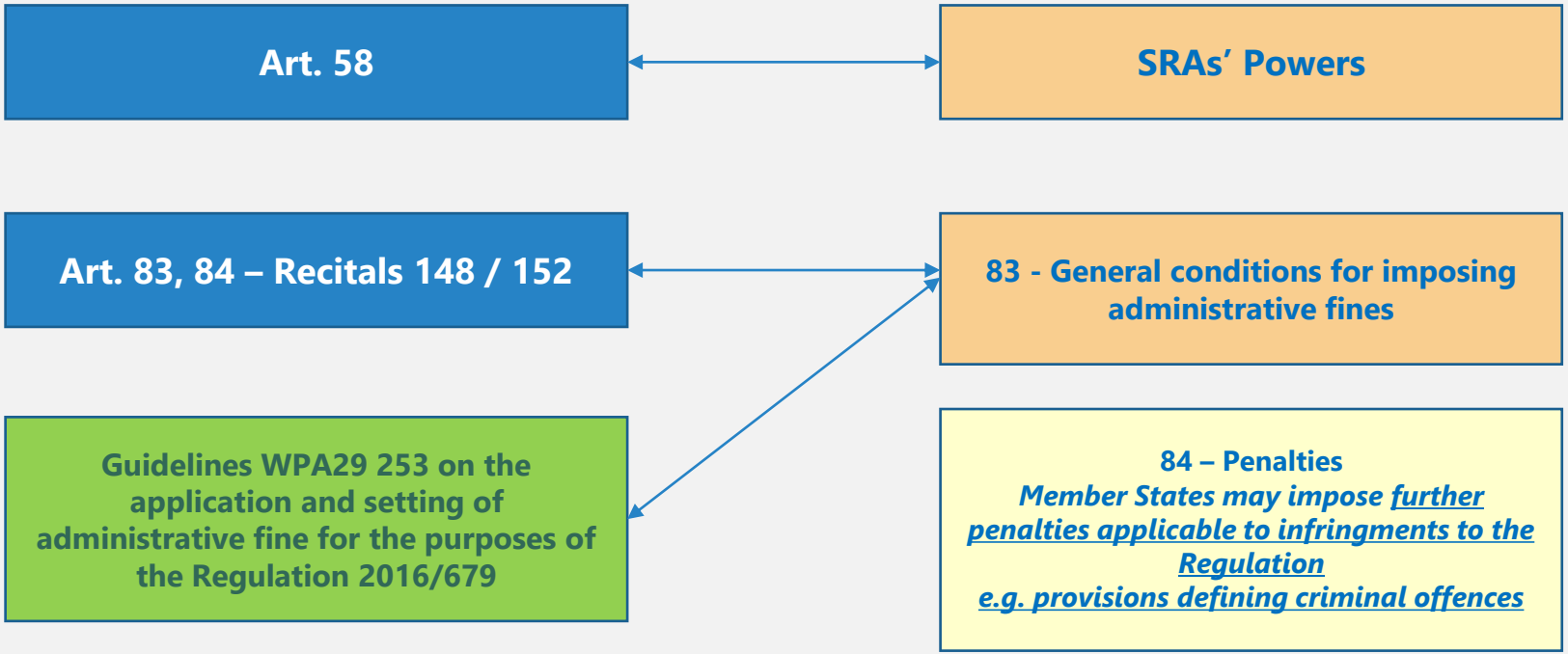
Determining the entity of the fines. The SRAs' powers

Avv. Lorenza Villa

GDPR Anniversary

MAY 25, 2021
ONLINE CONFERENCE

REGULATORY FRAMEWORK



Art. 84 implementation in the Italian Legal System

Amendments to D.Lgs 196/2003 («Code of Privacy»)

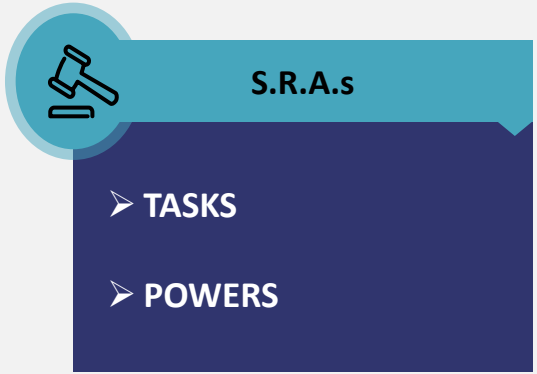
a. 167	Unlawful data processing
a. 167 bis	Unlawful disclosure and dissemination

Art. 84 implementation in the Italian Legal System

Art. 167 - ter	• Fraudolent acquisition of personal data
Art. 168	• False statements to the SRA
Art. 168	• Interruption of the performance of the tasks or the exercise of the SRA's powers

Art. 84 implementation in the Italian Legal System

Art. 170	• Non-compliance with an SRA's order
Art. 171	• Non-compliance with the provisions of the «Workers' Statute» (art. 4 and 8 - remote control and surveys on workers' opinions)



TASKS – art. 57

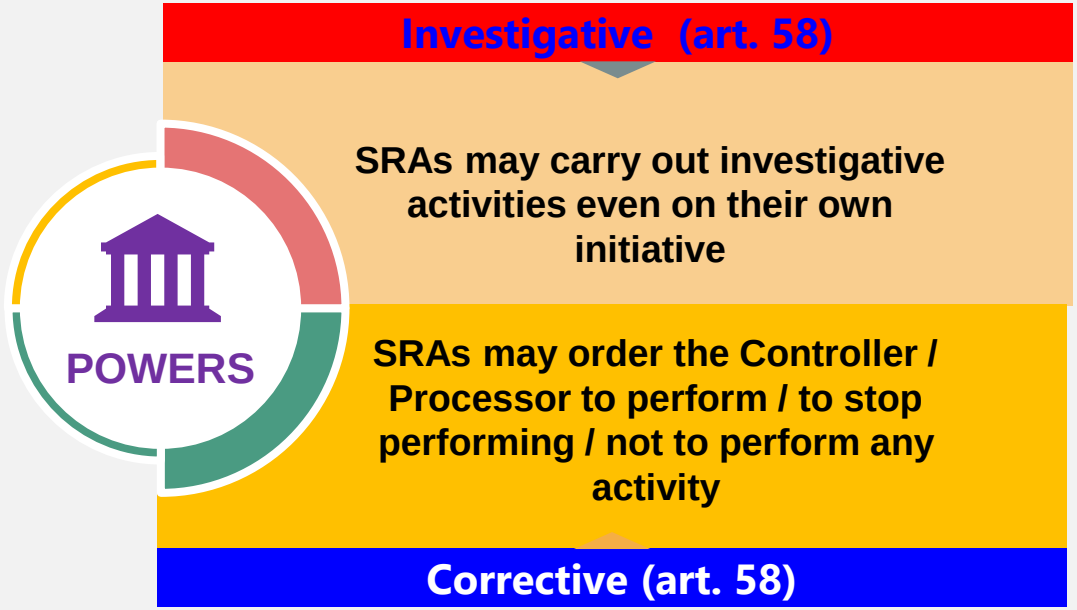
- ✓ Monitoring and enforcing the application of the Regulation
- ✓ Promoting public awareness and unerstanding of the risks, rules, safeguards and rights in relation to processing

POWERS

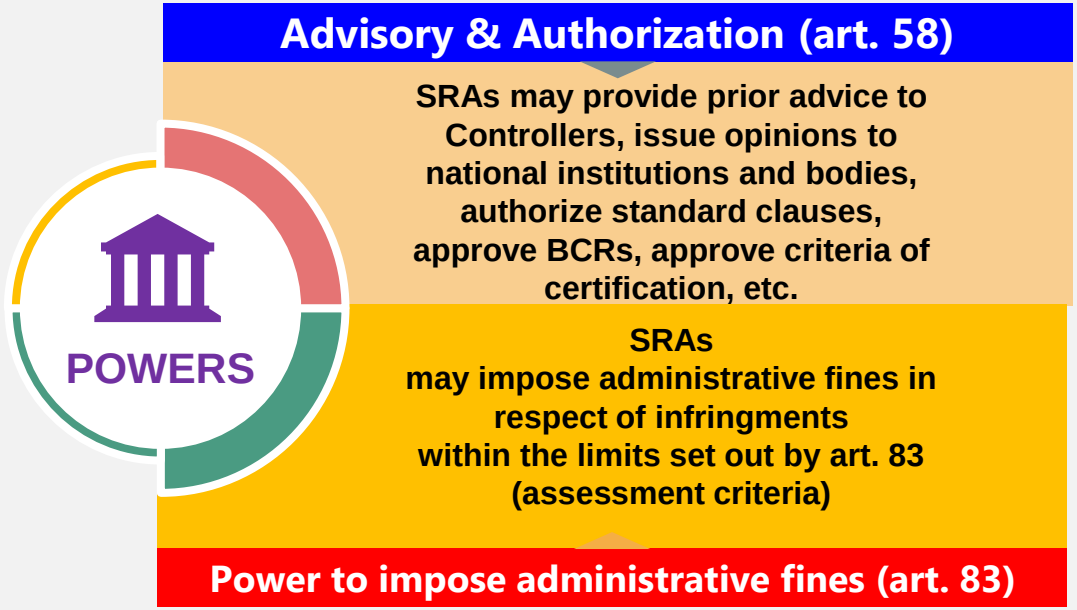
Art. 58

Art. 83

Art. 58 and 83 GDPR



Art. 58 and 83 GDPR



➢ **The powers provided for in each section of art. 58 are structured gradually**

Investigative Powers

a. Request for information to Controller / Processor

b. Investigations in the form of data protection audits

e. Access to all personal data and to all information held by the Controller / Processor necessary to perform the SRA's tasks

f. Access to any premises of the Controller and the Processor, including any data processing equipment and means, in accordance with Member State procedural law

E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars

➢ **The powers provided for in each section of art. 58 are structured gradually**

1 - Investigative Powers

- **Alleged infringment notification**
- **Infringment assessment**

2 - Corrective Powers

CORRECTIVE MEASURES – a.58

a. Warnings

b. Reprimands

e. Compliance orders (Data subjects' requests, GDPR provisions, Data Breach communications)

f. Personal Data rectification / erasure orders

g. Temporary or definitive limitations, bans on processing

h. Suspensions of data flows to a recipient in a third Country

58 + 83 + 84

ADMINISTRATIVE FINES – a. 83

Application and quantification of the fines – Principles & Limitations

E-Compliance EU GDPR INSTITUTE Academy
E-learning platform for Insights/Online Seminars

FINES MUST BE:

a) Effective

b) Proportionate

c) Dissuasive

PRINCIPLES

- **Nature, gravity and duration of the infringment (nature, scope or purpose of the processing activity; categories of personal data affected, number of data subject affected and level of damage suffered & action taken by the Controller / Processor to mitigate the damage. Number of infringed provisions. Intention or negligence?**
- **Previous infringments, if any, or previous art. 58 measures.**
- **Degree of cooperation with SRA and how the infringment became known to SRA.**
- **Adherence to an approved Code of Conduct / Certification mechanism.**
- **Other aggravating or mitigating factor applicable to the circumstances of the case → financial benefits gained, or losses avoided - directly or indirectly - from the infringment**

CIRCUMSTANCES OF THE CASE

Application and quantification of the fines – Principles & Limits

E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars

FINES MUST BE:

a) Effective

b) Proportionate

c) Dissuasive

PRINCIPLES

LIMITS

Major breaches of data protection are subject to administrative fines: whichever is higher of the following:

- up to **20,000,000 EUR**
- **up to 4 % of the total worldwide annual turnover of the preceding financial year**
- **Focused on incidents likely to cause damage and distress**

Medium breaches of data protection are subject to administrative fines: whichever is higher of the following:

- up to **10,000,000 EUR**
- up to 2 % of the total worldwide annual turnover of the preceding financial year
- Focused on process failures

QUANTIFICATION OF THE FINE

Total amount of fines since 2018

Total amount of sanctions / yr.	
2021	€ 17,060,000
2020	€ 113,217,430
2019	€ 440,515,407
2018	€ 400,000,000

https://www.coreview.com/blog/alpin-gdpr-fines-list/

Grounds for sanctions

E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars

2021 (Jan)	• Insufficient legal basis for data processing • Non-compliance with general data processing principles • Insufficient fulfilment of information obligations • Insufficient fulfilment of data breach notification obligations	11 2 1 1
2020	• Insufficient legal basis for data processing • Non-compliance with general data processing principles • Insufficient fulfilment of information obligations • Insufficient fulfilment of data breach notification obligations • Insufficient technical and organisational measures to ensure information security • Insufficient fulfilment of Data Subjects Rights • Insufficient cooperation with DPA • Lack of appointment of DPO	124 54 16 5 68 30 16 3
https://www.enforcementtracker.com/		

A “Model” for calculating the fines

- Danish Model
- German Model
- Dutch Model

NO COMMON EUROPEAN MODEL

The German Model

E-Compliance Academy
E-learning platform for Insights/Online Seminars

STEP 1 - assessment of the overall turnover of the business in the previous year. According to the average medium turnover within the category to which the business belongs, the business may be classified as: 1) very small, 2) small, 3) medium, 4) big.

STEP 2 - Assessment of the «basic economic value» = annual turnover : 360 (days).

STEP 3 – Assessment of the gravity of the infringment.
The basic economic value is multiplied by a factor that varies according to the gravity of the infringment with a value from 1 to 12.
Subsequent distinction between:

a) **Material infringment and Formal infringment (art. 82, 4 and 5), and**
b) **Gravity of the infringment on the basis of art. 83, (2): light / medium / medium-severe / very serious.**

STEP 4 – Final value adjustment, based on the elements referred to in art. 83, (2). In order to reduce / increase the final amount of the fine through specific coefficients (e.g: mitigation measures adopted by the Controller / Processor or manager: from - 25% to + 25%).

The «importance» of the DPO

- A Municipality dismisses one of its employees. The employee challenges the dismissal.
- The Municipality resists and – according to the Italian law – publishes the power of attorney along with some personal details of the claimant (namely her initials) and the subject matter of the dispute
- The claimant makes a complaint to the Italian SRA , claiming that the initials made her identification possible , being the Municipality a small one.
- Defendants, *inter alia,* opposes that the DPO was asked a prior advice on the matter, confirming thus the processing was GDPR compliant
- Italian SRA held:

  - Infringment of art. 4, par. 1, being the data subject "potentially" identifiable

  - Consultation with DPO should be retained as a mitigating factor

- Reduced fine of € 4.000,00

Telemarketing

TIM

€ 27.000.000

+ 20 corrective measures

- 4 % of the total worldwide annual turnover of the preceding financial year,
- Several illegitimate processing of personal data related to marketing activities from 2017 to 2019: promo and cold calls without consent, notwithstanding the data subject's registration in the “Register of oppositions”,
- Non-transparent information on data processing was provided and invalid consent acquisition methods. Paper forms used with a request for a single consent for various purposes, including marketing.
- A few million people involved

Infringment without fine: the Mailchimp case

E-Compliance EU GDPR INSTITUTE Academy
E-learning platform for Insights/Online Seminars

- Infringment of artt. 44 ss. GDPR and prescriptions from «Schrems II» ,
- Newsletter activity through a provider with data center located in the USA not supporting the additional measures prescribed by the German SRA after the CJEU judgment (17 July 2020),
- No fine imposed ,
- The SRA's decision was based on the fact that at the time of the infringment the EDPB Recommendations n. 01/2020 had not been published yet.

SLV Consulting
Lorenza Villa
avv.villa@pm.me

Linked in
Connect to Opportunity™

www.linkedin.com/in/lorenzamaria-villa