

**EURIM and
The Politics of Information
Governance
or
1984 Revisited**

Philip Virgo
Secretary General, EURIM
and 30 years as piggy-in-the-middle
between politicians and the world of information systems
www.eurim.org.uk

The politics of Information Governance

The Political Triangle

Access, Protection and Retention

What is EURIM

Current and Planned Legislation

National, EU, International

The Corporate Balancing Act

Practical Risk Assessment

Protection as a Service

Fight Your Corner for

RELEVANT REGULATION

EURIM

The All-Party Parliamentary – Industry Group concerned with the politics of the Information Society

71 MPs, 16 MEPs, 26 Peers: inc. 9 Ministers (2 Cabinet),
+ PPS's, whips, committee chairs, opposition spokesmen etc
31 Corporate and 18 Associate Members (incl. ISSA)
Observers from BER, Cabinet Office, DCSF, DIUS, EU
Commission, FSA, Home Office, ITC, LCD, MoJ, OCI,
ODPM, Oftel, Ofcom etc. etc.

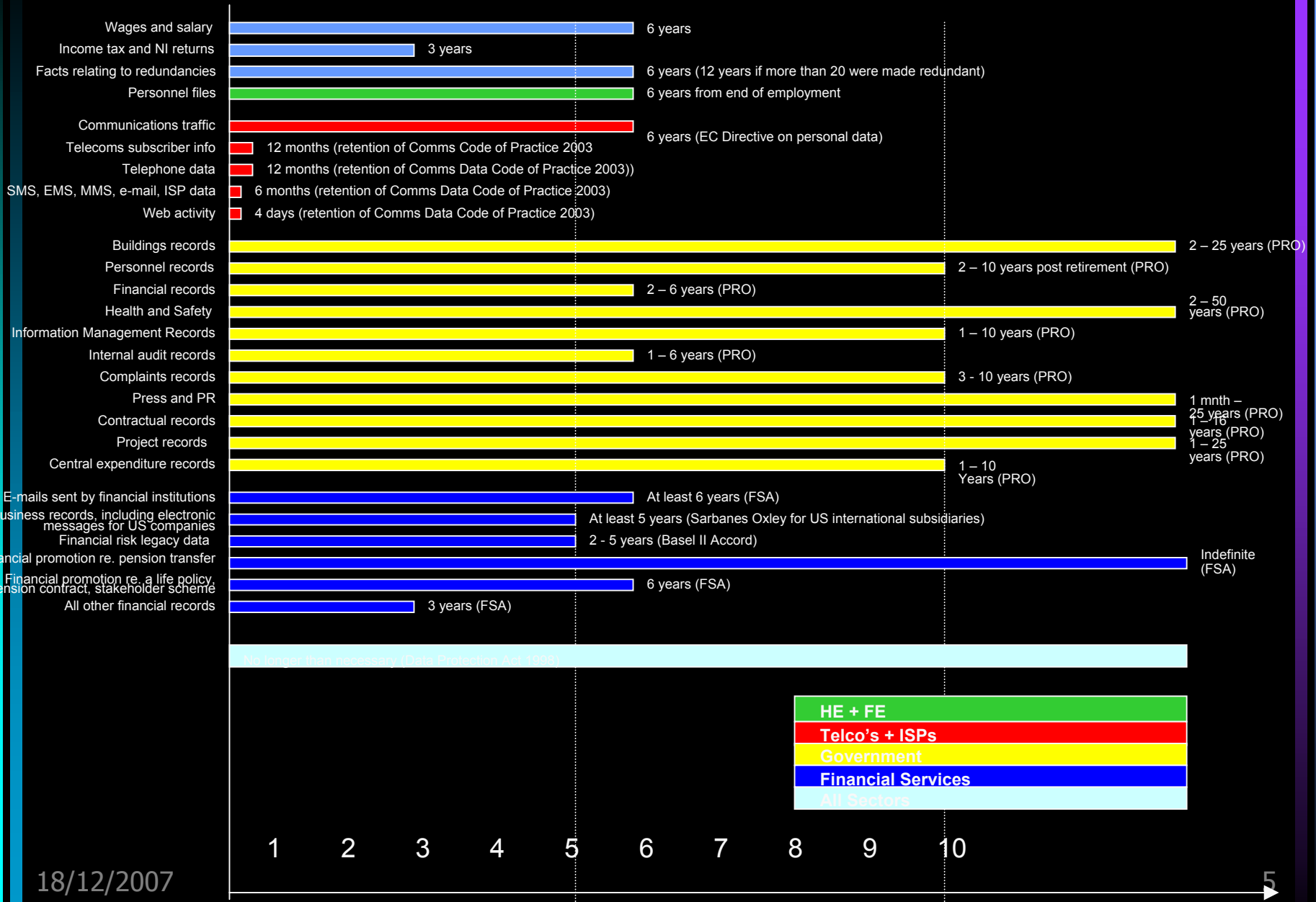
Funded by Corporate and Associate Members
(but can accept funding from HMG/EU to run consultations)

The Current EURIM Priorities

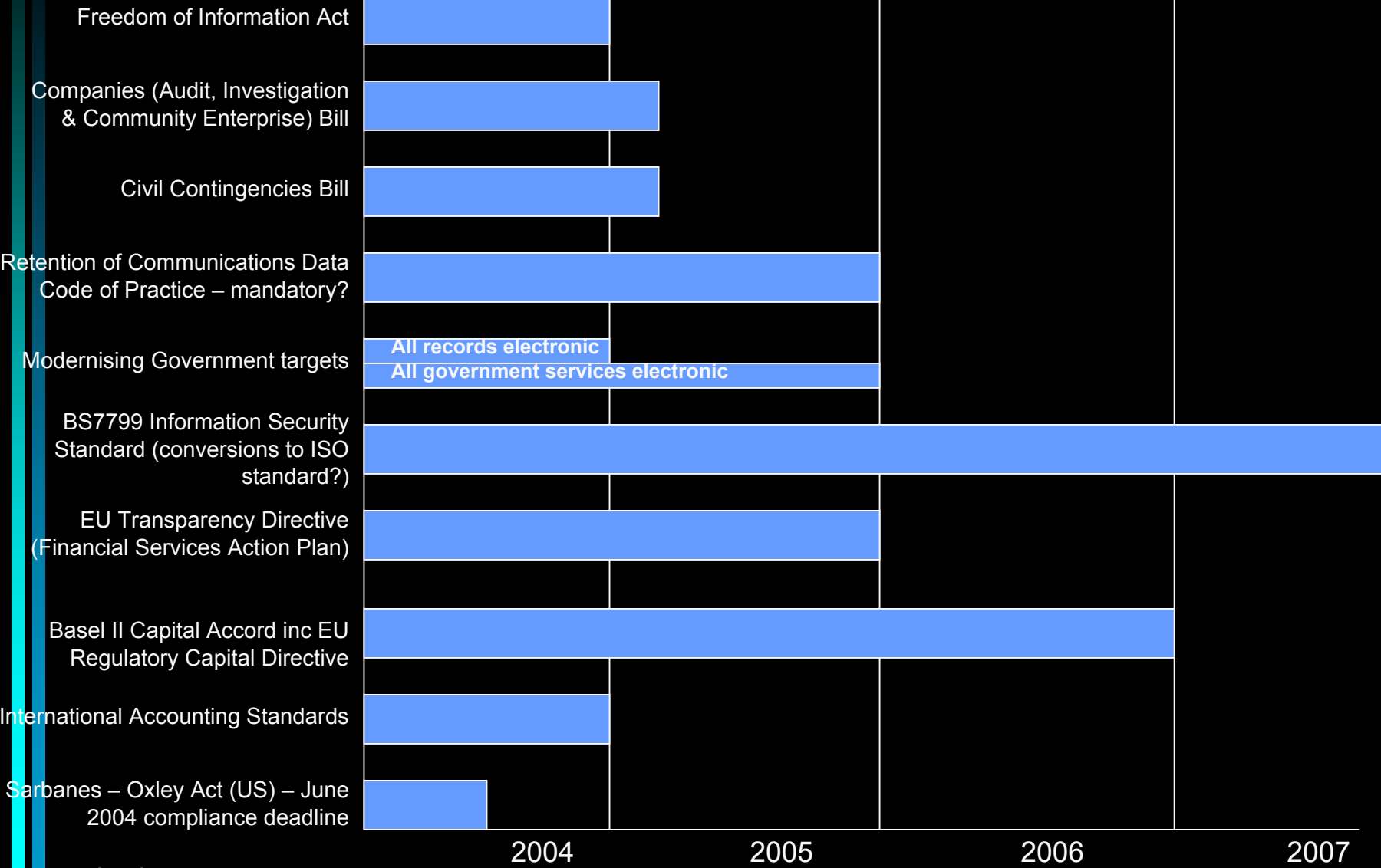
- **Confidence in the On-line World**
- **Transforming Public Service Delivery**
- **Secure Information and ID Sharing**

**Information Governance cuts across ALL
Current structures are part of the problem**

SUMMARY OF UK DATA RETENTION REQUIREMENTS



IMPENDING DATA LAWS & REGULATIONS



The Corporate Balancing Act

Objective: organisational survival

- neither shut down for non-compliance
- nor put out of business by overheads

Demands versus Needs

- Form 42
- Money Laundering reports
- Data Retention

Kafka (The Trial, The Castle)

v Hasek (The Good Soldier Schweik)

Practical Risk Assessment

The biggest risks are:

- Insiders: Top management, IT staff, marketing, cleaners, untrained users
- Digititis: cock-up compromising or crashing “over-integrated” databases or networks
- Mother Nature: storm, flood, flu etc.
- Accident: fire, explosion
- Then comes outside attack

Information Security as a Customer Service

- A Consent driven cycle of trust and validation (akin to financial services)
- Publicly accountable 3rd party governance for statutory powers
- Cost, risk and liability assessment for trust and governance models
- Clear (and published) rules, responsibilities and liabilities for operational staff
- Rolling validation programmes
- Intelligible and enforceable policies with training for ALL in their meaning and use

Data Sharing

Reactive

Proactive

“Reacting to a request to access data I hold as the data controller”

Flow A



Is there a statutory obligation for me to provide this information to the requestor? e.g. SSFA

Yes

No

Did I notify the individual at the time their data was collected that it would be used in this way? And if so did they freely give their consent?

Yes

No

Has the requestor obtained specific consent from the individual to allow the requestor to initiate the request to me and obtain the information from me?

Yes

No

Is the data requested sensitive e.g. from racial, ethnic, physical or mental health perspectives?

Yes

No

Is the processing necessary as part of my processes and the processes of the requestor?

Yes

No

Is the 'legitimate interest' test satisfied?

Yes

No

Flow D

Flow B

Flow C

Information Security as a Customer Service

- A Consent driven cycle of trust and validation (akin to financial services)
- Publicly accountable 3rd party governance for statutory powers
- Cost, risk and liability assessment for trust and governance models
- Clear (and published) rules, responsibilities and liabilities for operational staff
- Rolling validation programmes
- Intelligible and enforceable policies with training for ALL in their meaning and use

Fight Your Corner for Better (not more) Governance

**Contribute through ISSA and its planned awareness
programmes for directors and SIGN the Number 10
Petition - <http://petitions.pm.gov.uk/ecrime/>**

**For details of the EURIM work
visit www.eurim.org.uk
or e-mail virgo.philip@eurim.org**