Data Protection Risk Management

Martin Aust

Head of Intelligence

Hertfordshire

DPA – Key requirements

- Personal data processed fairly and lawfully
- Should be adequate, relevant & not excessive
- Shall be accurate and kept up to date
- Not kept longer than necessary
- Appropriate technical and organisational measures in place

Hertfordshire

Our organisational approach….

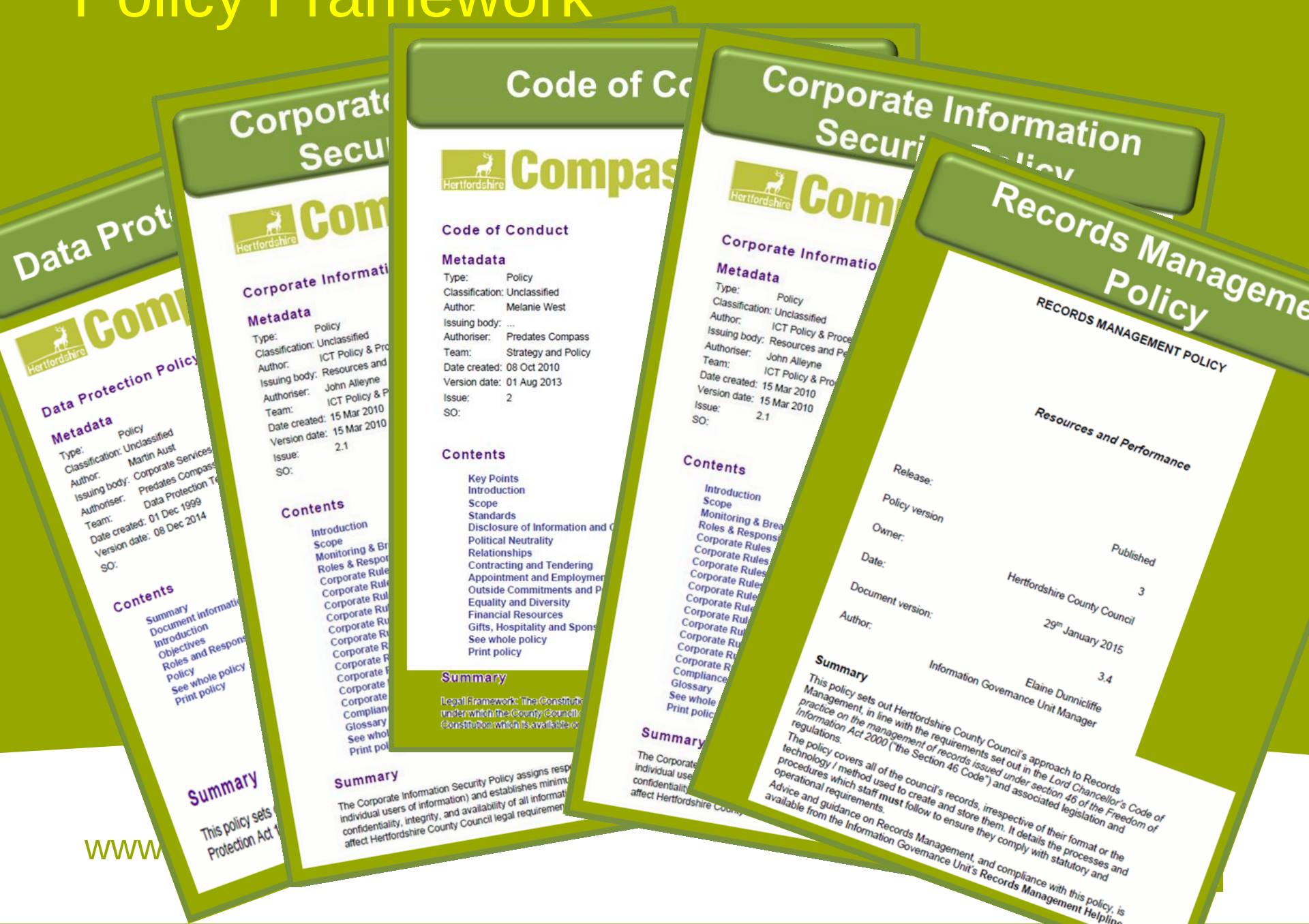
- Prevention better than cure
- Focus on preventing harm foremost
- DP as enabler, not a barrier
- Equip staff with knowledge and tools
- Built on management & personal responsibility
- Transparency and openess
- Continuous improvement – learn lessons

Organisational framework - features

- Included on the Corporate Risk Register
- Audit oversight – Committee & Internal Audit
- Visibility – weekly DP report to management
- Central DP team integrated with FOI/SAR/RM
- Advice and guidance on DP compliance
- Privacy by design methodology employed
- Robust and extensive policy framework…

Hertfordshire

Policy Framework



www

So what do we do? – Technical (1)

- Industry approved security measures (firewalls, email filtering software, desktop AV)
- Network security standards, including penetration testing
- ICT service provider compliance with security standards
- Encryption – laptops & other portable media

Hertfordshire

So what do we do? – Technical (2)

- HertsFX allows secure transfer of documents between HCC and any invited partner
- GCSX/N3 - secure email exchange with other key partners – Police, NHS
- Smart Worker – electronic access/working
- Technical procedures for avoiding unintended disclosure of personal data
- 2016 Printer roll-out – reduce paper left visible and unintended data added to mailing

So what do we do? – Training

- Training – vital link between policy & practice
- DP iLearn module mandatory for new staff
- Not “spray and pray”
- Targeted training for staff handling sensitive personal data – e.g. Social care, HR, Legal
- Supplemented by role based training
- Awareness raising – reinforce best practice

Hertfordshire

So what do we do? – Procedural (1)

- Apply learning – “sum of marginal gains”
- Peer checking for sensitive paper/post or email address
- Make sure undelivered post returns to HCC – return address; mark envelope “personal & confidential”
- Separation of secure high value IT kit targeted by thieves and paper-based information

Hertfordshire

So what do we do? – Procedural (2)

- Data sharing agreements/toolkit in place
- For use in partnership settings – care focus but applied in other settings
- Integrated with Privacy Impact Assessment which identifies risks
- Caldicott Guardian in place and trained for social care data sharing
- Governance through data sharing workstream in ICT Strategy

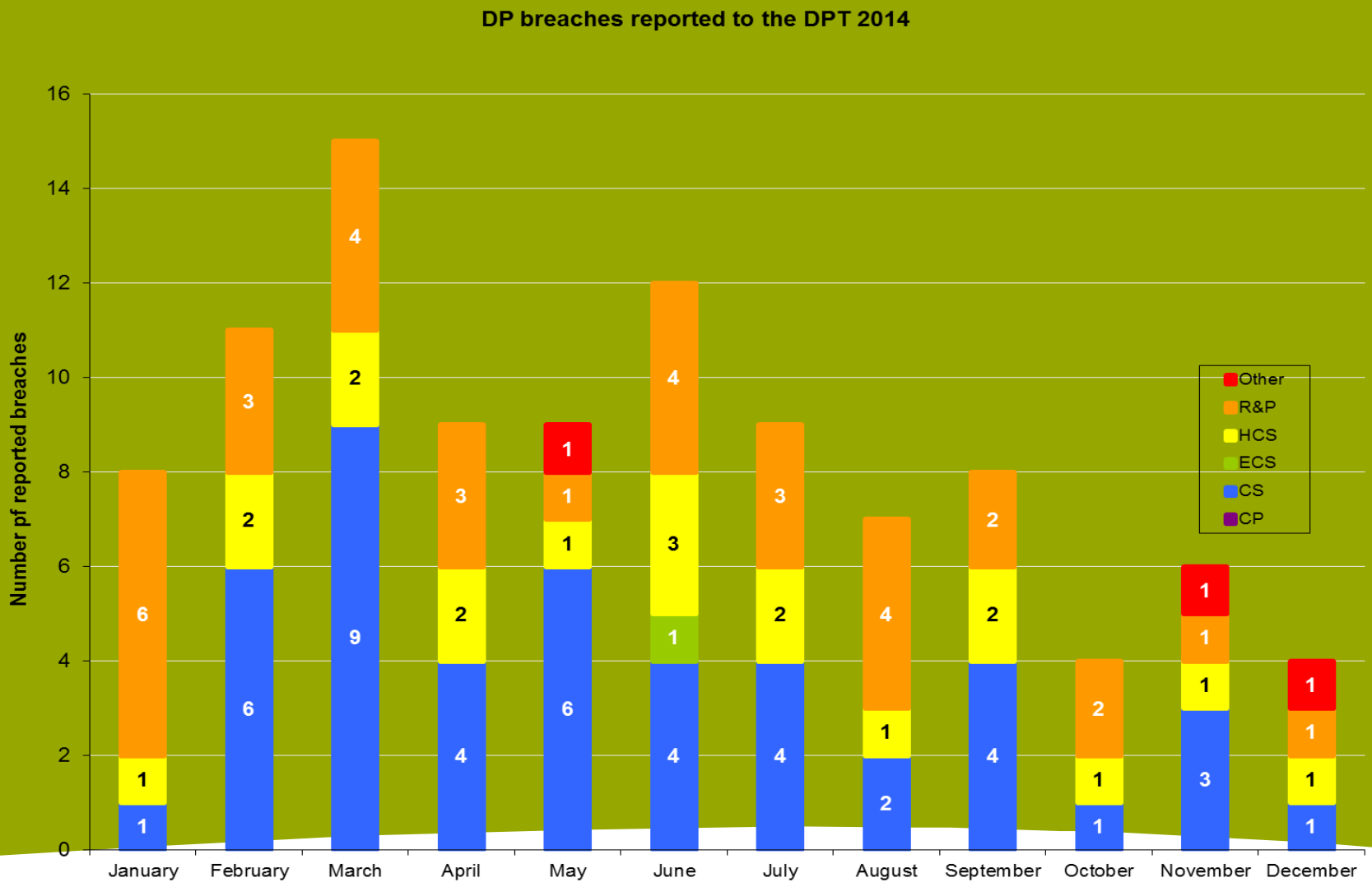
Hertfordshire

So what ……what is our record?

- Potential breaches per year – 40,000,000+
- Subject to ICO fine - £500,000
- No potential breaches met threshold for reporting to ICO since 2010
- No potential breaches met threshold for reporting to NHS
- IG Level 2 toolkit NHS accreditation achieved
- Significant decline in number of breaches…..

Hertfordshire

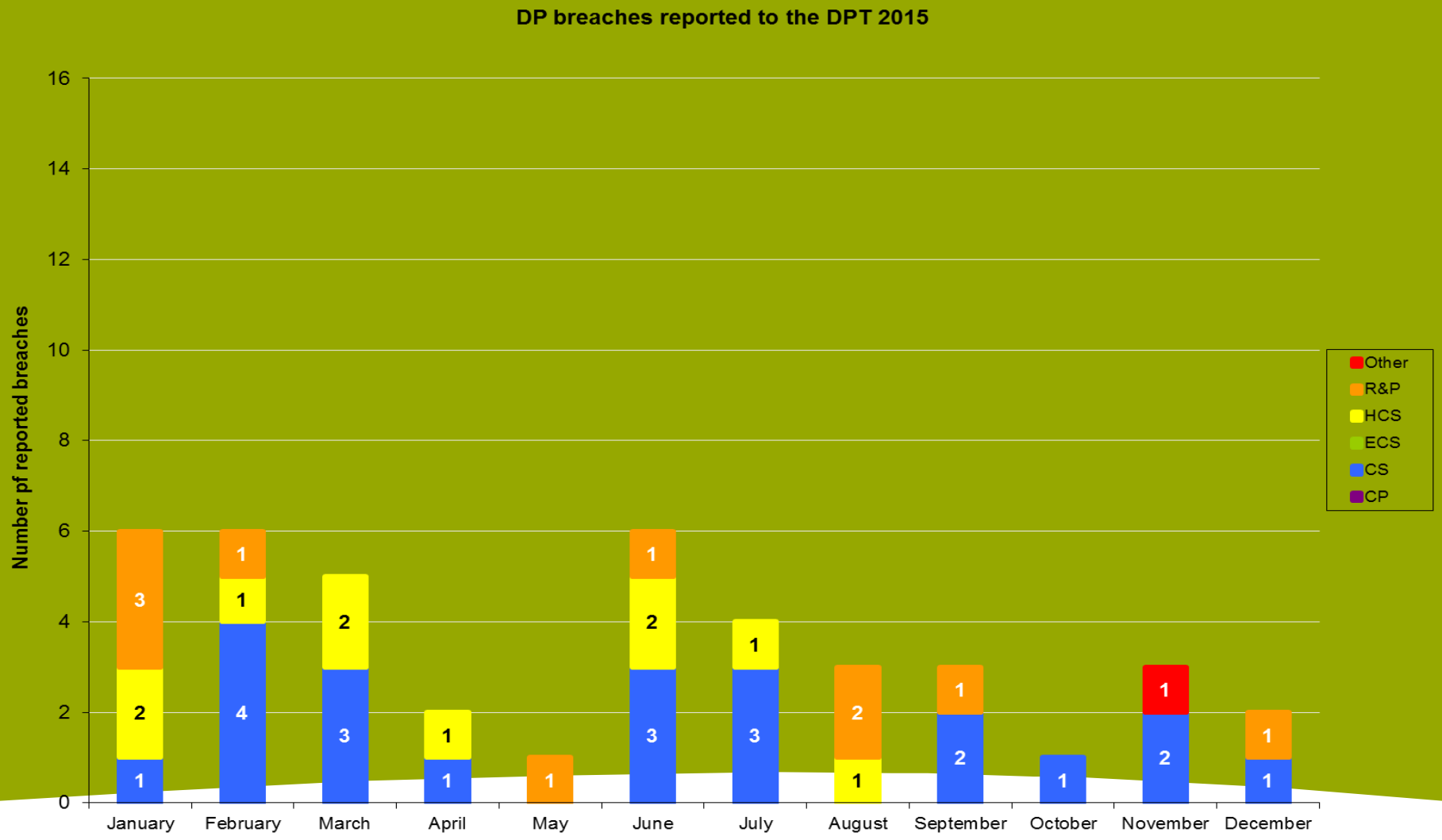
Data Protection Breaches 2014



www.hertsdirect.org

Hertfordshire

Data Protection Breaches 2015



www.hertsdirect.org

Hertfordshire

Looking forward - EU General Data Protection Regulation 2018 (GDPR)

- European Directive which formed the basis of 1998 DPA not now fit for purpose…..
  - New forms of personal data
  - Internet and technical facilities for sharing/publishing personal data
  - Commercial exploitation of personal data Facebook; Fitbit; donor data passed between voluntary organisations.
- All member states will adopt this and measures will need to be in place for implementation in 2018

EU GDPR 2018 - implications

- Maximum of €10m for some breaches - Data loss feature here
- Maximum of €20m for other breaches, e.g. unlawful processing, right to be forgotten
- Mandatory breach reporting to regulator within 72 hours *unless the breach is unlikely to result in a risk for the rights and freedoms of individuals*
- Responsibility to inform Data Subject where high risk to the rights and freedoms of individual
- Aligns with current approach – but impact greater

thank you

www.hertsdirect.org

Hertfordshire