GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Data breach notification

4 April 2019

Giuseppe D'Acquisto

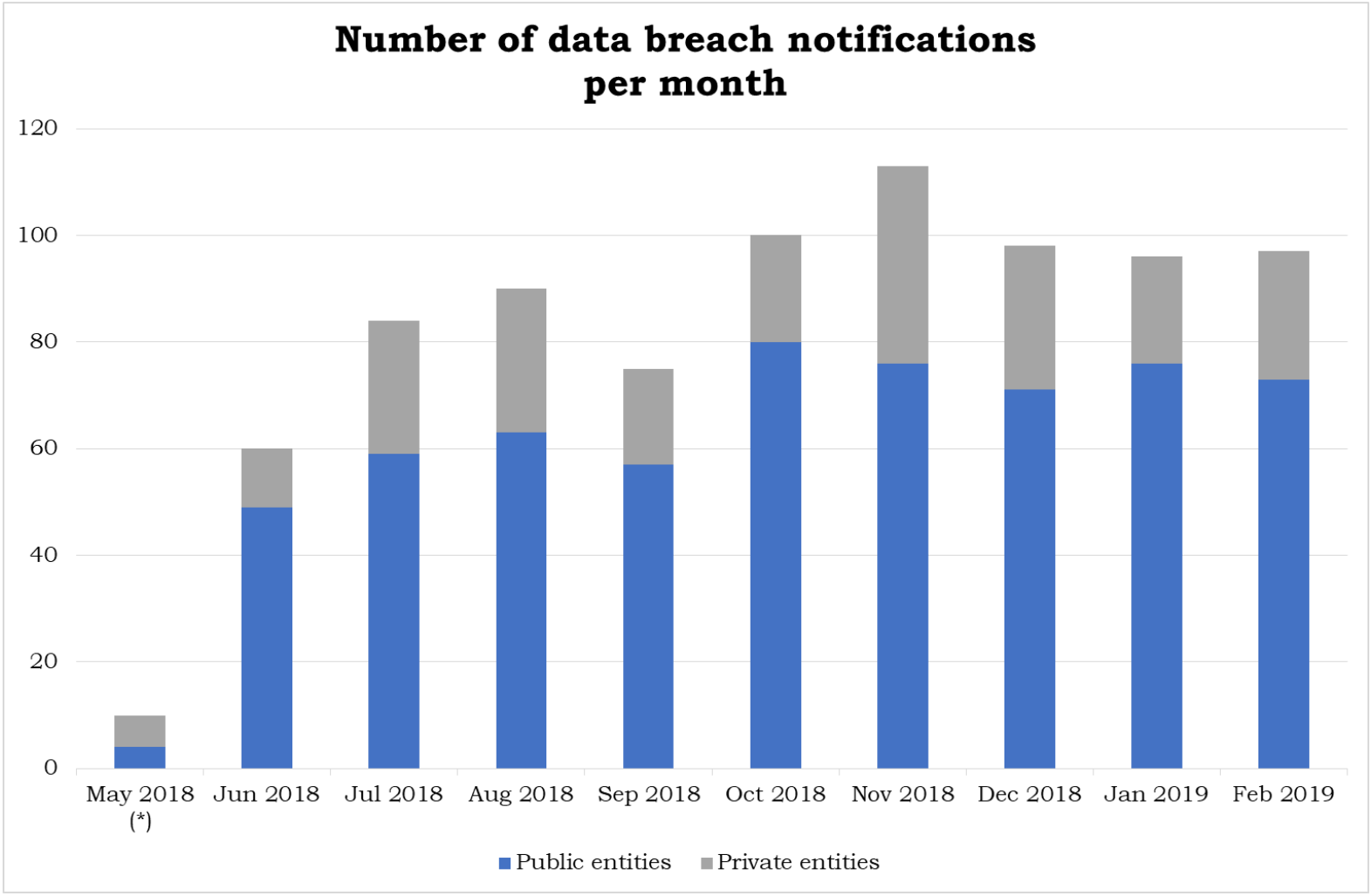
Outline

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

- Statistics
- Workload: past, present, future
- Effectiveness
- A way forward (incentive compatibility, public interest and interplay between art. 32 and art. 33-34)

Statistics

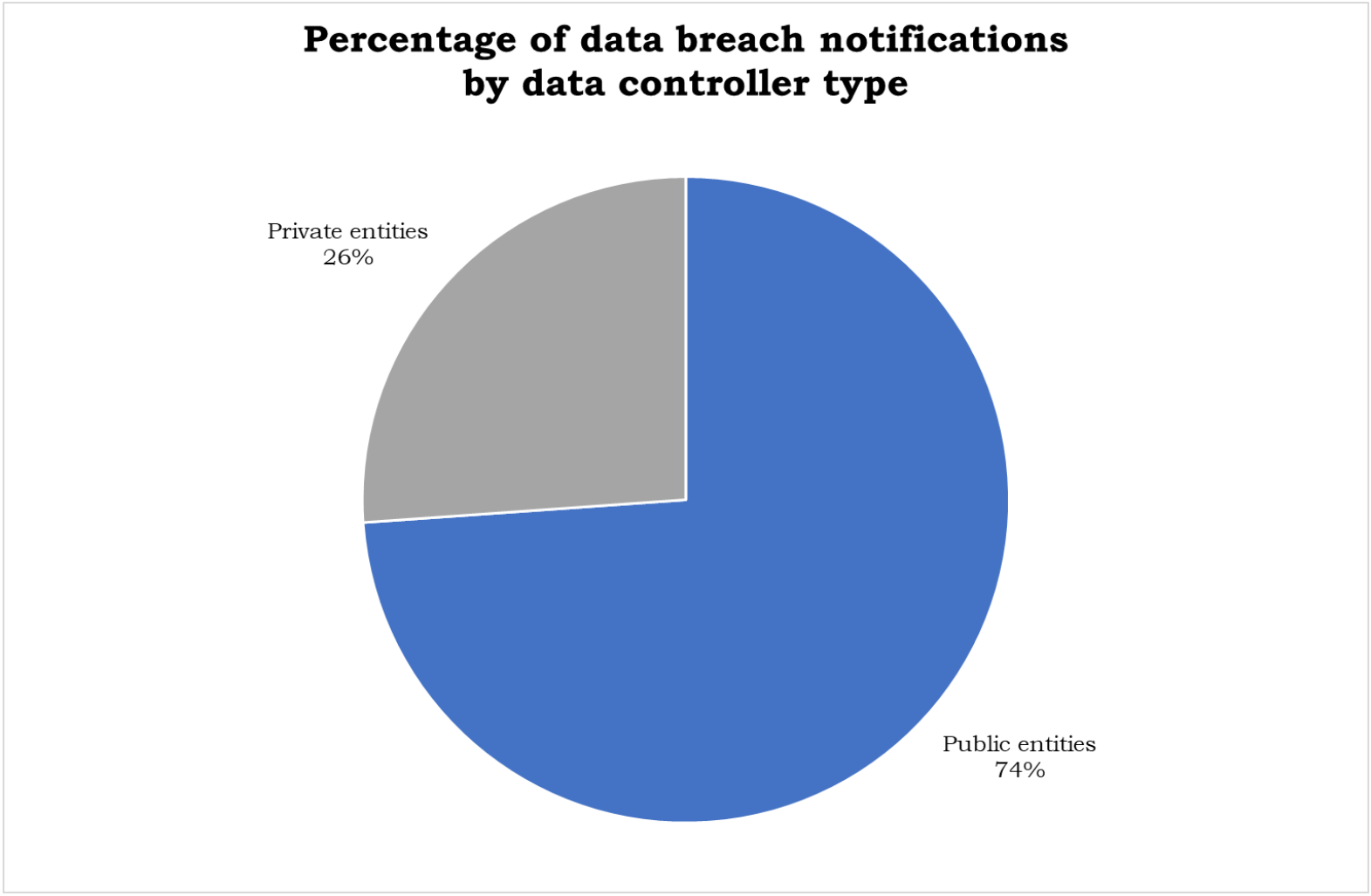
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



(*) from 25 May 2018

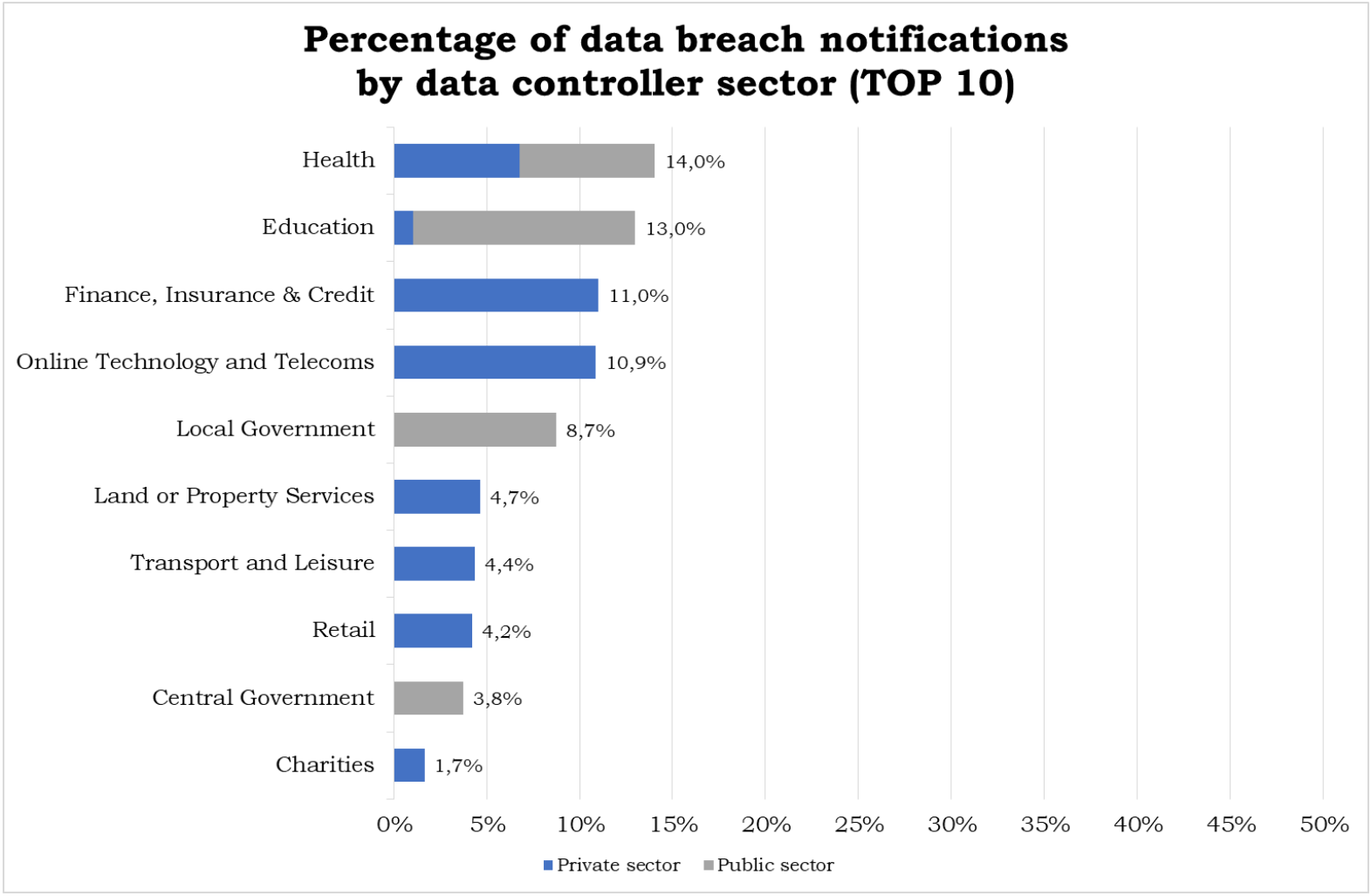
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



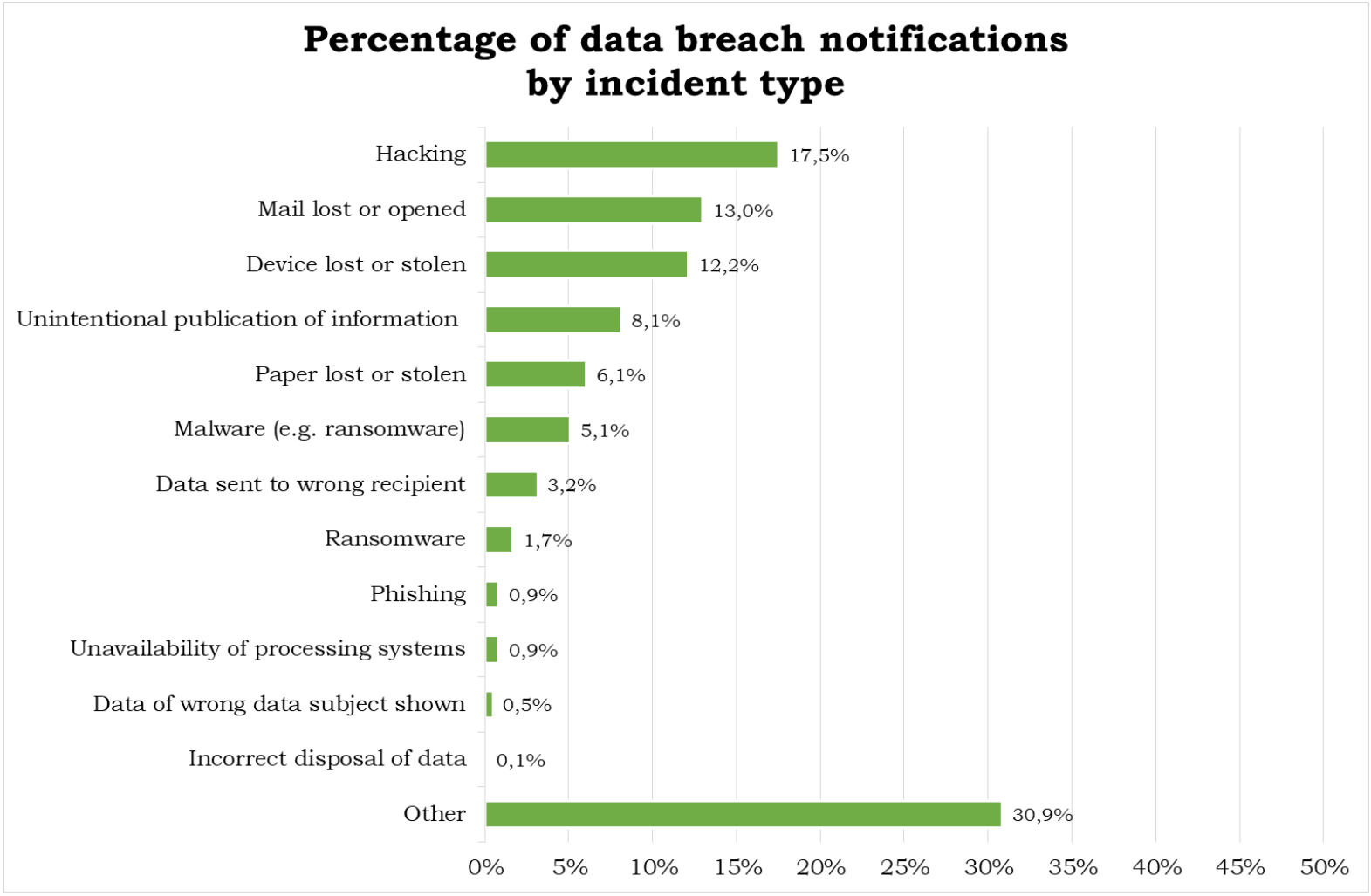
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



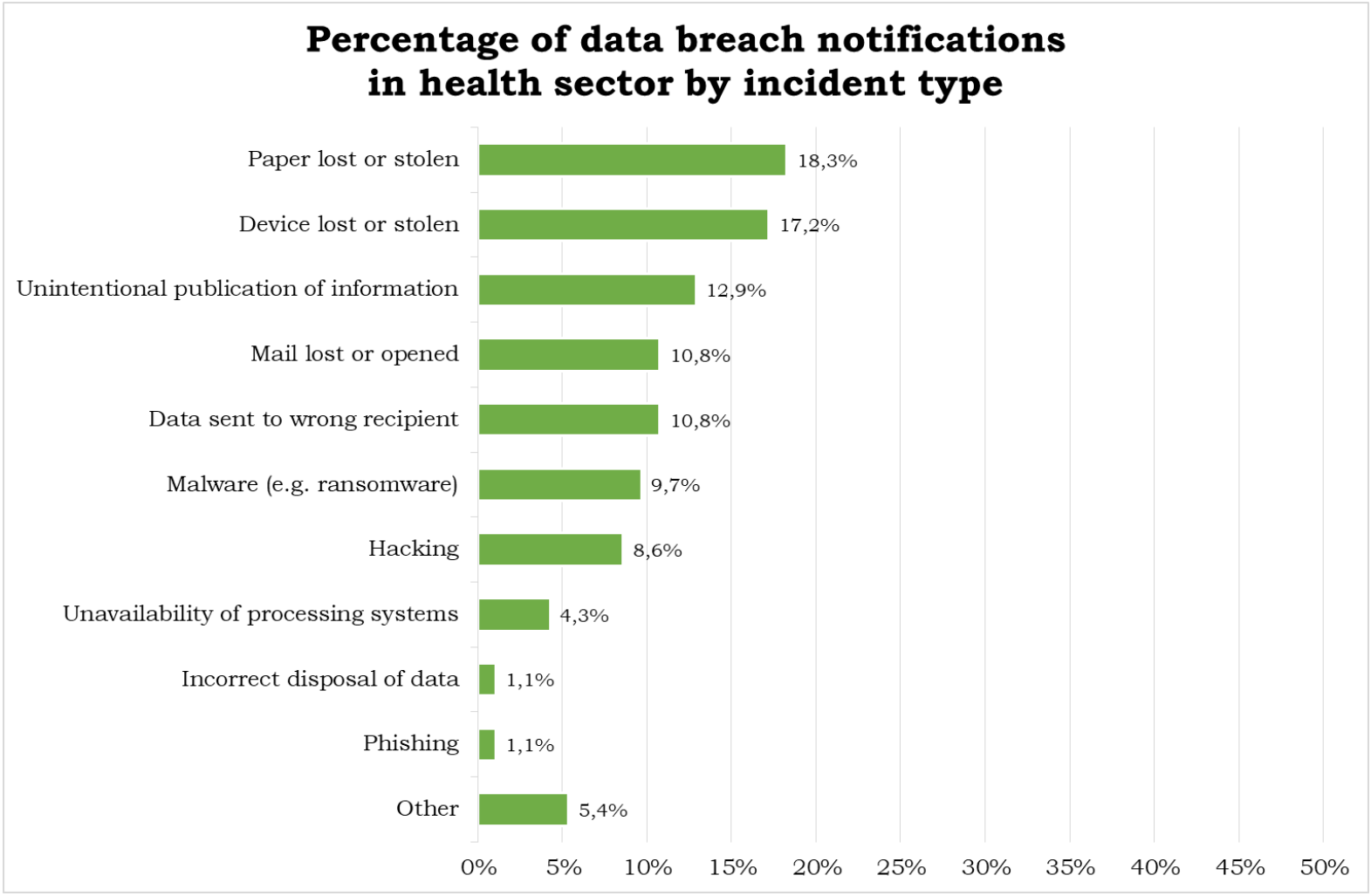
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



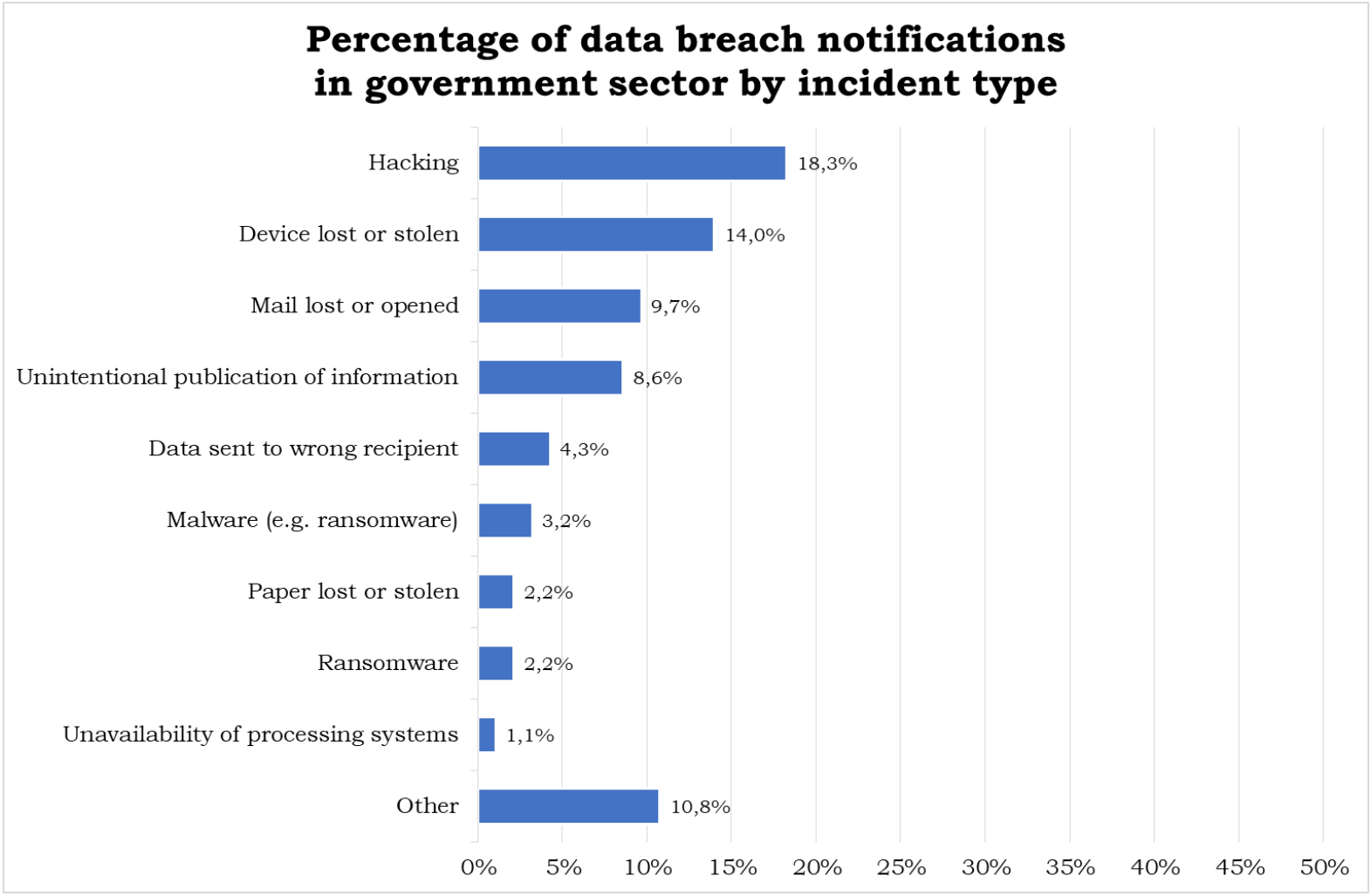
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



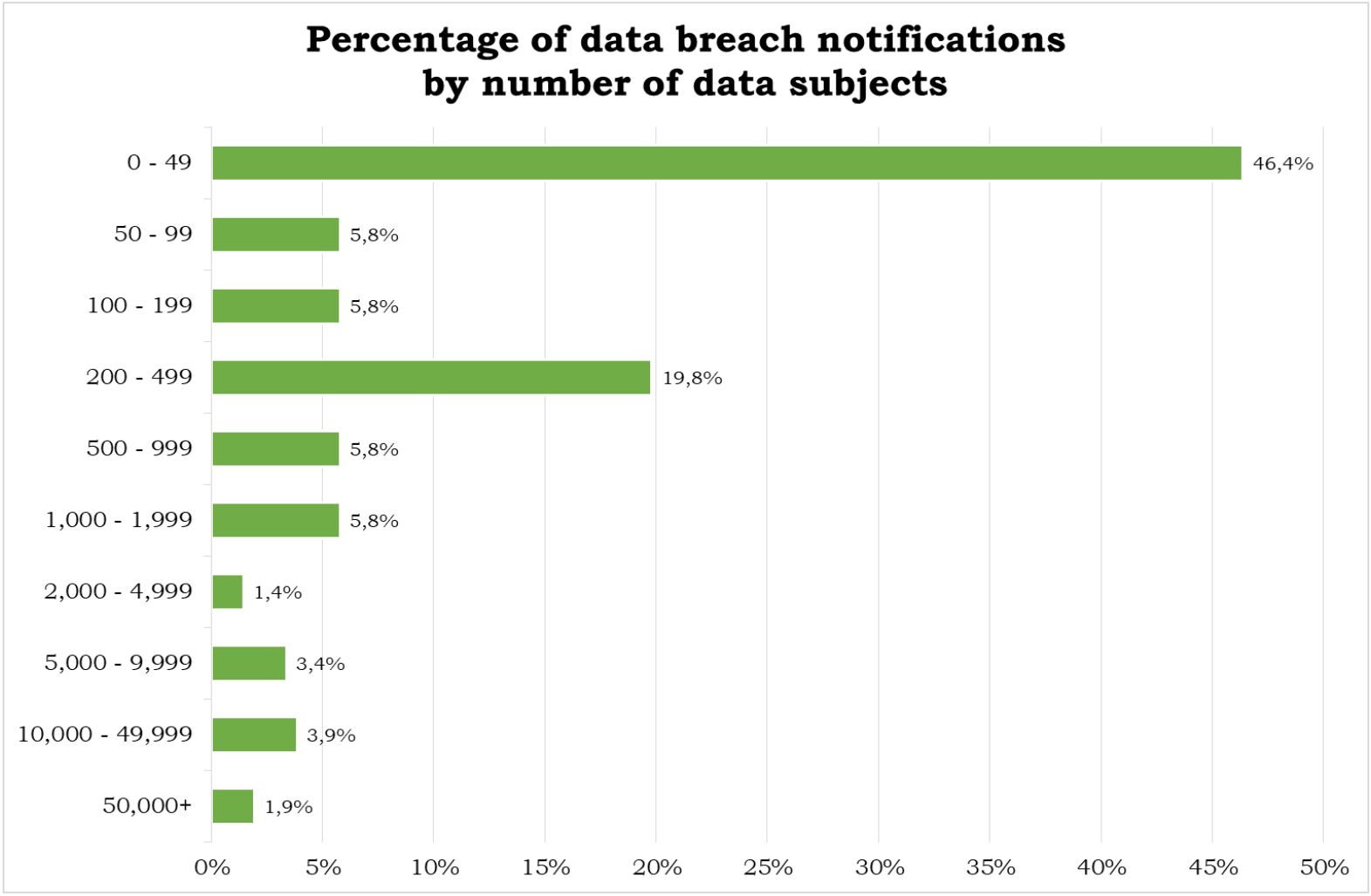
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



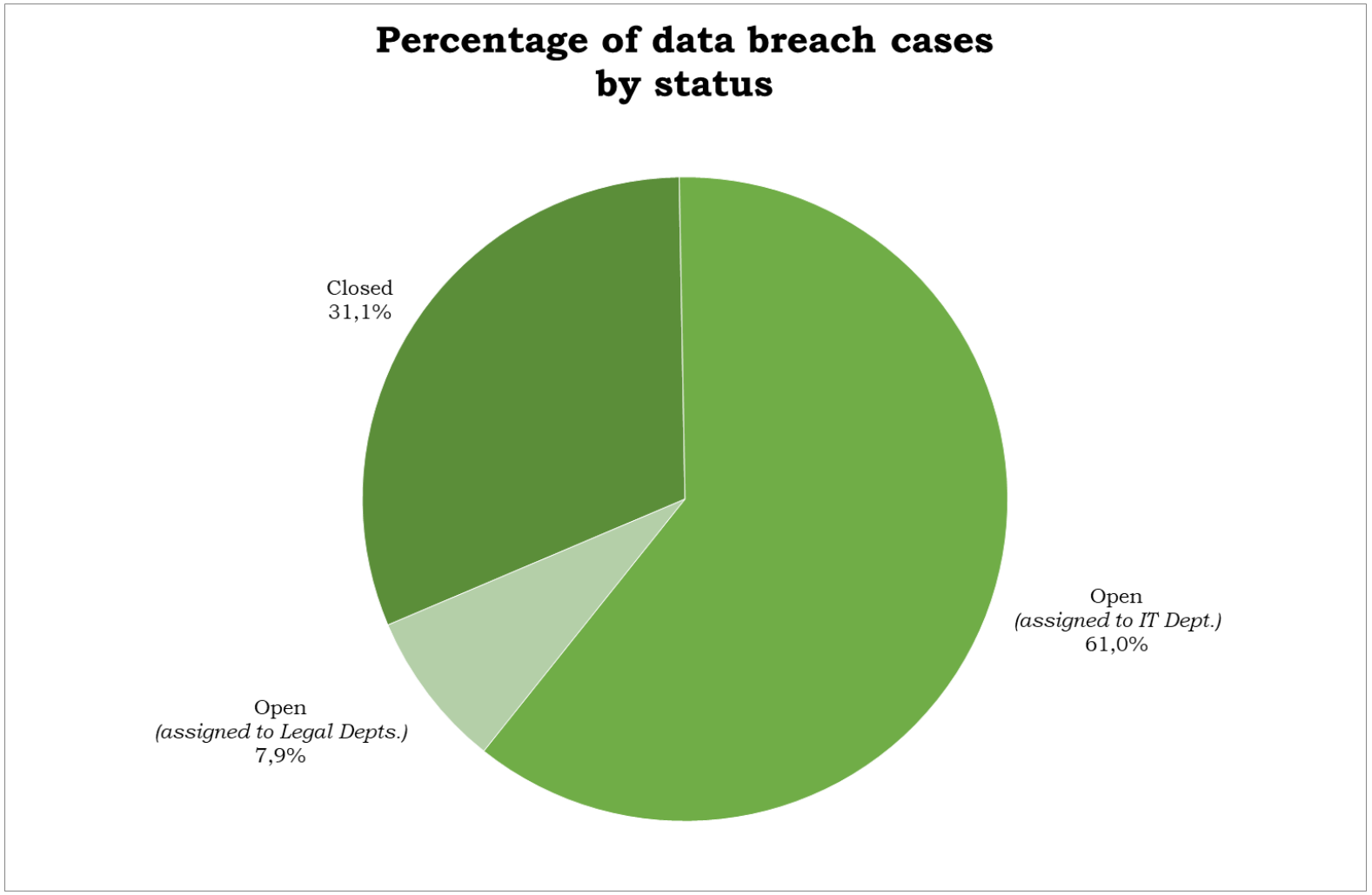
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



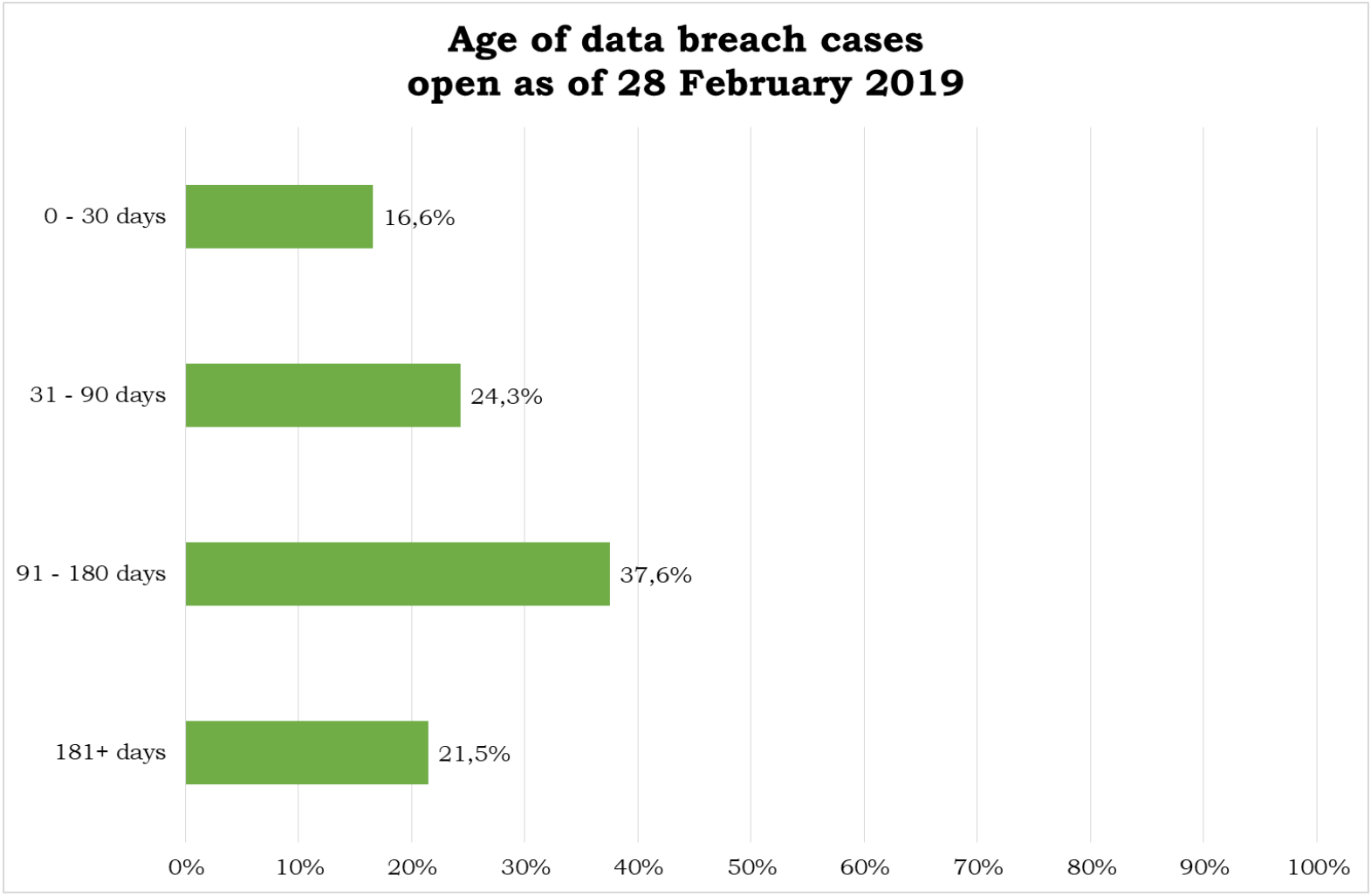
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



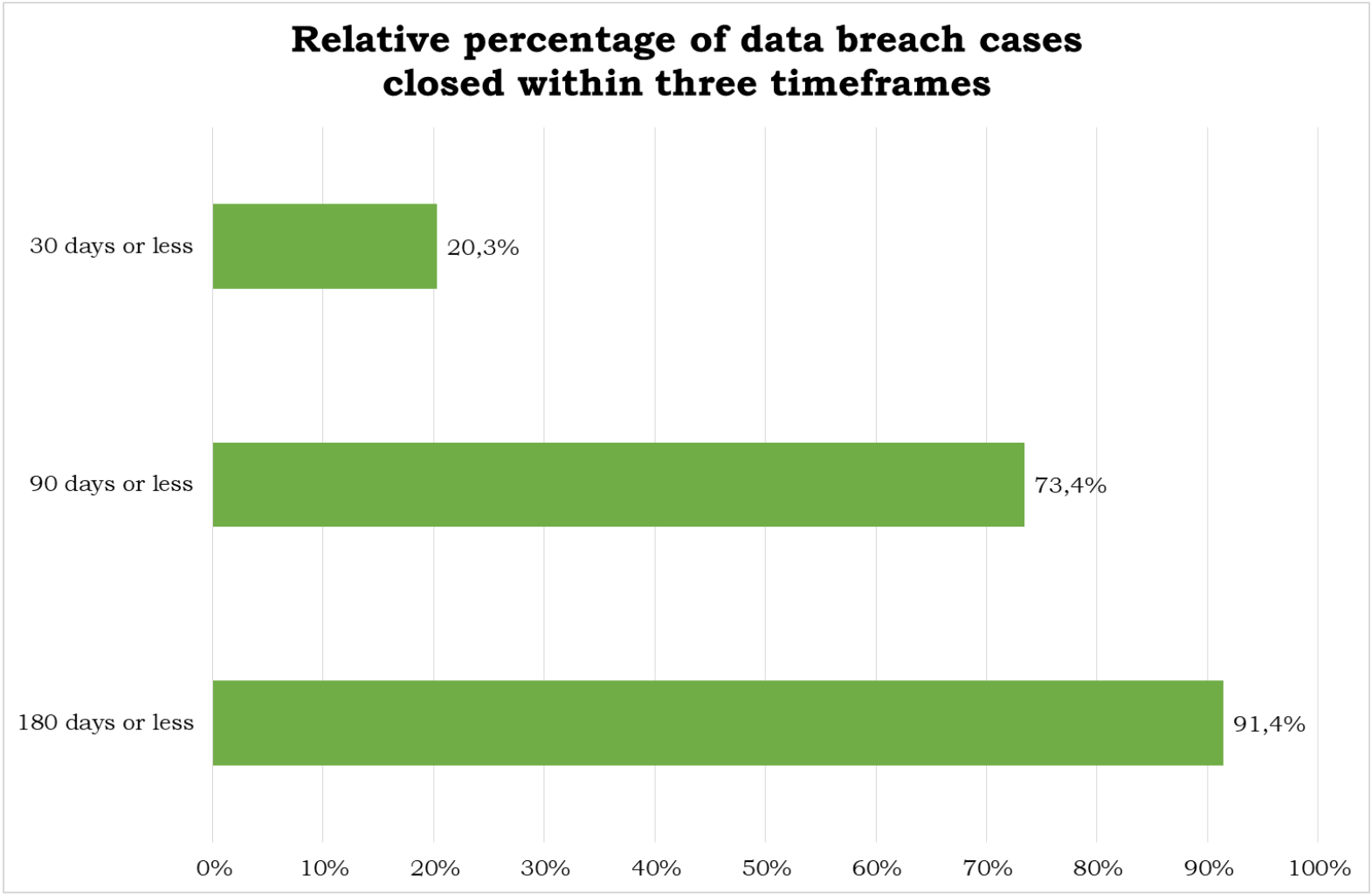
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



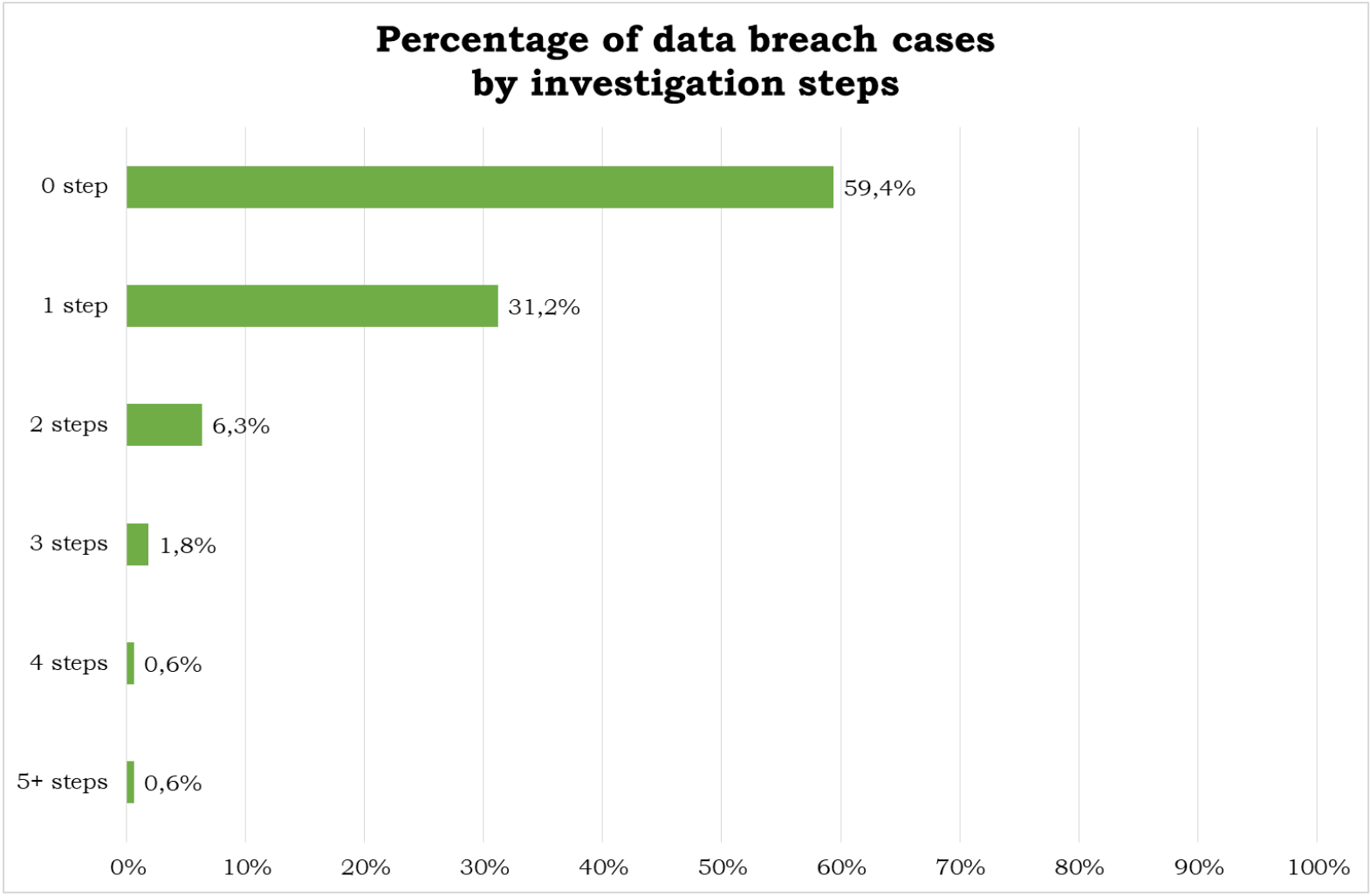
Statistics

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Statistics: some Italian DPA numbers

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



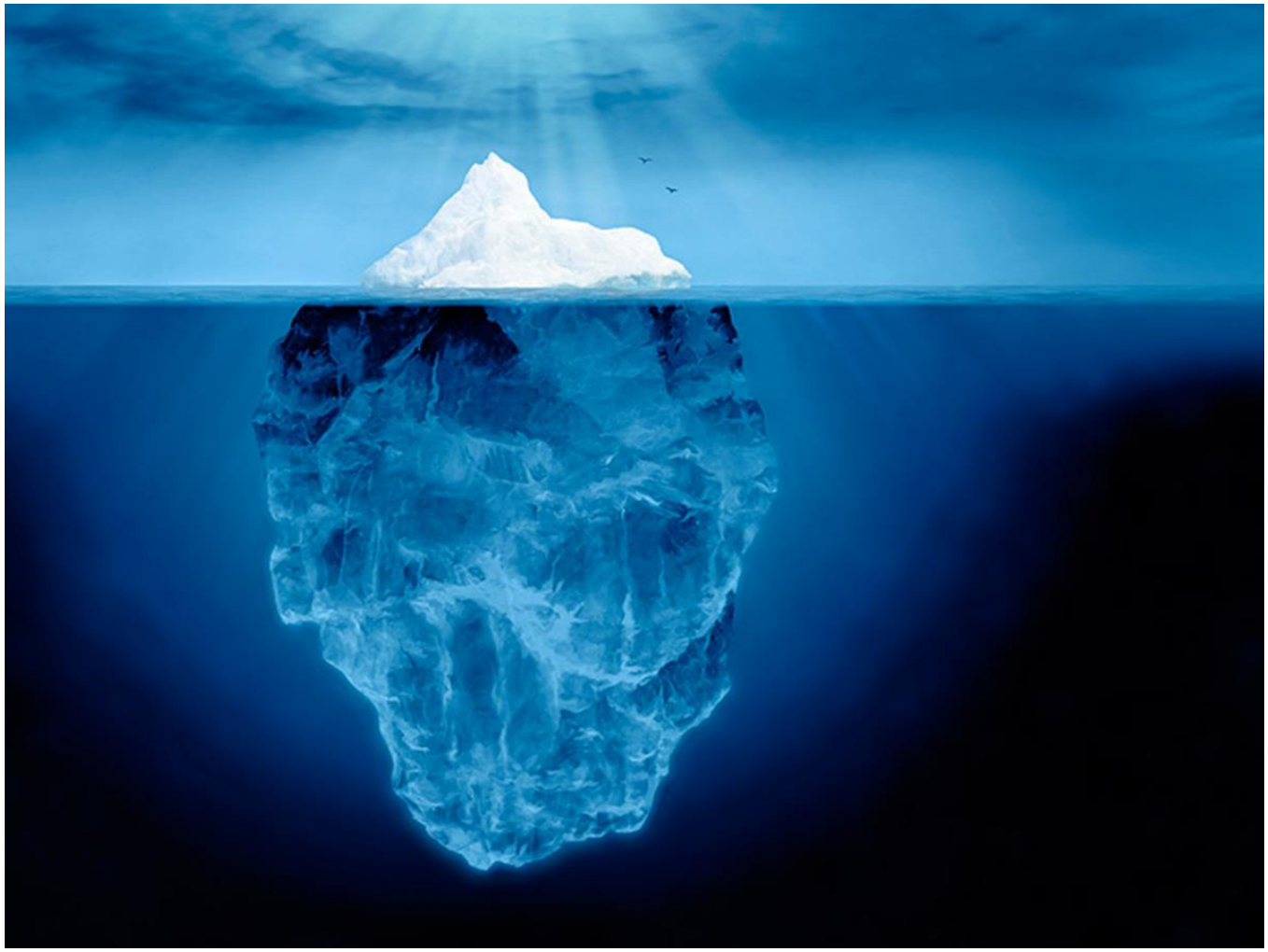
Workload: past, present, future

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- 56% of businesses have suffered at least one security incident within the last year (Ponemon Institute, 2018)
- Let's make some computations
  - According to the national statistic bureau (ISTAT) in Italy we have 4 Million businesses
  - We should expect 2 Million security incidents
  - How many notified in 1 year? 2000 (conservative estimate)

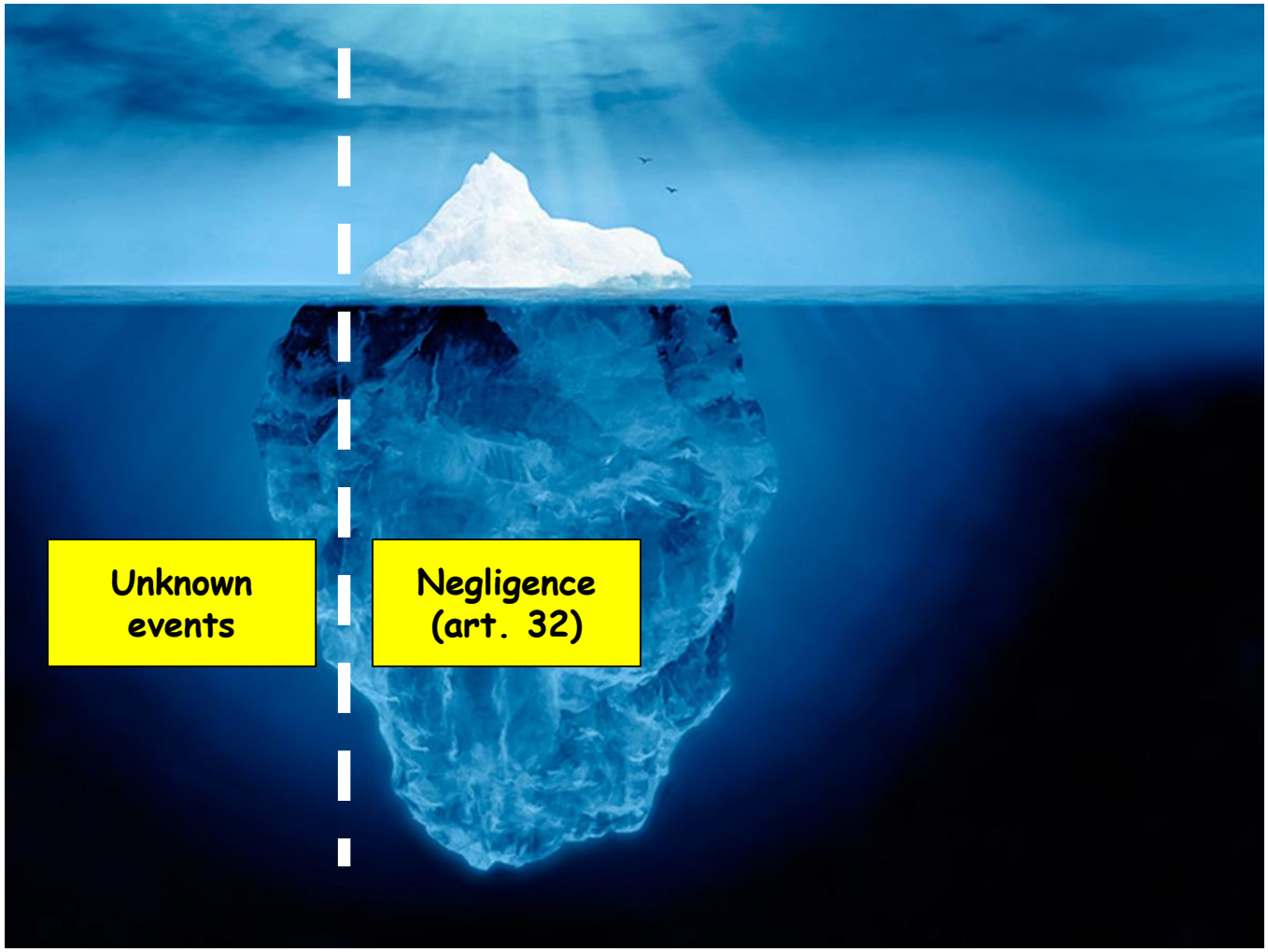
Workload: past, present, future

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI



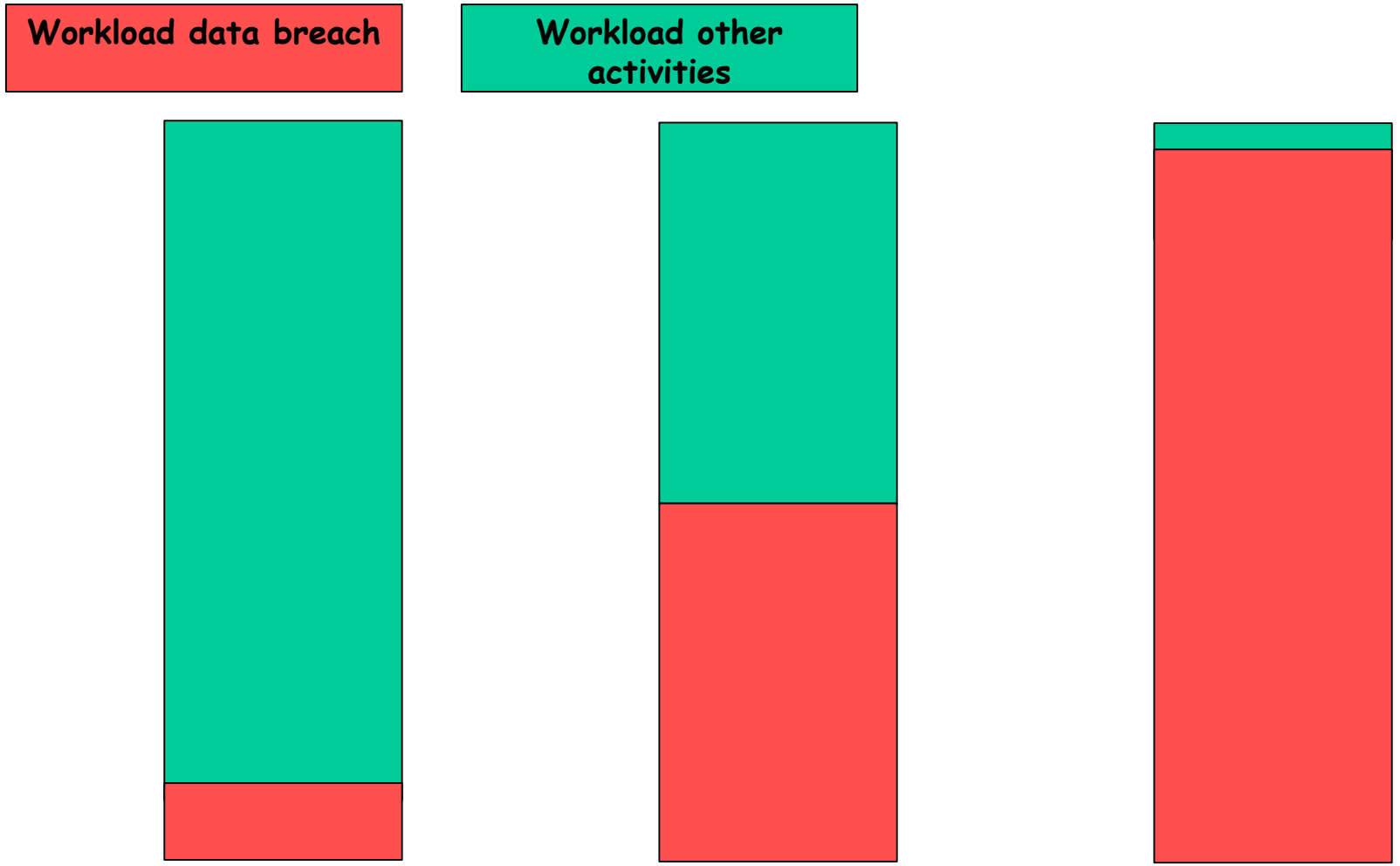
Workload: past, present, future

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI



Workload: past, present, future

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Effectiveness

Negligence

Investigate

Discard

Effectiveness

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- When we discard
  - We assess the risk (where is accountability?)
  - We give «on call» assistance (not exactly our job!)
  - We open and close a formal case
- When we investigate
  - We can prescribe technical and organizational measures (requiring investments)
  - We can prescribe the communication of the data breach to the affected data subjects (that may impact reputation)
  - We can impose fines (requiring expenditures)

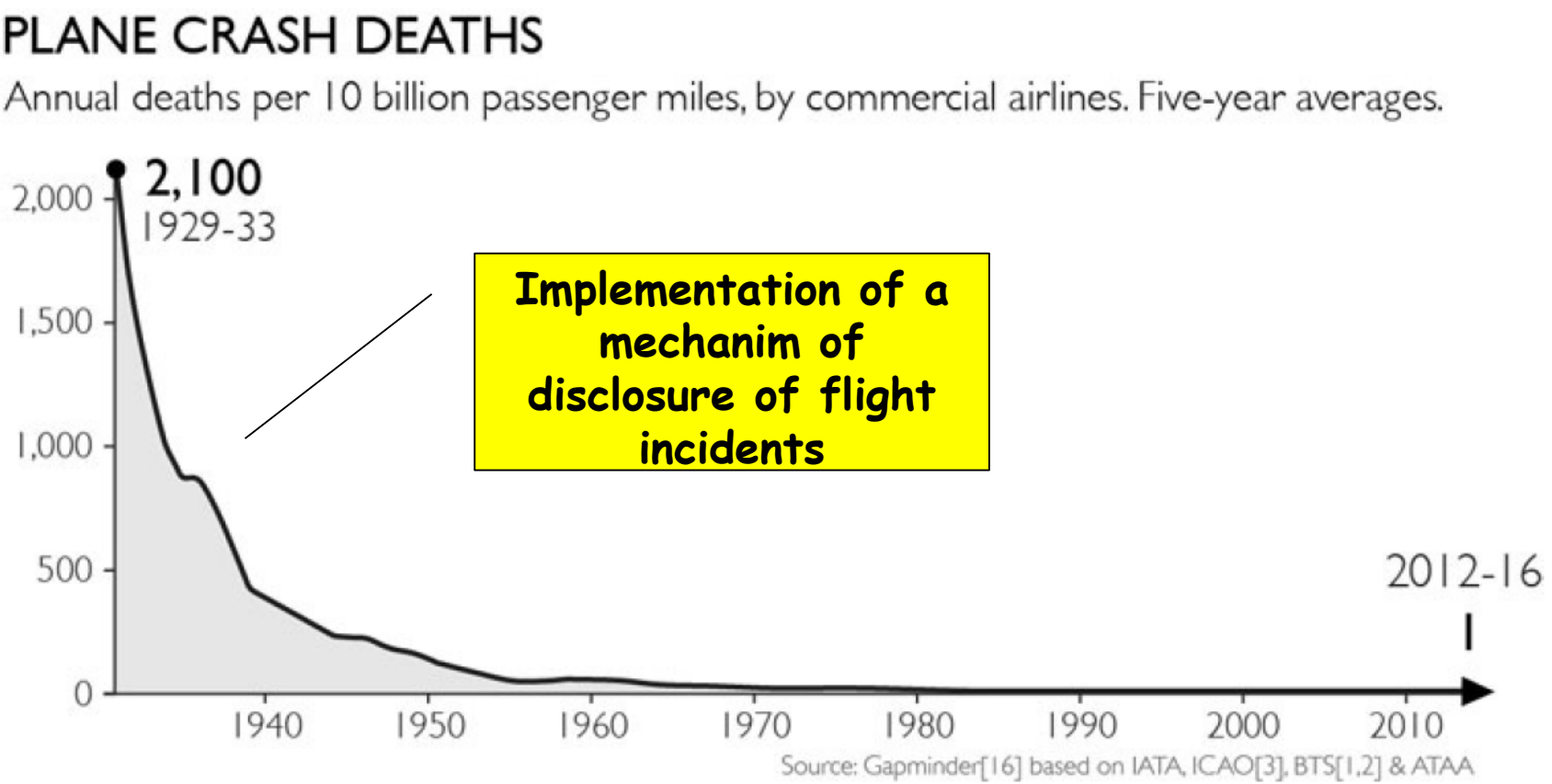
Effectiveness

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- Consequences of discarding
  - Workload with poor societal benefit
  - It's a sort of public audit to private companies
  - Not manageable in «full iceberg» scenario
- When we investigate
  - We observe a slow down in notifications (it's just a correlation!)
  - DPOs who suggested their controllers to notify are disappointed

A way forward

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



Implementation of a mechanim of disclosure of flight incidents

A way forward

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Notification in the public interest (of gaining knowledge on unknown incidents and increase trust in digital services)

Known

Known

Unknown

Known

A way forward

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Interface

Negligence

Investigation

Conclusions

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- Notification is very useful to enhance trust and to protect individual's rights in data economy
- It is less suited for discovering negligence (few incentives)
- We don't need to restructure the mechanism, but we need to work on the «notification interfaces»
  - For notification we need trust between DPAs and controllers and very skilled authoritative DPOs
  - For discovering negligence we need to promote users' role and certification mechanisms, finding the right incentives for disclosure

Thanks

g.dacquisto@gpdp.it