knowit

# CREATING DIGITAL OPPORTUNITIES

knowit

# Knowit Secure

## GDPR – EU General Data Protection Regulation

*Anna Borg*

knowit

1. Introduction  to the GDPR
2. GDPR focus areas
3. Challenges
4. Where do we start?

knowit

# Introduction to the GDPR

knowit

# GDPR - EU General Data Protection Regulation

**REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016**
**on the protection of natural persons with regard to the processing of personal data and on the free movement of such data**

Protection of

Digitalized

Personal Data

knowit

# GDPR: Why, when, where, what?

## WHY?

”GDPR is about harmonization of the protection of fundamental right and freedoms of natural persons  in respect of processing activities”

## WHEN?

May 25th 2018

## WHERE?

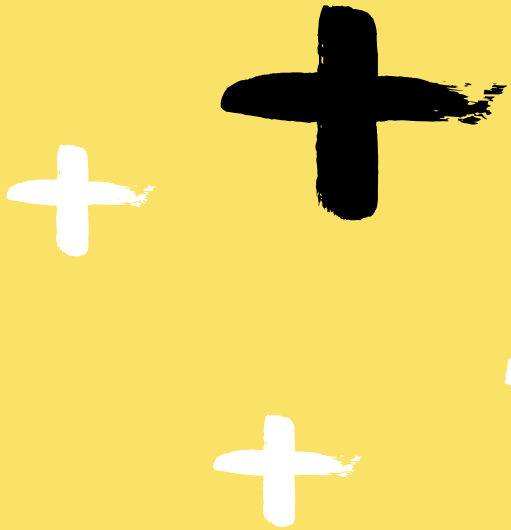
- All 28 EU member countries (national interpretations of parts of the regulation)
- EU businesses, organizations, authorities, non-profit organisations
- Businesses outside of the EU registering personal data about EU citizens

## WHAT?

Protection of personal data through organizational, administrative, and technical means, -and to provide evidence of that protection

knowit

# GDPR focus areas



knowit

# Focus on…

## …areas that you'll need to start addressing right now

I. General Provisions

**II. Principles**

**III. Rights of data subject**

**IV. Controller and Processor**

**V. Transfer of personal data to 3rd countries or international organisations**

VIII. Remedies, liability and penalties

IX. Provisions relating to specific processing situations

# II Principles

- When is it legal to process personal data?
  - Consent: by data subject, specific purpose, written, withdrawal at any time, parental consent children under 16
  - Necessity of processing: Contracts, legal obligations, legitimate reason, public interest, vital interest for registered
- Special Categories -is generally prohibited
  - Race, political opinions, health, union membership, genetic data, biometric data, sexual orientation or sex life

…unless strictly regulated consent or necessity

knowit

# III Rights of the data subject

- Information about what type of personal data is collected about a data subject (meta data) -how is the data collected, where is it processed/stored, how is it processed, who will have access to it… (data flow)
- Access to data subjects personal data and Portability
- Rectification
- Erasure -”the right to be forgotten”
- Restriction of processing
- Right to object
- Right to lodge a complaint

knowit

# IV Controller and Processor

Tasks and responsibilities of Controller, Processor and Data Protection Officer:

- Records of processing activites and Logging
- Personal data breach handling (Incident handling)
- Data protection impact assessment and Prior consultation
- Security of processing and Data protection by design and by Default
- …

knowit

# IV Controller and Processor:
# Records of Processing activities and Logging

- Record of all personal data processed or stored (data flows)
  - Purpose of processing
  - Description of processing
  - Data subjects and categories of personal data;
  - Recipients of personal data, (incl. transfers to and onwards transfer within 3rd country or international organization)
  - Time limit for storage
  - Security measures

  …Provide record to Supervisory Authorities on request

- Logging: ”collection, alteration, consultation, disclosure including transfers, combination and erasure of personal data”

knowit

# IV Controller and Processor:
# Incident handling of personal data breach

- Notify authorities within 72h of discovery
  - describe breach (what, when, data subjects, etc.)
  - Contacts
  - likely consequences
  - measures taken/proposed, including mitigating measures
- Document incident
- Communicate breach to data subjects (exceptions)

knowit

# IV Controller and Processor:
# Data Protection Impact Assessment and Prior Consultation

When performing processing that "…is likely to result in a high risk to the rights and freedoms of natural persons…"

- Data Protection Impact Assessment (DPIA)
  - processing operations
  - purposes
  - assessment of necessity in relation to the purposes;
  - assessment of the risks
  - measures to address the risks (safeguards, security measures and mechanisms to ensure protection and to demonstrate compliance)
- Prior Consultation: Supervisory Authority to be consulted if high risk

knowit

# IV Controller and Processor: Security of processing

Appropriate technical and organisational measures shall be implemented, for example:

- confidentiality, integrity, availability and resilience
- ability to restore availability and access within timely manner
- Testing and assessment
- pseudonymization and encryption

# IV Controller and Processor:
# Data protection by design and by default or ”Privacy by Design”

knowit

## Built-in protection of data:

- Minimization
- Transparency
- Informed consent
- Proactive verifiable protection
- Withdrawal of consent

*-extract from ”Hur står det till med den personliga integriteten? –En kartläggning av Integritetskommittén”, SOU 2016:41, Stockholm 2016*

knowit

# V Transfer of personal data to third countries or international organisations

## Prior assessment and ensurance of:

- appropriate safeguards to ensure adequate protection:
  - Cooperation mechanisms - legally binding enforceable instrument with public authorities, Binding Corporate Rules, Supervisory Authority, controllers and processors have approved code of conduct or certification to protect rights of the data subject, etc
  - Technical safeguards to ensure confidentiality – encryption, access management, etc.
- enforceable data subject rights and legal remedies are available

## Or with authorization by supervisory authority

knowit

# V Transfer of personal data to third countries or international organisations

"Adequacy decision" made by EU Commission for 3rd countries, territories, regions

- applicable to all member states, no prior assessment or specific authorization needed
- e. g. US – "Privacy Shield"

Specific situations: explicit consent, legal claims, to protect vital interest of data subject, etc.

knowit

# Challenges

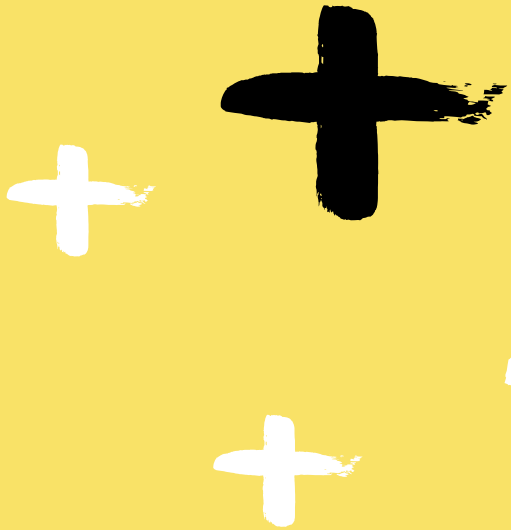
knowit

# What are the main challenges with the GDPR?

- Where’s is the personal data?
  - Scanning of systems, logging, the record of processing (data flow)
- Provide for the rights of the data subject & Privacy by Design
  - Processes  and automation of consent handling, of retrieving, rectifying and erasing personal data for a data subject, system and information classification, etc
- Reporting and handling of personal data incidents
  - Logging and event monitoring, incident management process, record of processing
- Transfer and processing in 3rd countries or International Organisations

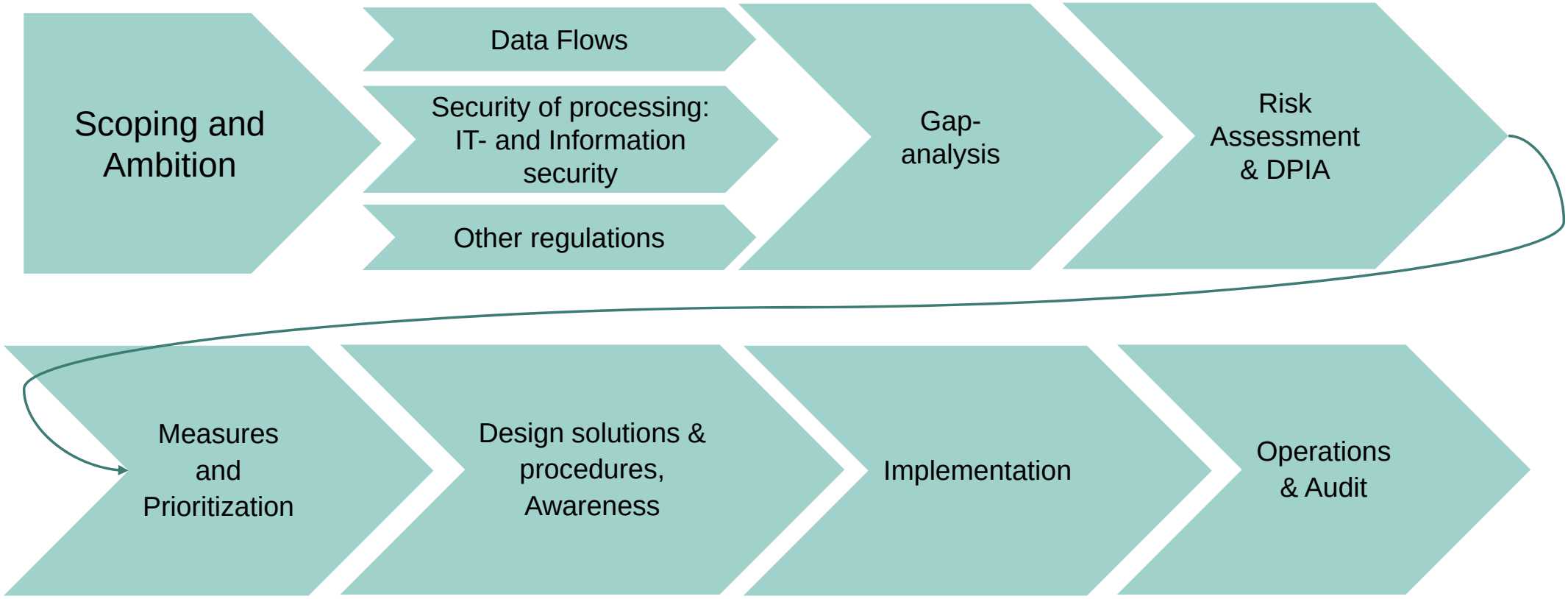
knowit

# Where do we start?



knowit

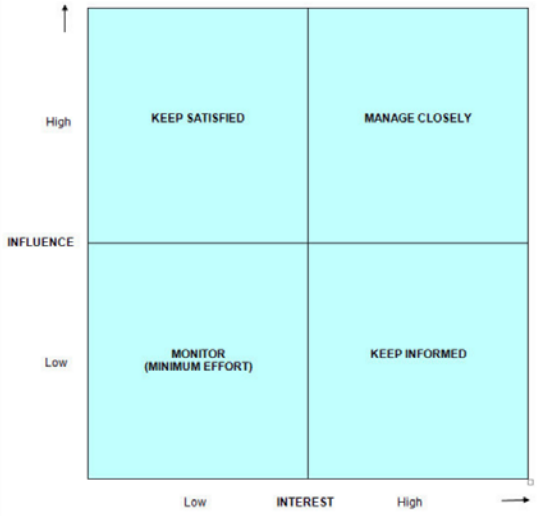
# ”Road to compliance”



knowit

# Phase: Scoping

- What sections of the GDPR are applicable to my organization?
    - Do we process or transfer data to 3rd countries or international organizations?
    - Do we handle personal data that are of ”special categories”?
    - Do we process large quantities of data that are subject to automatization or profiling?
    - Do we need a Data Protection Officer?
- Stakeholder analysis
- If large organisation: do we do it all at once?




## Output: Scope

knowit

# Phase: Ambition Level

- Clarify compliance and project ambition
- Data Protection Policy -outlined

## Output: Goals

knowit

# Phase: Analyze – 1. Identify Data Flows

- What type of personal data flows does the organisation handle?
  - Recruitment data
  - Employee data
  - Customer data
  - Incident data
  - Patient data
  - User data
  - ….
- Describe the data flows: input, transferring, processing, storage, erasure, relevant systems/applications, current safety measures…

## Output: Data Basics

knowit

# Phase: Analyze – 2. Security of Processing

- What does the IT-environment look like?
  - General infrastructure
  - Systems and applications processing and/or storing Personal Data

- Which supporting processes and procedures are in place?

…Current level of IT- and Information Security

## Output: data basics

knowit

# Phase: Analyze – 3. Other regulations

Are there other regulations applicable to the organisation which have precedency towards the GDPR?

- Tax Laws
- Public Procurement Act
- Patient Data Act
- …

## Output: Data Basics

knowit

# Phase: Analyze – 4. Gap analysis

- General requirements
- Requirements related to each data flow
- …and subsequently also to
  - Processors (Personuppgiftsbiträden – PUB))
  - Receivers of transferred information
  - Application and system processing/storing personal data
- Requirements on the protection of the IT-environment in general (”…appropriate technical and organzational measures…”)
- Requirements related to each 3rd country or international organization (where personal data is transferred or processed)

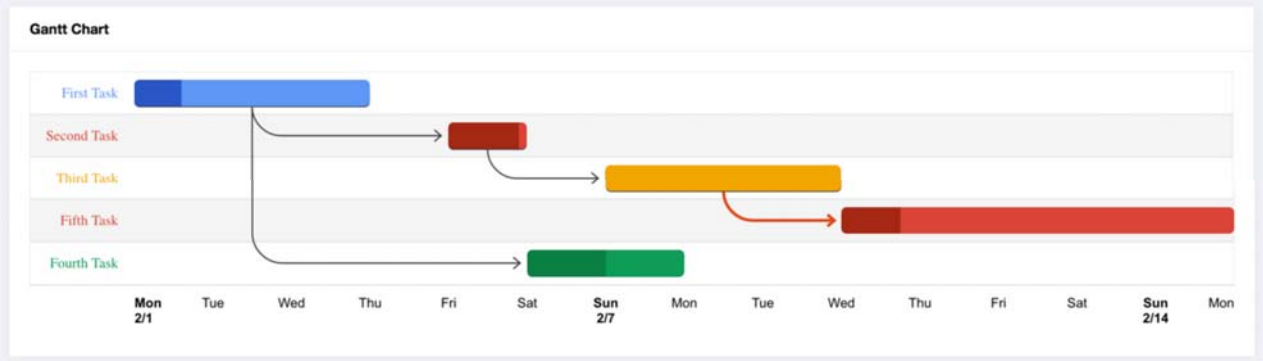
## Output: Data Basics

knowit

# Phase: Assess

- Risk Assessment, including Data Protection Risk Assessment (DPIA) on data flows
- Measures
- Dependencies
- Synergies

## Output: Action plan



knowit

# Phase: Solutions

- Design technical solutions
- Design processes and procedures,
- Complete Data Protection Policy
- Create Legal documents (Binding Corporate Rules, consent, Processor contract, requirements on receivers of PD)
- Create information, documentation and reporting templates to: the registered, processors (internal and external), receivers of PD, supervising authority, Subcontrollers etc.
- **Awareness**

## Output: SOP, Design

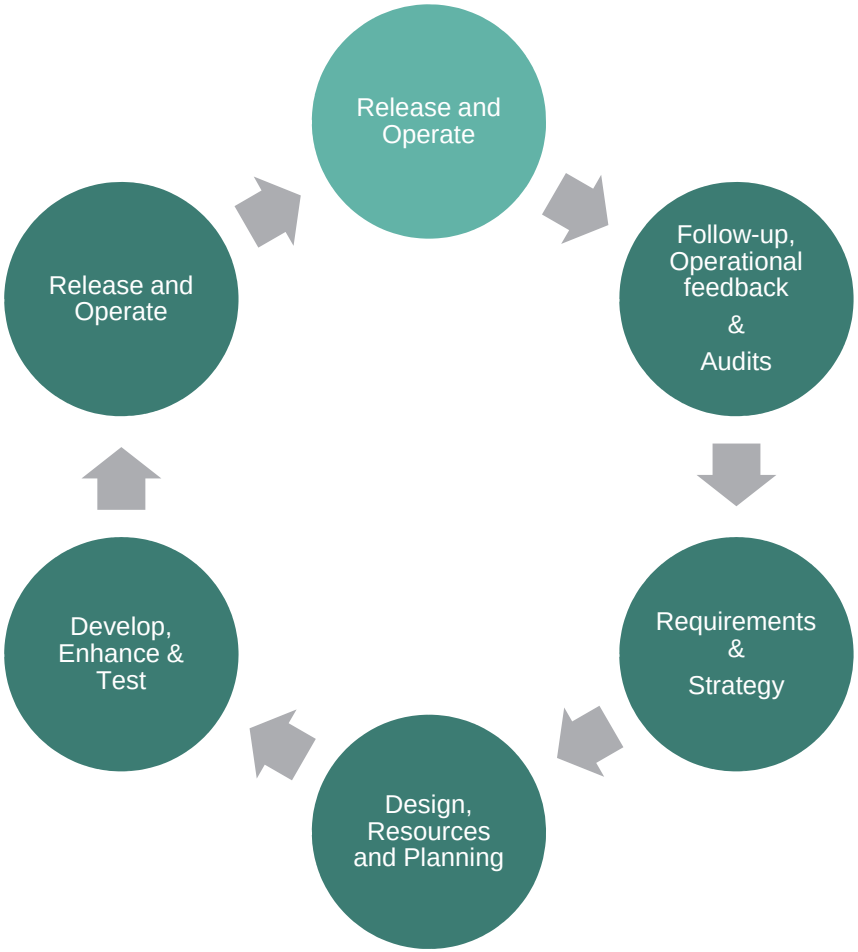
# Phase: Implement

- Implement Procedures & technical measures
- Data Protection Policy
- Training and Awareness

Output: Skills, awareness

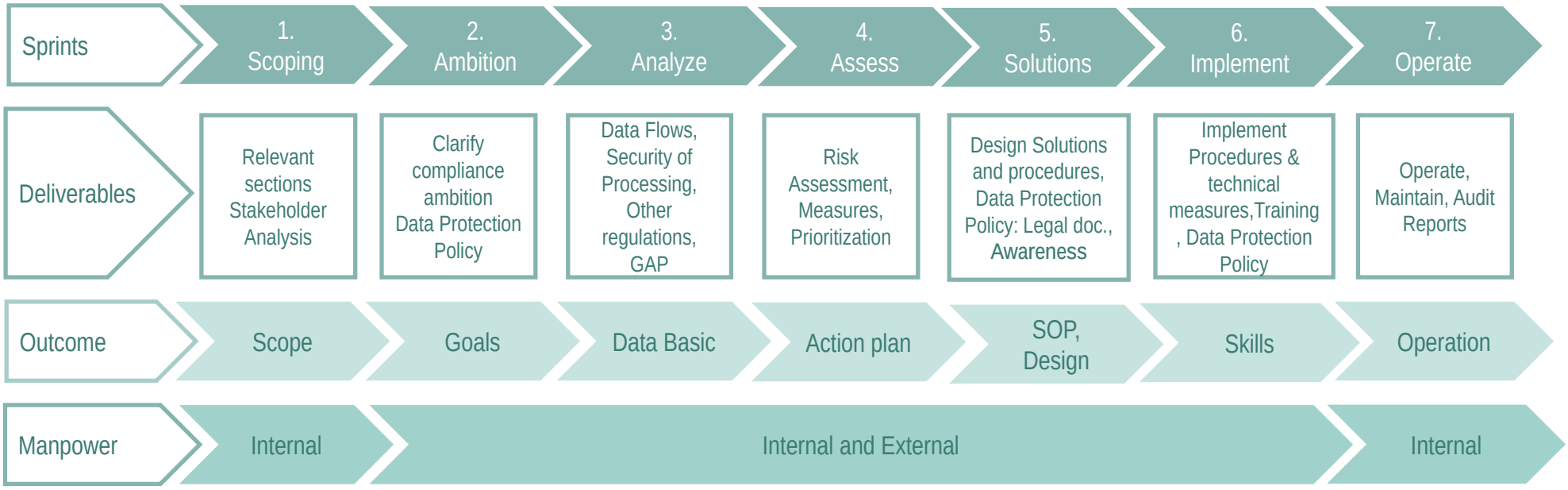
knowit

# Phase: Operate



knowit

# Summarizing Project Flow



knowit

# Thank You!

knowit

**Knowit Secure AB**

anna.borg@knowit.se

“Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.”

*-extract from item (6), Regulation (EU) 2016/679 of the European Parliament*