Data administration in Italian associations: navigating the European legislative landscape

Cervino Agnese, Marconi Sonia, Orlandi Damiano

"*Ultimately, Entropy is the measure of the equilibrium level reached by a system at a given moment*"

[Focus]

INTRODUCTION

In the rapidly evolving landscape of data privacy and protection, the General Data Protection Regulation (GDPR) has emerged as a pivotal piece of legislation with significant implications for various sectors. Against this backdrop, the objective of this paper is to examine the interaction between the GDPR and associations in Italy, particularly regarding the essential elements required for drafting a privacy policy. Associations, much like other organizations in the digital age, are navigating the complex terrain of data protection regulations, and understanding their compliance requirements and challenges is central to this exploration. This goal has arisen from our individual experiences, which have been nurtured over the years by associative environments frequently lacking awareness of the bureaucracy related to data processing.

Throughout the paper, the path leading to the current structure of the GDPR will be explored. This will be accomplished through a historical analysis that highlights the increasing need over time for unified rules among states in response to the increasingly complex data management, necessitating regulations that surpass national standards.
Following the historical introduction, the focus will shift to an analysis of the GDPR's structure. Particularly, emphasis will be placed on the drafting of a privacy policy, identifying key components and various categories of data involved. This section will examine the impact of associations in Italy, emphasizing the importance of increased support from public institutions to the associations in order to reach a cultural and community growth among the population. It will also illustrate how these entities need to interact with data protection and its associated limitations.

Subsequently, attention will turn to Article 13 of the GDPR, which concerns the information that needs to be provided when collecting personal data from the data subject. This is because one of the primary interactions between associations and the GDPR involves drafting a privacy policy, necessary whenever personal data is collected during the planning of an event, activity, or any other associative initiative.

Lastly, in the final chapter, a practical case involving a cultural association named Entropia APS (operating in the Trentino region) will be examined, specifically in the process of drafting a privacy policy for an event organization. The fundamental steps of policy drafting and the reasons prompting the association to request data will be analyzed: types of data, GDPR compliance requests, and how members have encountered legal requests.

As can be inferred from the aspects listed so far, this paper does not aim to provide a definitive solution to the many challenges that may arise. For instance, the absence of a legal reference within an association to consult for the drafting of a privacy policy; or the difficulty, especially for a small local entity, in understanding when and how to implement a privacy policy in its activities. In general, there is a lack of suitable information channels. Rather, the aim is to highlight an application of the GDPR in an everyday context that often lacks the suitable tools to address the demands of such a complex regulation.

1. EUROPEAN HISTORICAL AND LEGISLATIVE CONTEST

1. Legislative development

The evolution of data protection legislation in Europe is a fascinating journey through history, marked by the increasing recognition of the importance of safeguarding individuals' privacy and personal data. The story begins in the early 1970s and unfolds through various milestones, including national laws, European directives and treaties, and, ultimately, the GDPR.

It all started in the 1970s and 1980s with the technological advancements that led to the mass digitization and collective awareness about data relevance. In those years the states of Assia and Bavaria took significant steps by introducing data protection regulations (Hessisches Datenschutzgesetz and Bayerisches Datenschutzgesetz, October 1970) as well as Sweden (Datalagen, 1973) and France ("Loi Informatique et Libertés", 1978), marking the inception of the raising collective understanding that the protection of personal information was paramount. All the European institutional entities were participating in the process too. It is noticeable the effort of the Council of Europe in establishing the Convention 108 in 1981 and the cooperative role played by the Council of European Union, European Parliament and Commission in the signature of the Charter of Fundamental Rights of the European Union in 2000 (integrated into the Lisbon Treaty in 2009). A significant turning point came in with the adoption of the Data Protection Directive (95/46/EC), Directive (97/66/EC) and Directive (2002/58/EC), thanks to the European legislators purpose of fostering and harmonizing data protection laws regulation, providing a common framework for the member states. Although many European countries were adapting their national laws to align with the directives (such as England, Spain, Italy, etc.), in the early 2000s, the European Commission recognized the limitations of these legal tools and proposed a more robust data protection framework. Through the public consultation launched in 2009, the European Commission came with a proposal for the General Data Protection Regulation in 2012, igniting a lengthy legislative process involving negotiations between the European Parliament and the Council of the EU. On April 14, 2016, the European Union finally adopted the General Data Protection Regulation (GDPR) which officially came into effect on May 25, 2018, heralding a new era of data protection in Europe.

2. Comprehensive definitions of interpretative tools: roles, rights and data

Starting from this point, it is necessary to underline the main interpretative tools defined in the GDPR framework regarding roles, responsibilities and rights of all the involved players and the more complete differentiation about the types of data. As previously stated, GDPR is a milestone in the European system of law under many points of view. Although, in some cases it only refines what was already included in the Protection Data Directive (Directive 45/95/EC) of 1995. Roles, rights and data are some examples of the European state-of-the-art legislative enhancement process.

One of the most important underlined features is the distinction among the various potential actors interested in data exchanges and elaborations. These roles, as defined within the GDPR's articles n.4, n.26, are integral to the regulation's mission to safeguard individuals' privacy and data rights. Data Subjects are at the core of this framework. They are the individuals to whom the personal data belongs. As specified in Article 4(1) of the GDPR, data subjects possess a set of rights, including the right to access their data, be forgotten, and data portability. So, all the parts involved in an agreement or a privacy policy are considered as such, no matter if they are employed, employers, contractors or users. Consequently, there are the main roles of Data Controllers, defined in Article 4(7) and Data Processors as Article 4(8), entities entitled to the major responsibilities.

The first ones are natural persons or legal entities responsible for determining the purposes and means of personal data processing. They carry the accountability for ensuring that data processing aligns with the GDPR's principles as stated:

"means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; (...)" (art. 4, n. 7, GDPR)

Though, the seconds are tasked with processing personal data on behalf of data controllers. Their obligations encompass following the controller's instructions and upholding the GDPR's standards. Sub-Data Processors may be brought into the fold by the primary data processor, extending the data processing. These players adhere to the same stringent data protection standards and responsibilities as the primary processor.

Additionally, "Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by

means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a point of contact for data subjects." Therefore, in complex scenarios dense with parties and stakeholders, joint controllers are an additional subject entity that could have legal responsibilities and obligations. Furthermore, there are the technical legal advisors present in all companies, consortia and public agencies entitled for ensuring an organization's compliance with the GDPR, named DPOs, data protection officers. Usually they provide expert guidance, monitoring data protection activities and serving as a point of contact between data subjects, supervisory authorities and entity's interests.

As briefly mentioned before, each player is entitled to many and different rights. The ones discussed in this part are described and pointed out among article 15 to 23 of the GDPR and exclusively concern data subjects. One of the key pillars of this regulation is the Right of Access (Art. 15), which embodies the principle of transparency. It ensures that individuals have the ability to gain insights into what happens with their data. By having the right to access information about the processing of their personal data, people can hold organizations accountable for how their data is used. This transparency allows individuals to maintain a sense of control over their personal information. Furthermore, the GDPR provides the Right to Rectification (Art. 16). This right ensures that individuals have the ability to correct any inaccuracies or incompleteness in their data. The Right to Erasure ('Right to Be Forgotten') (Art. 17) is another remarkable facet because it grants individuals the authority to request the deletion of their personal data. On the other hand the Right to Restriction of Processing (Art. 18) allows individuals to control the extent to which their data is processed. It comes into play when the accuracy of data is questioned, the processing is unlawful, or the data is no longer required. Moreover, the Right to Data Portability (Art. 20) facilitates individuals' ownership of their data and the Right to Object (Art. 21) is a reflection of the GDPR's commitment to individual autonomy. It ensures that data subjects have a say in how their data is used, particularly in scenarios where the processing is based on public interest or official authority. This right underscores the importance of ensuring that individuals are not merely passive subjects in the data processing cycle but active participants. Furthermore, in the world of automated systems, the Right to Obtain Human Intervention and Challenge the Decision (Art. 23, Par. 3) plays a crucial role. This provision signifies that the GDPR recognizes the potential pitfalls of purely automated decisions, particularly those that significantly affect individuals. It ensures that individuals have

recourse and can challenge these decisions, advocating for human involvement in the decision-making process.

Data subjects also benefit from distinctive types of data - personal and special - mainly defined by Art. 4. On one hand Personal Data are meant as " any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." On the other hand, special data are dealt with the uniquenesses that distinct one human being to another, in terms of biological and genetic data but also in terms of architectural structure of belief and opinions (political, trade union support, religious, philosophical, tr). Moreover, health data and sexual orientation are findable in this category. For the first time there has been a definition for genetic, biometric and health data in the European system of laws, which defines the developed legal process we all are in.

2. THE ASSOCIATIVE LANDSCAPE IN ITALY: An Analysis of the Impact of Associations on Italian Territory and Challenges Related to Data Protection

The associative landscape in Italy is vast and diverse, encompassing 363,499 active associations and approximately 870,000 employees. These organizations are of various natures, including sports associations (32.9%), cultural and artistic organizations (15.9%), recreational and socialization activity associations (14.3%), social assistance and civil protection (9.9%), labor relations, representation, and union interests (6.8%), religious associations (4.7%), education and resources (3.8%), health care (3.5%), protection of rights and political activity (1.8%), environmental associations (1.7%), economic development and social cohesion (1.7%), international cooperation (1.3%), philanthropy and promotion of volunteering (1.1%) and other activities (0.6%) - according to Istat - The National Institute of Statistics in Italy- 2021 data. This variety reflects the richness of Italian civil society, with a broad network of entities playing a crucial role at social, cultural, and economic level. Furthermore, the scope of social engagement involves 4.661 million annual volunteers distributed across different organizations. Many groups are active in including and educating young citizens, offering spaces, projects, and activities aimed at developing leadership skills, active participation, and social responsibility. This engagement contributes to shaping a conscious and committed generation capable of actively contributing to the country's social and cultural life. Consequently, associations organize events, regular activities, and various engagements, interacting with administrative, political, musical, and technical fields. By their structural nature, associations collect data not only during the registration of members but also during the execution of events and initiatives.

It is natural to question how non-professional entities, often having fewer tools to support fund and resource management compared to professional spheres, interface with technical needs. Among these, albeit with the limitations we will highlight shortly, emerges the relationship between associations and the GDPR. Associations, often managed by volunteers or with limited financial resources, might find it challenging to comply with GDPR requirements. Regulations necessitate understanding and adherence to obligations concerning notification, consent, transparency, data security, and more. Insufficient resources and the complexity of regulations can jeopardize compliance. Indeed, limited financial resources might hinder access to specialized legal consultations regarding data

protection, leading to inadequate awareness of privacy regulations and data security measures, consequently risking improper management of personal data.

To address these challenges, providing practical and accessible resources to associations, such as guides and specific tools for personal data management, could be beneficial. Financial support and specific training could significantly contribute to compliance with privacy regulations and the safe and lawful promotion of associative activities.

However, there are resources that associations can rely on for support. Public bodies like the Guarantor Authority for the Protection of Personal Data in Italy provide guidelines and resources to help organizations understand and comply with privacy regulations.

Apart from public resources, there are non-governmental organizations and professional associations that offer support and legal advice at reduced or even no cost to associations with limited resources. These entities focus on providing legal advice, informative sessions, document templates, and practical tools for personal data management. An example is given by CSV (Centro Servizi Volontariato: Center for Volunteering Services), which assists and guides associations in fiscal and legal matters. Nonetheless, as mentioned earlier, some services are fee-based, which is among the issues associations encounter in meeting compliance requirements.

However, the core of the problem often lies not just in the absence of resources but frequently in the lack of communicative channels. There isn't a single information channel that guides associations through compliance steps, particularly concerning data management regulations. One of the compliance steps with GDPR frequently encountered in associative fields is drafting a privacy policy, essential for any kind of event, registration activity, initiatives, etc., where an association requests data.

In Chapter 4, we will address a practical case of drafting a privacy policy by an association organizing an event, aiming to highlight how it's not so straightforward for an association in their day-to-day operations to approach GDPR and its compliance requirements.

In general, the difficulty primarily arises from the absence of an informative channel: often, those organizing associative events and managing data are not informed about the necessity of complying with GDPR. And as much as this might be an individual's shortcoming, it's crucial to remember that the Italian associative landscape often comprises small entities managed by individuals without legal or financial backgrounds. Reality often differs from theory, and it happens that in data collection, there's a lack of awareness regarding the GDPR landscape. Therefore, associations should be guided and supported more in their paths towards data management regulation compliance, rather than leaving this

responsibility at the discretion/information of the individual. There can indeed be scenarios of small entities, like fundraising in a small town, where data is collected without considering that this is stepping into the data management realm.

Given the impact and importance that associations have on Italian territory, emphasizing greater support and guidance for these entities in their needs and obligations would align with the expression of our communities.

In essence, supporting associations in adhering to personal data protection regulations is crucial to ensure they can continue to play their vital role in society.

3. ASSOCIATIONS AND PRIVACY POLICY

1. Drafting a privacy policy

Starting from the previous chapters, it is now necessary to make a practical assessment of how GDPR regulates and affects the work of associations. GDPR applies whenever personal data comes into operation. This, within associations, can occur in a variety of situations. One of the most common situations occurs when people join associations or their events. Whether they are volunteers, employees or simple users of the services offered by the association, it is common to collect data from these individuals for various purposes.
Since the associations are dealing with personal data, sometimes even sensitive data, in accordance with the GDPR, they must ensure that they comply with all applicable regulations and laws. They must therefore take care of writing a privacy policy, intended for those whose data are collected.

2. The relevance of Article 13

Above all articles of the GDPR, the thirteenth seems to be the one to fit the necessity of associations. In fact, it seems to guide the association step by step into the complex process of writing a privacy policy. This article considers the scenario of personal data related to a data subject directly provided by the data subject itself, and that is exactly the most common scenario in the dynamics of association. This is especially crucial for volunteering associations, as they often rely on personal data to manage memberships, organize events, and communicate with their members.
Furthermore, the application of Article 13 allows associations to fulfill ethical and legal obligations in protecting the privacy of their members. Being transparent and clear in the communication of how the data of the subject are treated, makes associations more credible and trustworthy for the members themselves. Moreover, it allows associations to act within the full scope of legality. A brief illustration of all the four sub-articles of Art. 13 is reported below.

- Paragraph 1

This paragraph clarifies the context of application of Article 13 of the GDPR. This article applies whenever personal data is "*collected from the data subject*". A collection occurs whenever data comes into the possession of the data controller. It can happen both through

online form and through the compilation of paper forms. All the data must be provided from the data subject itself, and not, for example, from a third part. The associations must provide the following privacy information at the time of the collection, which implies before the data are processed.

(a) Identity and contact details of the controller: the identity of the data controller is the first information that must be provided. That meets the necessity of the data subject to contact the data controller, to exercise the GDPR rights. For this reason, the contact details should include different forms of communication, such as phone number, email, postal address etc.

(b) Contact details of the data protection officer: it is not necessary to always nominate a data protection officer. But when the DPO is nominated, the contact should be reported as well as the one of the data controllers.

(c) Purposes and legal basis: according to this piece of article, the data controllers must clarify the reason for the collection and the processing of personal data. Along with that, and in accordance with article 5 of the GDPR, data subjects should also be informed with an overview of the different processing of their personal data. Moreover, all the corresponding legal basis of the reason for the collection and the processing of personal data must be provided. These legal bases must be found either in Article 6 or in Article 9 of the GDPR.

(d) Legitimate interests: in accordance with Article 6, a controller can indicate the "legitimate interest" as the legal basis for the processing of personal data. When this occurs, the controller must inform the data subject about the nature of the interest. If the data subject finds the legitimate interest inappropriate, she or he may exercise the right to object. If the information provided by the controller is incomplete or incorrect, the controller itself can be fined for breach of Article 13.

(e) Recipients: as defined in Article 4, a "recipient" is any entity to which personal data are disclosed, not necessarily a third party. Also, all the processors are considered recipients. When the controllers identified in (a) disclose personal data to internal or external recipients, these should be clearly identified and their information must be provided to the data subject.

(f) International transfer: if the data controllers intend to transfer data to third countries, defined as countries located outside of the European Economic Area, they should inform data subjects. All the relevant countries should be named, as well as the safeguards relied

upon. Beside mentioning these countries, the controllers should also inform the data subject about how to obtain a copy of the applicable safeguards.

- Paragraph 2

In the second paragraph of Article 13, the reader can find further information that the controller shall provide to the data subject. These seem to be differentiated from the ones above in terms of purpose. In fact, the information indicated in the second paragraph are necessary to ensure fair and transparent processing. The individual steps are briefly explained below.

(a) Retention period: the controller must inform the data subject with the expected retention period of the data. When this is not possible, at least the criteria used to determine the period of retention should be provided. If different data have different retention periods, controllers must be clear about that.

(b) Information about data subject's rights: the data subject should be informed about their right regarding data protection law. In particular, this information should regard their right to access, rectification, erasure, restriction of processing, data portability and their right to object. However, merely informing the data subject about the existence of these rights is not enough. Controller should also include a summary of how the data subject can take steps to exercise every right and what are the limitations.

(c) Information about the right to withdraw consent: in the scenario where the legal basis for the processing of personal data is the consent of the data subject, he or she must be informed about the existence of the right to withdraw consent at any time.

(d) The right to lodge a complaint: the data subject must be informed about the right to lodge a complaint with a supervisory authority.

(e) Contractual or statutory requirement: controllers must inform the data subject whether the collection of its data is a statutory or contractual requirement, and what could be the consequences of not providing the data.

(f) Automated Decision-Making: if the processing of the personal data involves any sort of automated-decision making, including profiling, the data subject must be informed about it.

Also, controllers should provide brief but meaningful information about the logic involved in the process.

- Paragraph 3

This paragraph covers situations where a controller processes personal data for a new purpose, not specified above. In practice, controllers must update the privacy policy when a change of purpose occurs, and ideally notify those changes to the data subject. This must happen before the processing of the data for the new purpose. These changes are allowed only when the new processing is linked with the initial reason for collecting personal data.

- Paragraph 4

This paragraph covers the situation where the data subject was already informed by the controller itself or by a third party, for example a processor. In this scenario, the controllers are exempted from the obligation to provide this information a second time, but only if they are capable of demonstrating that the data controller was already informed. Of course, to apply this scenario, all the old information must still be valid and complete.

4. CASE STUDY - POPLAR FESTIVAL

1. What is the Poplar festival?

Poplar Festival is a cultural and music festival organized by the Entropia APS, which is a cultural association operating in the Trentino area. The festival, held annually, is entirely organized by volunteers, including members of Entropia and occasional contributors who help with festival organization from year to year without being associated with Entropia APS. For this reason, the festival organizers annually issue a Call to seek volunteers. The Call is published on social platforms and the association's website and involves the completion of a Google Form. The association then collects data for organizational purposes. In particular, volunteers collaborate for about a week, and that's why the requested data ranges from availability to dietary preferences/requirements (to provide meals). What happens is that an entity like this must deal with the drafting of a privacy policy and the collection and management of numerous data belonging to about 300 individuals. Attached, can be found the Google Form from the last edition of the festival and the related Privacy Policy, which we will analyze later in order to create an overlap between its drafting and the requested and necessary data.

2. Privacy Policy Analysis

The privacy policy starts by identifying the Data Controller, which is Entropia APS, providing contact information such as the legal address and reference email. The policy immediately clarifies that its aim is to inform the data subject (the one filling out the form) regarding the processing of their data. It also adds that a lack of consent for data processing implies ineligibility for participation as a volunteer. Next, the policy proceeds to analyze the role of Google Form, the tool used for data collection. Google Form is a tool of Google Ireland Limited, a company established and operating under Irish law. This company is referred to as an "external data processor." Therefore, information about the legal address and data processing by this external processor is also provided. Once the Data Controller and external data processor are identified, the policy then lists the types of data that will be collected.

3. Categories of data:

In particular, the types of data processed in this policy include:

- Name and surname of the data subject;
- Verification of legal age;
- Email address;
- Telegram username and phone contact;
- Acquisition of fire/BLSD/HACCP certificates;
- Possession of a driver's license and related data;
- Food allergies and dietary preferences.

Why is there a need to collect this data? As expressed in previous sections, the collected data must be strictly necessary. Specifically, name and surname are necessary for identifying the volunteer. Legal age attainment is a specific requirement of the association, which, for legal responsibility purposes, prefers to interact only with people of legal age. The email address is needed for communication related to the volunteer application. Meanwhile, the Telegram username and phone contact are necessary when confirming the role as a volunteer to manage interactions among the various parts of such a complex organization. Consider Telegram groups, which are more suited to a high number of users and require a phone number for urgent communications regarding the volunteer role.

Next, there are fire, BLSD and HACCP certificates. These certificates are not required for volunteer participation, but they are needed for the festival's operation. Although the certificates are not collected at the time of form completion, data resulting from these will still be included in the processed data since, in case of a positive response regarding possessing these certificates, they will be requested and collected by the association at a later time, and they must treat this data in accordance with the GDPR. Finally, the policy requests personal data falling under special categories, such as food allergies and dietary preferences, for which explicit consent of the data subject is required according to Art. 9 of the GDPR 2016/679.

4. Purposes and goals of the processing

The policy then proceeds to inform the data subject about the purposes and goals of the processing. In particular, it states that data will be processed in compliance with the

provisions of D.Lgs. 196/2003 and GDPR 2016/679 to ensure their integrity, confidentiality, and availability. It specifies that the data are collected by the Data Controller solely for the purpose of organizing Poplar Festival 2023. Furthermore, it guarantees that data are transmitted securely between the web browser of the form filler and the website. In particular, the transmission is encrypted and protects data from potential third-party attacks or interceptions. This is achieved through HTTPS (Hypertext Transfer Protocol Secure), which is a secure version of the HTTP protocol, a communication protocol for data transfer on the internet. The HTTPS variant also employs TCP (Transmission Control Protocol)/IP and the SSL (Secure Sockets Layer) layer that encrypts incoming and outgoing data through a mathematical algorithm. Finally, this section concludes by stating that the processing does not involve data profiling, and the data will be stored in an electronic archive and kept within the EU territory. They will not be used for marketing purposes, nor will they be sold or disclosed to third parties.

5. Data subject right:

At the end of the policy, in accordance with Articles 15 to 22 of EU Regulation No. 2016/679, the data subject's rights are outlined, which include the ability to:

a) Request confirmation of the existence of personal data.

b) Obtain information regarding the purposes of the processing, the categories of personal data, recipients, or categories of recipients to whom personal data has been or will be disclosed, and, where possible, the retention period.

c) Obtain rectification and erasure of data.

d) Obtain restriction of processing.

e) Obtain data portability, meaning to receive data from a data controller in a structured, commonly used, and machine-readable format and transmit it to another data controller without hindrance.

f) Object to processing at any time, even in the case of processing for direct marketing purposes.

g) Object to automated decision-making concerning individuals, including profiling.

h) Request the Data Controller access to personal data and rectification or erasure of personal data or restriction of processing concerning them, or to object to their processing, as well as the right to data portability.

i) Withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

j) Lodge a complaint with a supervisory authority.

The privacy policy of Poplar concludes with the list of the rights of the data subject. Within the form, the policy is then followed by the request for explicit consent and this is necessary because among the requested data are allergies, which fall under the category of special data: while the policy aims to inform the data subject about their data processing, the presence of allergies necessitates the request for explicit consent.

6. Issues

One element that seems to be missing from the privacy policy is the data controller's data retention period. However, in this case, the data controller, Entropia, has appointed Google as the data processor, attaching information regarding data management related to this platform. Therefore, data retention is deferred to the data processor.
Is it incomplete? It may be, but as mentioned above, Poplar, a small territorial entity dealing with data management, lacks the intrinsic legal tools within its structure and would need to seek them externally, likely utilizing paid channels.
Should it do so in any case? Certainly, but reality differs from theory; thus, this remains an open question.

Another critical issue arises from the lack of clear information on how to exercise one's rights in this specific case. Even though reference is made to Articles 15 to 22 of EU Regulation No. 2016/679, it would be advisable to provide clear and accessible guidelines for individuals without a specific background on how to initially approach exercising their rights.

CONCLUSIONS

Within the European legislative framework that has developed over the last three decades in an rapidly evolving technological contest, there has been a notable process of identification and acknowledgement of data protection rights. It culminated in the issuance of unique, unprecedented regulation that strives to safeguard and protect the privacy of European citizens. Although, five years after the GDPR came into effect, challenges related to its practical implementations persist, exemplified by specific cases involving certain Italian associations.

The legal language and legal structures are not always easy to understand by those who do not work with them on a daily basis. This difficulty is often accompanied by a meager understanding and culture of the value of personal data. In Italy, unless there is specific training or personal interest, caring for personal data is not widespread. If society were more widely and comprehensively educated in data management, there would likely be greater awareness even among associations. Also, these associations would receive direct feedback on their operations in terms of data management from informed individuals who are knowledgeable about their rights regarding data management. Consequently, associations would have more interest and sensitivity towards the issue.

So, this paper aims to bring to the attention of readers an issue that can affect anyone, not only in the role of associations but also as citizens who find themselves providing personal data. By focusing on the practical hurdles faced by associations, we have underscored the importance of crafting clear, transparent, and accessible privacy policies. The path to GDPR compliance is a transformative journey, and the development of comprehensive privacy policies is a cornerstone of this process. The focus is on highlighting the necessity to more actively steer associations into the sphere of data management, aiming to enhance the safety of an environment that holds a crucial and irreplaceable role within Italian territory.

References

DE HERT P., PAPAKONSTANTINOU V., *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, in *Computer Law & Security Review*, vol. 28, 2012, 130 e ss., available at: <http://www.sciencedirect.com/science/article/pii/S0267364912000295#>

GUARDA P., *Data Protection, Information Privacy, and Security Measures: an Essay on the European and the Italian Legal Frameworks*, in *Cyberspazio e dir.*, 2008, 65 (available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1517449>)

PASCUZZI G., *How to Find the Italian Law*, in U. MATTEI, J. LENA (eds.), *Introduction to the Italian Law*, Kluwer, The Hague, London, New York, 2002, 455-475S. SCARPONI (a cura di), *Il mobbing. Analisi giuridica interdisciplinare (Atti del convegno tenutosi a Trento l'8 novembre 2007)*, Trento, Università degli studi di Trento, 2009

VOSS W. GREGORY, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting (January 5, 2017). Business Lawyer, Vol. 72, No. 1, pp. 221-233, Winter 2016/2017*, Available at SSRN: https://ssrn.com/abstract=2894571

KUNER CHRISTOPHER AND BYGRAVE, LEE A. AND DOCKSEY, CHRISTOPHER AND DOCKSEY, CHRISTOPHER AND DRECHSLER, LAURA AND TOSONI, LUCA, The EU General Data Protection Regulation: A Commentary/Update of Selected Articles (May 4, 2021). Available at SSRN: https://ssrn.com/abstract=3839645 or http://dx.doi.org/10.2139/ssrn.3839645

Sitography

https://gdpr-info.eu/

https://gdpr-info.eu/issues/personal-data/

https://gdprhub.eu/Article_13_GDPR

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31997L0066

https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32002L0058

https://www.garanteprivacy.it/home/autorita

https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29

https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

https://ec.europa.eu/newsroom/article29/items/622227/en

https://www.istat.it/it/files//2023/05/Censimento-non-profit-primi-risultati.pdf

https://www.arqaam.org/2021/08/17/how-ngos-can-safely-and-securely-collect-and-store-data/

https://siamoentropia.org/

https://forms.gle/8KBuJoQCHqbPCCBs8

https://docs.google.com/document/d/19cS1eeI7vnID1AYnhzEKvMn5Xn9tIJhq7sw2s1iKl3A/edit?usp=sharing