PSE Payment Gateway Conference

GDPR: Gateway and merchant impacts and opportunities

Tuesday 23 May 2017

Chris Jones, Director, PSE Consulting

+44(0)20 3771 8522
chris.jones@pseconsulting.com

Vikki Hoyle, Senior Associate, Regulatory & Compliance

+44(0)113 283 2513
vikki.hoyle@walkermorris.co.uk

pse consulting

WALKER MORRIS

Introduction to Walker Morris

- Top 100 UK law firm
- Largest single site practice outside London
- Over 470 staff including 48 partners and 250 lawyers
- Full service commercial law firm with 27 practice areas ranked in Chambers & Partners
- Nearly 90% of our partners are ranked by Chambers & Partners and Legal 500
- 54% of our top 50 clients have been clients for over 10 years
- Revenue from international clients increased by 12% in last 5 years. International clients now account for a fifth of our revenue

pse consulting

WALKER MORRIS

Regulatory & Compliance Group

- Financial services
  - team includes former FCA and SFO investigators
  - payment services
- Information law
  - data protection
- Other services include:
  - anti-bribery / anti-money laundering
  - environment
  - health & safety / inquests
  - food safety
  - fraud
  - modern slavery

pse consulting

WALKER MORRIS

What is GDPR and why should I care?

European data protection law

- What about Brexit?

12 months to go

- No transitional provisions

Applies to all personal data

- Not just payment card data

Significant increase in fines

- up to greater of €20 million or 4% of global annual turnover

pse consulting WALKER MORRIS WM

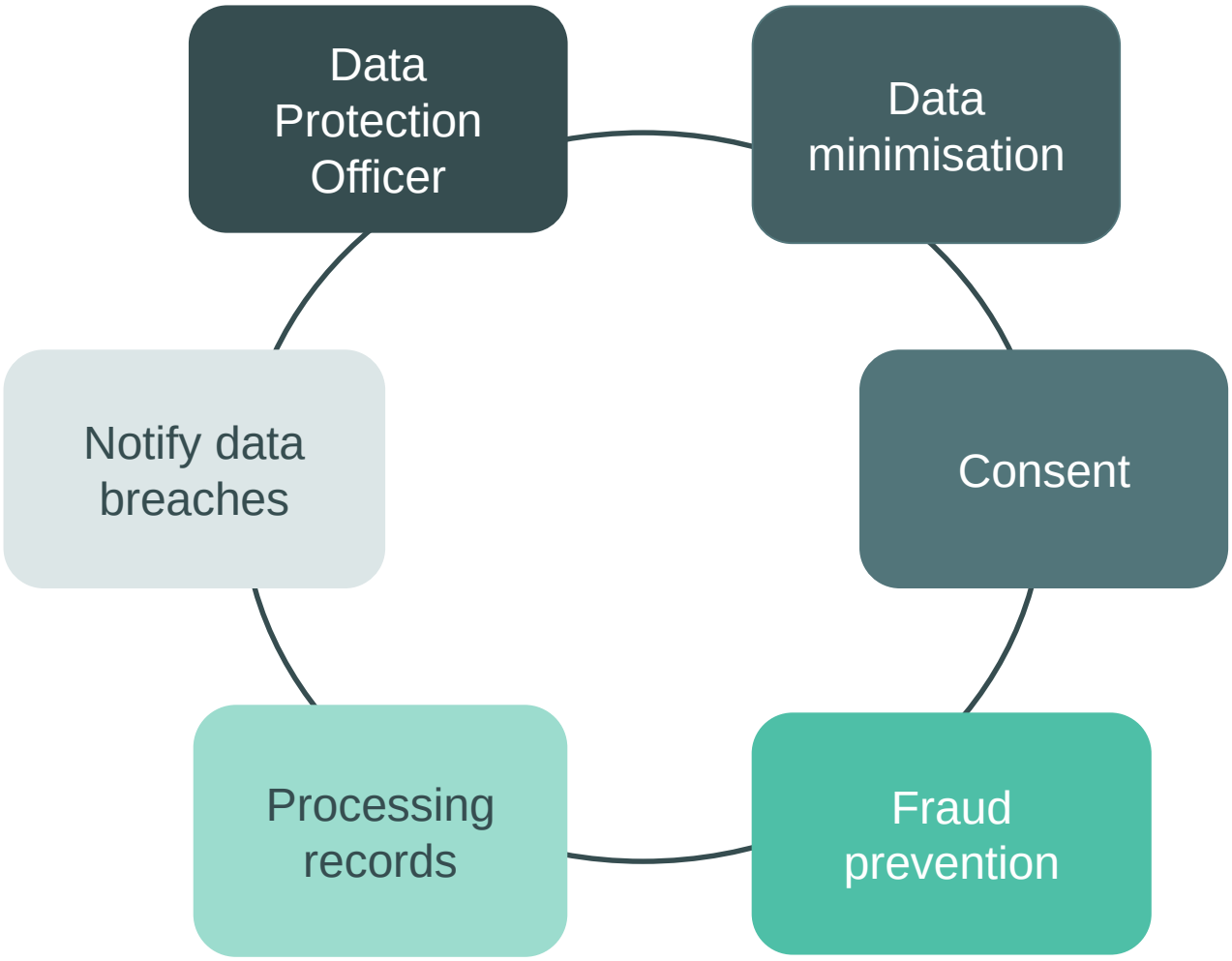
Overview of key changes under GDPR

- Harmonisation
- Territorial scope
- Personal data definition
- Registration with ICO*
- Data protection officers
- Privacy by design and default
- Obligations on data processors
- Consent
- Right to be forgotten
- Right to object to profiling
- Right to data portability
- Subject access requests
- Security of processing
- Pseudonymisation
- Data security breaches
- Enforcement

*Information Commissioner's Office

pse consulting WALKER MORRIS

What does this mean for a gateway's operations?



pse consulting

WALKER MORRIS

What does this mean for a gateway's IT systems?

- Appropriate technical and organisational security measures
  - "Appropriate" not defined
  - no "one-size fits all"
  - risk-based approach depending on circumstances
  - similar to PCI DSS but for all personal data
- Right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff

pse consulting

WALKER MORRIS

What about a gateway's data centres and call centres?

- EU and UK
  - Brexit
- US
  - Privacy Shield
- Rest of the world
  - adequacy decisions
  - model contract clauses

pse consulting

WALKER MORRIS

What does this mean for contracts with gateways?

- Greater service costs for gateways?
- Lengthier negotiations re allocation of risk?
- Review existing contracts
  - Contracts with processors must include specific provisions
- “Future-proof” new contracts?
  - BUT still waiting for ICO guidance

pse consulting

WALKER MORRIS

GDPR Gateway Opportunities

PSE Payment Gateway Conference

23rd May 2017

Opportunities for Payment Gateway Providers

1	Tokenise	Wider Tokenisation of Payment Details	Wider Pseudonymisation of Customer Data
2	Secure	Secure Data Access	Secure Data Storage
3	Audit & Insure	Impact/ Compliance Audit	Data Breach Insurance

pse consulting

WALKER MORRIS

1a. Tokenisation

Wider Tokenisation of Payment Details	**Wider Pseudonymisation of Customer Data**
Secure Data Access	**Secure Data Storage**
Impact/ Compliance Audit	**Data Breach Insurance**

- Extension of current tokenisation services for PANs to bank account details (and possibly other APMs)
- Replace structured payment details with proxy tokens
- **In-house** delivery using existing tokenisation services

Gateway Benefits	MEDIUM
Effort to Deploy	LOW

pse consulting

WALKER MORRIS

1b. Pseudonymisation

Wider Tokenisation of Payment Details	**Wider Pseudonymisation of Customer Data**
Secure Data Access	**Secure Data Storage**
Impact/ Compliance Audit	**Data Breach Insurance**

- Pseudonymisation = anonymising data so that it can only be used to identify individuals by using additional info eg a unique identifier
- Obfuscate/anonymise a wide range of in-scope customer data from name through to address, DOB, etc.
- More complex due to different structure of the data and the difficulty in using proxy tokens
- **In-house** delivery using existing tokenisation services

Gateway Benefits	MEDIUM
Effort to Deploy	HIGH

pse consulting

WALKER MORRIS

2a. Secure Access

Wider Tokenisation of Payment Details	**Wider Pseudonymisation of Customer Data**
Secure Data Access	**Secure Data Storage**
Impact/ Compliance Audit	**Data Breach Insurance**

- The GDPR expects personal data to be protected against unauthorised or unlawful processing and against loss, destruction or damage; It also gives individuals a right of access to their data
- Provide higher security data access to customer data (e.g. strong customer authentication – 2FA, biometrics)
- **In-house** extension of services offered by 3DS 2.0 and other identity management services

Gateway Benefits	MEDIUM
Effort to Deploy	MEDIUM

pse consulting

WALKER MORRIS

2b. Secure Storage

Wider Tokenisation of Payment Details	**Wider Pseudonymisation of Customer Data**
Secure Data Access	**Secure Data Storage**
Impact/ Compliance Audit	**Data Breach Insurance**

- GDPR requires strong, secure storage of data
- Provide data processing services for in-scope data in a secure manner – particularly for data captured for payments
- **Partner** with secure storage 3rd parties, or deliver **in-house** using existing services

Gateway Benefits	MEDIUM
Effort to Deploy	LOW

pse consulting

WALKER MORRIS

3a. Impact Assessment

Wider Tokenisation of Payment Details	**Wider Pseudonymisation of Customer Data**
Secure Data Access	**Secure Data Storage**
Impact/ Compliance Audit	**Data Breach Insurance**

- The GDPR provides the ICO with the power to carry out investigations in the form of data protection audits.
- Carry out an audit of a merchant's business to determine impact, gaps and path to resolution
- Could be provided on a one-off or regular basis – can be linked to insurance premiums
- **Partner** with a relevant QSA to deliver services

Gateway Benefits	MEDIUM
Effort to Deploy	LOW

pse consulting

WALKER MORRIS

3b. Insurance

Wider Tokenisation of Payment Details	**Wider Pseudonymisation of Customer Data**
Secure Data Access	**Secure Data Storage**
Impact/ Compliance Audit	**Data Breach Insurance**

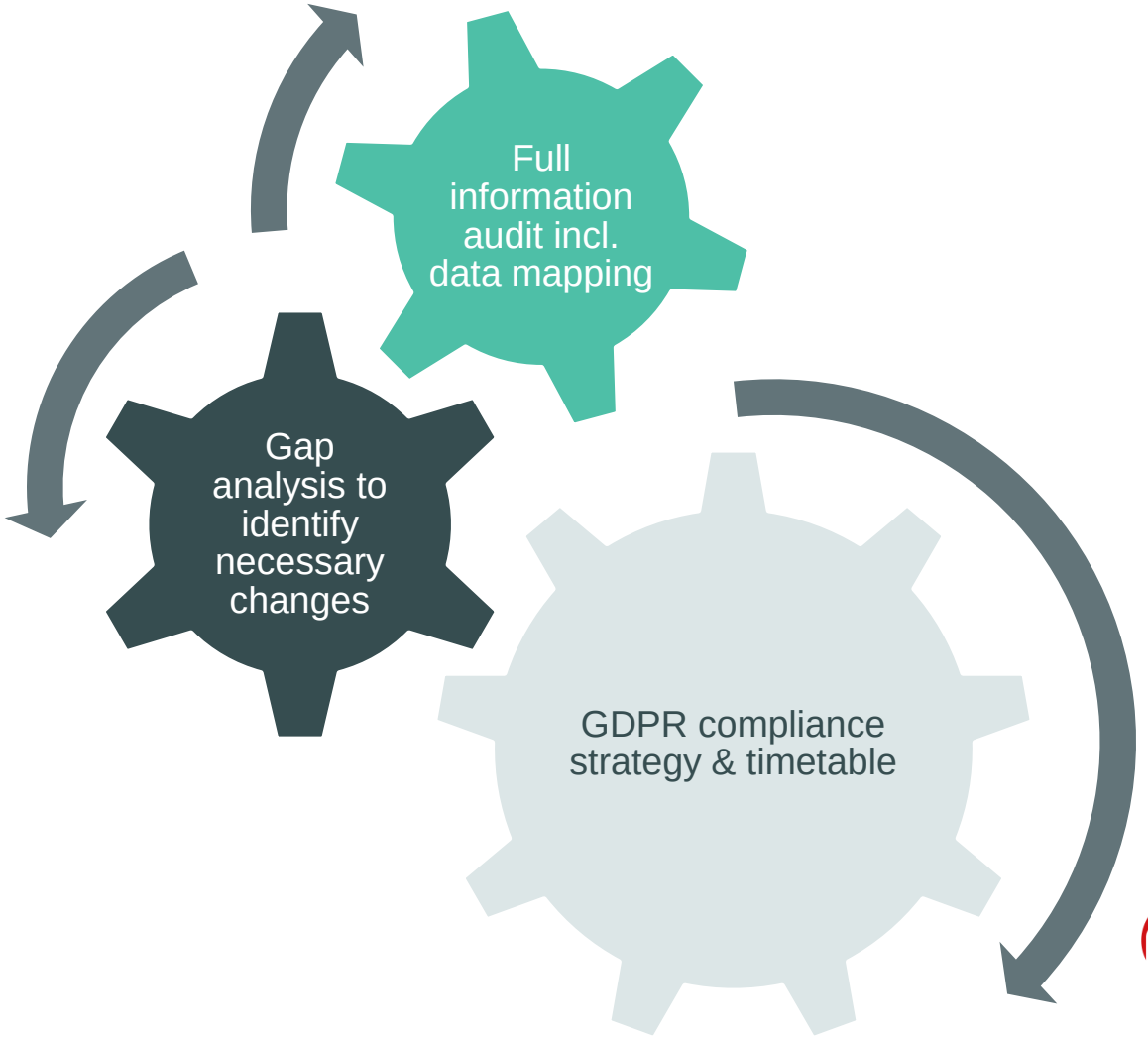
- Similar to PCI DSS insurance product, with premiums reduced as a result of technical implementation of services and audit
- Would pay out if the merchant was subject to a breach
- Could be linked to the impact/ compliance audit list
- **Partner** with an insurance company

Gateway Benefits	LOW
Effort to Deploy	LOW

pse consulting

WALKER MORRIS

The countdown is on



pse consulting

WALKER MORRIS

Don’t panic, be prepared

pseconsulting

WALKER MORRIS

Any Questions?

pse consulting

WALKER MORRIS

Contact

Vikki Hoyle

T: +44 (0)113 283 2696

M:+44 (0)7944 091 951

vikki.hoyle@walkermorris.co.uk

@VikkiHoyle

Chris Jones

T: +44 (0)20 3771 8522

M:+44 (0)7930 354 270

chris.jones@pseconsulting.com

@Pseconsulting

@WM_Regulatory

Walker Morris LLP

T: +44 (0)113 283 2500

Disclaimer

pse consulting

WALKER MORRIS