

@zwnne

Biometrics in Banking and Payments
Amsterdam 26 November 2016

BIOMETRICS AND (NEW) DATA PROTECTION LAW

prof. dr. Gerrit-Jan Zwenne



Universiteit Leiden
The Netherlands



security obligation

to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and [...] having regard to the state of the art and the costs of their implementation

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf



Opinion 3/2012 on developments in biometric technologies

Adopted on 27th April 2012

'side effects'

Systems analysing the face of a person as well as systems that analyse the DNA of a person can contribute very efficiently to the fight against crimes and efficiently reveal the identity of an unknown person suspected of a serious crime.

*These systems [...] produce **serious side effects**. In the case of facial recognition where biometric data can be easily captured without the knowledge of the data subject a widespread use would **terminate anonymity in public spaces** and allow consistent tracking of individuals. In the case of DNA data the use of the technology comes with the risk that sensitive data about the **health of a person** could be revealed.*

changes

as of 1st of January 2016

Dutch Data Protection Act

- data breach notification obligation
- data protection authority can impose substantial fines

up to €810,000 or 10 percent of annual turnover

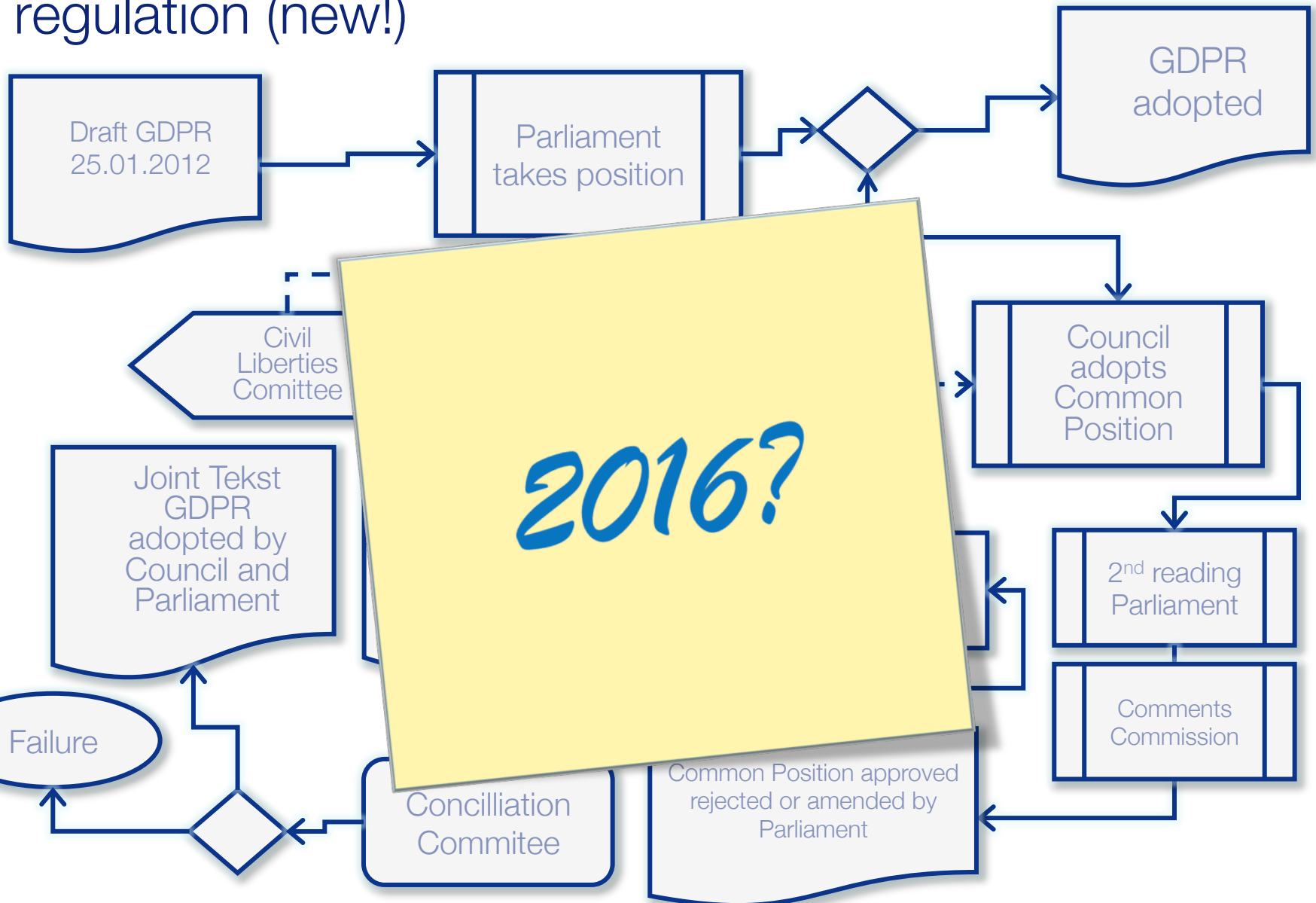
as of May 2018 (...?)

General DP Regulation (GDPR)

- more rights for data subjects
- more obligations for controllers and processors
- even more substantial fines
- and new rules for biometric data...!

up to €100,000,000 or 5 percent of annual worldwide group turnover

general data protection regulation (new!)



biometric data in the GDPR

EC 25 Jan 2012

any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data

EP 22 Oct. 2013

*any **personal** data relating to the physical, physiological or behavioural characteristics of an individual which allow his or her unique identification, such as facial images, or dactyloscopic data*

Council 15 June 2015

*any **personal** data **resulting from specific technical processing** relating to the physical, physiological or behavioural characteristics of an individual which allows **or confirms the** unique identification **of that individual**, such as facial images, or dactyloscopic data;*

biometric data is 'special data' ...

EP 22 Oct.
2013

*the processing of personal data, revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, and the processing of **genetic or biometric data** or data concerning health or sex life or, administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures **shall be prohibited***

the processing of genetic or biometric data shall be prohibited, unless...

prohibited, unless...

EP 22 Oct.
2013

- with data subject **opt-in consent**
- for the performance or execution of a **contract** to which the data subject is party
- for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of **employment law**
- to protect the **vital interests** of the data subject or of another person where the data subject is physically or legally incapable of giving consent
- in the course of **legitimate activities** by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim...
- data is **manifestly made public** by the data subject
- for the performance of a task carried out for reasons of **high public interest**, on the basis of Union law, or Member State law...
- for administrative **sanctions, judgments**, criminal offences, convictions or related security measures, if necessary for compliance with a legal or regulatory obligation

data protection impact assessment (dpia)

an assessment of the impact of the envisaged processing operations on the rights and freedoms of the data subjects, especially their right to protection of personal data.



@zwnne

g.j.zwenne@law.leidenuniv.nl

THANK YOU!