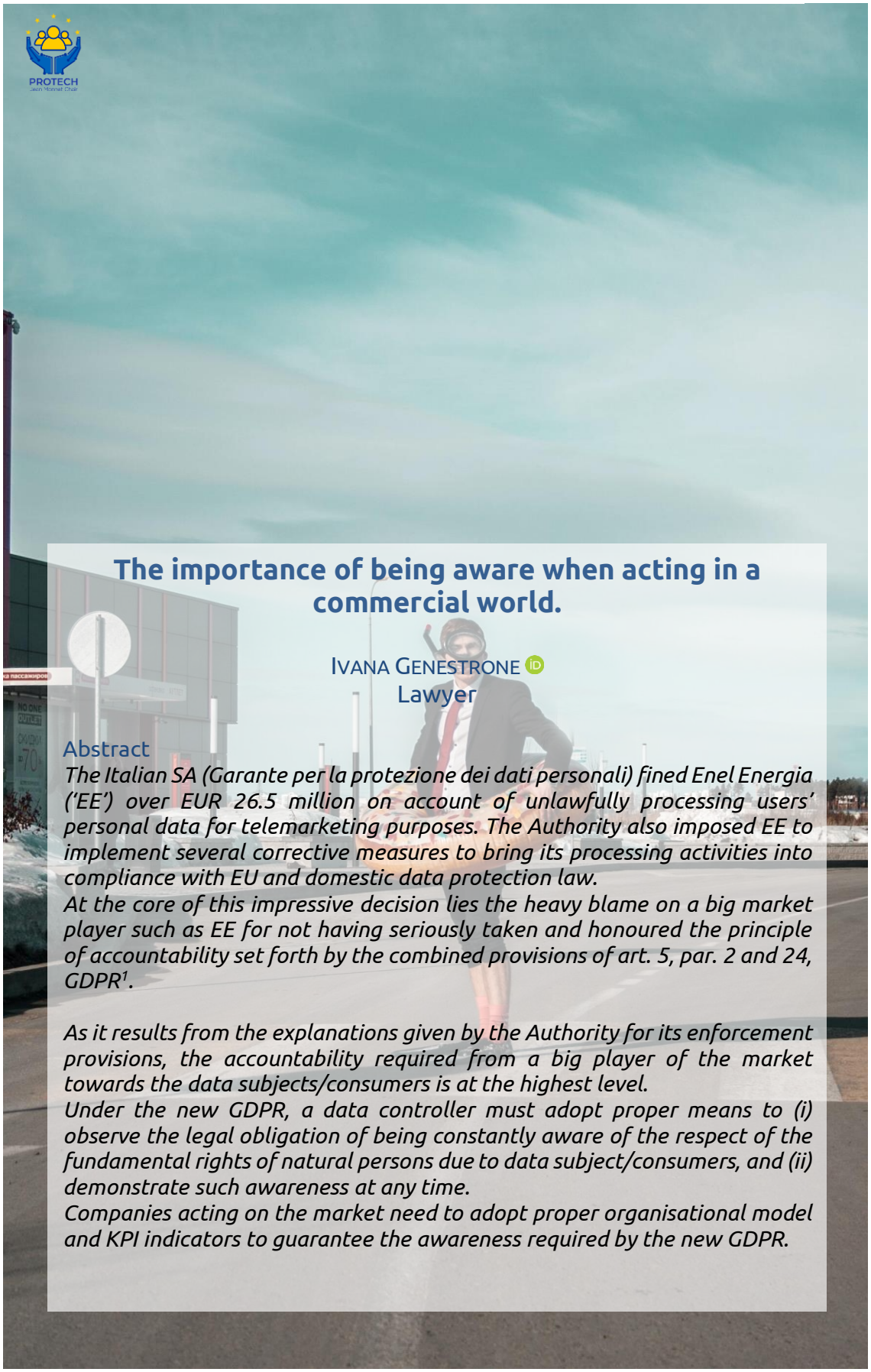
Genestrone I, 'The importance of being aware when acting in a commercial world' (2022) 1 EJPLT, 365-378.
DOI: https://doi.org/10.57230/EJPLT221IGENESTRONE

EJPLT
ISSN 2704-8012



The importance of being aware when acting in a commercial world.

IVANA GENESTRONE
Lawyer

Abstract

The Italian SA (Garante per la protezione dei dati personali) fined Enel Energia ('EE') over EUR 26.5 million on account of unlawfully processing users' personal data for telemarketing purposes. The Authority also imposed EE to implement several corrective measures to bring its processing activities into compliance with EU and domestic data protection law.

At the core of this impressive decision lies the heavy blame on a big market player such as EE for not having seriously taken and honoured the principle of accountability set forth by the combined provisions of art. 5, par. 2 and 24, GDPR[1].

As it results from the explanations given by the Authority for its enforcement provisions, the accountability required from a big player of the market towards the data subjects/consumers is at the highest level.

Under the new GDPR, a data controller must adopt proper means to (i) observe the legal obligation of being constantly aware of the respect of the fundamental rights of natural persons due to data subject/consumers, and (ii) demonstrate such awareness at any time.

Companies acting on the market need to adopt proper organisational model and KPI indicators to guarantee the awareness required by the new GDPR.

Keywords: accountability; privacy by design; GDPR; telemarketing; unsolicited communications; Italian SA; Garante per la protezione dei dati personali; EDPB; D.Lgs 231/01; sales network; organisational and technical measures; organisational model; KPI.

Introduction.

The Italian SA (*Garante per la protezione dei dati personali*) fined EE over EUR 26.5 million on account of unlawfully processing users' personal data for telemarketing purposes. In addition to paying the fine, the company was also ordered to implement several corrective measures imposed to bring its processing activities into compliance with EU and domestic data protection law.

Hundreds of complaints were to be addressed by the Italian SA, regarding Italian citizens who had received unsolicited calls made on behalf of EE, found it difficult to exercise their data protection rights, or more generally complained various issues related to the handling of their data in connection with the supply of utility services, including the processing of data performed on the dedicated area in the company's website and/or through the app released to manage power consumptions.

This act of enforcement marked an important take of the Authority, observing the dramatic rise of telemarketing issues in the utilities sector linked with the upcoming switch to the unregulated market regime for electricity and gas suppliers, who compete to get clients.

In effect, the investigations carried out in response to the above complaints showed 'pervasive, unrelenting as well as increasingly invasive reliance on unsolicited promotional calls without the required consent, addressed to off-directory users or to users listed in the opt-out register; additionally, the feedback to users requests to access their personal data or to object to processing for marketing purposes is increasingly delayed or is missing altogether'[1] which led to the following enforcement measures:

- a Euro 25,513,977 fine
- the order to implement appropriate organizational and technical measures to ensure the respect of the GDPR, also with specific regard to (i) marketing and promotional schemes involving actions within EE sales network based on calls admitted by the Register of Communications

[1] Garante per la Protezione dei dati personali, Press Release, 'Aggressive telemarketing: Italian SA fines Enel Energia EUR 26.5 millions. Consumers' data were used without their consent and the accountability principle was not complied with' < https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9737661 > accessed 27 May 2022.

Operators[2] and (ii) the handling of data subjects' requests to exercise their rights.

At the core of this impressive decision lies the heavy blame on a big market player such as EE for not having seriously taken and honoured the principle of accountability set forth by the combined provisions of art. 5, par.2 and 24, GDPR.

As it results from the explanations given by the Authority for its enforcement provisions, the accountability required from a big player of the market towards the data subjects/consumers is at the highest level, based on the consideration that such accountability, as supported by various GDPR provisions, shall consist in the legal obligation of being constantly aware of the respect of the fundamental rights of natural persons due to data subject/consumers in relation to the processing of personal data, where such legal obligation results out of the combination of the accountability and other GDPR provisions and principles.

1. The complaints.

The decision was issued following complex inquiries the SA had started to clarify the circumstances which originated hundreds of complaints against the conducts synthetised here below.

Several complaints regarded the circumstance of receiving unsolicited calls made for telemarketing purposes on behalf of EE. Within such complaints, some of the calls were:

- received on telephone numbers not shown in public directories and without the consent of the data subject;
- received on telephone numbers shown in public directories but contained in the Public Opt-Out Register in order to block promotional calls[3];

[2] The Italian Communications Regulatory Authority (AGCOM) was established by Law, 31 July 1997, no. 249. With Deliberation, 26.11.2008, no. 666, AGCOM adopted the Regulation for organizing and maintaining the Registry of Communications Operators (ROC), as further integrated by Deliberation, 25.11.2010, no. 608/10/CONS. The so called 2017 Italian budget law (Law, 11.12.2016, no. 232), amending Article 24-bis, Decree Law 22.06.2012, no. 83, provided, among others, that all economic operators carrying out call centres activities using Italian phone numbers must enroll with the ROC, and disclose AGCOM all the telephone numbers made available to the public for call centres activities.

[3] The combined provisions of Article 6, paragraph 1, GDPR and Article 130, Italian Personal Data Protection Code (Legislative Decree, 30.06.2003, no. 196) require that the use of automated calling systems without human intervention for the purposes of direct marketing or sending advertising material, or else, for carrying out market surveys or interactive business communication shall only be allowed with the subscriber's consent. The same provisions also apply to electronic communications performed by e-mail, facsimile, MMS or SMS-type messages or other means for purposes referred to therein. Except as provided above, further communications for the same purposes, as performed by different means, shall be allowed in pursuance of Articles 6 and 7, GDPR as well as under the further terms set forth by Article 130, comma 3-bis, Italian Personal Data Protection Code. This latter provides that processing by telephone and mail of the personal data as contained in publicly available paper or electronic directories shall only be allowed in respect of any entities that have non exercised their right to object, via simplified mechanisms including the use of electronic networks, by entering such data in a public opt out register (Public Opt Out Register). With Presidential Decree, 07.09.2010, no. 178, the public register of contractors opting out of the use of their personal data and telephone number for sales or commercial promotions was established, along with the provisions to manage it. Consequently, the operator who intends to carry out advertising campaigns by telephone must consult the Public Opt Out Register and respect the data subject's choice for opting out. Recently, the Italian Legislator further dealt with such register, by issuing the Presidential Decree,

- performed through pre-recorded messages.

The complaints about receiving marketing messages and being profiled without the due explicit consent of the data subject were lodged by several citizens in connection with the access and use of online and app services made available by EE to facilitate the monitoring of the contractual relationship and the payments of the bills.

In some cases, the data subjects complained about having unsuccessfully requested EE to exercise their rights to (i) object the processing of their numbers for marketing purposes and (ii) request the erasure of personal data when no longer needed from the controller.

2. EE's defense.

EE's first and primary defense consisted in affirming that the above calls had not been made or authorised by EE: they had been carried out by third parties, unlawfully using EE's name and/or operating unbeknownst to EE[4].

EE affirmed this even if the promotional calls had been made, in effects, to the advantage of EE: the calls were actually aimed at inviting the data subjects to subscribe an electric and gas contract with EE. In some cases, the goal of the call was to propose a visit by the commercial partner of EE.

In many cases EE was not able to provide the Authority with the information and documentation requested.

As to the complaints about the unsuccessful exercise of the right of the data subject based on GDPR, EE pointed out that it faced problems to respond precisely because it was overwhelmed by such requests, not caused by EE itself.

With specific regard to the data of subjects who complained about unsolicited calls performed through pre-recorded messages, EE disclosed it had collected such data directly or through some commercial partners, based on previous activities, such as handling preceding requests to exercise the rights of the data subjects or monitoring the client appreciation.

Finally, in respect to the complaint about receiving marketing messages or being profiled in connection with the access and use of the online and app services made available by EE without explicit consent of the data subject, EE disclosed that, in order to simplify such facilities, a so called 'Single Profile' (Profilo Unico) had been implemented, consisting in one single account for each

---

27.01.2022, no. 26, Regulation laying down provisions on the establishment and operations of the public register of contractors who opt out of the use of their personal data and their telephone number for sales or commercial promotions, pursuant to Article 1, comma 13, Law 11.01.2018, no. 5. In particular, it is now provided that the Public Opt Out Register is extended to all national telephone numbers, both landline and mobile, allowing the citizens to opt out both of unsolicited telemarketing calls, also by revoking consent to advertising, and of the transfer to third parties of previously provided personal data.

[4] This specific defense is completely similar to other ones adopted in analogous cases regarding other big energetic and communication market players, also sanctioned by the Italian SA. In this respect, see, among others, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9570997 Autorità Garante per la Privacy, Ordinanza ingiunzione nei confronti di Fastweb, Doc. web Nr. 9570997. In particular, during the investigation at hand, as well as in other similar ones, it has emerged the use of telephone numbers either fictitious or not entered into the ROC by such big market players, to carry out telemarketing activities. As pointed out by the Italian SA in the above mentioned ordinance against FASTWEB, it seemed to be dealing with a sort of undergrowth of abusive call centers which carried out telemarketing activities in total contempt of the provisions set forth by the GDPR and the Italian Personal Data Protection Code.

customer, allowing to access not only all ENEL web portals, but also any app of ENEL Group companies. In order to complete the profile and get the above accesses, the user was only requested to confirm the information provided by the data controller, without being required to express consent to the aim of receiving promotional communications and getting profiled. Basically, by creating a single username and password, it was possible for each customer to access any digital service provided within the ENEL Group, without a new registration being needed to enter into a new web portal, especially in case the new portal was provided by a different company.

EE asserted that within the ENEL Group only the Single Profile, i.e., the single Username and Password was shared, and that the personal data of the customer were not being communicated by the relevant company (which has the direct contractual relationship with the customer) to the other entities of the Group.

In particular this issue, combined with the lack, for the Authority, of proper evidence and information regarding the manner of collecting, storing and using the consent for marketing and profiling purposes by EE, led to the decision of the Authority to directly carry out a specific inspection. In this way the Italian SA found out that the registration process to create the Single Profile of the customer only allowed in a separate and successive step to express or reject the consent to marketing and profiling purposes, both for EE and other companies within the ENEL Group, in a confusing and not 'user-friendly' manner.

3. The Italian SA allegations.

At the end of its complex and articulated investigation activities, the Italian SA notified EE the 15 infringements to the GDPR provisions synthetised below

1. Art. 31, GDPR (Cooperation with the Supervisory Authority), for not having provided the Authority with a relevant amount of the information and documentation requested especially regarding the possible communication of personal data to third parties, while limiting itself to insisting that most of the complaints referred to processing of personal data not carried out by EE[5].

2. Art 5, par. 2, combined with Art. 25, par. 1, GDPR (Accountability and Privacy by Design), for not having adopted effective countermeasures even when the huge dimension of unlawful use of personal data of EE's customers had been made manifest to EE itself[6]. In the view of the Italian SA, in such

[5] Recital 82, GDPR makes clear the close relationship between the accountability principle and the provision set forth by Article 31, GDPR, which imposes both the controller and the processor to cooperate on request with the supervisory authority in the performance of its tasks: 'in order to demonstrate compliance with this Regulation, the controller and the processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations'.

[6] Recital 74, GDPR underlines the importance, for both the controller and the processor, of being constantly able to demonstrate that the measures adopted are not only appropriate but also effective throughout the life of specific processing of personal data: 'the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures'.

circumstances EE should have exercised (and been able to demonstrate) - in a complete and exhaustively aware manner - its legal obligations of accountability and Privacy by design, by adopting proper measures (characterized by the inclusion of elements of prevention, functionality, safeguard, transparency) to protect the data subjects. In facts, precisely the circumstance that the calls were made using EE's name should have caused proper actions for constant supervision and monitoring of the complained phenomena, taking into account the primary role of the ENEL Group in the energy market and its significant possibilities to adopt organizational and managing measures.

In this regard, EE showed no evidence of having adopted any of such measures not even towards its commercial partners, while such measures should have been adopted based on the legal obligation of accountability and privacy by design. EE should have evidenced specific measures to automatically control the means used and/or shared by EE's personnel and further commercial partners/members of EE's sales network to activate promotional campaigns or services towards EE's customers. For instance, a proper organization and scheduling of such promotional campaign could have been considered and implemented, including the design of the relevant actions to ensure that, by default, in real time, attempts to upload on the EE's digital platform contracts not evidencing the requirements of correctness and transparency or manifestly infringing GDPR provisions could be detected and blocked.

The Italian SA further questioned that EE neither did evidence the criteria and requirements defined for proper selection of commercial partners, nor the audit activities to be made from time to time to the aim of assessing the maintenance of such requirements, including automatic means to control the processing of personal data. This also with regard to both the continuous safeguard of the access to the personal data of the customers, and the constant monitoring that only correct contracts as mentioned above are uploaded on platforms withing ENEL Group.

The general comment of the Authority on this issue is that measures of the kind suggested above, if adopted, could have put EE in condition to correctly demonstrate the awareness of the company (even in terms of proper actions taken by its governance board) at the time when such circumstances emerged that could undermine and compromise not only the rights of the customers, but also the reputation of the Group.

3. Art.5, par., 2, GDPR (accountability), for not being able to demonstrate the compliance with the principles relating to processing personal data, with specific regard to unsolicited promotional communications made by a commercial partner.

A major role in this allegation is played by the lack of evidence of whatsoever action taken by EE towards its commercial partners, after EE had been made aware about the existence of complaints regarding unsolicited communications[7].

[7] Already in the so called Fastweb ordinance (see above, note no. 5) the Italian SA raised the theme of the control of the whole chain of the effective partners regarded by marketing activities on behalf of the data controller. In facts, FASTWEB was sanctioned for not having implemented proper measures to control and

4. Art. 5 par. 2 and 24, GDPR (accountability and responsibility of controller), for not having monitored the activity of commercial partners, and not having adopted proper organizational and technical measures, with respect to the calls made to the advantage of EE even if not carried out by EE's personnel[8].

5. Art. 5, par.1, lit. d), GDPR (principle of accuracy), for having erroneously, and in an automatic manner, associated to the contact data of a customer the telephone number dialed by such customer at the time when he contacted the free line exclusively dedicated to the customer service.

6. Art. 5, par. 1, lit. d), and 6 GDPR (principle of accuracy and lawfulness of processing) for having transmitted the personal data of a customer to another one, based on an incorrect association of such data (the data was simply similar to one another).

7. Art. 12, GDPR (transparency and modalities for the exercise of the rights of the data subject), for not having responded in a timely manner to the requests of the customers to exercise their right to access the data processed by EE and to object the use of their data for marketing and/or profiling purposes.

8. Art. 5, par. 1, lett. a) and 12, par. 2, GDPR (principle of Accuracy and transparency) for having given an inconsistent response to the Authority with regard to the request of a customer to exercise the right to object the receiving of promotional calls performed through pre-recorded messages, by affirming both (in the answer given to the customer) that there effectively was an erroneous contact on the EE side, and (in the documentation given to the Italian SA for the defense in this proceeding) that another customer was to blame for such error, i.e. the other customer declared to EE the data of another person when subscribing a new energy contract.

9. Art. 21, GDPR and art. 130, comma 1 and 2, D. Lgs. 196/2003 (unsolicited communications and the right to object), for having unduly sent unsolicited communication via e-mail, notwithstanding the explicit denial expressed by the customer at the time when the energy contract was subscribed and a further communication (properly executed) to EE about the right to object such processing of data.

10. Art. 130, comma 4, D. Lgs. 196/2003 (soft spam) for having sent to a customer the notification of the registration to a fidelity program, without having any evidence of the previous proper information given to the customer.

11. Art. 31 (cooperation with the Supervisory Authority), for not having provided the Authority with the information and documentation requested twice regarding the manner to obtain consent for marketing and profiling purposes within the digital facilities made available to the customers.

12. Art. 5, par 1, lett. a), 12 and 13, GDPR (principle of transparency and obligation of providing information as to where personal data is collected from

not being able to clearly represent the whole chain effectively used to collect personal data for marketing purposes, with the result that the data controller was not in condition to demonstrate that the processing of personal data were performed in accordance with GDPR from the first contact. A similar position of the Italian SA can be found also in another recent ordinance against Iren Mercato Spa. See https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9670025 Autorità Garante per Privacy, Ordinanza ingiunzione nei confronti di Iren Mercato S.p.A., Doc web Nr. 9670025.

the data subject) for having shown on the same website two information pages inconsistent with one another, with specific regard to the identity of data controller (it resulted unclear whether the data controller was EE or Enel Italia SpA).

13. Art. 5, par. 1, lett. c), GDPR (principle of minimisation), for having designed a procedure for processing personal data on the web portals of Enel Group companies, which consented the transmission to other companies of the Group of data which is not adequate, relevant and necessary. In facts, the above-described Single Profile, allowed the customer to access the digital service of several companies of the Group and, in turn, allowed the companies included in this portal network to share the data of the customer. Furthermore, in order to avail himself of the services provided by the web portal and applications of the Group, the customer was conditioned to give more data than necessary.

14. Art. 12 and 13, GDPR (Transparency and information to the data subject) for having released poor information about the activation of the Single Profile and, in particular, the consequent possibility of other companies of the Group and other commercial partners to be recipients of the personal data submitted with the Single Profile.

15. Art. 6, par.1, GDPR and 130, comma 1 and 2 (Lawfulness of processing and unsolicited communication) for not having acquired specific and proper consent with regard to the specific processing activities performed by several, distinct data controllers.

4. The accountability principle as a legal obligation of the data controller to be constantly aware.

Following the description of the above infringements, and the defense of EE, the Italian Authority further exposed its considerations in facts and in law.

Such considerations point out that the accountability of the data controller include the legal obligation to be constantly aware of its legal obligations of accountability and privacy by design as existing from time to time, so that, while some assessments of the supervisory authority are to be made necessarily *ex – ante* (taking into account the possibility of the data controller to design, adopt and maintain organisational and technical measures adequate to protect the data subject as required by the GDPR at the time of the design of the processing data structure), other evaluations of the Authority shall take into account (i) the possibility of reaction and response of the data controller in case anomalies or complaints of data subject arise, and (ii) the capacity of the data controller to constantly be aware of its compliance to the provisions protecting the data subject.

Furthermore, the dimensions and the relevance of the data controller as a market player shall have a specific impact on the assessment of the supervisory authority both requirements that are to be met *ex-ante*, and the ones which are to be valued *ex-post*, particularly in terms of the ability to react and correct anomalies and non-compliance cases which may emerge from time to time during the economic life of the data controller.

Here below are exposed the concepts articulated by the Italian Authority in such meaning.

The principal theme used by EE for defense was that most of the unsolicited communications received by the complaining data subjects were not made by EE itself.

In this regard, the Authority explained that Articles 5, par.2, 24 and 25, par. 2, GDPR, outline a precise frame of accountability of the data controller, which imposes not only that proper measures are adopted to guarantee the respect of the principle governing the processing of personal data as required by GDPR, but also that the controller is able, at any time, to demonstrate with proper evidence the compliance to the GDPR of its processing activities.

To this aim it is necessary for the data controller to give evidence also of the preliminary evaluation made on the handling of data concretely carried out in its economic life, together with proper evidence of the evaluation of the risks as well, and the effectiveness of the measures adopted.

Within this legal frame, the evidence requested to the data controller imposes an adequate selection and monitoring of other parties possibly involved in the handling of personal data made in the interest of the data controller, so that it continues to maintain the accountability of handlings of data made on its behalf or to its advantage, without the possibility to set free form such accountability merely based on the formal affirmation 'It was not me'[9].

The GDPR accountability principle, articulated both from a legal perspective (art. 5, par, 2 and art. 24, GDPR) and a more modern and technological one (art. 25, GDPR), outgrows, in facts, the merely formalistic compliance logic, by providing that the data controller adopt mechanisms for systematic control, and in the *ex-ante* evaluation of the perimeter of the data processing and its peculiar risks, and in the *ex-post* circumstances as they evolve during the time[10], involving the monitoring and control of the risks deriving from data processing carried out by other entities, acting on behalf of the data controller or, in any case, to its advantage.

In this view, the circumstance that several complaints are lodged by the Italian Authority for unsolicited communications to the advantage of EE should have been an alarm bell for such entity, causing proper reaction to protect the personal data and the fundamental rights of its customers.

Furthermore, the Italian Authority pointed out that the history, the structure and the organisational dimensions of EE should have made possible to this leader player in the energetic market, to adopt advanced organisational measures to protect the personal data of its customers, including proper mechanisms to control the entire chain of controllers and processors of such data involved by the economic activity of EE, if only EE had applied the diligence

[9] Here again, recital 74 is to be pointed out with specific reference to EU Legislator's position with regard to the 'responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf…'.

[10] In this regard, see also *G BUTTI*, 'Audit e GDPR: competenze e line guida per svolgere correttamente le verifiche in ambito privacy', 15 October 2019, Cybersecurity 360, https://www.cybersecurity360.it/legal/privacy-dati-personali/audit-e-gdpr-competenze-e-linee-guida-per-svolgere-correttamente-le-verifiche-in-ambito-privacy/, accessed 05 September 2022.

due to its dimensions, also considering the volume of its customers (9 millions of customers at the time of the decision).

As a consequence, when facing such an amount of complaints for unsolicited marketing activities, EE should have controlled that the other companies of the Group and commercial partners would not have infringed any of the GDPR provisions.

A mechanism of control should have been designed and adopted from the beginning of the activities of data processing and been maintained along all the activities of the Group which involve the handling of personal data. And EE, as data controller, should have been able to demonstrate with proper evidence to have done so.

To better assess the possibility for EE to adopt proper controls, the Italian Authority points out that, in facts, EE is already organised to validate the energetic contracts, because precisely for the phase of validation of the agreement with the customer, an amount of information is gathered and associated to the single contract, such as: contract code, code of the officer in charge for the contract, channel code, each of them well visible on the application form sent to the customer for subscription and available on EE website. Notwithstanding these links, and, with them, the ability to control the validation phase of the contract based on the traceability of the officers and the channels used to close the agreements, still, EE did not offered any evidence of having made controls to prevent unfair commercial practices, which boils down, for EE, to accept being vulnerable towards the business finders EE should have known and taken into consideration within its sales network.

Also, the lack of measures adopted by EE for the registration to the aim of creating the Single Profile to protect the rights of the data subject as set forth by the GDPR, in the view of the Italian Authority, paves the way for possible unauthorized 'business finders', able to 'grab' the data of the customers who constantly and consistently complained to the Authority unsolicited calls made on behalf of EE.

In previous decisions[11]the Italian Authority had already given, in precedent decisions, indication on the need to respect the Privacy by design principle by adopting organisational measures aimed to prevent the contractual activation of contracts in case the conclusion of the agreement is not clearly and unambiguously connected and traceable to activities carried out in the respect of the provisions protecting the rights of the data subjects/consumer from the first contact and acquisition of the data.

The same measures required as above are to be considered requested with regard to the marketing campaigns which admittedly EE launched following the pandemic emergency

Two more issues of this decision are to be mentioned:

a) the responsibility of EE for unlawfully processing of data is not exempted just for the 'good faith' of the controller: the Italian SA explains that the accountability under art. 5, GDPR can achieve exemption only if the

[11] See <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9485681> Autorità Garante per la Privacy, 'Ordinanza ingiunzione nei confronti di Vodafone, 12 November 2020', Doc. web Nr. 948568, and the ordinance against FASTWEB mentioned above (see note no. 5).

controller is able to demonstrate that the unlawful treatment, even if generated by an error, was inevitable. In this view, the accountability set forth by art. 5, GDPR is similar to the one provided by D. Lgs. 231/01 in the Italian law, imposing that companies must demonstrate that they have effectively adopted compliance programs called 'models of organisation, management and control' (the so called '231 Models') with the aim of identifying, preventing and mitigating the risk of commission of crimes in relation to business activities[12].

b) the absence or delay of proper response to the requests of the data subjects to exercise their rights based on GDPR is not acceptable, so EE's defense is not excusable, because it is just based on the affirmation that the difficulty to respond is due to the huge amount of requests. In facts, once again, this is another critical issue derived by a lack of proper organization of the data controller, who has to adopt proper means to assure the respect of the rights of the data subjects, even introducing corrective measures and penalties within its network in case of violation of the instructions given by the data controller. In this case, it is recalled the logic of the '231 Model' again, which can exempt the company from the accountability in case of noncompliance of certain legal provision only if it is proofed to be effective, that is, it must[13] a) identify the activities in relation to which offences may be committed; b) provide for specific direct protocols and schedule training and implementation of decisions by the body regarding offences to be prevented; c) identify procedures for managing financial resources which are fit to prevent the commission of offences; d) provide for obligations to disclose information to the organisation tasked with overseeing the working of and compliance with the models; e) introduce a new disciplinary system to punish noncompliance with the measures set out in the model.

The final decision of the Italian SA is based on the appraisal of the organisational model adopted by EE to be compliant to the GDPR. Such organizational model (art. 24, GDPR) should have had at its backbone, the

---

[12] *M Iaselli, Manuale operativo del D. P. O.* (2nd edn, Maggioli Editore 2021) 10; *C Santoriello*, 'Il Modello Organizzativo' in M Iaselli and others, *I rapporti tra normativa privacy e modello 231* (Maggioli Editore 2022), 57; *R Panetta*, 'Le 5 sfide che attendono il futuro del DPO', in R Panetta, T Mauro, F Sartore, *Il data protection officer tra regole e prassi '* (Giuffrè Francis Lefebvre, 2021), 158; *M Perego, S Persi, C Ponti*, Il *modello organizzativo Privacy – MOP (*1st edn, Giuffrè Francis Lefebvre 2020) 5; *D Costa*, 'I modelli 231 e la compliance aziendale sulla tutela dei dati personali. Aspetti comuni e divergenze a quattro anni di distanza dall'entrata in vigore del GDPR' [2020] Giurisprudenza Penale Web, nt. 5. .<https://www.giurisprudenzapenale.com/2020/05/01/i-modelli-231-e-la-compliance-aziendale-sulla-tutela-dei-dati-personali-aspetti-comuni-e-divergenze-a-quattro-anni-di-distanza-dallentrata-in-vigore-del-gdpr/> accessed 16 May 2022; *M Maglio, P Ghini,* 'Privacy, nuovo regolamento Europeo. L'importanza delle misure Organizzative. Punti di contatto con la Normativa 231/2001' (2017) 1 (1) Rivista231, 41 ff; *V Visicchio* 'MOG231/01 e GDPR: sue sistemi di compliance a confronto' (2018) Università Cattolica del Sacro Cuore, available at www.rivista231.it; *A Laudati*, 'Le possibili convergenze tra la recente Normativa privacy e il decreto Legislativo 231/2001' (2019) 1(1) Rivista231, 11 ff: *C Matteuzzi, A Pedico*, 'The paradigm: Model 231/01 & cybersecurity quality system' [2019] Diritto di Internet, <https://dirittodiinternet.it/wp-content/uploads/2019/11/Versione-inglese.pdf>,accessed 16 May 2022; *A Ciccia Messina*, 'Modelli organizzativi privacy e 231: differenze e possibili sinergie per le imprese', 19 June 2018, Quotidiano Ipsoa, <https://www.ipsoa.it/documents/lavoro-e-previdenza/amministrazione-del-personale/quotidiano/2018/06/19/modelli-organizzativi-privacy-231-differenze-possibili-sinergie-imprese> accessed 16 May 2022; *Federprivacy* Online Workshop, 'Privacy e Dlgs 231/2001', 15 May 2021, with the participation, among others, of *A Ghiglia (*member of the Italian SA) – *L Carrozzi (*official of the Italian SA). <https://www.federprivacy.org/attivita/modelli-organizzativi-gli-spunti-di-integrazione-tra-dlgs-231-2001-e-gdpr> accessed 16 May 2022.

[13] Art. 6, comma 2, D. Lgs. 231/01.

respect of the principle of accountability (art. 5, 2, GDPR) and Privacy by design (art. 25).

The kind of appraisal made by the Authority was aimed to prove, in particular, the effectiveness of such organisational model.

A shift in the cultural approach of the companies is needed, in order to really comprehend what does 'accountability' stands for[14].

Art. 25, paragraph 1, GDPR clearly states that 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects'.

In this regard it is useful to recall a key message of the Article 29 Working Party: 'Fundamental principles applicable to the controllers (i.e. legitimacy, data minimisation, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable.'[15]

This key message has been reaffirmed by EDPB, when insisting that effectiveness at any moment is at the heart of the concept data design[16]:

'13. Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller. This observation has two consequences.

First, it means that Article 25 does not require the implementation of any specific technical and organizational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk.

---

[14] In this regard the former European Data Protection Supervisor, Giovanni Buttarelli, was very clear since 2016. See, <https://edps.europa.eu/data-protection/our-work/publications/speeches/accountability-principle-new-gdpr-0_en>, *G Buttarelli*, 'The accountability principle in the new GDPR', Speech at the European Court of Justice, Luxembourg, 30 September 2016.

[15] See,<https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2014/wp218en.pdf, > , Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', adopted on 30 May 2014, Doc. Number 14/EN WP218, page 3, Key Message 4.

[16] See<,https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, 'Addressing effectiveness' , EDPB, Guidelines 4 (2019) on Article 25 Data Protection by Design and by Default, Version 2.0.

Second, controllers should be able to demonstrate that the principles have been maintained.

The implemented measures and safeguards should achieve the desired effect in terms of data protection, and the controller should have documentation of the implemented technical and organizational measures… To do so, the controller may determine appropriate key performance indicators (KPI) to demonstrate the effectiveness. A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves their data protection objective. KPIs may be quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively, to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.'

In the light of the above, after having considered several aggravating circumstances, (the gravity of the infringements, their duration, the number of the data subject involved, the negligence and the specific reiteration of the conducts representing infringements), the Italian SA imposed on EE an Eur 25,513,977 fine.

Additionally, EE was ordered to:

a) bring all processing of data by its sales network into compliance with proper arrangements and measures, in order to become able to demonstrate that promotional schemes and services or contracts are only activated following promotional calls addressed to numbers that are listed in the Opt-Out Public Register and

b) implement further technical and organisational measures in order to correctly handle data subjects' requests to exercise their rights including, in particular, the right to object to processing for promotional purposes, in such a manner that proper response is given to such requests by no later than thirty days after the Italian SA's order.

Conclusions.

In its decision regarding EE, the Italian SA expressly considered the accountability principle under GDPR as a legal obligation, for the data controller, to be constantly (i) aware of the risks involving the data subject and the effectiveness of the countermeasures adopted from time to time, and (ii) able to demonstrate that awareness.

Such an obligation necessarily imposes to the data controller the adoption of an organisational model, based on the concrete risks assessment and the adoption of adequate measures to prevent such risks concretely and effectively. To be effective, the organisational model shall (i) take into consideration the dimensions and possibilities of the data controller, (ii) consequently allocate adequate resources for adoption and constant maintenance of the preventive measures, and (ii) comprehend a disciplinary system (internal or external, in this case through proper arrangements) to

punish violations of the instructions given by the data controller to assure the respect of GDPR.

This position recalls the experience (and the jurisprudence) of D. Lgs. 231/01 in the Italian Law, regarding the responsibility of the companies for certain unlawful conducts.

It is clear that

a) the accountability under GDPR is to be assessed in its necessary combination with the principle of privacy by design set forth in art. 25, GDPR;

b) the assessment of the measures adopted, including their respect of the principle of privacy by design, are aimed at checking their effectiveness, on the basis both of an *ex-ante* evaluation (taking into account the risks and the relating appropriate countermeasures that the data controller could envisage at the moment of designing the GDPR model) and on a '*ex-post*' appraisal of the measures applied at the time of the processing itself;

c) in order to maintain proper awareness along the time, and the ability to demonstrate it, the data controller has to adopt adequate and, when possible, automatic mechanisms of control, which should include Key Performance Indicators;

d) the KPI to be adopted in order to constantly monitor and collect evidence of the effectiveness of the 'privacy organisational model', should necessarily include (i) the formalised detection of anomalies or incorrect conducts based on complaints or even just consistent requests of the data subjects to exercise their rights (setting what circumstances are to be held as an 'alarm bell'), (ii) adequate keys to monitor the providers of services who could be involved in the data processing activities of the data controller;

e) the data controller, when designing its GDPR model, shall be aware of all the providers of services or other parties involved in its economic sphere of action who could have access to personal data. Therefore, all the risks carried with the involvement of such parties shall be correctly mapped, the map of the risks shall be maintained updated, and proper countermeasures shall be set forth and maintained updated, too;

f) the model should provide proper sanctions in case of infringement of the instructions given by the data controller (i.e., with adequate termination and penalty clauses in the relevant agreements with external parties or, also, disciplinary sanctions in case of personnel);

g) the GDPR model should also include automatic mechanisms aimed at correcting the adopted countermeasures, whenever anomalies or incorrect actions are detected, with proper evidence of the detection system and the corrective measures adopted.