred to in the […] Regulation" (Article 12 of the Regulation and recital 59).

The cases reported, if traced back to the system through the indications provided by Fastweb, show how the lack of adequate information and the lack of adequate procedures for withdrawing consent have prevented the interested parties (i) from giving free, specific and informed, through an unambiguous positive action; (ii) to interrupt the flow of calls, hindering them in exercising their rights.

The fact that Fastweb has not adopted a system that "facilitates the exercise of the data subject's rights" including the right to object as well as the failure to comply with the provisions on information constitutes a violation of the related provisions of the Regulation, contained in the articles 5, 6, 7, 12, 13 and 21.

2.2.4. With reference to the disputes referred to in points 4) and 5), the violation of articles 24 and 32 of the Regulation, in relation to multiple and systematic accesses to corporate databases containing personal data (including personal data, telephone numbers, telephone traffic and payment data), for having failed to implement measures of proportionate effectiveness to in order to: guarantee (and be able to demonstrate), that the treatment is carried out in compliance with the Regulation; ensure the confidentiality and integrity of processing systems and services on a permanent basis; and regularly test, verify and evaluate the effectiveness of the technical and organizational measures to ensure the security of the processing (files 147286, 154212, 146491, 146238, 146260, 139824, 148138). The violation of art. 33, par. 1, and 34 of the Regulation, for having failed to submit to the Guarantor and to the interested parties the notification of a violation of personal data, with reference to the multiple accesses referred to above.

It is undisputed that the Company has been aware since July 2019 of the phenomenon involving hundreds of Fastweb customers, who have been the recipients of illicit contacts by unknown persons who, posing as Fastweb operators, requested to send a copy via Whatsapp of their identity documents, which a substantial number of users have actually done. As stated by the Company itself, the phenomenon has wider dimensions and this can also be inferred from the high number of reports received by Fastweb which have been the subject of complaints by the Company to the competent Authorities, also originating from reports of technical failures in the proposals branches of the company.

In this regard, the measures adopted by the Company, including the process of reporting unknown persons to the Postal Police, awareness-raising and information activities towards and to protect its customers and the market, or the activities carried out on system security, are not considered effective and adequate in order to protect customer data and verify, also through log file analysis, the existence of illegal accesses.

In the face of a substantial number of episodes brought to the attention of the Company, the interventions carried out do not appear to have constituted a serious contrast to the attempts to exfiltrate data from the company databases considering that these episodes also occurred in very recent periods.

In this regard, the Guarantor in the aforementioned provision of 12 November 2020 n. 224 observed that, "while within the previous regulatory framework, security in the privacy field could be considered formally ensured with the application of the minimum security measures indicated in articles 33 et seq. of the Code, in the formulation prior to the changes introduced by Legislative Decree lg. no. 101/2018, and the rules referred to in the connected technical specification, regardless of the functional and dimensional configuration of the systems, the judgment of adequacy of the aforementioned measures remaining confined to the assessment of the civil liability of the owner in the event of destruction or loss, even accidental , of the data themselves, of unauthorized access or of treatment that is not permitted or does not comply with the purposes of the collection, with the current structure dictated by the Regulation, it is precisely the events described above that determine, due to the risks for the rights and freedoms of natural persons, a first and qualifying judgment of adequacy on the security measures adopted. This in particular, as indicated in recital 75 of the Regulation, with reference to treatments 'likely to cause physical, material or immaterial damage, in particular: if the treatment can lead to discrimination, theft or usurpation of identity, financial losses, prejudice to reputation […] or any other significant economic or social damage; [...] if the processing concerns a significant amount of personal data and a large number of data subjects'".

It is clear that, given the seriousness of the events reported by the complainants, and the resulting potential prejudice to the rights and freedoms of the data subjects, the Company should have intervened promptly with drastic and suitable measures to prevent the occurrence of similar episodes. That didn't happen. On the contrary, the documentation in the documents shows that, although the first reports had already been received by the Company in mid-2019, still in October 2020 users reported that they had been contacted by unknown subjects who presented themselves as Fastweb operators and they request copies of their identity documents.

Nor would the circumstance for which "the leakage of data [would take place] outside the systems pertaining to it" exclude liability. Even if Fastweb's assumptions were proven, it is undisputed that the object of illicit contacts were all Fastweb customers, so that any "presence of a distinct ownership in the processing" would not exonerate the Company from the duty to protect data security personal data of its customers (for which there is no doubt that the Company is the data controller), or

from the obligation to communicate a data breach pursuant to articles 33 and 34 of the Regulation, in relation to the violation of personal data relating to its customers.

2.2.5. With reference to the objection referred to in point 6), the observations expressed by Fastweb in the exercise of the right of defense confirm the existence of the Company's responsibility for failure to comply with the principle of accuracy of data (violation of Articles 5, paragraph 1, letter d) in relation to articles 15-22 of the Regulation, since in various instances of exercising the rights proposed by the interested parties, system errors and delays in the realignment and correction of the data were found (files 136409, 146607, 148287, 147619, 152006, 137155).

On the aforementioned reports and complaints it must be highlighted that the generic indication of a "manual error" and/or an undocumented system error is not suitable for eliminating the Company's responsibility for undue contacts and/or inadequate management of requests to exercise rights, since, also on the basis of the principles established by art. 3 of the law n. 689/1981 on the subject of good faith, the error on the lawfulness of the fact can be considered as a cause for exclusion of administrative liability only when it is inevitable, and for this purpose a positive element is needed suitable for inducing such an error, which cannot be remedied by the interested party with ordinary diligence. This element was not provided by the Company. Furthermore, on the basis of what is established in general terms by art. 25 of the Regulation and, more specifically, by art. 12, par. 1, in terms of transparency, an adequate structuring of systems, organization and work cycles should lead to the exclusion of the recurrence of this type of error.

It should be added that, as already noted in the dispute, in some of the aforementioned cases, even years have passed for the resolution of the problems raised.

In the cases as identified above, the existence of the violation of the provisions pursuant to articles is therefore confirmed 5, par. 1, lit. d), with reference to the principle of "accuracy" of the data processed, in relation to articles 15-22 of the Regulation.

With regard to the number of disputed cases which would represent a modest percentage compared to the amount of requests to exercise rights that Fastweb processes every month, it is reiterated that: i) the number refers only to cases brought to the attention of the Authority, not clearly excluding that there are many others; ii) the reports are examples of a problem detected in Fastweb's feedback system, which could potentially involve hundreds of thousands of users; iii) in any case, this element cannot eliminate the need to ensure the individual protection to the interested parties that the Regulation provides for, through the adoption of corrective and sanctioning measures.

Nor can Fastweb's thesis be shared according to which "having changed the sanctioning mechanism" one would no longer "reason[ed] in terms of 'micro-sanctions'" based "on individual 'micro-fulfilments'" but "of sanctions calculated on the total turnover of the enterprise" founded "on the overall vision of accountability". Contrary to Fastweb's claims, the new system of sanctions does not prohibit at all (much less it prohibited it in the past) from reasoning for individual violations, and at the same time, for violations of the systems. There is a tool, the art. 83 par. 3 which allows for the unification of the violations, ensuring that the individual conducts can be relevant for the overall assessment of the sanction.

2.2.6. With reference to the dispute referred to in point 7), the violation of articles 5, par. 1 and 2, 6 and 7 of the Regulation, in relation to the processing of personal data carried out for promotional purposes of own products and services, carried out in the absence of the prescribed consent and pending the unsuitability of the legal basis of legitimate interest (files 149390, 153360) .

As far as Fastweb's defensive observations are concerned, we agree with what is represented in relation to the fact that "the consent for commercial treatments [...] concerns proposals identified in the product categories [...] which [...] must not be connected to the services already offered to the customer" and which "could also disregard the existence of an ongoing contractual relationship"; otherwise, contacts based on legitimate interest can only concern commercial proposals linked to services already offered to the customer, and cannot disregard the existence of an ongoing contractual relationship.

However, the reconstruction proposed by the Company appears to be contradicted by the cases in question. In such cases, the promotional activities are carried out in partnership with another subject for which they cannot be included among those compatible with the original purpose of the collection (the execution of a contract of which the interested party is a part), nor among those for which the legal basis of legitimate interest can be used. The operators, in fact, do not limit themselves to presenting commercial proposals linked to services already offered to the customer, but promote commercial initiatives even for other subjects. The aforementioned activities are therefore lawful only in the presence of an express consent of the interested party to the processing of their data for marketing purposes which, in the cases highlighted, does not appear to have been released. It should be added that, precisely because they had expressly denied consent to processing aimed at promotional contacts, the interested parties could not have any "legitimate expectation" of being the subject of promotional contacts, moreover referring to products and/or services of different subjects. In this regard, the prospect of a discount on services already subscribed to with Fastweb appears to be a mere commercial expedient which cannot in any way lead to a

change in the legal basis of the aforementioned treatments.

As for the information (including that transmitted to all customers since February 2019), although it has not been the subject of specific disputes by the Authority, for the sake of completeness of treatment it should be noted that the same does not appear, with reference to the indication of the basis of the legitimate interest and of the methods of opposition, sufficiently clear and directly understandable to the interested party in compliance with principles of correctness and transparency of personal data identified in the articles 5, par. 1, lit. a, and 12 of the Regulation.

In addition, also in the content, the information indicates treatments whose legal basis would reside in the legitimate interest and which do not seem to be able to be traced back, for the aforementioned reasons, to this institution (e.g., the use of contact data for "for inform you of [...] our promotions or those of our partners that allow you to have discounts and other advantages on already active services") given that the mere recognition of a discount referring to already active services does not constitute a pertinent link to allow binding the new promotions to the overall profile of the customer, much less in the case of promotions relating to third parties.

3. CONCLUSIONS

In view of the above, Fastweb's responsibility for the following violations is deemed to have been established:

1. violation of articles 5, par. 1 and 2, 6 par. 1, 7, 24 and 25, par. 1 of the Regulation, since Fastweb S.p.A. has not implemented control systems of the personal data collection "chain" from the moment of the first contact of the potential customer, capable of excluding with certainty that illicit or unwanted promotional calls have led to the activation of services or the signing of contracts then merged into the Fastweb databases. The violation involves the entire customer base of the company and the complaints referred to in files 117698, 144450, 152962, 138241, 151747, 154404, 144577, 149829, 150096, 150853, 151543, 152330, 152792, and 154;

2. violation of the art. 5, par. 1 and 2, of the art. 6, par. 1, and of the art. 7 of the Regulation, since Fastweb S.p.A. acquired personal data lists from third parties (the partners of its sales network) who, in turn, had acquired them as independent data controllers and who transferred them to Fastweb's systems. The transfer of data to Fastweb took place in the absence of the required consent for the communication of personal data between independent data controllers. The breach involved at least 7,542,000 data subjects in 2019;

3. violation of articles 5, 6, 7, 12, 13 and 21, in relation to the methods of activation, release of the information and revocation

of the "Call me back" service;

4. violation of articles 24 and 32 of the Regulation, in relation to multiple and systematic accesses to corporate databases containing personal data, telephone numbers, telephone traffic and payment data, for having failed to implement proportionately effective measures to guarantee, and be able to demonstrate, that the processing is carried out in accordance with the Regulation, to ensure the confidentiality and integrity of the processing systems and services on a permanent basis and to regularly test, verify and evaluate the effectiveness of the technical and organizational measures in order to guarantee the security of the treatment (files 147286, 154212, 146491, 146238, 146260, 139824, 148138);

5. violation of the art. 33, par. 1, and 34 of the Regulation, for having failed to submit to the Guarantor and to the interested parties the notification of a violation of personal data, with reference to the multiple accesses referred to in the preceding point;

6. violation of articles 5, par. 1, lit. d), with reference to the principle of "accuracy" of the data processed, in relation to articles 15-22 of the Regulation, in relation to the various requests to exercise the rights proposed by the interested parties for which system errors and delays in the realignment and correction of the data were found (files 136409, 146607, 148287, 147619, 152006, 137155);

7. violation of articles 5, par. 1 and 2, 6 and 7 of the Regulation, in relation to the processing of personal data carried out for promotional purposes of own products and services, carried out in the absence of the prescribed consent and pending the unsuitability of the legal basis of legitimate interest (files 149390, 153360) .

Having also ascertained the unlawfulness of the Company's conduct with reference to the treatments examined, it becomes necessary:

- order Fastweb S.p.A., pursuant to art. 58, par. 2, lit. d) of the Regulation, to adapt the telemarketing treatments in order to provide and prove that the activation of offers and services and the registration of contracts takes place only following promotional contacts made by the Company's sales network through registered telephone numbers and registered in the ROC - Register of Communication Operators;

- order Fastweb S.p.A., pursuant to art. 58, par. 2, lit. d) of the Regulation, to reformulate the information relating to the "Call me back" service, specifically indicating how Fastweb S.p.A. can contact you again. and, always in relation to the aforementioned service, to provide for an automated method for deactivating the service;

- order Fastweb S.p.A., pursuant to art. 58, par. 2, lit. d) of the Regulation, to adapt the security measures for access to its

databases in order to eliminate or in any case significantly reduce the risk of unauthorized access and processing that does not comply with the purposes of the collection;

- impose, pursuant to art. 58, par. 2, lit. f) of the Regulations, to Fastweb S.p.A. the prohibition of any further processing for promotional and commercial purposes carried out through lists of personal data of third parties who have not acquired from the interested parties a free, specific and informed consent to the communication of their data to Fastweb S.p.A.;

- impose, pursuant to art. 58, par. 2, lit. f) of the Regulations, to Fastweb S.p.A. the prohibition of any further treatment of products or services in partnership with the company Eni Gas e Luce S.p.A. towards interested parties who have not given free, specific and informed consent to the processing of their data for promotional purposes by Fastweb S.p.A.;

- adopt an injunction order, pursuant to articles 166, paragraph 7, of the Code and 18 of the law n. 689/1981, for the application against Fastweb S.p.A. of the pecuniary administrative sanction provided for by art. 83, para. 3 and 5, of the Regulation.

4. ORDER-INJUNCTION FOR THE APPLICATION OF THE PECUNIARY ADMINISTRATIVE SANCTION

The violations indicated above require the adoption of an injunction order, pursuant to articles 166, paragraph 7, of the Code and 18 of the law n. 689/1981, for the application against Fastweb S.p.A. of the pecuniary administrative sanction provided for by art. 83, para. 3 and 5 of the Regulation (payment of a sum up to Euro 20,000,000.00 or, for companies, up to 4% of the annual worldwide turnover of the previous year, if higher).

To determine the maximum statutory fine, it is deemed necessary to refer to the turnover of Fastweb S.p.A., in accordance with the previous provisions adopted by the Authority, and therefore to determine this maximum statutory amount, in the case in question, at Euro 90,037 .367.00;

In order to determine the amount of the fine, it is necessary to take into account the elements indicated in art. 83, par. 2, of the Regulation;

In the present case, the following are relevant:

1. the seriousness of the violations (Article 83, paragraph 2, letter a) of the Regulation) with reference to the disputes referred to in points 1), 2), 4), 5), and 7) due to the particular pervasiveness illicit contacts in the context of telemarketing activities (potentially harmful to various fundamental rights and, in particular, in addition to the right to the protection of personal data, the right to individual tranquility and the right to privacy); the level of damage actually suffered by the interested parties, who

with reference to the violations referred to in point 1) have been exposed to nuisance calls; of the growing difficulties they encounter in curbing the phenomenon; the multiplicity of conducts implemented by Fastweb S.p.A. in violation of several provisions of the Regulation and of the Code; episodes of illegal acquisition of contractors' data, with reference to the violations referred to in point 4), which the multiple unlawful accesses to company databases have resulted in, with high risks of identity theft, spamming and phishing activities, and unlawful communications authorized to third parties;

2. as an aggravating factor, the duration of the violations (Article 83, paragraph 2, letter a) of the Regulation), due to the permanent and still existing nature of the violations referred to in points 1), 2), 3) , and 7) as well as the duration exceeding six months of the violations referred to in points 4), 5) and 6);

3. as an aggravating factor, the very high number of subjects involved (Article 83, paragraph 2, letter a) of the Regulation) who, for the violation referred to in point 1) must take into account the entire Fastweb customer base S.p.A. and for the violation referred to in point 2) it includes the over 7 million interested parties present in the lists acquired from third parties;

4. as an aggravating factor the significantly negligent nature of the conduct (Article 83, paragraph 2, letter b) of the Regulation) in consideration of the extensive and constant interlocution with the Guarantor on all aspects of telemarketing, as well as the significant regulatory activity of the Authority, elements that should have constituted a valid support in the organizational choices of the Company but which instead, in particular with reference to the violations referred to in points 1), 2) and 7) were largely disregarded. The violations referred to in points 4) and 5) also assume a significantly negligent character due to the serious vulnerabilities found in the company databases, which have not yet been fully resolved, and the serious delay in notifying an important "data breach";

5. as aggravating factors the specific recurrence of the conduct (Article 83, paragraph 2, letter e) of the Regulation) and the previous adoption by the Authority of similar corrective and sanctioning measures with reference to treatments of the same type (Article 83, paragraph 2, letter i) of the Regulation);

6. as a mitigating factor, the adoption of measures aimed at mitigating the consequences of the violations (Article 83, paragraph 2, letter c) of the Regulation), with particular reference to the control and containment of anomalies in contacts promotions operated by the sales network; the implementation of new platforms to adapt the treatments for promotional purposes to the legislation and to the indications of the Authority; the progressive discontinuation of telemarketing activities that do not meet reliability requirements; the strengthening of security measures for access to corporate databases; and the

adaptation of information and feedback procedures to data subjects;

7. as a mitigating factor, cooperation with the Authority (Article 83, paragraph 2, letter f) of the Regulation) during the preliminary investigation;

8. as a mitigating factor, participation in working groups to combat phenomena attributable to wild marketing activities (Article 83, paragraph 2, letter j) of the Regulation) during the preliminary investigation;

9. as additional factors to be taken into consideration to parameterise the sanction (Article 83, paragraph 2, letter k) of the Regulation), the ample time margin granted to all data controllers in order to allow them to complete and consistent adaptation of systems and procedures to the new European legislation, already in force since 25 May 2016 and fully operational since 25 May 2018; the particular attention that the legislator has dedicated to the regulation of the telemarketing phenomenon, also with recently adopted regulatory interventions (e.g., law no. 5/2018); the significant market position of Fastweb S.p.A. in the telecommunications sector and the overall economic value of the Company.

Based on the set of elements indicated above, and the principles of effectiveness, proportionality and dissuasiveness provided for by art. 83, par. 1, of the Regulation, and taking into account the necessary balance between the rights of the interested parties and the freedom to conduct a business, in the initial application of the pecuniary administrative sanctions envisaged by the Regulation, also in order to limit the economic impact of the sanction on the organisational, functional and employment conditions of the Company, it is believed that it should apply to Fastweb S.p.A. the administrative sanction of the payment of a sum of Euro 4,501,868.00 equal to 5% of the maximum statutory sanction, in line with the recent provisions adopted by the Authority on telemarketing.

In the case in question, it is believed that the ancillary sanction of publication on the Guarantor's website of this provision should be applied, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019, taking into account the conduct of the Company, its partners, as well as the high number of subjects potentially involved in the treatments examined;

Finally, the conditions set forth in art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THIS CONSIDERING THE GUARANTEE

a) orders Fastweb S.p.A., pursuant to art. 58, par. 2, lit. d) of the Regulation, within 30 days of notification of this provision, to

adapt the treatments in the field of telemarketing in order to provide and prove that the activation of offers and services and the registration of contracts takes place only following promotional contacts carried out by the Company's sales network through telephone numbers surveyed and registered in the ROC - Register of Communication Operators;

b) prescribes to Fastweb S.p.A., pursuant to art. 58, par. 2, lit. d) of the Regulation, in the same term referred to in point a), to reformulate the information relating to the "Call me back" service, specifically indicating how Fastweb S.p.A. can contact you again. and, always in relation to the aforementioned service, to provide for an automated method for deactivating the service;

c) requires Fastweb S.p.A., pursuant to art. 58, par. 2, lit. d) of the Regulation, in the same term referred to in point a), to adapt the security measures for access to their databases in order to eliminate or in any case significantly reduce the risk of unauthorized access and processing that does not comply with the purposes of the collection ;

d) imposes, pursuant to art. 58, par. 2, lit. f) of the Regulations, to Fastweb S.p.A. the prohibition of any further processing for promotional and commercial purposes carried out through lists of personal data of third parties who have not acquired from the interested parties a free, specific and informed consent to the communication of their data to Fastweb S.p.A.;

e) imposes, pursuant to art. 58, par. 2, lit. f) of the Regulations, to Fastweb S.p.A. the prohibition of any further treatment of products or services in partnership with the company Eni Gas e Luce S.p.A. towards interested parties who have not given free, specific and informed consent to the processing of their data for promotional purposes by Fastweb S.p.A.;

f) orders Fastweb S.p.A., pursuant to art. 157 of the Code, to communicate to the Authority, in the same term indicated above, the initiatives undertaken in order to implement the provisions and prohibitions adopted; any failure to comply with the provisions of this point may result in the application of the administrative fine provided for by art. 83, paragraph 5, of the Regulation.

ORDER

to Fastweb S.p.A., in the person of its pro-tempore legal representative, with registered office in Milan, Piazza Adriano Olivetti 1, Tax Code and VAT number: 12878470157, to pay the sum of Euro 4,501,868.00 (four million five hundred one thousand eight hundred and sixty eight/00) as an administrative fine for the violations indicated in the justification, representing that the offender, pursuant to art. 166, paragraph 8, of the Code has the right to settle the dispute, with the fulfillment of the instructions given and the payment, within thirty days, of an amount equal to half of the fine imposed

ENJOYS

to the aforementioned company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of Euro 4,501,868.00 (four million five hundred one thousand eight hundred and sixty-eight/00), according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting the consequent deeds executive pursuant to art. 27 of the law n. 689/1981

HAS

the application of the accessory sanction of publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Regulation of the Guarantor n. 1/2019, and believes that the conditions set forth in art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

Pursuant to articles 152 of the Code and 10 of Legislative Decree no. 150/2011, opposition to this provision may be lodged with the ordinary judicial authority, with an appeal filed with the ordinary court of the place where the data controller has its registered office, within the term of thirty days from the date of communication of the provision itself .

Rome, 25 March 2021

PRESIDENT

station

THE SPEAKER

guille

THE SECRETARY GENERAL

Matthew