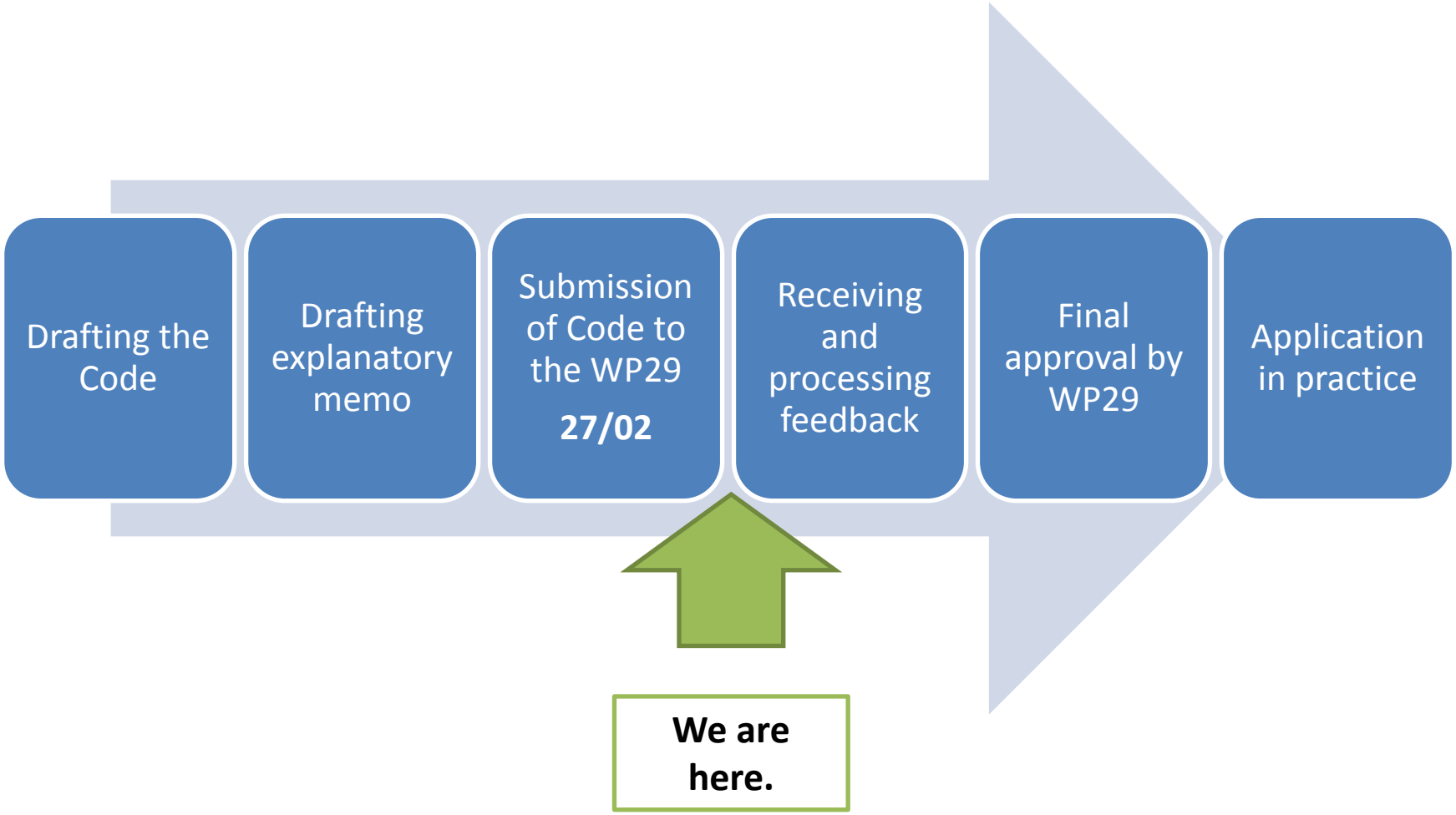
Code of Conduct for Cloud Service Providers

Overview of content and state of play

Presentation to the C-SIG Plenary

19 May 2014

Basic process



Content of the Code

Introduction – Structure – Purpose – Scope – Adherence

Data protection - substantive rights and obligations

Security requirements – defining security objectives ('what', not 'how')

Governance - management, application and revision, including bodies

Transparency annex

Security annex

Declaration of adherence

Checklist

Data protection

- Contractual specification – T&Cs
- Processing Personal data lawfully
- Transfer within the CSP's Group
- Transfer to a third party
- Right to audit
- Liability
- Cooperation with the customer
- Data Subject complaint handling
- Data Protection Authority request handling
- Confidentiality obligations
- Law enforcement requests
- Data breaches
- Termination of the Services Agreement

Governance bodies

General assembly

All CSPs in the register + admitted representatives

Votes on Code changes

Steering board

CSPs, customers, rep. bodies, DPAs, A29 WP, academia, expert, Commission as observer

Policy governance and dispute resolution

Secretariat

Administrative staff

Maintain register, prepare meetings, promote Code

Competent bodies

Independent organisations with correct expertise

Review and approve declarations and audits; decide on complaints

Expected questions

- What about SaaS – PaaS – IaaS? Not addressed in the Code
- Security: is it sufficient to have objectives?
- International data transfers: can we be more binding?
- Globally: provide a clear statement of non-negotiable rights and assurances
- More control mechanisms for the end users combined with stronger transparency on e.g. data location and governmental access requests

Generally: expected to be manageable