IDEAS | PEOPLE | TRUST

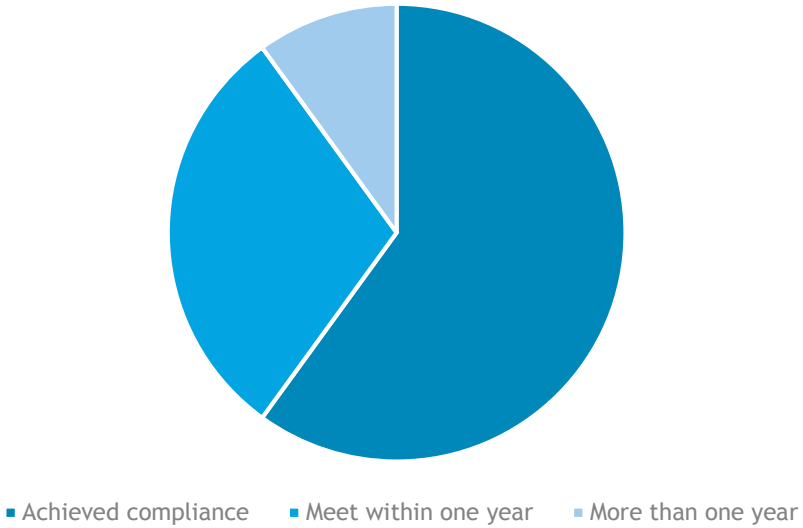
BDO

GDPR ONE YEAR ON

Progress

- A survey by CISCO Systems found that **60% of organisations** are meeting the requirements of GDPR
- **37% of GDPR-ready organisations** experienced a breach costing more than $500k compared to **64% of non-GDPR** ready organisations
- As consultants we still receive requests for assistance around implementation
- Audit work reveals many organisations not where they think they are

Fig 1. GDPR Readiness



GDPR ONE YEAR ON

Regulatory cases

- 240,000 cases across the EU (data protection complaints, data breaches, investigations)
- The UK Information Commissioner's Office (ICO) received a total of 14,072 data breach notifications in the year following the introduction of GDPR.
- The number of complaints from the public has also increased, from around 21,000 to 41,054 this year.
- Figures covering all countries where GDPR is applied show a total of 89,271 notifications of data breaches, with 144,376 as a result of complaints.

GDPR ONE YEAR ON

Fines - What the UK regulator said

Imposing a 4% fine will not be de facto penalty

"it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm"

"the GDPR gives us a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. While these will not hit organisations in the pocket – *their reputations will suffer a significant blow*".

GDPR ONE YEAR ON

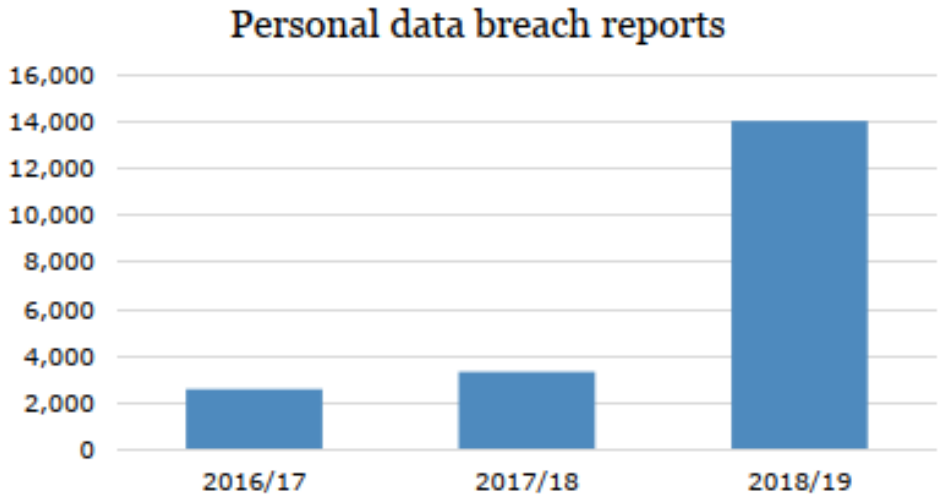
Fines

- 91 fines levied across Europe (Feb 2019) – extrapolated to circa 120
- Largest fine in Europe under GDPR was for Google (€50 million) for lack of transparency around advertising personalisation
- The ICO notes that the first fines under the General Data Protection Regulation "are due to be issued soon, once the necessary legal processes have been completed".

GDPR ONE YEAR ON

UK Personal Data Breaches – Reported by Organisations

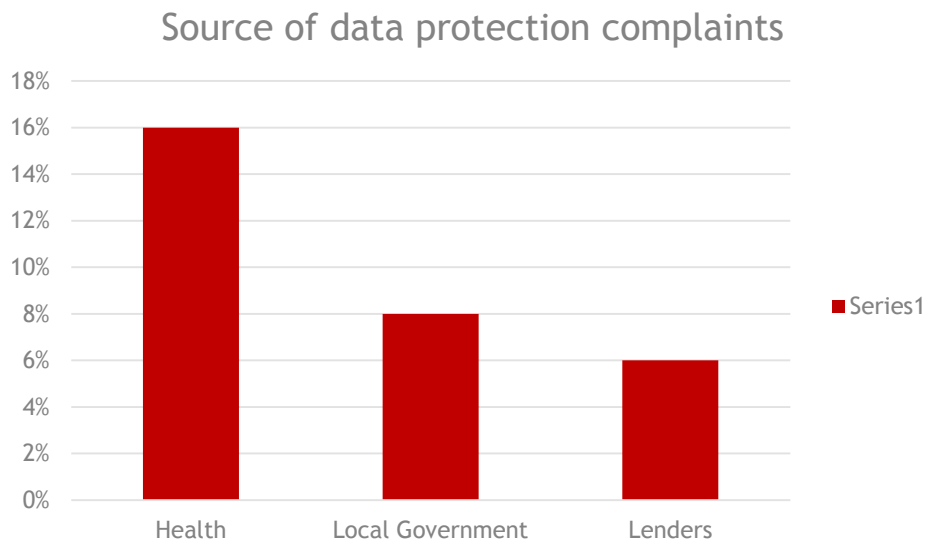
- Approximately 14,000 data breach reports in first year of GDPR
- Only 17.5% required action from the organisation – seen as indicator that companies are taking GDPR seriously
- <0.5% involved an improvement plan or monetary penalty



GDPR ONE YEAR ON

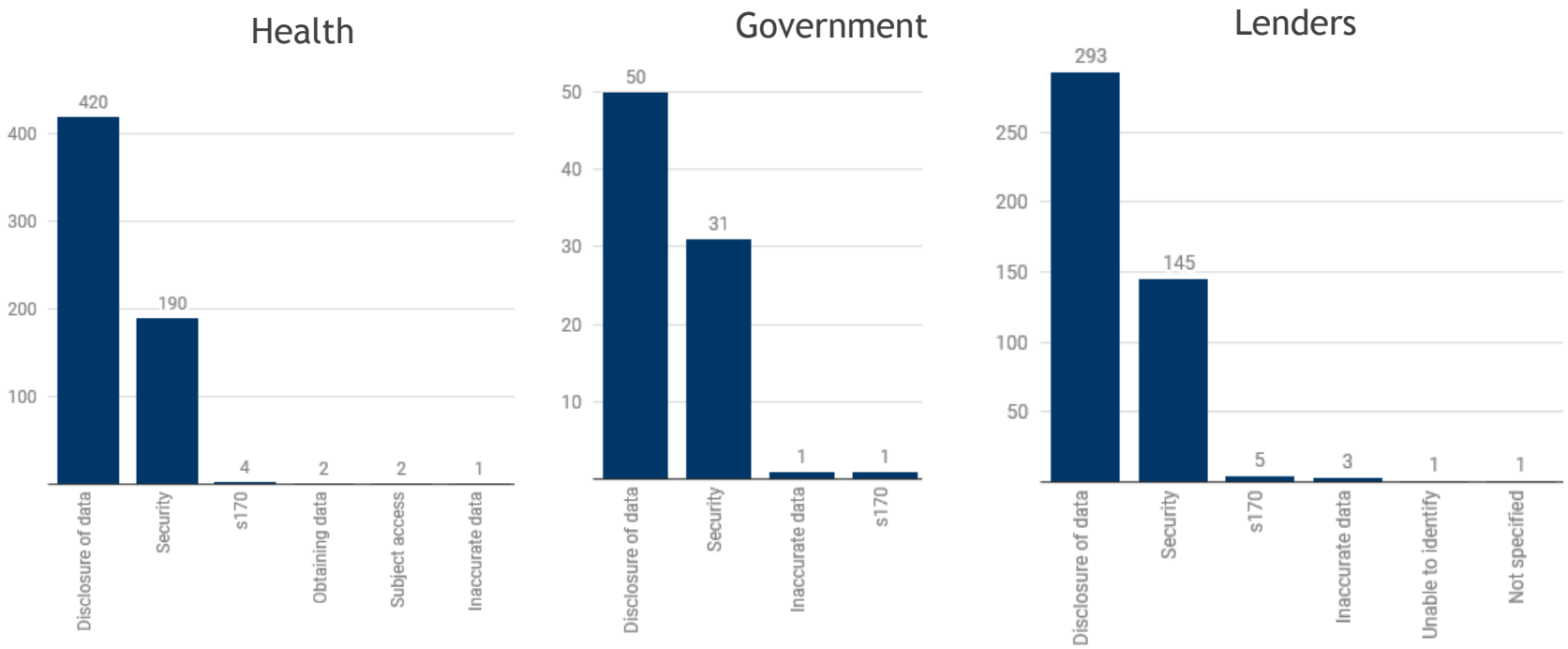
UK Personal Data Breaches – Reported by the Public

- Over 41,000 data protection concerns from the public
- Subject access requests most frequent complaint category (38%)
- Health industry source of most complaints



GDPR ONE YEAR ON

Personal Data Security Breaches - Sources

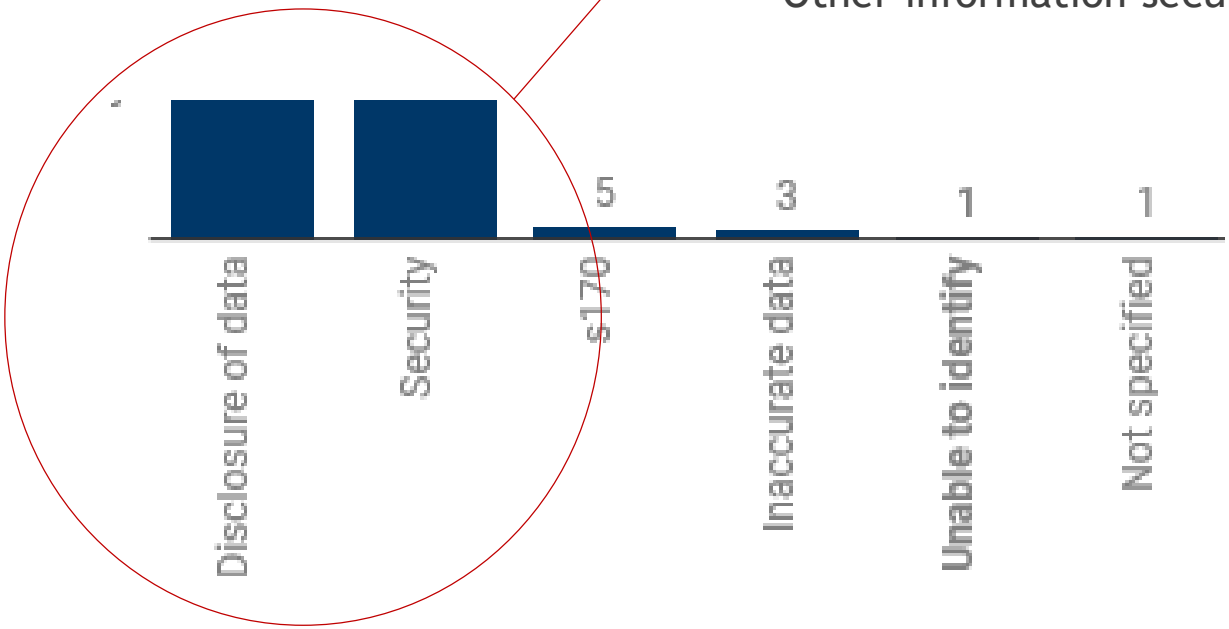


Source: https://ico.org.uk/action-weve-taken/data-security-incident-trends/

GDPR ONE YEAR ON

Personal Data Security Breaches - Sources

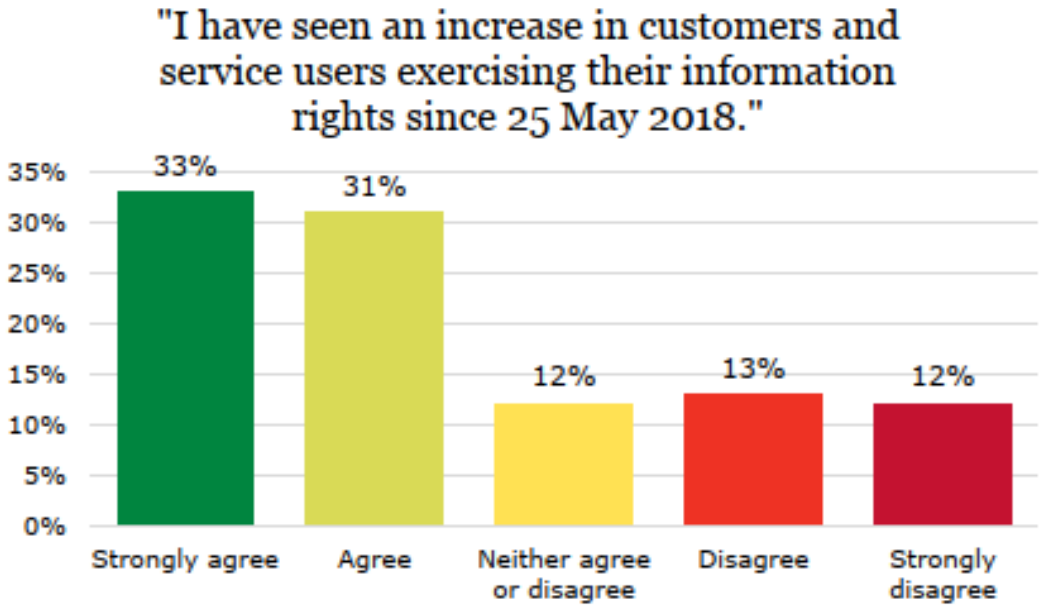
- Incorrect mail recipient
- Lost hard copy
- Erroneous publishing
- Cyber attack
- Other information security



GDPR ONE YEAR ON

Public Perception

- Now a greater awareness of the law and the rights of individuals
- 64% of Data Protection Officers agreed with the following statement:



GDPR ONE YEAR ON

Remaining challenges – overseas transfers

- OK to transfer data within the European Economic Area – Brexit will impact on transfers to the UK from the EU
- Does the receiving country have an adequacy decision?
- Application of appropriate safeguards required e.g.
  - Legally binding and enforceable contract
  - Binding corporate rules – internal code of conduct within a group, requires approval from supervisory authority
  - Standard data protection clauses
  - Certification under an approved mechanism – not yet in place

GDPR ONE YEAR ON

Areas receiving further clarification and focus

- Age appropriate design codes - design codes for online processors processing child data
- Data sharing - guidance for controllers around secure and responsible data sharing
- Direct marketing – to avoid intrusive marketing and be compliant with forthcoming ePrivacy Regulation

GDPR ONE YEAR ON

Key priorities for next 12 months

- Keeping pace with technology
- Some of most significant data protection risks derived from cyber attacks, AI, machine learning etc
- Children's privacy
- Use of surveillance and facial recognition technology
- Data broking
- Use of data in political campaigns
- Freedom of information compliance

GDPR ONE YEAR ON

What did we learn?

- Can take a significant amount of time for complex or high risk organisations (1 year +)
- Multi-disciplinary undertaking – generally involving IT, Legal, Sales & Marketing, Compliance with significant input also from the wider business
- Multi national organisations face the challenge of co-ordinating concurrent GDPR programs
- Resources can be scarce
- Costly
- Get it wrong – can be expensive and business restricting

GDPR ONE YEAR ON

What does good look like?