

GDPR SANCTIONS

NUMBERS, REFLECTIONS, SOLUTIONS

SURVEY 2018-2021

THE ROLE OF THE CFO

IN PROTECTING THE COMPANY
RISKS, OPPORTUNITIES
AND RESPONSIBILITIES

WHITE PAPER
MAY 2021



GDPR Sanctions

Numbers, Reflections, Solutions

What the CFO really risks and its responsibility in protecting the company

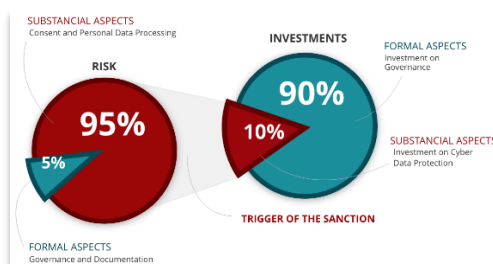
Almost 4 years after the implementation of the GDPR we find that **the number of sanctions that the Italian Data Protection Authority imposes every year, including in Italy, is steadily increasing both in quantity and amount** while companies are running for cover, **but on the wrong side.**

The direction to follow outlined by the Authority is very clear and can be understood from the most frequent and "costly" sanctions imposed, or rather from the articles of the Regulation most targeted by the inspectors. At the same time, companies are trying to protect themselves, but paradoxically without considering the root cause that leads to the sanction, i.e. **the trigger of the sanction**, which, had it not happened, would have avoided it altogether. What emerges from the survey is that companies that have invested in the Governance of the GDPR very often then fail to convey the good intentions written on paper. **The trigger of the sanction for well over 95% concerns the way in which data and consent have been managed (or rather, poorly managed)** and not the form or content of the documentation that companies often feel is the conclusion of their process of compliance with the GDPR.

Governance is the domain of Legal, Cyber Security of ICT, but
the transition from theory to facts of the GDPR,
which is known as **Cyber Data Protection**,
concerns everyone and is still **no man's land**.
Only the CFO is in a position to change things.
Here's why...

While GDPR Governance is guided by the legal team and Cyber Security is the responsibility of ICT, **Cyber Data Protection**, which must guide the company with processes and tools in the transition from the theory of Governance to the facts of *Privacy by Design*, avoiding critical situations, sanctions and loss of reputation, still seems to be **no man's land**.

In this scenario of distractions and disengagement where everyone loses out (from the company for damages and penalties, to managers for lack of responsibility up to the citizen whose rights are violated), **proper leadership can only come from the CFO**, who guides investments and corporate strategy with a vision that is certainly prudent but which considers the interests of the company, both in terms of prosperity and protection.



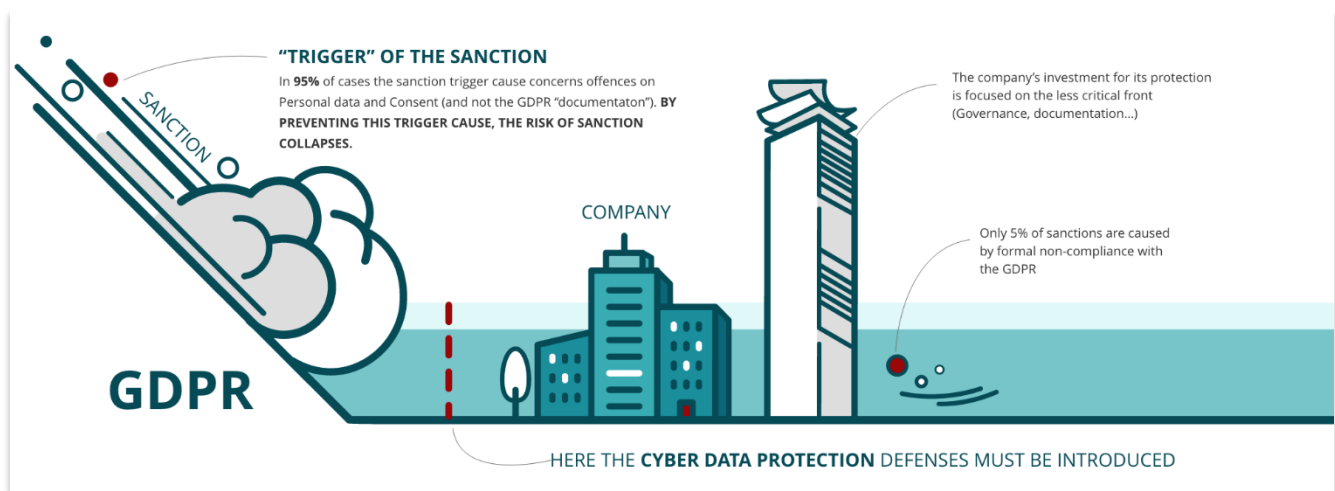
The risk/investment paradox: in order to protect themselves from sanctions, companies are focusing their investment on Governance, which is the least exposed to sanctions, compared to substantive violations, which instead account for 95% of the causes of sanctions in Italy and in Europe.

That sanction trigger to be understood and defused

By "**sanction trigger**" we mean the trigger leading to the sanction, i.e. that small event which, had it been avoided, would have spared the great damage to the company (uncovering Pandora's boxes of offences, ranging from governance to processing).

The analysis carried out reveals an extraordinary result: more than 95% of the sanctions are triggered by unlawful processing, or by the complaint of an interested party on the way in which the company processes their personal data and consent, and not by how it drafted the documentation.

Naturally, once triggered, the avalanche drags everything towards the sanction, including missing, incorrect or incomplete documentation related to privacy, even if the weight of the latter in the final sanction does not reach 30% either in frequency or in value.



This diagram illustrates the inadequate protection of companies on the "triggering causes" of sanctions, 95% of which start from personal data and consent offences and not from "formal offences".

The real cause of the "sanction trigger" and the iceberg paradox

The paradoxical aspect to deal with is that if the ratio of offences to sanctions is at least 9:10, **the effort of companies to minimise the penalties is aimed at the wrong side**, with a ratio that is often 9:10 (or less) but in favour of the "paper" instead of Cyber Data Protection tools that would have a far greater positive impact in terms of protection and minimisation of damage. The sanction is most often triggered by the **customer**, the **prospect**, the **employee**, the **former employee (or manager)** and the **competitor**. These people (who have a ready-made toolbox within their rights) challenge the company about one or more cases of processing of their personal data, such as a simple newsletter or one too many phone calls.

This costly "distraction" of companies is not so much due to the underestimation of the damage by Legal/DPO and CIO/ICT but to the lack of formal accountability. Cyber Data Protection, which is responsible for protecting the company from the majority of GDPR related damages, must be coordinated between Legal and ICT, which, without the conviction of even the CFO, will just stand at the window watching the iceberg approach.

Companies are still focused on the Form of the GDPR (but in more than 95% of sanctions the fault lies with the Substance)

Form

There are two major categories of obligations that the GDPR imposes: the first concerns the failure to prepare the basic tools necessary to be able to comply with the GDPR.

This is the large group of so-called "preparatory" requirements for the GDPR.

They include:

- Insufficient technical and organisational measures aimed at ensuring information security. **Art. 24, 29, 30, 35, 36** GDPR.
- Lack of compliance with information obligations. **Art. 13-14** GDPR
- Failure to designate a DPO. (Art. **37-39** GDPR)
- *Data processing agreement* (insufficient contract between data controller and data processor). **Art. 28** GDPR.

These are all "preparatory-structural" violations that, very often, are fulfilled with proper preparation "on paper" but **constitute only the first fulfilment, the starting point for correctly fulfilling the GDPR.**

Substance

The second group, on the other hand, includes all those sanctions imposed for the way in which the consent and personal data collected have been (badly) managed.

These sanctions concern the constant control, surveillance, monitoring and correct use of the data collected.

- Insufficient legal basis for data processing.

All data must be processed lawfully, correctly and transparently. In order to fulfil this, **Art. 6 (coordinated with the following articles 7-8)** of the GDPR requires the existence of a valid legal basis for the processing of data.

- Non-compliance with the general principles for data processing.

This concerns in particular **Art. 5** GDPR (but also **Art. 44-45-46-47-48-49** on the precautions for transferring data to third countries).

- Privacy by Design and Default, security measures **Art. 25-32.**

These cover the design of data protection and the minimum processing required by default, as well as pseudonymisation, confidentiality, integrity and resilience, always with regard to personal data and consent.

- Lack of respect for subjective data rights.

The Regulation formalises an extensive catalogue of rights to which the data subject is entitled and that the company has the duty (the obligation) to uphold and fulfil within 30 days of the request.

These are the right of **access**, the right of **rectification**, the right to **erasure** (better known as the right to be forgotten), the right to **restriction of processing**, the right to **data portability**, the right to object **to processing**.

What do all these violations have in common?

They share the erroneous way in which the data controller has concretely used, manipulated, stored, processed – in a word, "managed" – the data entrusted to him/her by the data subjects and the relevant consent, and they represent the company's most critical issue.

Let's look at the facts: the quantity and the economic impact of sanctions in Europe (and in Italy) are constantly increasing.

By highlighting the data from the [enforcementtracker.com](https://www.enforcementtracker.com) study, we can see that from the first 19 sanctions of 2018 (5 months), with a value of € 436,388, we have gone up to a **total of 2,277 sanctions in 2021 (4 months), with a value in that month alone of € 35,799,100**, with a continuously growing trend.

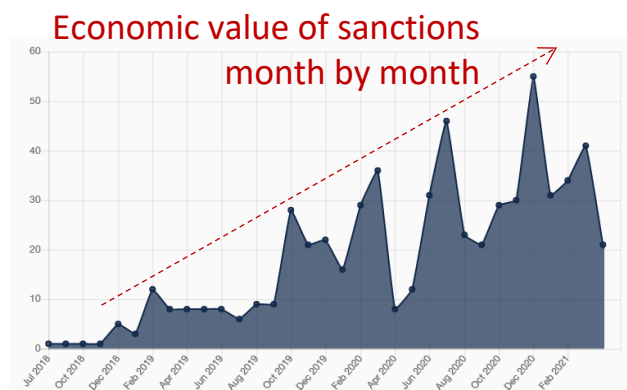
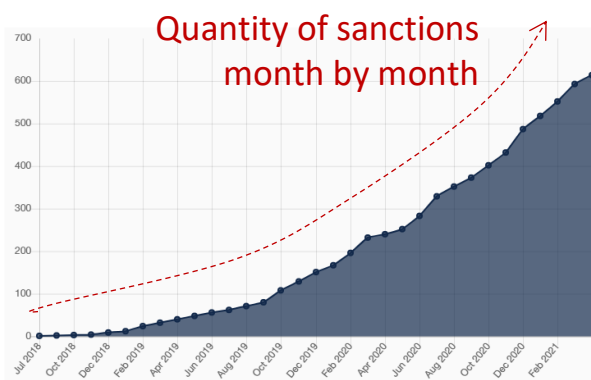
Month	Total value of sanctions	Number of sanctions	Increase over the previous month
July - 18	€ 400,000	1	
September - 18	€ 300	2	+50%
October - 18	€ 388	3	+33%
November - 18	€ 20,000	4	+25%
December - 18	€ 15,700	9	+56%
January - 19	€ 50,000,888	12	+25%
February - 19	€ 65,108€	24	+50%
March - 19	€ 462,300	32	+25%
April - 19	€ 309,135	40	+20%
May - 19	€ 559,526	48	+17%
June - 19	€ 883,700	56	+14%
July - 19	€ 367,575	62	+10%
August - 19	€ 3,252,835	71	+13%
September - 19	€ 921,523	80	+11%
October - 19	€ 2,012,374	108	+26%
November - 19	€ 1,116,570	129	+16%
December - 19	€ 12,207,530	151	+15%
Sanctions 2018/19	€ 72,595,452	832	

17 months

Month	Total value of sanctions	Number of sanctions	Increase over the previous month
January - 20	€ 28,116,160	167	+10%
February - 20	€ 775,690	196	+15%
March - 20	€ 5,869,000	232	+16%
April - 20	€ 804,200	240	+3%
May - 20	€ 483,400	252	+5%
June - 20	€ 2,020,308	283	+11%
July - 20	€ 20,006,548	329	+14%
August - 20	€ 627,948	352	+7%
September - 20	€ 738,900	373	+6%
October - 20	€ 78,121,158	402	+7%
November - 20	€ 18,421,929	432	+7%
December - 20	€ 15,041,295	487	+11%
January - 21	€ 17,570,150	518	+6%
February - 21	€ 1,752,550	552	+6%
March - 21	€ 15,068,000	593	+7%
April - 21	€ 1,408,400	614	+3%
Sanctions 2019/20	€ 206,825,636	6022	

16 months

As can be seen from the table, both trends relating to the number of sanctions and their economic value are constantly growing, with the first even showing an exponential trend from 2018 to today.

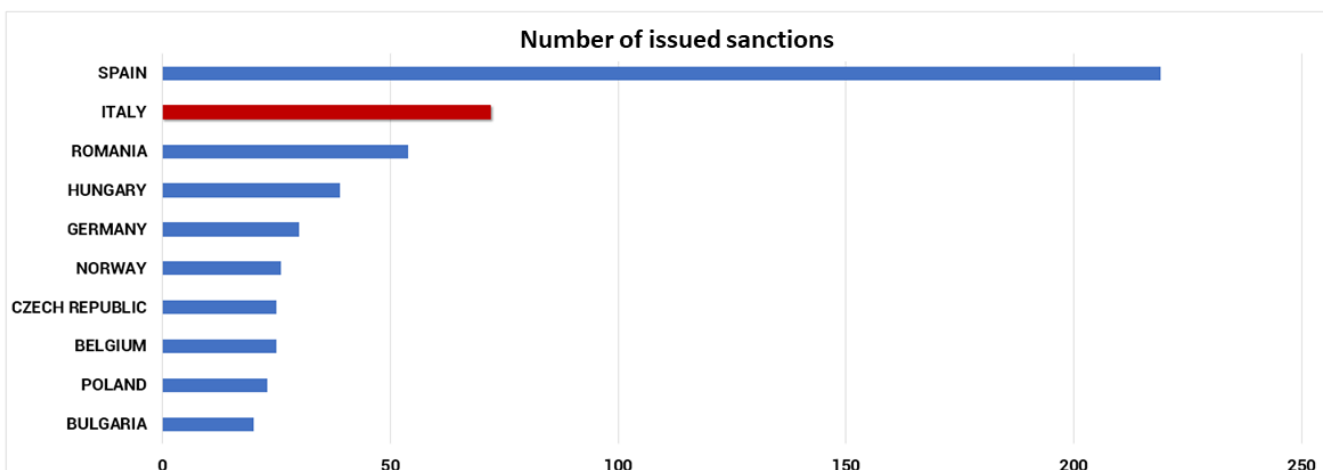
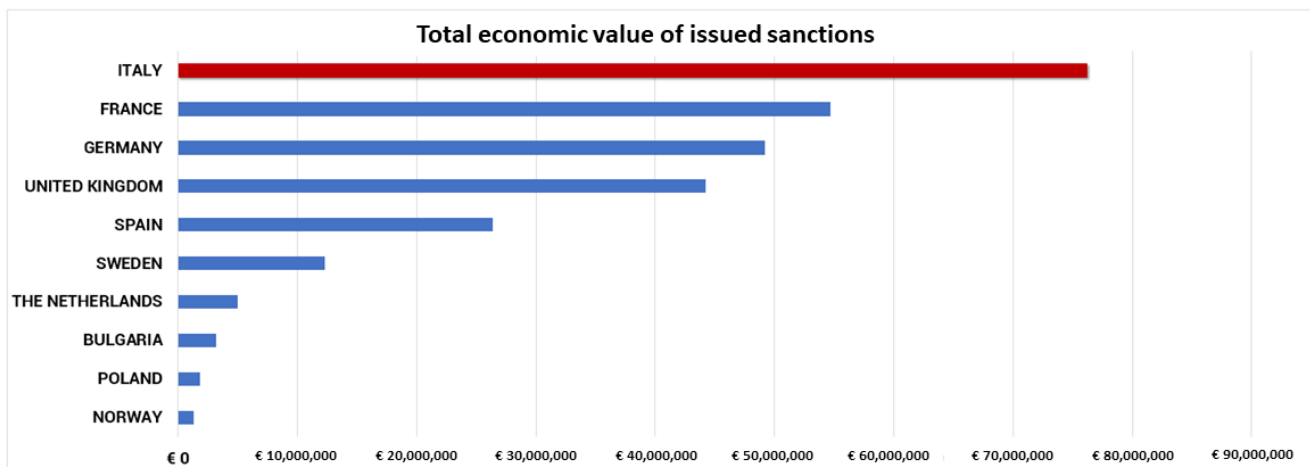


Italy is ranked first in Europe in terms of the economic value of sanctions issued and second for the quantity

As regards Italy specifically, the Italian Data Protection Authority has issued 67 sanctions totalling € 76,065,601 (excluding all sanctions based on the previous Privacy Law), making it the second largest authority in Europe by total number of sanctions and the largest by total value in euros of sanctions imposed. (Note that Spain, in first place with 213 penalties, is only fifth by total value in euros).

Total economic value of issued sanctions	
ITALY	€ 76.213.601 (at 72 fines)
FRANCE	€ 54.661.300 (at 14 fines)
GERMANY	€ 49.186.833 (at 30 fines)
UNITED KINGDOM	€ 44.221.000 (at 4 fines)
SPAIN	€ 26.369.510 (at 219 fines)
SWEDEN	€ 12.332.430 (at 17 fines)
THE NETHERLANDS	€ 5.005.000 (at 9 fines)
BULGARIA	€ 3.210.690 (at 20 fines)
POLAND	€ 1.816.498 (at 23 fines)
NORWAY	€ 1.277.550 (at 26 fines)

Number of issued sanctions	
SPAIN	219 (with total € 26.369.510)
ITALY	72 (with total € 76.213.601)
ROMANIA	54 (with total € 691.150)
HUNGARY	39 (with total € 780.088)
GERMANY	30 (with total € 49.186.833)
NORWAY	26 (with total € 1.277.550)
BELGIUM	25 (with total € 1.018.000)
CZECH REPUBLIC	25 (with total € 165.903)
POLAND	23 (with total € 1.816.498)
BULGARIA	20 (with total € 3.210.690)



What is challenged in companies and how to avoid the damage

Violation	Sanction value
Insufficient legal basis for data processing	€ 164,764,848 (on 229 sanctions)
Insufficient technical and organisational measures aimed at ensuring information security	€ 65,904,419 (on 138 sanctions)
Non-compliance with the general principles for data processing	€ 24,620,264 (on 114 sanctions)
Failure to respect subjective data rights	€ 16,024,025 (on 59 sanctions)
Failure to comply with information obligations	€ 5,660,445 (on 35 sanctions)
Lack of compliance with the notification obligations of a data breach	€ 1,238,291 (on 17 sanctions)
Failure to designate a DPO	€ 186,000 (on 5 sanctions)
Insufficient cooperation with the supervisory authority	€ 183,229 (on 25 sanctions)
Insufficient <i>Data Processing Agreement</i> (agreement between data controller and data processor)	€ 89,380 (on 3 sanctions)
Unknown	€ 500 (on 1 sanctions)

Out of 626 total sanctions, **36.58%** concern an insufficient legal basis for data processing; **22%** insufficient technical and organisational measures aimed at ensuring information security; **18.21%** non-compliance with the general principles for data processing; **9.45%** Failure to respect subjective data rights; **5.6%** Failure to comply with information obligations; **4%** insufficient cooperation with the supervisory authority; **2.72%** the Lack of compliance with the notification obligations of a data breach; **0.8%** Failure to designate a DPO; **0.48%** an insufficient Data processing agreement and the remaining 0.16% for unknown reasons

Complaints detected in 2020 point the finger at the **unlawful processing of personal data and consent**, as opposed to those in 2018 and 2019, which were more oriented towards formal aspects.

GDPR violations in 2020: an overview

The Federprivacy observatory has published an interesting dossier analysing the institutional sources of the thirty countries of the European Economic Area and creating a statistical framework of the administrative sanctions issued during 2020 on the basis of various variables, such as time, economic value, type of violation and sector¹. The various data collected and the graphs presented confirm the same trend as previously illustrated.

Furthermore, they show how **the 2020 sanctions, unlike those of 2018 and 2019, focused more on the way in which companies concretely approached personal data in a substantive way (i.e. collected and managed personal data and consent)** rather than on the failure to comply with the GDPR from a more formal point of view (i.e. in the preparation of all those preliminary aspects, such as documentation, information, register of processing operations, etc.).

¹ The entire dossier is available at: <https://www.federprivacy.org/attivita/studi-statistiche?download=393:report-statistico-sanzioni-privacy-see-2020-italiano>

Types of violations and their economic impact.

From the 2020 sanctions list, Italy ranks second in terms of both the number of sanctions and their economic value, with an **average sanction value of € 1,662,188**.

Compared to the European average of € 903.002, penalties in Italy are 84% higher.

Compared to the European average of 11 sanctions per state, Italy has 300% more sanctions.

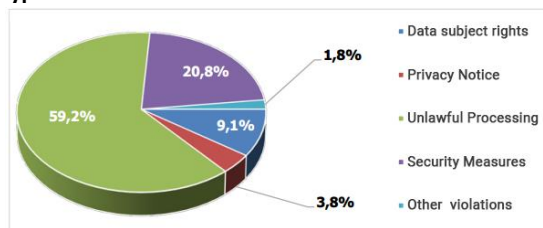
List of issuing countries classified according to the economic value of sanctions

Country	Amount (€)	Number of Sanctions	Medium sanction value (€)
France	€ 138,316,300	8	€ 17,289,539
Italy	€ 58,176,601	35	€ 1,662,188
UK	€ 45,067,000	5	€ 9,013,400
Germany	€ 37,398,708	3	€ 12,466,236
Sweden	€ 14,278,800	15	€ 951,920
Spain	€ 8,080,710	133	€ 60,757
Netherlands	€ 1,355,725	3	€ 451,908
Hungary	€ 1,002,525	13	€ 77,117
Norway	€ 805,200	11	€ 73,200
Belgium	€ 798,000	14	€ 57,000
Ireland	€ 630,000	4	€ 157,500
Poland	€ 531,698	9	€ 59,078
Czech Republic	€ 312,178	8	€ 39,022
Finland	€ 207,500	5	€ 41,500
Denmark	€ 202,300	6	€ 33,717
Romania	€ 184,650	26	€ 7,102
Estonia	€ 148,500	3	€ 49,500
Slovakia	€ 107,000	4	€ 26,750
Austria	€ 100,750	3	€ 33,583
Malta	€ 64,500	11	€ 5,864
Greece	€ 45,000	7	€ 6,429
Cyprus	€ 32,000	5	€ 6,400
Iceland	€ 29,600	2	€ 14,800
Latvia	€ 21,250	2	€ 10,625
Lithuania	€ 15,000	1	€ 15,000
Bulgaria	€ 12,230	4	€ 3,058
Croatia	N.A.	1	N.A.
Portugal	€ 0	0	€ 0
Slovenia	€ 0	0	€ 0
Liechtenstein	€ 0	0	€ 0
Luxembourg	€ 0	0	€ 0
Total	€ 307,923,725	341	€ 903,002

List of issuing countries classified according to the number of sanctions

Country	Amount (€)	Number of Sanctions	Medium sanction value (€)
Spain	€ 8,080,710	133	€ 60,757
Italy	€ 58,176,601	35	€ 1,662,188
Romania	€ 184,650	26	€ 7,102
Sweden	€ 14,278,800	15	€ 951,920
Belgium	€ 798,000	14	€ 57,000
Hungary	€ 1,002,525	13	€ 77,117
Norway	€ 805,200	11	€ 73,200
Malta	€ 64,500	11	€ 5,864
Poland	€ 531,698	9	€ 59,078
France	€ 138,316,300	8	€ 17,289,539
Czech Republic	€ 312,178	8	€ 39,022
Greece	€ 45,000	7	€ 6,429
Denmark	€ 202,300	6	€ 33,717
UK	€ 45,067,000	5	€ 9,013,400
Finland	€ 207,500	5	€ 41,500
Cyprus	€ 32,000	5	€ 6,400
Ireland	€ 630,000	4	€ 157,500
Slovakia	€ 107,000	4	€ 26,750
Bulgaria	€ 12,230	4	€ 3,058
Germany	€ 37,398,708	3	€ 12,466,236
Netherlands	€ 1,355,725	3	€ 451,908
Estonia	€ 148,500	3	€ 49,500
Austria	€ 100,750	3	€ 33,583
Iceland	€ 29,600	2	€ 14,800
Latvia	€ 21,250	2	€ 10,625
Lithuania	€ 15,000	1	€ 15,000
Croatia	N.A.	1	N.A.
Portugal	€ 0	0	€ 0
Slovenia	€ 0	0	€ 0
Liechtenstein	€ 0	0	€ 0
Luxembourg	€ 0	0	€ 0
Total	€ 307,923,725	341	€ 903,002

Types of violations



59.2 % related to unlawful processing, 20.8% to security measures, 9.1% to the proper handling of the rights of the data subject, while Privacy Notice breaches accounted for 3.8% of the total.

Economic impact of the types of violation

Type of Violation	Number of sanctions	Incidence on type (€)	% Incidence on total
Unlawful processing	202	249,857,221	81.1 %
Security measures	71	55,350,505	18 %
Data subject rights	3	1,908,821	0.6 %
Privacy Notice	3	51,28	0.1 %
Other violations	24	755,898	0.2 %
Total	341	307,923,725	100%

Looking at the time period from March 2020 (the start of the Covid-19 pandemic) to mid-April 2021, it is evident that the articles subject to sanctions due to their violation are 80:20 in favour of those related to substantial processing of personal data and consent.

“Substantial” Violations		
Violated Article	How many times	
	Europe	Italy
5	243	50
6	160	28
7	11	4
8	2	0
9	24	14
12	33	9
15	26	6
16	1	1
17	11	2
18	1	0
21	15	2
25	13	5
31	14	0
32	100	12
35	9	2
36	1	0
37	6	2
TOTAL	670	137

“Form” Violations		
Violated Article	How many times	
	Europe	Italy
13	52	11
14	22	2
24	12	3
28	12	7
29	3	1
30	2	1
33	21	2
34	9	1
44	1	0
48	1	0
58	26	0
TOTAL	161	28

It should be noted that the presence of formal violations in 20% of cases is independent of the frequency of the causes of triggers, which remains linked to **violations of substance** at 95% of all sanctions.

Italy is in line with Europe:
more than 80% of the sanctions are related to improper handling of personal data and consent,
including failure to erase data beyond the retention period (data retention)

By aggregating the data, it emerges that, within the EU, out of 831 articles of the GDPR violated, 161 concern "structural-preparatory" provisions (19%), while 670 concern the "handling of personal data and consent" (81%).

In Italy, on the other hand, in one year, out of 165 violated articles of the GDPR, 28 concerned "structural-preparatory" provisions (17%), while 119 concerned the "management of personal data and consent" (83%).

The rather surprising result is that Italy is perfectly in line with the European average.

The danger of leaving good intentions on paper

Both in Europe and in Italy, the vast majority of sanctions in the last year concern the improper management of personal data and consent, rather than the "preparatory-structural" aspects of GDPR compliance, despite the fact that companies have so far directed the greatest energies and resources precisely to these.

From this we can derive two possible interpretations: the first is that European companies have properly prepared for the advent of the GDPR by adopting a whole series of documents and procedures.

The second is that, most likely, these procedures have remained on paper and that, once completed, companies have continued to operate without really caring about how to properly manage all the data in their possession.

This is confirmed by the fact that the second group collects 83% of all sanctions for Italy and even more so from an economic point of view.

**Trials of companies that end
in a civil conviction or a financial settlement are not public
because no one has an interest in disclosing them**

The additional dangers:

It should be borne in mind that the data made public do not include, and are the overwhelming majority, all those proceedings that have not reached a final decision after the case has been opened by the Italian Data Protection Authority.

Having the Authority on your back is not a pleasant thing. Having to fulfil all the requests that are made to the company becomes the more damaging and risky from a financial point of view the more the company has a fragmented and unstructured organisation of data and especially of consents.

The administrative sanction is just the tip of the iceberg: the nightmare of the class action

Legal proceedings against companies for mishandling personal data are steadily increasing, and case law is particularly harsh on companies that violate their rights under the GDPR.

The trials that end with a civil conviction of the companies or with a settlement are certainly not public because no one has an interest in disclosing them.

Not to mention that in the event of a conviction, it is very likely that the Data Protection Authority will decide to investigate the matter.

On the contrary, it is even more common to file a report with the Data Protection Authority against the company so that it can use the report produced by it to support its claim in court and obtain greater compensation for the damage, perhaps by creating a class action.

Who is responsible for ensuring the protection of the company?

In order to properly protect the company, it is necessary to understand from the data and statistics that administrative and civil sanctions arise from “glitches” related almost exclusively to the incorrect management of personal data and consent rather than from inappropriate documentation. However fundamental they are, in order for someone to contest the processing register or the governance policies, they must be able to access them and therefore we are already at the point of an inspection or request for documentation by the Authority. **But what leads the company to find itself in this situation?**

More than 95% of the time the **triggering cause** is the dispute of a customer, a prospect, a candidate, a former customer who detects an offence against them and, simply by exercising their rights, gets the company in trouble with a trivial email or phone call.

If this is so obvious, why do companies still find themselves exposed on the most critical side?

The transition from theory (and the controller's promises) written on paper to the everyday practice of collecting, processing and deleting personal data and consent still seems to be **no man's land** in companies.

While Governance is clearly the responsibility of the DPO and Legal, Cyber Security of ICT, Privacy by Design – understood as the review of business processes and applications in terms of Data Protection – is a topic for which everyone is at risk but no one is responsible. Unlike Cyber Security, which the ICT department rightly sees as its own responsibility, Cyber Data Protection does not relate to any one single department in the company and needs, in order to be implemented, the multidisciplinary collaboration of Legal and ICT, areas that are culturally very distant and not used to cooperating.

Only the CFO can provide the only possible spark to create a bridge between Legal and ICT in order to direct resources (also) towards Cyber Data Protection.

In the trap in which companies find themselves, where everyone is at risk but no one feels called upon to mitigate 95% of the causes of sanctions, **the only one who can do it is the CFO**, giving the DPO and ICT the direction and resources to also invest in Cyber Data Protection with the appropriate technology to properly manage personal data and consent to avoid unlawful processing.

Simple questions to ask the CIO and DPO to assess the degree of protection both of themselves and of the company are:

- Do we have a tool capable of centralising and consolidating consent, gathering proof of genuineness, avoiding misalignment and minimising unlawful processing?
- Do we comply with the retention periods and related erasure of the personal data we hold (Data Retention)?
- Are we able to respond adequately to the rights of data subjects within the timeframe?
- Are we able to trace consent (implicit and explicit) in order to reconstruct the history of the data subject in defence of the company?

What is at stake is not only the risk of sanctions but also **the image and reputation of the company** to be defended in the eyes of customers, **the stability and future attractiveness in the market** that will increasingly value personal data, provided they are legally usable.

The instruments of protection are there, it is a question of understanding the need for them and acquiring them.

By preventing trigger causes, the company can reduce the risk of sanctions (and loss of reputation) by up to 95%

More than 95% of the time, the **sanction trigger** (which then, like an avalanche, drags everything downstream, often uncovering Pandora's boxes of offences) is provoked by a prospect, a customer, an employee, a former customer or competitor who complains about one newsletter or one phone call too many and in any case the failure to respect their rights. In other words, the best advice remains **"don't pick a fight if you want to avoid the consequences"**. But how do you do it?

In the management of personal data, there are two main critical areas in companies:

- **CEO: documenting everything in order to have proof (and protect the company and themselves)**
The GDPR is based on Accountability, i.e. on the responsibility of **the Data Controller who has the burden of proof** in demonstrating their good faith and who is responsible for **recovering information and Proof of Genuineness in the event of disputes**. CEO is also responsible for doing everything possible to avoid offences **"[...] by adopting measures and instruments to minimise damage (to the citizen)"**.
- **CEO/CFO: introducing suitable measures and tools in the company to avoid offences**
Even in a prudent and careful business context, the main causes of (unintentional) offences are due to three factors:
 - misalignment of Consents due to Rectifications and Objections;
 - non-compliance with Data Retention and consequent erasures;
 - poor handling of data subjects' rights (main cause of complaint).

Monitoring these areas with adequate Cyber Data Protection tools means **preventing most critical situations** that the company and its managers might otherwise have to face (and justify to the Authorities during the inspection).

The first and indispensable Cyber Data Protection tool for managing these specific critical issues to protect the company is the **2nd generation Consent Manager**.

Protection in the company begins with the proper management of Consent

There are several considerations to be made in order to safeguard the company, and none of them disregards the proper management of Consents (both "explicit", i.e. based on the legal basis of Consent, and "implicit", linked to all other conditions of lawfulness).

For this purpose, there are specific tools called **2nd generation Consent Managers** (not to be confused with basic first generation consent managers or those for managing cookies), which can manage Consent throughout its life cycle, from collection to deletion. These tools collect and manage all privacy events, offering the company a very high level of protection and the DPO huge time savings in reconstructing privacy history and managing the rights of data subjects.

In addition to other unique and indispensable features that these dedicated solutions offer compared to any other alternative the company may adopt (including CRM or custom applications), other advantages are their impartial role with respect to corporate applications and (above all) the possibility of being able to relocate the risk of Consent management outside the company by choosing a Consent Manager in the cloud.

Authors of the survey



Mirco Caeran

Lawyer and PhD in Civil Law. Owner of the Studio Legale DMP law firm, he assists companies and corporations in labour law, contractual and compliance matters.

Giuseppe Ricci

Cyber Data Protection Specialist, Software Architect, founder and CEO of Active121, consultant and speaker on topics concerning software architectures for Digital Marketing and Cyber Data Protection.



Active121

www.active121.com



Active121 SRL is an Italian company (based in Veneto), founded in 2002 as a software R&D company in the digital marketing field for the collection, management (and exploitation...) of personal data.

Since 2016, it has completely refocused on **Cyber Data Protection** (protection of digital personal data) thanks to the skills gained in the development of technologies for the management of personal data, with the new purpose of protecting citizens and companies.

Today the mission of Active121 is to offer innovative and reliable software solutions on Cyber Data Protection for the GDPR-compliant protection of personal data and Consent to protect the reputation of companies and the relationship of trust between them and their customers.

In 2017, Active121 realised this mission through the development of the first software platform for the management of GDPR Consent throughout their life cycle: PrivacyOS. Today PrivacyOS is the most complete and innovative 2nd generation Consent Manager on the market chosen by international companies and groups.

PrivacyOS

www.privacyos.com



PrivacyOS is a cloud-based Cyber Data Protection platform for the management of Consent, classed as a **2nd generation Consent Manager** in terms of functionality and reliability.

It allows companies to manage the entire life cycle of Consent, from collection to deletion, in a secure and GDPR-compliant manner. It manages all legal basis, Data Retention, Rectifications, Objections, Right to be forgotten, Proof of Genuineness and all Privacy events. Through the Consolidation and Orchestration engines, PrivacyOS is able to collect and reconstruct the privacy history of each Data Subject in real time and to keep company applications updated and aligned, avoiding misalignments on Consents and illegal processing. PrivacyOS protects companies by helping them to minimise the risk of unlawful processing and to demonstrate compliance with GDPR in the event of disputes and inspections.

PrivacyOS helps prevent sanctions and loss of reputation

PrivacyOS has been designed to solve the two most critical GDPR issues in companies:

- **document and expose the evidence** that protects the company and the managers in the event of disputes, complaints and inspections;
- **avoid unlawful processing** (especially in Sales, HR and Marketing activities).

PrivacyOS offers a very high level of protection by helping companies and managers to **minimise the risk of offences** and **demonstrate their compliance with GDPR** in the event of disputes, complaints and inspections, including through showing Proof of Genuineness.

More importantly, PrivacyOS offers the company 4 additional indispensable benefits:

1. it is always **updated with the Italian and European Regulations**;
2. it can be listed among the "**Damage prevention and mitigation tools**" (measures required of Data Controllers by Art. 32 of the GDPR among the activities for Accountability);
3. it has the role of "**Authoritative Impartial Controller**" towards other applications, demonstrating, during the inspection, the good faith and Accountability of the Data Controller;
4. it allows the CFO **to relocate the Risk of Consent Management externally thanks** to the cloud architecture (this is probably the most strategic opportunity of all).

What are the alternatives for the company?

PrivacyOS is a unique solution in its category; however, it often faces two insidious "competitors":

- the company's choice not to do anything regarding Cyber Data Protection;
- custom solutions based on CRM.

Leaving aside the first scenario (which in some cases turns out to be the lesser evil), CRM cannot protect the company for the simple fact that it is not designed for this purpose:

CRM is designed to exploit personal data, not to protect it.

Although you may be reassured by those who, inside and outside the company, support this tactic, their protection risks being compromised without being aware of it, at least until the "moment of truth", during the inspection, when the evidence and the information **necessary for the defence of oneself and of the company is inadequate or absent** and even the Data Protection processes adopted to manage the consents are contested by the Authority.

The GDPR provides for retroactivity: a dispute that emerges today may force the company, in order to defend itself, to retrieve information and evidence even from months or years ago.

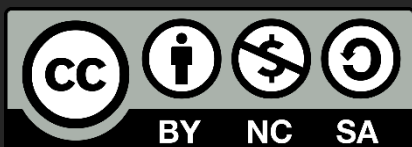
This is why it is vital for the company to immediately adopt a professional solution capable of defending the company from the most critical, current and future scenarios, one that is **always efficient and up-to-date with the GDPR** (a constraint that is particularly complicated and costly to guarantee with custom solutions, also considering that a CRM update may be enough to compromise or completely eliminate any customisation, however critical and costly it may be).

Some of the companies that have chosen to protect themselves with PrivacyOS



active121

ACTIVE121 SRL
hello@active121.com



License of the work

This work is original and based on public data,
authorship is by the authors and ownership is by Active121 SRL
Share our work freely
Always attribute the work to Active121
Do not use this work for commercial purposes