

Implementing a Group-wide Privacy Programme in 60+ Jurisdictions

Stephen Bonner



Why we initiated the programme

- **Privacy and data protection laws place obligations on us in relation to how we collect, store, use and dispose of information about people and corporations**
- **Data privacy is of increasing concern to customers, employees and also our regulators and has resulted in fines and findings within the Financial Services industry in a number of jurisdictions including:**
 - **The formal undertaking given by the CEO to the UK data protection regulator in relation to the disposal of customer information.**
 - **Investigations and fines imposed by the Spanish regulator.**
 - **Fines in the UK by the FSA in 2007 resulting from stolen laptops.**
 - **Widely reported data losses by HM Revenue & Customs and DVLA in late 2007.**

How did we manage risk

The scope of our programme covers a broad definition of privacy. We are not just fixing an incident or covering the Data Protection Act

- **We used experts to advise key roles in each area of the programme**
- **Segmented the programme and businesses to pinpoint accountability**
- **Prioritised the high risk data in the high risk jurisdictions**
- **Prioritised the outsourcers within the high risk jurisdictions**
- **Defined ongoing operating models to ensure our activities transfer into “Business as Usual”**

Barclays

<u>Theme</u>	<u>Description</u>
Size	147,000 employees, with multiple departments and organisational structures. There is no single model for a business
Range of Business	Retail and commercial banking, credit cards, investment banking, wealth management and investment management services
Volume of data	Huge volumes of personal data which must be protected
International footprint	Extensive international presence in Europe, the USA, Africa and Asia.
Amount of change	Significant IT and process change programmes are running throughout the organisation
Outsourcing	Increasing dependencies on outsourcing and overseas operations

Key components to make this programme successful

- **Senior Management support**
- **Funding**
- **Clear definition of baseline requirements for your organisation which comprehensively covers the legal and regulatory obligations and is usable by the business**
- Division of the organisation into manageable segments
- Identification of the high risk data within the organisation
- An ongoing compliance monitoring process / system
- A significant and ongoing awareness and cultural change campaign

Key components to make this programme successful

- **Clear definition of baseline requirements for your organisation which comprehensively covers the legal and regulatory obligations and is useable by the business**

Reference	The Law	Barclays Detailed Questions
UK DPA Principle 1 Dir 95/46/EC Article 6.1a	If vetting (screening of candidates against certain criteria, outside of the interview process) is carried out, it should only be undertaken where justified	Do you carry out pre-employment vetting?
		If so, do you limit this to positions which carry particular and significant risks to the security of the company or others associated with the position being filled?
		Do you take steps to limit the inquiries to information sources that have been judged relevant to the selection of the candidate?
		Do you explain to the subject of the vetting the nature, extent and range of sources of the information that will be sought?
		Do you obtain their agreement to the release of necessary details to Third Parties?

And on the Privacy system it looks like this....

Law001-001 Actions

Description: UK Data Protection Act - Principle 1

Additional Description: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Requirements Results 1-25 Prev Next Actions

Name	Description
Req-007	Decisions on recruitment should be taken in a way that is fair to the Data Subjects, i.e. the same criteria for selection should be applied to all Data Subjects.
Req-008	If vetting (screening of candidates against certain criteria, outside of the interview process) is carried out, it should only be taken where justified.
Req-009	Personal data should be processed fairly and lawfully, which includes informing the Data Subject about what personal data is held, how it is used, where it was obtained from and where it will be disclosed to.
Req-010	Sickness records are the most likely type of sensitive personal data that will be held by HR. Where these are

Req-007 Actions

Description: If vetting (screening of candidates against certain criteria, outside of the interview process) is carried out, it should only be taken where justified.

Name: Req-007

Q2-13-01-GBR Actions

Baseline Question: Do you carry out pre-employment vetting?

Q2-13-02-GBR Actions

Baseline Question: If so, do you limit this to positions which carry particular and significant risks to the security of the company or others associated with the position being filled?

Q2-13-03-GBR Actions

Baseline Question: Do you take steps to limit the inquiries to information sources that have been judged relevant to the selection of the candidate?

Q2-13-04-GBR Actions

Baseline Question: Do you explain to the subject of the vetting the nature, extent and range of sources of the information that will be sought?

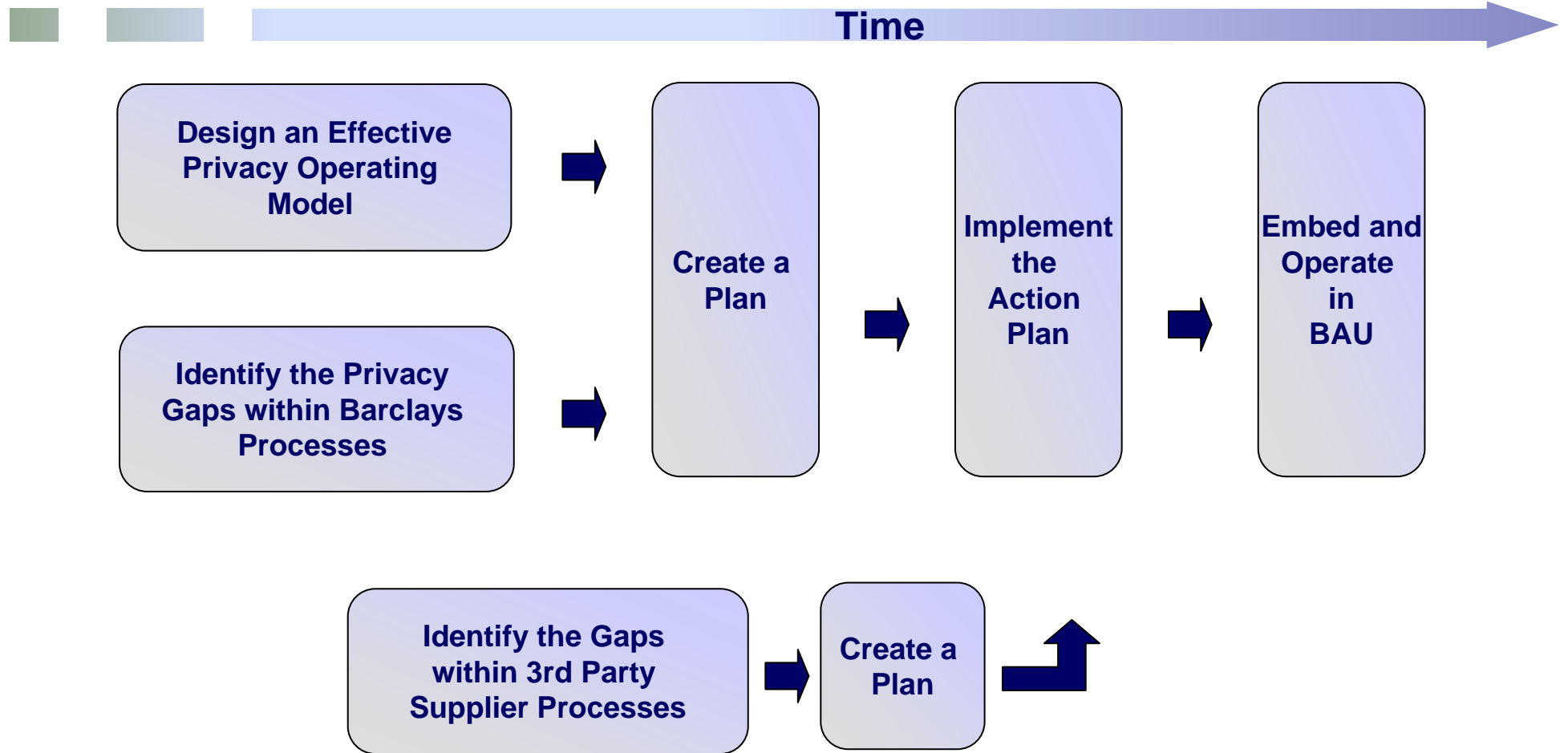
Q2-13-05-GBR Actions

Baseline Question: Do you obtain their agreement to the release of necessary details to Third Parties?

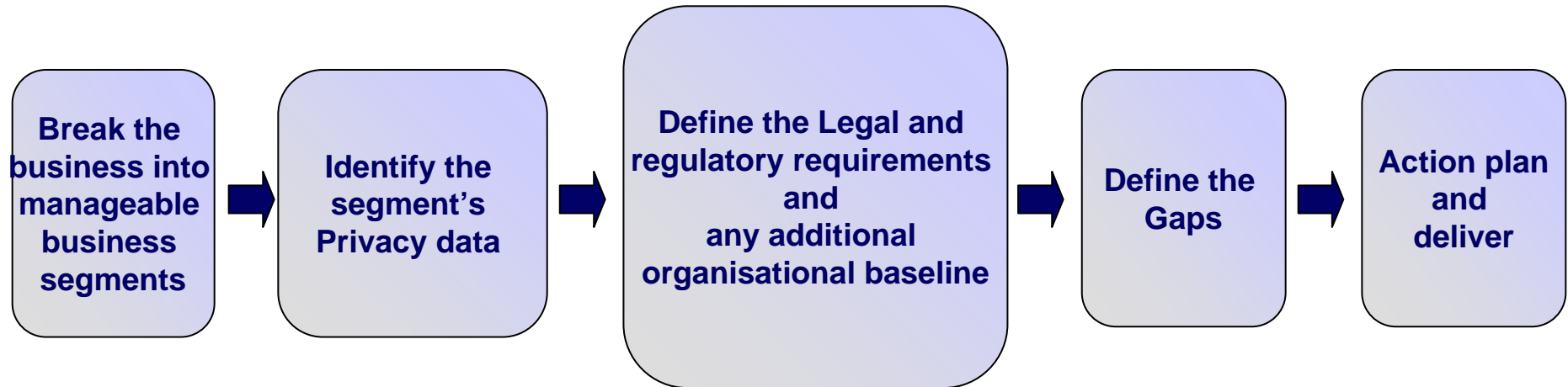
Key components to make this programme successful

- Senior Management support
- Funding
- Clear definition of baseline requirements for your organisation which comprehensively covers the legal and regulatory obligations and is usable by the business.
- **Division of the organisation into manageable segments**
- **Identification of the high risk data within the organisation**
- **An ongoing compliance monitoring process / system**
- **A significant and ongoing awareness and cultural change campaign**

The Programme Overview



The Programme Process



We assess our data against the legal and regulatory requirements in the these 8 categories

- Personal Data
- Employee Data
- CCTV
- IT & Organisation
- Intranet
- Internet
- Marketing
- Cross Jurisdiction & Outsourcing

How we are measuring success

- 1. Definition and agreement of an organisational structure (including responsibilities and authorities) covering Privacy Risk**
- 2. Ensure the appropriateness of Group, and where appropriate, Business Privacy policies / processes and identification of the legal and regulatory requirements in our high risk jurisdictions**
- 3. Implementation of a privacy awareness campaign and evaluation of its effectiveness**
- 4. Identification, capture and reporting of privacy management information and metrics which provides evidence to inform management of the effective operation of Privacy policies and processes**
- 5. Operation of an effective incident management and reporting process to cover data privacy issues**
- 6. Evidence of compliance by third party providers to our data privacy requirements relating to critical data**

What did we learn?

- 1. There is a global shortage of privacy professionals so the approach had to work with project managers and business analysts without a technical privacy background**
- 2. Quality assurance of the output is vital and should be integral to the process**
- 3. Training in the privacy methodology should be little and often**
- 4. Link in with key stakeholders, e.g. Internal Audit, Compliance, IT Security etc**
- 5. Awareness and training is a long term exercise and is not fixed overnight**
- 6. Migrate to a robust system as soon as possible.**



Awareness Material



BARCLAYS

DATA CAN BE DANGEROUS

THINK PRIVACY

Ex eu fugiat la feugiat magniam dōlent nūman veniāro dōlorpe rīllumny noncupat dēl utpar tōre. faccum dō odī Oreo odignatē dōlorem līs rīsim. Ex eu feugit la feugae magniam dōlent nūman veniāro dōlorpe rīllumny noncupat dēl utpar tōre. faccum dō odī Oreo odignatē dōlorem līs rīsim.

Awareness Material



Awareness Material



Awareness Material



Awareness Material



Thank You and Questions?



Stephen Bonner
Barclays Head of
Information Risk Management

1 Churchill Place
Canary wharf
London
E14 5HP

Tel: +44 (0)20 7116 6452
stephen.bonner@barclays.com