Privacy and distribution of motor insurance in Covid19 time

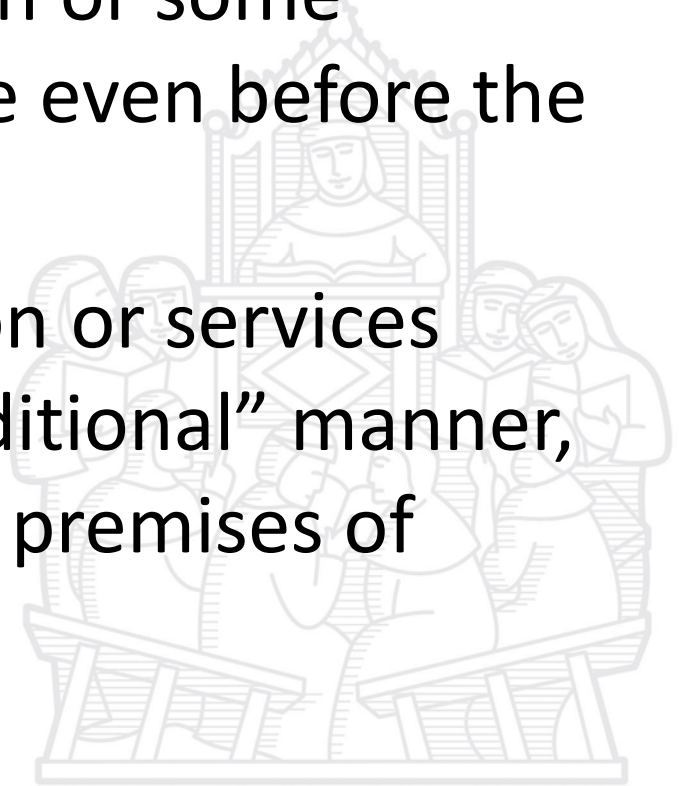
Maria Gagliardi

m.gagliardi@santannapisa.it

Sant'Anna
School of Advanced Studies – Pisa

the problem of privacy and data protection in the current phases in which the distribution of insurance products takes place mainly online:

- cases in which the distribution or some services were provided online even before the Covid19 crisis, and
- Cases in which the distribution or services before were provided in “traditional” manner, with the insured going to the premises of insurer or of an intermediary.



cases in which the distribution or some services were provided online even before the Covid19 crisis

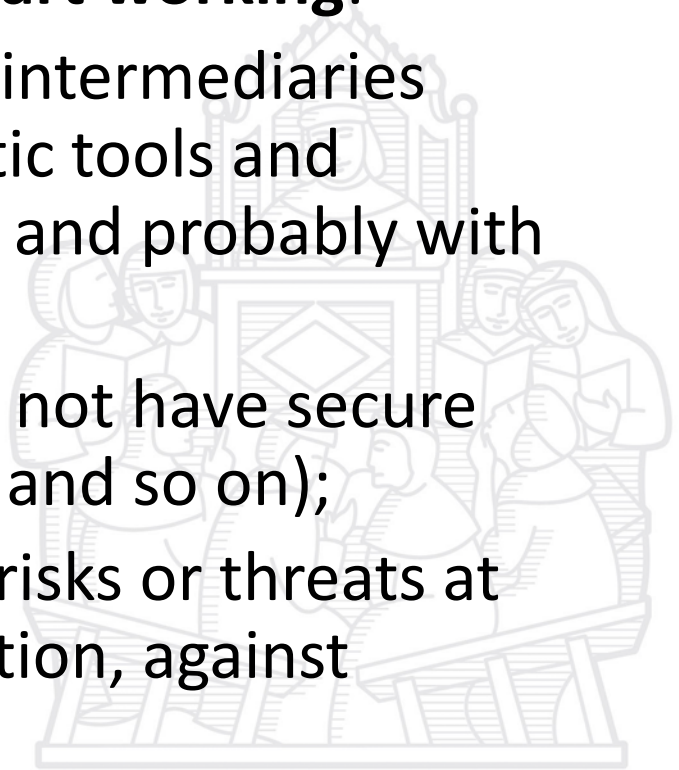
- the privacy issues have not changed, but
- we are facing a growth in risks of cyberattacks

Here the point is to monitor the scope of responsability in using websites and platforms, as well as security measures (in general: pay attention to the position of insurers/intermediaries in prevention of risks)

Cases in which the distribution or services before were provided in "traditional" manner

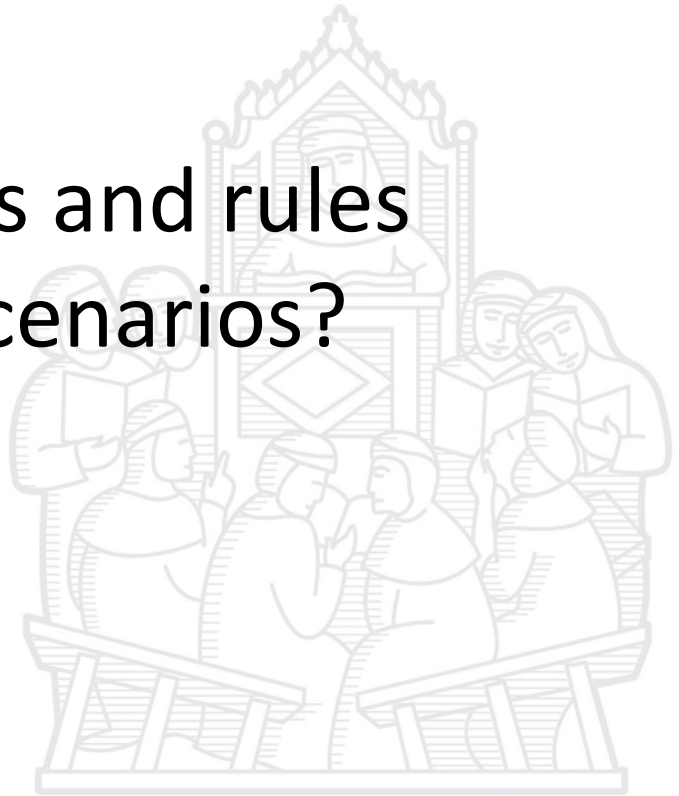
the are new situations to manage and therefore new problems, for instance **workers in smart working**:

- employers such as insurers and/or intermediaries should provide them with informatic tools and connections, not already available, and probably with specific training);
- workers working from home might not have secure connections or dedicated tools (pc and so on);
- also insureds are not aware of the risks or threats at stake (need for warning and education, against phishing for instance).



This is the picture, more or less.

What about legal issues and rules governing different scenarios?



In the *European legal framework on data protection and privacy* (mainly the General Data Protection Regulation, i.e. Reg. n. 679/2016, GDPR)

- for data processing in insurance production and distribution, Insurers are considered "**controllers**" (art. 4 GDPR). That means they decide goals and means of the data treatment/processing.

- To decide the means of the processing include how to conduct the activities, with what tools and technical and organizational solutions.

- The controller is on a **duty to implement security measures** (art. 32 GDPR), which ought to guarantee an adequate level of security. The choices of the controller are measured on their results and efficacy (**accountability**, see art. 24 and 82 GDPR).

- Accountability means also that controllers have to perform all other specific obligations posed in the Regulation, among which: alert and notification in case of data breach.

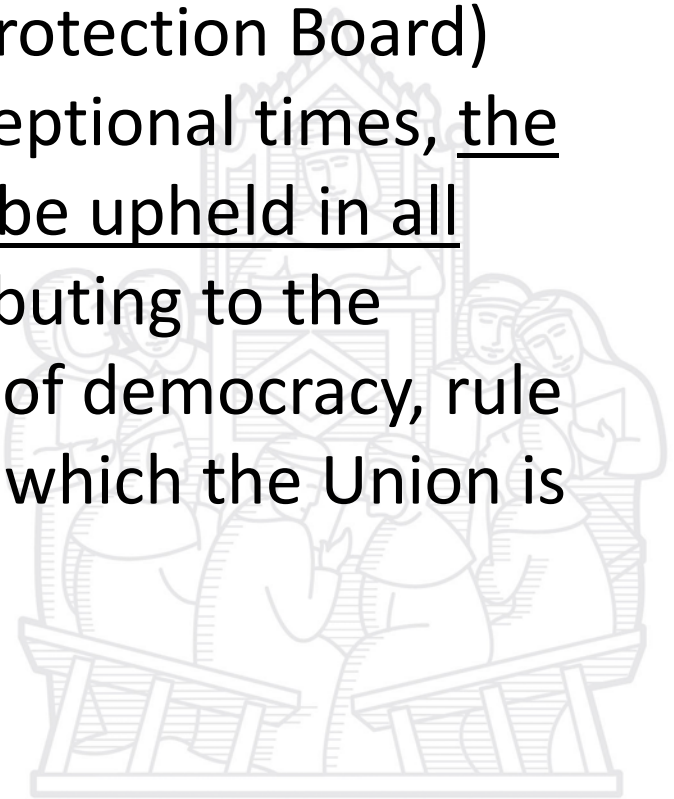
Sometimes a controller can appoint a "**processor**"

- sometimes intemediaries can be processors, when their data processing is *directed by* insurers and *in the insurer's interest*
- Sometimes intermediaries are *autonomous controllers* for the data processing that they operate for their own activity.

It is important to know which subject (whether insurer or intermediary) is the controller of a data processing, because the controller is accountable, and liable in case of violations of law provisions, and in case of damages resulting from the unlawful data processing in a sort of strict liability.

Due to the Pandemic crisis, is it possible to **escape liability**, because of *exceptional circumstances or legal provisions*?

- During its 30th plenary session at the beginning of June, The EDPB (European Data Protection Board) has stated that, even in these exceptional times, the protection of personal data must be upheld in all emergency measures, thus contributing to the respect of the overarching values of democracy, rule of law and fundamental rights on which the Union is founded.



Therefore, attention at least to:

- risk evaluation (greater exposure to cyber risks)
- attack reporting (alert, data breach, etc.)
- updating of softwares and security measures for websites, platforms and connections for employees
- warnings and education-like messages to customers, in order to inform and try to reduce risks.