



GDPR: One more challenge for the pharma companies



KYRIAKIDES GEORGOPOULOS
Law Firm



Put into public consultation, which ended on
March 5th 2018



Recent serious health data breaches



US (Aetna) :

Agreed to pay \$ approx. 17 m to settle federal class action (HIV status of 12.000 individuals revealed)



Norway:

South East Regional Health Authority breach. Result = 3 m patients data leaked



CNIL (France) :

French DPA sets ultimatum to National Health Insurance Fund (CNAM) on data security failures



Health Data

Law 2472/1997 (current law)

- “Sensitive Data” = including health data

Regulation 679/2016/EU

- “Special categories of personal data” = including among others health, genetic and biomedical data

What does health data mean?

Data
pertaining
to health
status

Information
collected while
registering for
health care
services and
for the
provision of
cross-border
healthcare

Numbers,
symbols or
particulars
assigned to a
natural person
so that the
latter can be
uniquely
identified

Genetic data
and
biological
samples

Any
information
on a
disease,
disability,
disease risk,
medical
history,
clinical
treatment or
physiological
or
biomedical
state
independent
of its source



Health data therefore may include:

- ❖ Medical Files
- ❖ Clinical Trial Data
- ❖ Pharmacovigilance Data
- ❖ M-health and E-health Data
- ❖ Employees' Health Data

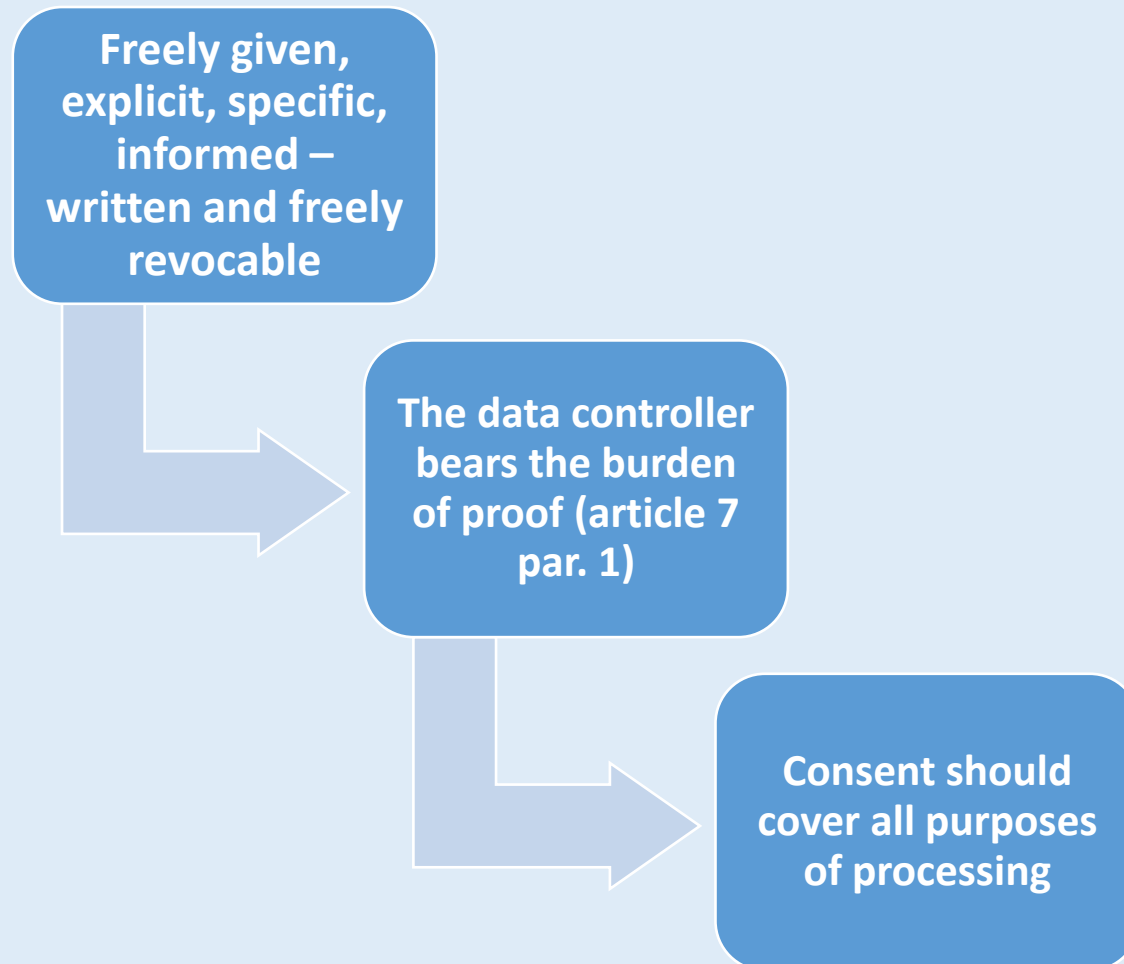


Principle= prohibition of processing
(article 9 of GDPR)

Exceptions:

- ❖ Provision of explicit written consent for one or more legitimate purposes.
- ❖ Exhaustively enumerated cases, such as:
 - processing is necessary for reasons of public interest in the area of public health,
 - for purposes of preventive or occupational medicine,
 - for scientific research or statistical purposes etc.

Consent





Clinical Trials (Recital 161)

For the purposes of consent to participation in scientific research activities in the context of clinical trials, the provisions of Regulation 536/2014/EU apply; i.e. in Greece currently **Ministerial Decision YA 59676/2016**, provides a specific form for the data subject's information and consent.

Scientific Research (Recital 33)

- The Regulation correctly states that it will not always be possible to fully specify the purpose of processing at the time of collection, i.e. from the beginning of processing.
 - Data subjects should give their consent only to certain areas of research, provided that the ethical standards for this research are followed.



Scientific Research :

Lack of definition in the Regulation
(Recital 159) “The purpose of scientific research shall be interpreted **in a broad manner**”.

However:

- ❖ Should the purpose be interpreted so broadly so as to include all researches relating to health?
- ❖ And including even those realized mainly for a commercial gain?

Further Processing :

The processing of personal data for purposes other than those for which the personal data were initially collected

Recital 50: «... *[further processing]* should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected...»



Processing for Direct Marketing Purposes

- Recital 47: «... *the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest...*»
- A balancing test between the data controller's and data subject's interest is crucial!

Caution! The provisions of Law 3471/2006 with regard to unsolicited communications shall remain in force up until the adoption of the ePrivacy Regulation

Action Plan - Procedures

- ❖ Detailed records of all processing activities (**Data mapping**) Art. 30 GDPR
- ❖ Gap analysis
- ❖ IT security measures
- ❖ Data Privacy Impact Assessment
- ❖ Executive Team & Personnel Training/Awareness
- ❖ Review of existing and/or Drafting of new Policies



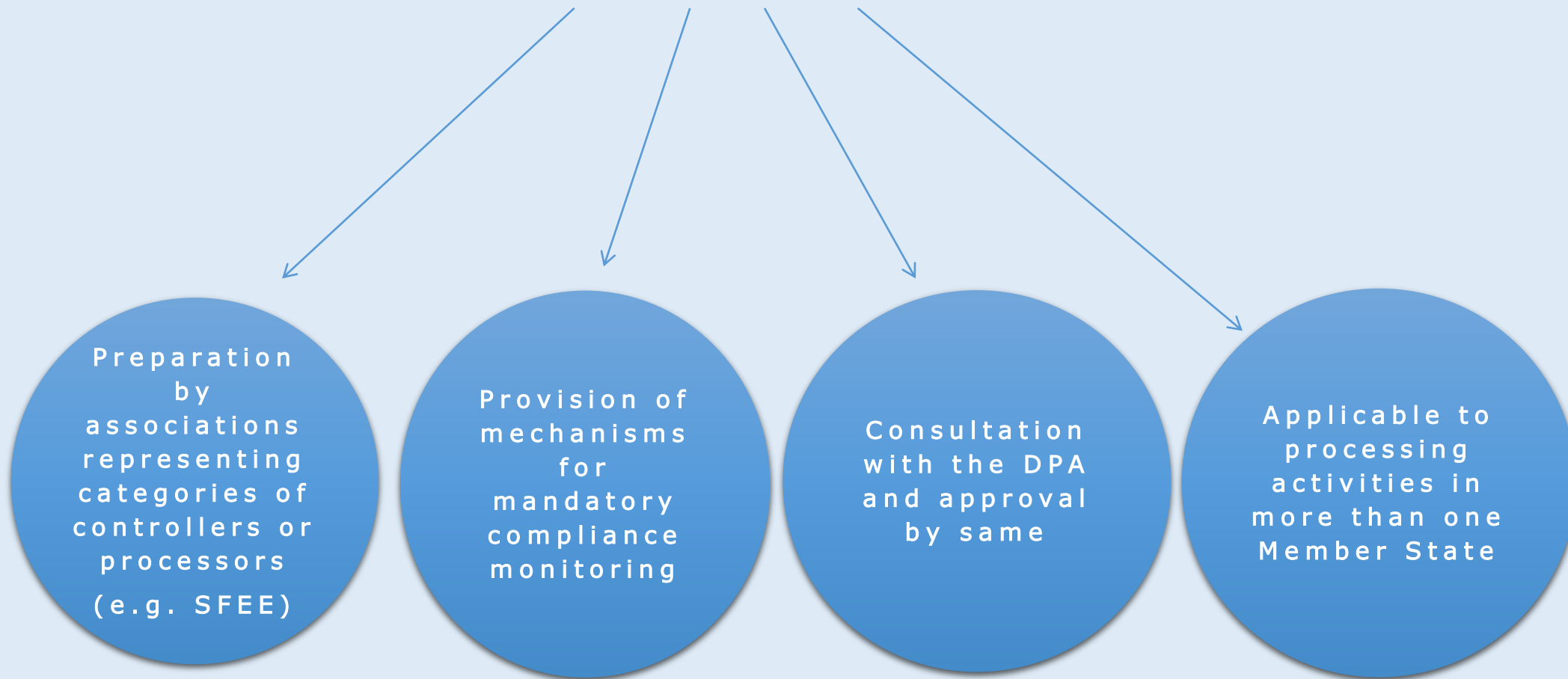


Appointment of a Data Protection Officer

- ❑ In principle, due to the nature of processing, pharmaceutical companies shall fall under this requirement
- ❑ Even if they are not obliged, or in case of doubt, assess the benefits of appointing a Data Protection Officer



Drafting of a Code of Conduct





Accountability: a new concept

Determining
internal
responsibilities

Implementation
of compliance
measures

**Evidence of
compliance at
all times**



❖ Compliance does not end in May 2018: compliance is for always.

❖ Personal data is valuable, but it does not belong to businesses, so they have to respect it!

Athens
Dimitriou Soutsou 28
115 21 Athens
T: +30 210 817 1500

Thessaloniki
Ethnikis Antistasseos 17
551 34 Thessaloniki
T: +30 2310 441 552



Effie Mitsopoulou
Partner

Email:
e.mitsopoulou@kglawfirm.gr



KYRIAKIDES GEORGOPOULOS
Law Firm

www.kglawfirm.gr