SEE ALSO Newsletter of March 15, 2023

[doc. web no. 9864063]

Injunction against Commify Italia S.r.l. - January 11, 2023

Register of measures

no. 12 of 11 January 2023

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 Regulation of the Guarantor n. 1/2000;

SPEAKER Dr. Agostino Ghiglia;

WHEREAS

1. THE INVESTIGATION ACTIVITY

On 8 and 9 November 2021, an inspection was carried out against Commify Italia S.r.l. (hereinafter "Commify" or "Company") to verify the functioning of the Skebby platform (www.skebby.it) with which it is possible to send text messages via a web application or via application programming interfaces (API, Application Programming Interface).

The platform in question had already been the subject of previous inspections by the Authority for partly different purposes. In particular, an initial activity – originating from a personal data breach notified by one of the companies using the Skebby platform services – was carried out on 28 and 29 November 2018 at Mobile Solution S.r.l., a company subsequently merged

by incorporation into Commify Italia S.p.A. (which then changed its name to Commify Italia S.r.l.). Subsequently, a further inspection activity was necessary as a result of the additions sent by Mobile Solution S.r.l. and a complaint, received on November 28, 2018, from which a further profile emerged relating to the retention, by the Company, of the text of the text messages sent by customers via the Skebby platform. This second activity took place on 30 and 31 January 2019 at Commify Italia S.p.A.

On 21 July 2021, a request was received from the data protection officer of XX (hereinafter "XX"), a company that uses the services offered through the Skebby platform, with which the Guarantor was requested to rule on the lawfulness of the procedures adopted by Commify regarding the conservation of text messages sent. In particular, the XX raised doubts regarding the procedures adopted by Commify for the conservation of traffic data, deeming the conservation of the content of the text messages sent to be excessive. The latter also represented that it had already requested clarifications from Commify and that it had received a refusal to its request not to keep the content of the text messages sent since, according to the Company, such conservation would be due in compliance with the provisions of articles 121, 123 and 132 of the Code.

In the light of this new request, taking into account that the elements acquired in the previous investigations were insufficient to fully assess the nature of the service offered and any illegality profiles, a new inspection was carried out to verify the current operating methods of the service, at the light of the time that has passed and also taking into account the changes that have occurred at the corporate level. In fact, it must be remembered that the first inspection activity, carried out in 2018, was carried out at Mobile Solution S.r.l., a legal entity that no longer exists after the merger by incorporation into Commify Italia S.p.A., and that this activity was actually aimed at verifying the procedures that could have originated the personal data breach involving a user of the Skebby platform. The second inspection activity, conducted in 2019, was instead carried out at Commify Italia S.p.A., now Commify Italia S.r.l., and was aimed at requesting further information regarding the personal data breach, also in light of the supplementary documentation sent, as well as acquiring elements regarding what was complained of in the aforementioned complaint.

Therefore, the last on-site activity was carried out on 8 and 9 November 2021, as soon as it was possible to resume the inspection activities suspended since March 2020 due to the pandemic.

During the investigation, the Company clarified that it was registered with the ROC as a virtual operator of electronic communication services accessible to the public with the right to issue SIM cards, both physical and virtual, to send and

receive text messages. To this end, the Ministry of Economic Development has assigned it a range of numbers starting from 43.

The Company also specified that the service is currently offered only to business-type customers (private individuals or public entities) as for over two years the use of the services by consumer-type customers has no longer been permitted.

To activate the service, customers must register on the Skebby platform by providing the following data: name, surname, e-mail address, company name, mobile phone number, to which the tax code/VAT number is added during the purchase and the address; they must also set up a username and password.

During the inspection activity, it was verified that the Company also stores in its systems the content of messages sent by its customers, including, for example: one time password (OTP) sent to operate with banking services, authentication credentials, reservations of appointments for health services, communications of availability of nominative medical reports, messages sent by political parties to their members. In this regard, the Company has justified this conservation by considering that the content of the messages is to be considered traffic data (art. 121, paragraph 1-bis, letter h), of the Code) with the consequent obligation of conservation pursuant to art. 132 of the Code. In the deed of appointment of the Company as data controller that customers - as data controllers - sign at the time of activating the service, there is a clause according to which the customer gives consent to the conservation of the content of the messages by Commify. In particular, in attachment 3 ("Data Protection Addendum") to the general contract conditions, in point 10.3, it is provided that "the Customer gives express consent for the Supplier to keep the Personal Data, the Traffic Data and the SMS contents for a period not exceeding 24 (twenty-four) months for purposes:

10.3.1. investigation and prosecution of crimes;

10.3.2. of documentation in the event of dispute of the invoice or for the claim of payment even in court;

10.3.3. for the marketing of electronic communications services or for the provision of value-added services;

10.3.4. consultation by the Customer, upon request;

10.3.5. of internal organization, maintenance interventions and statistical surveys;

10.3.6. to satisfy any requests for delivery and/or display of data made by authorized subjects such as, by way of example, administrative or judicial authorities or public security forces".

In the absence of the aforementioned consent, the Company limits itself to inhibiting access to the content of the text

messages sent by the customer but in any case provides for its conservation.

With regard to the methods of access to traffic data and their conservation, it has been ascertained that:

the traffic data (which, according to what the Company claimed, included the content of the text messages) were stored in various systems of the Company, without separate storage being envisaged for the traffic data stored for the purposes of prevention and prosecution of crimes (purposes of justice); all the data was stored without distinction in the systems that Commify also used for other purposes (invoicing or making it available to the customer for consultation);

the computer systems in question could only be reached through the company network which was accessed via VPN (after passing a one-factor computer authentication procedure, based on username and password) and accessible by authorized parties acting under the authority of the Company through users (after passing a one-factor computer authentication procedure, for access to both the operating system and the database management system);

the messages received were stored in the backend systems for a maximum period of two years: in the first 6 months they were made available to customers on the Skebby platform and subsequently, if requested by the customer, they were extracted from the backup copies;

with regard to the messages sent, since there was no separation (physical or logical) of the systems intended for the retention of data for justice purposes, there was also no provision for a definition of the retention times differentiated according to the purposes; at the time of the inspections (November 9, 2021) data relating to text messages sent in October 2019 was found in a database server, data relating to text messages sent in October 2020 were stored in a documentary database, while another database server contained data referring to text messages sent on 15 January 2021.

Finally, it was found that the Company carried out automated checks on the content of messages sent by its customers in order to prevent fraudulent use of the service which, according to what it represented, could have led to its involvement in legal proceedings with increased ordinary work activity. Therefore, the Company informed the customer, through the contractual conditions, of the fact that it reserved "the right to submit the Communications transmitted by the Customer to preventive analysis systems using detection algorithms (URL, domain, keywords)" by blocking the sending of messages in the event that potential fraudulent content has been detected in the alias (alphanumeric string that identifies the sender in place of the telephone number), or in the text (e.g. in the case of links not expressly requested by the customer or for which the customer was not enabled, as well as in the presence of prohibited keywords).

With a note dated November 30, 2021, the Company provided the information that had been subject to reservations during the inspections and, with specific regard to content controls, attached a document relating to the keywords searched by the algorithm both in the alias than in the text of the message.

Furthermore, with the aforementioned note of November 30, 2021, the Company represented that, following the inspections carried out by the Guarantor in January 2019, it had launched a project for the disposal of the API endpoints that used the http protocol. However, Commify has stated that "there are some legacy APIs, inherited from the old Skebby platform before the current one, that still use the http protocol" and that "this is solely due to the fact that some older customers have never updated their systems". In this regard, the Company highlighted that "it has planned to achieve the elimination of all active http endpoints by 2022".

Lastly, following the inspections carried out in November 2021, it emerged that the Company did not keep track of the operations performed on the systems containing traffic data and the content of the messages, by the subjects acting under its authority (cf. Annexes 9 and 10 to the note of 30 November 2021). In particular, it has been ascertained that the operations performed, directly or indirectly, on traffic data and other personal data connected to them, through the interactive use of the systems (at the operating system or database management system level), they were not recorded in special log files. The only operations subject to registration were those relating to logical access (login) to the computer systems or to the Company's network (via VPN remote access).

2. DISPUTING INFRINGEMENTS

With a note dated 4 April 2022, the start of the procedure was communicated, pursuant to art. 166, paragraph 5, of the Code, for the adoption of corrective measures and sanctions based on the results of the last inspection activity.

Preliminarily, the nature of the services offered by the Company was ascertained - taking into account the characteristics of the messaging service offered through the Skebby platform - in the belief that it qualifies as a provider of electronic communication services accessible to the public, to which the regulations relating to communications apply not only due to the qualification that the Company itself has attributed to itself (and recognized with the release of the necessary authorisations), but also taking into account the specific characteristics of the services offered, similar in result to traditional telephone services although provided using a different technology (1).

Having ascertained this, each evaluation was carried out taking into account this particular role assumed by the Company and

the related provisions of a special nature which regulate the conservation of telephone and telematic traffic data. In particular, based on the description of the services rendered through the Skebby platform, it is believed that the processing concerns exclusively data relating to an "electronic" service (see general provision of 17 January 2018, web doc. no. 1482111, as amended by subsequent provision of 24 July 2008, web document No. 1538224, which, in its paragraph 4, establishes that "telematic" services also include "faxes, as well as SMS and MMS messages, via the Internet").

Furthermore, although it must be noted that the Company only allows legal persons to use its services, it must in any case be kept in mind that the service could also be used by natural persons representing sole proprietorships(2) or, residually, in the phase of using the free trial service. In any case, the provisions relating to data processing in the context of electronic communications also apply to legal persons as contractors or users. Finally, it must be taken into account that the service offered by the Company also involves the processing of personal data (also belonging to particular categories) of natural persons who are recipients of the text messages.

Based on the elements acquired during the inspection activities carried out in November 2021 and the subsequent additions received on 30 November 2021, Commify was charged with violating the following provisions:

articles 5, par. 1, lit. f), and 32 of the Regulation and articles 123, 132 and 132-ter of the Code, with regard to the security measures adopted to ensure the conservation of electronic traffic data;

articles 5, par. 1, lit. a), b) and c), and 6 of the Regulation and of the articles 123 and 132 of the Code, believing that the conservation of the content of the text messages was carried out in the absence of an appropriate legal basis;

articles 5, par. 1, lit. a), and 6 of the Regulation, believing that the preventive scanning of the text message content was carried out in the absence of an appropriate legal basis;

art. 25, par. 1 and 2, of the Regulation, for not having complied with the principles of data protection since the design and by default.

3. THE DEFENSE OF THE OWNER

The Company, in exercising its right of defence, sent a memorandum on 4 May 2022 in which it indicated the corrective measures adopted.

Preliminarily, the Company objected that the act of initiation of the procedure would have arrived late since it was notified "... 146 days after the last inspection and 1223 days from the first ..." and therefore, having to consider the duration of the

investigation phase to be illegitimate, the deed would be considered flawed in origin.

With regard to the specific disputed points, the Company then declared that:

a) "even before the notification of the Communication, the Company had started the implementation of the two-factor authentication system (already in use in the other group companies) for each user/person in charge who logs into the internal administration area" using , in addition to the username and password, additional authentication factors for access at the application level (OTP verification code generated via Google Authenticator) and for access at the system level (which are only permitted after setting up a VPN with computer authentication procedure two-factor);

b) "the Company had already begun abandoning the http protocol used by some customers for accessing the platform through APIs some time ago [...] not one that, for mere technical reasons, will maintain http access only until May 20, 2022";

c) the function that allowed authorized subjects operating under the authority of the Company to view the content of messages via the XX application has been deactivated;

d) all preventive checks on sender and text have been disabled for customers who send text messages on the Company's Gateway; in this regard, the Company justified itself by representing that it had acted on the basis of a legitimate interest in carrying out this activity also taking into account that, in the period in which the control procedure was activated, the phenomenon of fraudulent text messages had disappeared. The same also reiterated that the check was carried out in a totally automated manner and that the customer whose message was blocked would receive immediate communication;

e) "two log management and storage systems" have been adopted which guarantee "the completeness, non-modifiability and authenticity of the recordings" and which make it possible to "detect unusual user behavior (e.g. access from a country from which normally no person in charge accesses), reporting them with a specific e-mail, so that, if necessary, we can promptly intervene";

f) a specific database has been created for the storage of traffic data for the purposes of ascertaining and prosecuting crimes physically and logically separated from the documentary database with access allowed through two-factor authentication, one of which is biometric; moreover, the Company has specified that this database keeps the traffic data in encrypted mode, distinguishing the storage time according to the purposes of the law (6 months or a total of 72 months); access to this database and the operations carried out are traced using a specific procedure;

g) the authorization profiles [for access to the Skebby platform systems ...] were updated on the basis of the various corporate

functions, having regard to the specific purposes and types of data";

h) regarding the conservation of message contents, a new procedure has been instituted, both for new customers and for those already registered on the Skebby platform, according to which the Company will proceed to keep the text of messages sent for six months for only customers who have expressed specific consent via a flag in the personal area. In case of failure to provide consent, which can always be revoked in the same manner, no content will be kept. All customers were informed of the new procedure by e-mail dated 21 and 28 April 2022. The contents of the messages, sent by customers who have given their consent to storage, are now recorded in a single database, in encrypted form, and are made visible only to the customer. For all those who have not given consent, the messages have been deleted. However, the Company specified that the systems keep the messages sent for 72 hours in order to ensure the delivery of the message in the event that the transmission is not successful immediately and several sending attempts are required; only the deletion from the backup systems, although started, was not completed at the time of presentation of the defense brief.

However, the Company clarified that many corrective measures had already been taken immediately after the first inspection of 2018 when, for example, it proceeded to "unify the privacy models of the four different companies (Mobyt S.p.A., Digitel Mobile S.r.l., One Etere S.r.l., Mobile Solution S.r.l.) merged by incorporation into Commify". Other corrective measures had been evaluated and their implementation had started, also slowed down by the pandemic for economic reasons, such as the migration from the http protocol to the https protocol, the adoption of a strong authentication system, but also "the rationalization and limitation of privileges of the persons in charge, the encryption of the texts, the minimization of the data stored by reducing the databases, the revision of the retention".

With regard to the conservation of the contents of the communications, erroneously considered traffic data, the Company has "acknowledged its error, the result of an evidently non-punctual interpretation of the regulatory framework and of some operating methods "inherited" by the merged companies" and added that "the retention policy was not changed from 2018 to 2022 due to the legitimate expectation that the Company has developed with respect to what emerged during the inspections and in the absence of an indication, even if only informal, about the 'wrongness of the same".

Lastly, the Company invited the Authority to take into account certain elements in order to postpone the application of a sanction or, alternatively, to quantify it to a lesser extent:

good faith regarding the necessity and opportunity of certain conducts (such as the preservation of the text of the messages or

the preventive scanning of the same to prevent fraud);

the absolute lack of economic advantage and indeed the significant costs incurred to keep ultroneous data (such as text messages) in the erroneous belief of having to comply with a legal obligation;

the constant collaboration provided to the Authority and the timely adoption of corrective measures in the absence of previous violations;

the absence of damages and prejudices for the interested parties taking into account that "indeed, some critical issues that emerged were, albeit erroneously, aimed at trying to offer a better service to the user and greater protection for the interested parties";

the effort made in training the appointees and the intention to appoint a third party to carry out an audit at the end of the implementation of the measures;

the significant losses recorded as a result of the pandemic such that "a fine, even a minimal one, would cause its default with dramatic negative repercussions also in terms of employment".

Finally, on 26 May 2022, a hearing was held, requested by Commify itself, with which the Company acknowledged the completion of the latest corrective measures still being implemented at the time of presentation of the defense brief, ensuring that it has fully stopped using the http protocol and that I have completed deleting the text messages from the backup copies.

4. LEGAL ASSESSMENTS

With reference to the factual profiles highlighted above, also on the basis of the declarations of the Company for which one responds pursuant to art. 168 of the Code, the following assessments are made in relation to the profiles concerning the regulations on the protection of personal data.

4.1 On the lateness of the dispute

The Company argued that the act of initiation of the procedure would have arrived late since it was notified 146 days after the last inspection and 1,223 days after the first, arguing that this constitutes an incurable flaw in the administrative procedure.

This assumption cannot be shared since it must first of all be noted that - as already mentioned - the act of initiation of the procedure, notified on 4 April 2022, had as its object only the contestation of the violations detected during the inspection activities of 8 and 9 November 2021. These assessments were followed by the sending by the Company of the additional information subject to reservations which was received with PEC dated November 30, 2021. Subsequently, the deeds, after

being assessed, to the extent applicable, by the internal divisions of the The authorities, who have provided their respective notices, have been forwarded to the Prosecuting Department. Taking into account that the internal regulation of the Guarantor n. 2/2019(3) quantifies the deadline for notification of the dispute at 120 days and that this deadline runs from the moment of the assessment, the act of initiation of the procedure is to be considered more than timely since the actual phase assessment must be identified not in the moment in which there is the mere acquisition of the deeds (which, moreover, dates back to the date of receipt of the information and documents that the Company had reserved the right to produce and not to that of the inspection assessment), but in the moment in which the Authority, having examined them, is enabled to form its own judgment(4) all the more so in complex cases such as the one we are dealing with where the juridical assessments have been accompanied by insights of a technical nature.

On the other hand, no objection was raised with regard to the inspections carried out in 2018 and 2019, for the following reasons:

- the previous investigations concerned legal entities other than Commify Italia S.r.l. (Mobile Solution S.r.l. and Commify Italia S.p.A.);
- the 2018 activity had a different object being aimed solely at verifying the causes of a personal data breach notified by a user of the Skebby platform;
- the 2019 activity, launched to complete the 2018 investigations and to verify what was reported in a complaint, had only partially touched on some aspects, also the subject of this proceeding, which however needed further study to be fully assessed (first of all the conservation of traffic data and the legal basis for the conservation of the contents of sent messages);
- the performance of a new inspection activity, also due to the notification of XX, was considered a guarantee measure for the Company since the elements acquired during the previous investigations, now dating back, were insufficient to fully evaluate the conduct .

Given this, the preliminary objection cannot be accepted and it is necessary to proceed and proceed on the merits.

4.2 On the measures adopted to guarantee the security of the processing of electronic traffic data

From the investigations carried out it was possible to verify that the Company, which operates as a provider of electronic communication services accessible to the public, adopted security, technical and organizational measures, which were not adequate for the high risks, to be considered by now known, for the rights and freedoms of the interested parties.

We refer, in particular, to the following elements acquired in the documents:

1) the traffic data processed for justice purposes were stored in the same IT systems used by the Company also for other purposes, without any logical or physical separation measures being adopted;

2) differentiated retention times for traffic data for the various purposes had not been defined (remember that articles 123 and 132 of the Code provide that traffic data may be processed for a period not exceeding 6 months for the purpose billing and that the electronic traffic data must be kept for 12 months for justice purposes; while Article 24 of Law No. 167 of 20 November 2017 extended the retention of such data to 72 months for verification purposes and repression of certain specific types of crime); telematic traffic data generated for more than 12 months was found in the Company's IT systems (in November 2021 the most recent data was from October 2019) but, as mentioned, these systems were not separated for the different purposes set out in the articles 123 and 132 of the Code; moreover, taking into account the considerations set out above regarding the qualification of the Company as a supplier of electronic communication services accessible to the public, we do not understand the reasons why Commify has deemed it able to apply only partially the rules on data retention of traffic (see single privacy document, annex 4 to the minutes of 8 November 2021, point 14.6);

3) access to the computer systems on which the traffic data (and the content of the messages) were stored, or in any case processed, by subjects acting under their authority (e.g. customer care operators, system administrators , etc.), was allowed after passing a single-factor computer authentication procedure; this, both at a systemic and application level;

4) the traffic data processed for justice purposes were not protected with cryptographic techniques that would allow them to be made intelligible to anyone who was not authorized to access them, as they were stored unencrypted both within the databases and on the file systems of the company's computer systems Society;

5) the transmission of data between the computer systems of some customers and the Company took place via unsafe communication protocols (http), thus exposing the transmitted data (including the computer authentication credentials necessary for the use of the API) to risks of illicit acquisition or manipulation;

6) the operations carried out on the computer systems containing the traffic data, by the subjects acting under the authority of the Company, were not recorded, with the exception of those relating to logical accesses (login); moreover, the Company did not keep the log files of this latter type of operation with IT procedures capable of certifying their integrity;

7) traffic data generated more than six months ago was made available to customers on the basis of a specific request; this

approach does not comply with the provisions of the current provisions of art. 132, paragraph 3, of the Code which, following the recent amendment made by art. 1 of the legislative decree 30 September 2021, no. 132, provides - for data kept for justice purposes - that "the data are acquired subject to authorization issued by the judge with a reasoned decree".

The Company's conduct was assessed in the light of the provisions of art. 123, 132 and 132-ter of the Code which dictate specific indications regarding the measures to be adopted in the conservation of traffic data. In particular, the art. 132-ter requires electronic communication service providers to adopt, pursuant to art. 32 of the Regulation, technical and organizational measures appropriate to the existing risk. In this regard, it is believed that the measures and precautions to guarantee the interested parties who, with the general provision of 17 January 2008 on the security of telephone and telematic traffic data (web doc. n. 1482111), had been prescribed by the Guarantor , must be, currently, considered as technical and organizational measures that a supplier of electronic communications services is required to adopt to guarantee a level of security adequate to the risk presented by the treatment pursuant to art. 132-ter of the Code and art. 32 of the Regulation. In particular, with reference to the case in question, it must be considered that the aforementioned provision of 17 January 2008 provides, inter alia, that:

the processing of telephone and telematic traffic data by suppliers must be allowed only to specifically authorized persons in charge and solely on the basis of the preventive use of specific IT authentication systems based on strong authentication techniques, consisting in the contextual use of at least two different authentication technologies; for traffic data stored for the exclusive purpose of ascertaining and prosecuting crimes (and generated for more than six months), one of these technologies must be based on the processing of biometric characteristics of the person in charge; these authentication methods must also be applied to all technical personnel (system, network, database administrators) who can access the traffic data stored in the supplier's databases (par. 7.1);

as regards the processing of telephone traffic data for the exclusive purposes of justice, a trace must be kept in advance in a special "access register" of the event, as well as the reasons that led to it, with a subsequent summary description of the operations carried out, also through the use of electronic systems (par. 7.1);

the supplier must define and assign specific authorization profiles to the data processors, differentiating the traffic data processing functions for ordinary management purposes from those for the purpose of ascertaining and prosecuting crimes (par. 7.2);

the computer systems used for the processing of traffic data stored for the exclusive purpose of justice must be different from those used for other purposes (such as billing, marketing, anti-fraud); however, an initial period is admissible, not exceeding 6 months from generation, during which the data can be processed with computer systems not exclusively reserved for the purposes of justice (par. 7.3);

the supplier must adopt suitable IT solutions to ensure control of the activities carried out on traffic data by each person in charge of the processing, whatever his qualification, his skills and the areas of operation and the purposes of the processing; these solutions include the recording, in a special audit log, of the operations performed, directly or indirectly, on the traffic data and on the other personal data connected to them, both when they consist of or derive from the interactive use of the systems, and when they are carried out through the automatic action of computer programs; the audit log systems must guarantee the completeness, non-modifiability, authenticity of the records contained therein, with reference to all processing operations and all events relating to IT security subjected to auditing (par. 7.6);

the traffic data transmission flows between the supplier's computer systems must take place via secure communication protocols, based on cryptographic techniques, or in any case avoiding the use of unencrypted data transmission; secure communication protocols must also be adopted to guarantee the security of the systems more generally, avoiding exposing them to vulnerabilities and the risk of intrusion (par. 7.9).

Having said that, it is noted that the conduct of the Company, in the manner described before the adoption of the corrective measures, has integrated the violation of articles 5, par. 1, lit. f), and 32 of the Regulation and of the articles 123, 132 and 132-ter of the Code.

However, we must acknowledge the timely intervention of the Company which, at present, has declared that it has adopted corrective measures for all the violation profiles listed above. Therefore, it is not considered necessary to exercise corrective powers in this regard. However, due to the violations found, it is deemed necessary to adopt an injunction order against the same Company, pursuant to Articles 58, par. 2, lit. i), of the Regulation.

4.3 On the retention of message content

The Company, both during the inspection activities carried out in November 2021 and in the explanatory note of 30 November 2021, declared that it kept the content of the text messages "...because it believes it is obliged to do so by law, given the combined provisions of articles 121, 123 and 132 of the Code, from which it emerges that the content of the SMS is traffic data

and must be treated and stored as such".

In this regard, it is noted that the art. 121, paragraph 1-bis, lett. h), of the Code defines traffic data as "any data subjected to processing for the purpose of transmitting a communication over an electronic communications network or for the related billing". This generic definition can be fully applied only by integrating it - in conjunction with the principles of proportionality and data minimization - with the purposes expressed in the following articles 123 and 132, which allow for the retention of traffic data as an exception to the general cancellation obligation.

The art. 123 of the Code, in fact, provides that the traffic data are canceled when they are no longer necessary for the transmission of the communication, without prejudice to the possibility of keeping them for a maximum of six months for billing verification or, with the user's consent, for the marketing of services. It is clear that, for the processing of the invoice and for the dispute of the same, the content of the message has no relevance and therefore has no reason to be kept. In this regard, Commify specified that it also used the content of the messages to verify billing since, once the maximum number of characters per message is exceeded, the cost of two text messages is charged. However, this justification cannot be shared since today's technical solutions allow such counts to be made automatically without having to view the message.

In the context of value-added services (Article 121, paragraph 1-bis, letter l), of the Code), on the other hand, it is possible to store the content of the messages but only with the user's consent issued pursuant to the art. 123, paragraph 3, of the Code. In the approach adopted by Commify, on the other hand, the conservation of the content was imposed by Commify itself - on the basis of the erroneous presumption of having to fulfill a legal obligation (which will be discussed in more detail below) - while the the customer's will not to keep such data (as in the case reported by customer XX). Furthermore, taking into account that the purpose of storage is linked to the provision of a value-added service to the customer, access to such data should only be allowed to the latter and not also to Commify's employees. From what was verified in the documents, however, the content of the messages was viewable by the Company's representatives and was instead made available to the customer only upon specific request.

With regard to art. 132 of the Code, its paragraph 1, in extending the retention terms of traffic data for purposes of ascertaining and prosecuting crimes, expressly mentions the exclusion of the contents of communications(5). This exclusion is reaffirmed in the following paragraph 4-ter.

See also recital 15 of directive 2002/58/EC which, in defining traffic data, only mentions data external to the communication, as

well as art. 5 of the same directive according to which "Member States shall ensure, through national provisions of law, the confidentiality of communications made via the public communications network and electronic communications services accessible to the public, as well as of the related traffic data. In particular, they prohibit the listening, capture, storage and other forms of interception or surveillance of communications, and related traffic data, by persons other than users".

Directive 2006/24/EC - even if invalidated by the CJEU due to the insufficient guarantee offered by generalized conservation - nonetheless remains an important point of reference, in terms of interpretation, for principles and definitions and, in this case, provides a useful clarification of the perimeter of data to be kept; to art. 5, in fact, provides a list of the categories of data to be kept with the express exclusion of the content of the communications.

Clarifications in this sense were also provided by the Guarantor with the aforementioned general provision of 17 January 2008.

On the basis of the regulatory framework just described, it is evident that no legal provision imposes the conservation of the contents of communications which, on the contrary, is expressly prohibited(6) unless authorized by the user with specific consent for the provision of value-added services pursuant to art. 123, paragraph 3, of the Code. This last requirement of consent could be taken into consideration precisely in relation to the characteristics of the service provided by Commify since the customer, unlike traditional telephone services, does not have his own device where he can view the messages sent; therefore, a service - ancillary to the sending and specifically requested by the customer - may be necessary for the conservation of such messages that Commify could provide as data controller (qualification it already holds towards its customers). Furthermore, in compliance with the principles of proportionality and data minimisation, access to view these messages should be reserved for the customer and should instead be prohibited for Commify representatives.

Having said all this, it is evident that the conservation of the contents of the messages was carried out in the absence of a suitable legal basis, not only because it was founded on the erroneous belief of having to fulfill a legal obligation (despite the clarity of a regulatory provision in force from years), but also because while recalling the consent (in the privacy policy) as a prerequisite for the marketing of the service, in fact it deprived this consent of the fundamental requirement of freedom (the contractor was obliged to give consent and could not oppose the treatment) . This profile was also confirmed by the grievances of the XX. From this erroneous assumption also derives the failure to comply with the principles of purpose limitation and data minimization since the content of the messages, which in the absence of the user's consent would have to be canceled after sending, was further stored without the need for purposes other than those that led to the original processing.

For these reasons, the violation of the articles 5, par. 1, lit. a), b) and c), and 6 of the Regulation and of the articles 123 and 132 of the Code.

Also in this case, the Company promptly intervened to adopt measures capable of guaranteeing access to the content of the messages only to customers who have expressly consented to it, preventing access to their representatives. Therefore, it is not considered necessary to exercise corrective powers. However, due to the violations found, it is deemed necessary to adopt an injunction order against the same Company, pursuant to Articles 58, par. 2, lit. i), of the Regulation.

4.4 On automated checks on text messages for anti-fraud purposes

The Company scanned the content of the communications and the alias used for sending in order to prevent fraudulent use of its services, with immediate blocking of the sending by the control systems. During the inspections, the Company justified this conduct with the need to avoid involvement in any judicial proceedings initiated against third parties with a consequent increase in its work activity, taking into account the ever increasing frequency with which fraudulent uses of digital services occur (credential theft, phishing, spamming, etc.).

While it is true that these phenomena are now widespread and increasingly harbingers of risks for the data subjects, it is also true that there is currently no specific obligation for providers of electronic communication services accessible to the public to carry out such preventive checks (7). The public interest related to the need to curb online fraud could be considered an appropriate legal basis, pursuant to art. 6, par. 1, lit. e), of the Regulation, only in the presence of a specific legislative source that does not currently exist.

This activity does not even seem to find a basis in the need, and in the corresponding right/duty, of the service provider to adopt security measures aimed at protecting its systems and guaranteeing the correct execution of the service. In fact, unlike scanning aimed at searching for viruses or what happens to anti-spam filters in e-mail, the sending of fraudulent text messages should normally not entail technical consequences for the service provider, therefore semantic scanning of communications aimed at repressing this type of illegal activity (certainly reprehensible but without effects for the provision of the service) cannot be left to a free choice of service provider(8) and also risks blocking the sending of messages that could be perfectly lawful, resulting in an undue interference with the freedom of communications.

At the same time, however, the increasingly probable risks associated with the use of digital services cannot be underestimated. The regulatory context dictated by the Regulation fits into this perspective, which introduces the possible

existence of a legitimate interest of the owner or third parties among the reasons for justifying the processing pursuant to art. 6, par. 1, lit. f), of the Regulation. The specific ability to invoke legitimate interest in anti-fraud controls is expressly mentioned in recital 47(9). However, the possibility of attributing a treatment to legitimate interest presupposes the existence of certain requirements:

a) the existence of an interest of the owner or of third parties which must be legitimate as well as connected to a concrete and not merely hypothetical situation;

b) the need to carry out the processing to satisfy that interest and the proportionality of the intervention;

c) the demonstration that the holder has carried out a balancing test to ensure that the rights and freedoms of the interested parties do not prevail over the legitimate interest of the holder or of third parties.

It being understood that the documentation does not show that this type of assessment has been carried out by the Company, it should be noted that the performance of a treatment that is highly prejudicial to the freedoms of the interested parties, such as scanning the content of communications with the consequent blocking of themselves, cannot be considered admissible only to protect an interest of the data controller consisting in the desire to avoid an indirect involvement in judicial activities, an involvement which is only purely hypothetical and which must in any case be considered connected to the business risk.

On the other hand, the consequences on third parties and on the interested parties themselves deriving from the unlawful use of these services may have greater importance. In this regard, the provisions of art. 32 of the Regulation on the basis of which the owner is required to adopt all the technical and organizational measures he deems necessary to guarantee a level of security adequate to the risk generated by the processing. Although the service provider does not have a generalized obligation to carry out preventive checks, it is necessary, in the provision of digital services, to pay the utmost attention to the potential risks associated with their use, bearing in mind the general precautionary principle . In these terms, technical and organizational measures are allowed, aimed at preventing or curbing the abusive use of the service, without however exceeding the limit of respect for the rights and freedoms of the interested parties. Any measure involving a sacrifice of these rights and freedoms, to be considered as an extrema ratio, should be adopted only if effectively necessary and proportionate in the absence of less harmful alternatives.

Based on common experience, it can be hypothesized that the greatest risks associated with this type of service could derive from the abusive use of existing accounts by unfaithful employees of the customer or by third parties(10); less probable should

be the activation of new accounts directly by malicious agents (who, to succeed, would have to circumvent the identification system). Therefore, with a view to balancing interests and in compliance with the principles of necessity and proportionality, the solutions aimed at preventing or curbing the abusive use of the service should first of all be sought among the measures aimed at preventing unauthorized access to the accounts of clients; the same preventive value could be obtained by strengthening the measures aimed at blocking the use of aliases connected to potential fraudulent intentions (possibly) before packaging the message itself.

Finally, this treatment could be the object of a value-added service offered to those customers who want greater guarantees to protect their account in order to prevent improper use by their appointees or in the event of access by unauthorized third parties. In this case it is clear that this type of treatment should be based on a free and specific consent of the user.

Recalling the considerations already expressed regarding the conservation of the content of communications, it is believed that even in the case of automated control of the text of messages - in the absence of the necessary precautions - there is excessive interference in the confidentiality and freedom of communications. This is because scanning the content of the message in search of keywords still requires an examination of the entire text and, as a consequence, immediately blocks the sending.

Therefore, the choice of the measures to be adopted must be preceded by accurate assessments by the owner, remembering that each treatment must be carried out in the presence of an appropriate legal basis.

From what has emerged in the documents, it does not appear that Commify has carried out this type of assessment, limiting itself to deeming its actions compliant with the practices in use in the reference market and generically invoking a legitimate interest only in the defense brief of May 4, 2022, without however documenting the existence of the requirements indicated above for the application of this legitimate interest. Furthermore, no legal basis for this type of treatment has been identified by the owner (since it is not possible to find information on this matter either from the information on the processing of personal data, or from the register of processing activities or from the document called "Single privacy document") and, as described above, none of the legal bases provided for by art. 6 of the Regulation is correctly applied or applicable to the specific case, in the terms in which the treatment is set up: the consent cannot be expressed in a free and specific way; the treatment is not currently necessary for the execution of a contract; there is no legal obligation which requires the owner to carry out preventive checks on the content of the messages or which makes the processing necessary for the execution of a task in the public

interest; the application of the legal basis of legitimate interest is allowed only in the presence of certain requirements which, in the case in question, do not appear to be present or have not been sufficiently weighted and justified, let alone documented.

However, it must be remembered that the fraud prevention activity cannot be defined as illegal in itself and can be carried out on the basis of the legitimate interest following the outcome of more complete assessments that take into account the necessity and proportionality of the treatment, the absence of alternative , the balancing of opposing interests and the most effective and least invasive methods for carrying out this treatment. After all, Commify itself observed that, since the preventive control mechanism was in place, the sending of fraudulent text messages had been eliminated.

Therefore, the processing is unlawful as it is carried out in the absence of an appropriate legal basis in violation of the articles 5, par. 1, lit. a), and 6 of the Regulation.

However, taking into account the absence of willful misconduct and indeed of good faith, also demonstrated by the fact that the Company would not have had an economic advantage from this activity, considering that mostly the treatment concerned legal persons, pursuant to art. 58, par. 2, lit. b), of the Regulation, it is considered sufficient to warn the Company regarding the violations found, inviting it to carry out further assessments of the legal basis and methods of treatment in the event that it intends to carry out anti-fraud checks in the future.

4.5 On data protection by design and by default

Based on the principle of "data protection from the design" (Article 25, paragraph 1, of the Regulation), the data controller is required to implement the principles of data protection (Article 5 of the Regulation) by adopting technical measures and adequate organizational and integrating in the treatment the necessary guarantees to meet the requirements of the Regulation and protect the rights and freedoms of the interested parties. The obligation to maintain, verify and update, where necessary, the processing also applies to pre-existing systems. This implies that the systems designed before the entry into force of the Regulation must be subjected to checks and maintenance to ensure the application of measures and guarantees that implement the principles and rights of data subjects effectively (see the "Guidelines 4/2019 on article 25 - Data protection from the design and by default" adopted by the European Data Protection Committee on 20 October 2020, spec. points 7 and 38).

Furthermore, the principle of "data protection by default" (Article 25, paragraph 2, of the Regulation) requires the data controller to make choices such as to ensure that, by default, only the processing strictly necessary for achieve a specific and lawful purpose. This therefore means that, by default, the data controller must provide limitations, both to the subjects authorized to

access and to the type of access to personal data, based on an assessment of the need, as well as provide that the data no longer necessary for the purposes of the processing they are canceled or made anonymous (see the aforementioned "Guidelines 4/2019 on article 25", specifically points 42, 53 and 55).

With reference to the case in question, in relation to the principle of "lawfulness, correctness and transparency" (Article 5, paragraph 1, letter a), of the Regulation), it is represented that the owner must identify a valid legal basis for the processing of personal data (see the aforementioned "Guidelines 4/2019 on article 25", specifically point 67). In particular:

the correct legal basis must be applied to the treatment;

the legal basis must be established before the processing takes place and be clearly related to the specific purpose of the processing.

With reference to the principle of "purpose limitation" (Article 5, paragraph 1, letter b), of the Regulation), the data controller must collect data for specific, explicit and legitimate purposes and not further process them in a way incompatible with the purposes for which they were collected (see the aforementioned "Guidelines 4/2019 on article 25", spec. point 71). In particular:

the legitimate purposes must be determined before processing is planned;

the purpose of the treatment must guide the planning of the treatment and determine its limits;

the purpose must determine which personal data are necessary for the processing;

the controller should periodically check whether the processing is necessary for the purposes for which the data were collected and test the design of such processing with regard to the purpose limitation principle.

With reference instead to the principle of "data minimization" (Article 5, paragraph 1, letter c), of the Regulation), the controller must predetermine the characteristics and parameters of the processing systems, in order to ensure that only the personal data which are adequate, relevant and limited to what is necessary for the purpose they are processed (see the aforementioned "Guidelines 4/2019 on article 25", spec. point 73). In particular:

the amount of personal data collected must be limited to what is necessary for the specific purpose;

data processing should be defined in such a way that a minimum number of persons need access to personal data to perform their duties, and access restricted accordingly;

each category of personal data must be necessary for the specified purposes and must only be processed if the specific

purpose cannot be achieved by other means.

Finally, with reference to the principle of "integrity and confidentiality" (Article 5, paragraph 1, letter f), of the Regulation), the controller must constantly assess whether he is using, at any time, the appropriate means of treatment and whether the measures adopted effectively counter existing vulnerabilities (see the aforementioned "Guidelines 4/2019 on article 25", spec. points 84 and 85). In particular, the owner must:

assess the risks to the security of personal data, considering the impact on the rights and freedoms of data subjects, and effectively counter those identified;

carry out periodic reviews of the security measures put in place to monitor and protect personal data;

take into account safety requirements as soon as possible in the design and development of the system, constantly integrating and carrying out relevant tests;

define data processing in such a way that a minimum number of people need access to personal data to perform their functions, and limit access accordingly;

protect personal data from unauthorized and accidental modifications and accesses, both during their transfer and during their conservation.

From what emerged in the documents (see paragraphs 4.2, 4.3 and 4.4), it does not appear that the Company has adopted, in compliance with the principles of "data protection since design" and "data protection by default", measures and adequate guarantees to effectively implement the principles of "lawfulness, correctness and transparency", "purpose limitation", "data minimization" and "integrity and confidentiality" (Article 5, paragraph 1, letter a), b), c) and f), of the Regulation), also taking into account the risks for the rights and freedoms of the interested parties deriving from the treatments in question.

For these reasons, the violation of the art. 25, par. 1 and 2, of the Regulation.

However, having regard to the fact that the effects of this violation have already been considered as the subject of a sanction at the points indicated above, taking into account the corrective measures already implemented by the Company, it is considered sufficient to address a warning to Commify, pursuant to art. 58, par. 2, lit. b), of the Regulation, with regard to the violations found and, so that conduct similar to that highlighted above is not repeated, we recall the need to periodically carry out assessments in order to check the adequacy of the technical and organizational measures adopted or to be adopted in the future .

5. INJUNCTION ORDER FOR THE APPLICATION OF THE PECUNIARY ADMINISTRATIVE SANCTION

On the basis of the above, various provisions of the Regulation and of the Code are violated in relation to connected treatments carried out by Commify, for which it is necessary to apply the art. 83, par. 3, of the Regulation, on the basis of which, if, in relation to the same treatment or related treatments, a data controller violates, with willful misconduct or negligence, various provisions of the Regulation, the total amount of the pecuniary administrative sanction does not exceed the amount specified for the most serious violation with consequent application of the sole sanction provided for by art. 83, par. 5, of the Regulation.

For the purpose of quantifying the administrative fine, the aforementioned art. 83, par. 5, in setting the statutory maximum in the sum of 20 million euros or, for companies, in 4% of the annual worldwide turnover of the previous year where higher, specifies the methods for quantifying the aforementioned fine, which must "in any case [be] effective, proportionate and dissuasive" (Article 83, paragraph 1, of the Regulation), identifying, for this purpose, a series of elements, listed in par. 2, to be evaluated when quantifying the relative amount.

In fulfillment of this provision, in the present case, having verified, on the basis of the latest available financial statements, the occurrence of the first hypothesis envisaged by the aforementioned art. 83, par. 5 and therefore quantified at 20 million euros as the applicable statutory maximum, the following aggravating circumstances must be considered:

1. the broad scope of the processing extended to the generality of customers of the Skebby platform services relating to approximately 7,250 customers, natural and legal persons, between October 2018 and October 2021 as shown in attachment 5 to the minutes of 8 November 2021 (Article 83, paragraph 2, letter a), of the Regulation);

2. the seriousness of the violations detected, due to the fact that, due to the inadequacy of the security measures, a type of personal data has been exposed to violations (telephone traffic data and communication contents) for which the legislator, in consideration of the high level of damage deriving from the processing, it has prepared special rules to protect conservation (Article 83, paragraph 2, letter a), of the Regulation);

3. the degree of responsibility of the data controller, taking into account that the technical and organizational measures used for the conservation of electronic traffic data have not been found to be adequate to the state of the art, despite the fact that the provisions of the Guarantor are by now considered widely known among operators of electronic communication services, as given with a general provision of 2008, repeatedly subject to specific application provisions (art. 83, paragraph 2, letter d), of

the Regulation);

4. the categories of personal data affected by the violation, also belonging to particular categories (information on the state of health or on membership of a political party), present in the messages stored by Commify (Article 83, paragraph 2, letter g), of the Regulation);

5. the manner in which the Supervisory Authority became aware of the violations, which emerged during an inspection activity (Article 83, paragraph 2, letter h), of the Regulation).

As mitigating elements, it is considered necessary to take into account:

1. of the intentions of the Company which, on the basis of what has been acquired in the documents, do not appear aimed at consciously realizing the effects of the disputed conduct and are rather attributable to a negligent and sometimes naive application of the rules; this also taking into account the corporate changes that have occurred in recent years and the consequent need to integrate different corporate systems and procedures (Article 83, paragraph 2, letter k), of the Regulation);

2. the degree of awareness of the Company regarding the effective extent of the violations due to the particular nature of the service provided such as not to allow an immediate attribution of Commify's activity to the charges applicable to electronic communication services accessible to the public and (Article 83, paragraph 2, letter k), of the Regulation);

3. of the absence of an economic return from the violations but, rather, of the increase in costs incurred for the conservation of volumes of data relating to the contents of the communications in the erroneous belief of having to fulfill a legal obligation (art. 83, paragraph 2, letter k), of the Regulation);

4. the timely adoption of corrective measures, some of which had already started before the 2021 inspections (Article 83, paragraph 2, letter f), of the Regulation);

5. the high degree of cooperation in interaction with the Supervisory Authority (Article 83, paragraph 2, letter f), of the Regulation);

6. the data of the latest available financial statements and the significant economic losses with consequent increased debt, as represented by the Company in attachment no. 8 to the defense brief (Article 83, paragraph 2, letter k), of the Regulation).

With an overall view of the necessary balance between the rights of the interested parties and the freedom to do business, taking into account that the Company, and in the initial application of the pecuniary administrative sanctions envisaged by the Regulation, it is necessary to evaluate the aforementioned criteria prudently, also in order to limit the economic impact of the

fine on the organisational, functional and employment needs of the Company.

Therefore it is believed that - on the basis of all the elements indicated above, the administrative sanction of the payment of a sum equal to 0.4% of the maximum statutory sanction of 20 million euros, corresponding to 80,000.00 euros (eighty thousand). The maximum statutory sanction is identified with reference to the provisions of art. 83, par. 5 of the Regulation, taking into account that 4% of Commify's turnover, on the basis of the latest available balance sheet, is less than 20 million euros.

It should be noted that the conditions set out in art. 17 of the Regulation of the Guarantor n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor, for the annotation of the violations detected here in the internal register of the Authority, provided for by art. 57, par. 1, lit. u) of the Regulation.

It is also believed - in consideration of the seriousness of the violations found - that, pursuant to art. 166, paragraph 7, of the Code, and of the art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019, it is necessary to proceed with the publication of this provision on the website of the Guarantor, by way of ancillary sanction.

ALL THAT BEING CONSIDERED, THE GUARANTOR

against Commify Italia S.r.l., with registered office in Via Manzoni 38, Milan, VAT no. 01648790382,

a) pursuant to art. 58, par. 2, lit. b), of the Regulation, issues a warning regarding the violations found in point 4.4, inviting you to carry out further assessments of the legal basis and methods of processing in the event that you intend to carry out anti-fraud checks in the future;

b) pursuant to art. 58, par. 2, lit. b), of the Regulation, issues a warning regarding the violations found in point 4.5 and, so that conduct similar to that highlighted above is not repeated, recalls the need to periodically carry out assessments in order to check the adequacy of the technical and organizational measures adopted or to be adopted;

ORDER

pursuant to art. 58, par. 2, lit. i), of the Regulations, to Commify Italia S.r.l., in the person of its legal representative, to pay the sum of 80,000.00 (eighty thousand) euros as an administrative fine for the violations indicated in the justification; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within 30 days, 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 80,000.00 (eighty thousand) euros, according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting the consequent executive deeds pursuant to art. . 27 of the law n. 689/1981;

HAS

pursuant to art. 166, paragraph 7, of the Code, the full publication of this provision on the Guarantor's website.

Pursuant to art. 78 of Regulation (EU) 2016/679, as well as articles 152 of the Code and 10 of Legislative Decree 1 September 2011, n. 150, opposition to this provision may be lodged with the ordinary judicial authority, with an appeal lodged with the ordinary court of the place where the owner of the processing of personal data has his residence, or, alternatively, with the court of the place of residence of the interested party. , within the term of thirty days from the date of communication of the provision itself, or sixty days if the appellant resides abroad.

Rome, 11 January 2023

PRESIDENT

station

THE SPEAKER

guille

THE SECRETARY GENERAL

Matthew

NOTE

1) In this regard, reference is made to the principles expressed in Directive (EU) 2018/1972, cons. 15, recently implemented in the revised Electronic Communications Code: "In order to ensure that end users and their rights are effectively and equally protected when they use equivalent services from a functional point of view, a definition of electronic communications services that is future should be based on a functional approach rather than exclusively on technical parameters".

2) In the list of customers 2019-2021, acquired in the file, there are also natural persons (see annex 5 to the minutes of 8 November 2021).

3) Regulation no. 2/2019 concerning the identification of the terms and organizational units responsible for administrative

procedures at the Guarantor for the protection of personal data (published in the Official Gazette n. 107 of 9 May 2019 and in www.garanteprivacy.it web doc. n. 9107640).

4) In these terms cf. also Cons. state, sent. 1330/2015, which Commify itself cited in the defense brief, as well as, ex plurimis, Cass. Civ. section II no. 21333 of 29.8.2018, Cassation civ. 17 August 2016, no. 17143, Civil Court section work no. 22837 of 10/28/2014, Council of State section VI, no. 4085 of 08/05/2013.

5) Art. 132, paragraph 1, of the Code: "without prejudice to the provisions of art. 123, paragraph 2, the data relating to telephone traffic are kept by the supplier for twenty-four months from the date of communication, for the purpose of ascertaining and suppressing crimes, while, for the same purposes, the data relating to electronic traffic, however excluding the contents communications, are kept by the supplier for twelve months from the date of communication".

6) See art. 132 of the Code. Furthermore, access to the contents of the communications could constitute an undue interference in private life in violation of art. 8 of the European Convention on Human Rights, as repeatedly clarified by the interventions of the Court of Justice of the European Union.

7) See articles 14 et seq. legislative decree 9 April 2003, n. 70.

8) See opinion on privacy aspects of email screening services (WP 118), adopted by the Article 29 Working Party on 21 February 2006.

9) See Guidelines 2/2019 on the processing of personal data pursuant to Article 6(1)(b) of the General Data Protection Regulation in the context of the provision of online services to data subjects, adopted by the European Committee for data protection on 8 October 2019, which recall opinion no. 6/2014 on the concept of legitimate interest of the data controller pursuant to Article 7 of Directive 95/46/EC (WP 217), adopted by the Article 29 Working Party on 9 April 2014, which highlights that "the processing for of fraud prevention may involve the monitoring and profiling of customers. According to the European Data Protection Board, it is probable that such processing goes beyond what is objectively necessary for the performance of a contract entered into with a data subject. However, the processing of personal data strictly necessary for fraud prevention purposes may constitute a legitimate interest of the data controller and can therefore be considered lawful if the data controller meets the specific requirements set out in Article 6, paragraph 1, letter f) " .

10) As already happened in 2018 on the occasion of the personal data breach involving a customer of the Skebby platform services whose account, subject to abusive access, had been used to massively convey phishing text messages.