SQUIRE PATTON BOGGS

CIPFA Pensions Network

How Safe Is Your Member Data?

(and what risks are you running if it's not?)

5th & 6th July 2016

What We're Covering

SQUIRE PATTON BOGGS

- Why data security matters
- Common risks/pitfalls
- Introduction to changes under General Data Protection Regulation

Why Data Security Matters

SQUIRE PATTON BOGGS

Legal Obligations

- Data Protection Act Principle 7
  - Requires taking of "appropriate technical and organisational measures against unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to, personal data"
- Common law duty of confidence to members

BUT ALSO

- Critical to ability to deliver other obligations
- Costs of remedying failures can be astronomical
- Reputational damage & loss of trust if it fails

Huge Increase In Quantity & Sophistication of Attacks

Fines/Monetary Penalties

SQUIRE PATTON BOGGS

- Power given to ICO in 2010 - If
  - Serious breach of the Act
  - Controller knew or ought to know could cause serious detriment

- Overwhelming majority of monetary penalties (and the highest) for data security breaches. Over 70% of those imposed on public sector bodies

- Many fines on controllers
  - When their processors at fault
  - Immediate breach caused by third party criminal act

- Current maximum fine £500,000 per breach
- GDPR will increase maximum to higher of €20m and 4% of global turnover

ICO's Core Security Requirements

SQUIRE PATTON BOGGS

- Protection in transit, at rest, in use
- Encryption
  - Main hosting servers
  - Hard drive of laptop & smart-phones
  - Memory sticks
  - Check level of encryption
- Weakest link – Bring Your Own Device
- ICO Guidance on commonest IT security mistakes

Some Key Risks/Risk Areas

SQUIRE PATTON BOGGS

- Inadequate central systems, patching, maintenance or monitoring
- Poor access control (physical and virtual) allowing unauthorised access
- Failure to securely erase data from hardware before disposal
- Uncontrolled use of new ‘cloud’ solutions e.g. cheap digital dashboards
- Third party processors
  - Poor security
  - Poor training
  - Lack of appropriate instructions

- Loss of unencrypted laptop or other device, such as a memory stick

Some Key Risks/Risk Areas

SQUIRE PATTON BOGGS

- Phishing – including spear phishing attacks
- Forwarding papers to home account
  - insecure home routers/systems
  - use of gmail and other cloud hosted accounts
- Sending email to wrong email address
- Sending "cc" rather than "bcc" emails to members
- Passwords
  - Not changing default passwords
  - Passwords linked to social media
  - Weak passwords

Data Security – Using Secure Passwords

SQUIRE PATTON BOGGS

Charac-ters	Numbers only	Upper case or lower case letters	Upper case and lower case letters	Numbers, upper case and lower case letters	Numbers, upper case, lower case and symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 seconds	10 seconds
6	Instantly	Instantly	8 seconds	3 minutes	13 minutes
7	Instantly	Instantly	5 minutes	3 hours	17 hours
8	Instantly	13 minutes	3 hours	10 days	57 days
9	4 seconds	6 hours	4 days	1 year	12 years
10	40 seconds	6 days	169 days	106 years	928 years
12	1 hour	12 years	600 years	108k years	5m years
14	4 days	8k years	778k years	1bn years	5bn years
16	1 year	512m years	1bn years	6tn years	193tn years
18	126 years	3bn years	1tn years	23qd years	1qt years

Data Security – Using Secure Passwords

SQUIRE PATTON BOGGS

- Password storage
  - Use robust hashing and salting
- Complexity of password
  - At least ten digits
  - Numbers, letters (upper and lower case), and special symbols

Data Security - Solutions

SQUIRE PATTON BOGGS

- Properly implemented data security **policy**
- **Nominated individual** with overall responsibility for data security
- **Technical security** applied to data held electronically eg encryption, password protection, rules about downloading to mobile devices
- **Physical security** to data in paper form and electronic devices on which data is stored
- **Vetting** and **training** those who have access to personal data
- **Access limited** to that which is necessary
- Secure **disposal** of hard copy data
- Secure **deletion** of electronic data
- Appropriate **due diligence** before using service providers
- **Contracts** with service providers

Data Security – Data Processors

When appointing processors – controllers are in breach of the Act unless:

- Upfront and ongoing due diligence into processor's security measures
  - Security questionnaire
- Written contract requiring
  - Only to process on controller's instructions
  - To comply with the Seventh Principle
  - General obligation not enough
- Under GDPR, much more extensive contracts required

Data security – Data Processors

Other strongly advisable contractual clauses

- Immediate notification of data security breach
- Remedial actions on security breach
- Audit rights
- Sub-contractor approval
- Responding to Data Subject Access Requests
- Indemnities for losses
- Restrictions on processing outside the EEA
- Deletion of data on termination

Managing a significant data breach

SQUIRE PATTON BOGGS

- Need to move fast
  - Actions to minimise adverse effects
  - Notifying
    - members
    - the ICO
    - the police
    - the pensions regulator
    - insurers
  - Remedial actions

- Best time to think about how to handle a major data loss/breach
  - Before the event
  - Policy on handling data breaches

- Importance of co-operation of service providers

Breach Notifications

SQUIRE PATTON BOGGS

- To the ICO
  - No obligation under the Act
  - ICO guidance – notify if:
    - Potential detriment to affected individuals
    - Large amount of data
    - Particularly sensitive (even if small amount)
    - Significant damage or distress to individuals
- Consequence of non-notification – higher penalty
- Consequences of notification
  - ICO will investigate data protection compliance
    - Security measures
    - Contracts

Breach Notifications

- To individuals
  - If notification will help them protect themselves eg against identity theft
  - If notify individuals, notify ICO?

- To the Pensions Regulator if s70 Pensions Act 2004 applies:
  - Breach of the law
  - Likely to be of material significance to the Pensions Regulator

GDPR Changes most likely to affect LGPS

SQUIRE PATTON BOGGS

Lawful processing (Articles 5 and 6)

- Processed lawfully, fairly, in a transparent manner
- Collected for specified, explicit and legitimate purposes, and not used in an incompatible way
- Accurate and up to date
  - Every reasonable step to correct or erase without delay
- Kept in form that permits identification no longer than necessary for purpose

Clarity of providing notices crucial

- Where information collected from individual (Article 14)
- Where information not collected from individual (Article 14a)

Changes most likely to affect LGPS

SQUIRE PATTON BOGGS

Records of processing activities (Article 28)

- Name and contact details of controller and DPO
- Purpose
- Categories of data and data subjects
- Categories of recipients
- Transfers to third countries, and documentation of safeguards
- Where possible, time limits to erasure
- Where possible, description of security measures
- Make available to Supervisory Authority on request

Changes most likely to affect LGPS

SQUIRE PATTON BOGGS

Data Protection Officer (Article 35)

- Mandatory because a public authority
- Potentially could be one DPO for several authorities
- Basis of appointment
  - Professional qualities
  - Expert knowledge of data protection law
  - Ability to perform required services (Article 37)

Changes most likely to affect LGPS

SQUIRE PATTON BOGGS

Privacy Impact Assessments? (Article 33)

- Required where "high risk" to rights and freedoms of individuals, including:
  - Systematic and extensive evaluation based on automated processing, including profiling, that significantly affects individuals; or
  - Large scale processing of sensitive personal data

Changes most likely to affect LGPS

SQUIRE PATTON BOGGS

Data subject access and other requests

- Response without undue delay, at latest one month from receipt of request
- May be extended up to a further two months when necessary
  - Complexity of request
  - Number of requests
- Provided free of charge
- Where requests "manifestly unfounded or excessive, in particular because of their repetitive character"
  - Charge a reasonable fee for providing information/taking requested action; or
  - Refuse

Changes most likely to affect LGPS

SQUIRE PATTON BOGGS

Data breach notification (Articles 31 & 32)

- Notification to the SA (Article 31)
  - Unless unlikely to result in risk for rights and freedom of individual
  - Notify without delay and, where feasible, within 72 hours of becoming aware
    - Outside 72 hours - reasoned justification for delay
  - Processor must notify controller without undue delay
  - Controller must document data breaches

- Notification to affected individuals (Article 32)
  - Where likely to result in high risk to rights and freedoms of individual
  - Without undue delay
  - Not required if technical and organisational measures mean data unintelligible to unauthorised person (eg by encryption)

Changes most likely to affect LGPS

SQUIRE PATTON BOGGS

Liability of Processors

- For first time, direct obligations on processors, including
  - Security measures
  - Records of processing activities
  - Compliance on cross-border transfers
  - Co-operation with controller on compliance

- Big change in risk profile for processors
  - So likely to look to limit liability/seek indemnities

Any questions?

This information has been prepared as a general guide and does not constitute advice on any specific matter. We recommend you seek professional advice before taking action. We accept no liability for any action taken or not taken as a result of this information.

Contact Info Slide

Stuart James
Partner
0121 222 2645
stuart.james@squirepb.com

Emma Ball
Senior Associate
0161 830 5222
emma.ball@squirepb.com

Kirsty Bartlett
Partner
0207 655 0298
kirsty.bartlett@squirepb.com

David Griffiths
Partner
0161 830 5359
stuart.james@squirepb.com

SQUIRE PATTON BOGGS

North America

Cincinnati
Cleveland
Columbus
Dallas
Denver
Houston
Los Angeles
Miami
New York
Northern Virginia
Palo Alto
Phoenix
San Francisco
Tampa
Washington DC
West Palm Beach

Latin America

Santo Domingo

Europe & Middle East

Abu Dhabi
Berlin
Birmingham
Bratislava
Brussels
Budapest
Doha
Dubai
Frankfurt
Kyiv
Leeds
London
Madrid
Manchester
Moscow
Paris
Prague
Riyadh
Warsaw

Asia Pacific

Beijing
Hong Kong
Perth
Seoul
Shanghai
Singapore
Sydney
Tokyo