MANAGING PRIVACY POST GDPR

The Ultimate Guide for General Data Protection Regulation

via resource
securing success

EXECUTIVE SUMMARY

The General Data Protection Regulation (GDPR) builds on the existing EU Directive to protect all EU citizens from privacy and data breaches in an increasingly data-driven world. Processing personal data securely and compliantly needs to be at the core of what your business does, failure to do this could let down both your customers, your employees, and risk significant damage to your valuable brand.

The 25/5/2018 compliance date has been and gone, however many business's have not been left with an effective process to show data privacy risk and maintain on-going compliance and improvement.
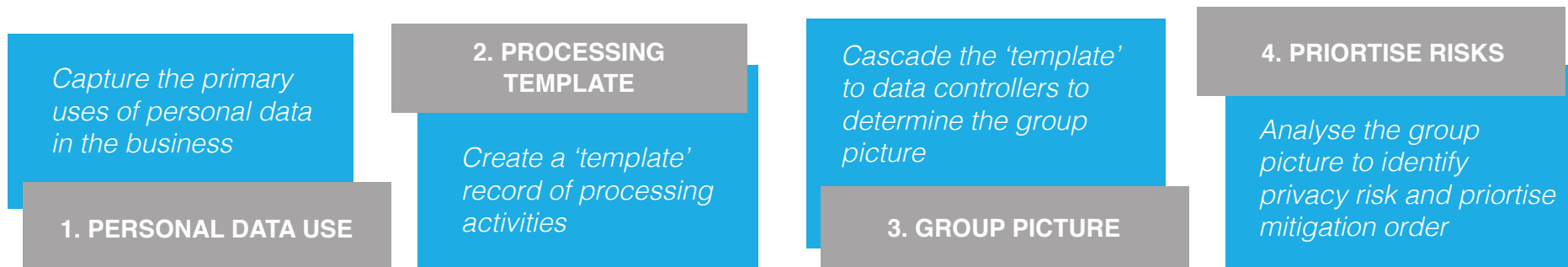
We have developed a simple 5 staged approach to address this problem, our first stage "Visibility" is a piece of work which is a requirement of GDPR and is referred to as 'Record of Processing Activities" - it will show how your business process's personal data.

via resource
securing success

VISIBILITY PHASE

Our "Visibility" phase will quickly establish an accurate Record of Processing Activities to avoid a fine and to determine what current risks need to be remediated immediately, this is "Ground Zero" on the privacy compliance journey.

We provide this service to those that may have previously worked towards GDPR and require a sense check or those who are at the beginning of their journey. We have delivered internationally and are aware of specific country requirements.

Steps to quickly achieve Personal data processing risk visibility

Capture the primary uses of personal data in the business

2. PROCESSING TEMPLATE

Create a 'template' record of processing activities

Cascade the 'template' to data controllers to determine the group picture

4. PRIORTISE RISKS

Analyse the group picture to identify privacy risk and priortise mitigation order

1. PERSONAL DATA USE

3. GROUP PICTURE

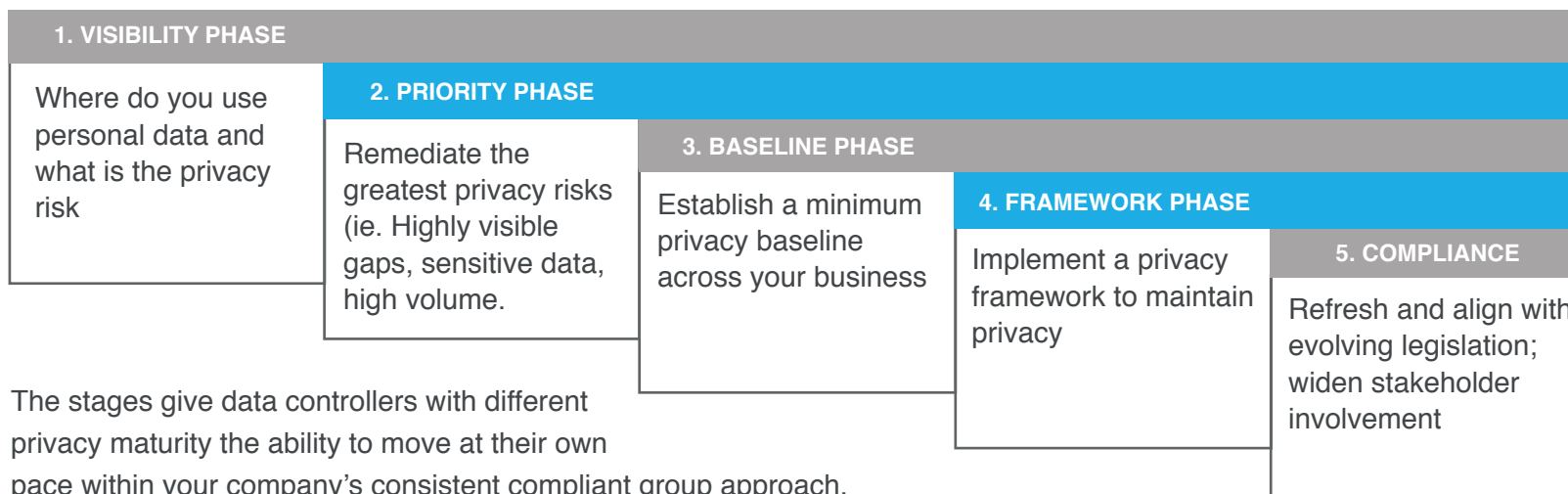'Ground Zero'

via resource
securing success

THE BIGGER PICTURE

Privacy Compliance Journey

Visibility – 'Ground Zero' is a demonstrable record of how a company uses personal data the privacy risk associated with that processing.

Establishing visibility of your privacy risk is the primary stage of the privacy compliance journey and it enables an organisation to understand the size and scale of the current use of personal data. After creating the initial record of processing activities it must be maintained and developed as it will change to mirror the business activities as they change. The knowledge available from the 'record' will inform the privacy journey, how far and how quickly you travel will be determined by the needs of your business, industry norms, risk appetite, existing privacy maturity and available. resources.

Privacy compliance journey phases

1. VISIBILITY PHASE

Where do you use personal data and what is the privacy risk

2. PRIORITY PHASE

Remediate the greatest privacy risks (ie. Highly visible gaps, sensitive data, high volume.

3. BASELINE PHASE

Establish a minimum privacy baseline across your business

4. FRAMEWORK PHASE

Implement a privacy framework to maintain privacy

5. COMPLIANCE

Refresh and align with evolving legislation; widen stakeholder involvement

The phases enable a business to improve privacy compliance based on risk, each completed stage reduces the overall privacy risk.

The stages give data controllers with different privacy maturity the ability to move at their own pace within your company's consistent compliant group approach.

via resource
securing success

VISIBILITY PHASE DELIVERABLES

PERSONAL DATA USE

PROCESSING TEMPLATE

GROUP PICTURE

PRIORTISED RISKS

1 Capture standard processes such as standards, policies, guidelines, communications, etc.

2 Capture your entity structure and data controllers

3 Capture information technology assets and enterprise architecture

4 Capture organisation and stakeholders

5 Establish a generic picture of the personal data used by a typical 'data controller' within your business

Deliverable

• A document describing the known processes in your business that use personal data including: HR, IT, IS, procurement, legal, customer facing operations, marketing and finance.

via resource
securing success

VISIBILITY PHASE DELIVERABLES

PERSONAL DATA USE

PROCESSING TEMPLATE

GROUP PICTURE

PRIORTISED RISKS

1 Select a specific business unit or company as a whole

2 Identify the functional owners of the generic uses of personal data

3 Divide the generic uses of personal data into discrete processes (ie. HR - recruitment; HR - performance review, HR - salary)

**4** Capture the personal data used in each of the discrete processes

5 Append the processes with the typical data handling/security processed followed, systems and or third-party suppliers

Deliverable

• A record of processing activities aligned to the GDPR article 30 requirements that will act as a template to be accessed by local data controllers to confirm their alignment and highlight any differences

via resource
securing success

VISIBILITY PHASE DELIVERABLES

PERSONAL DATA USE

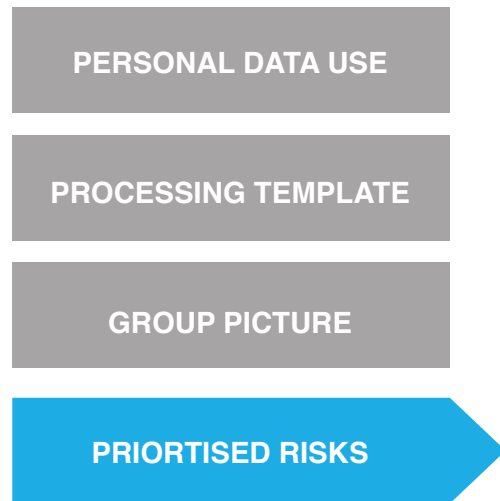**PROCESSING TEMPLATE**

GROUP PICTURE

PRIORTISED RISKS
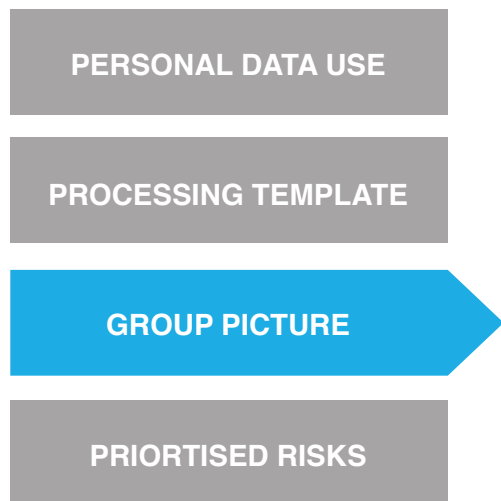
1 Cascade the generic 'record of processing activites template' to the data contrllers to update according to their local processes

2 Collate the feedback from local data controllers

3 Update the 'template' with processes that were missed

4 Differentiate between group-wide, regional and local processes and systems

5 Conduct holistic review to identify any potentially data quality gaps

Deliverable

- A rough-cut record of processing activities for each data controller in scope from which an article 30 report could be established.
- A consolidated Group view of personal data processing.

via resource
securing success

VISIBILITY PHASE DELIVERABLES

PERSONAL DATA USE

PROCESSING TEMPLATE

GROUP PICTURE

PRIORTISED RISKS

1 Identify high processes that are considered a high legal risk under GDPR

2 Identify the processes that are visible to customers, superviory authorities and other external stakeholders

3 Identify potential non-compliances
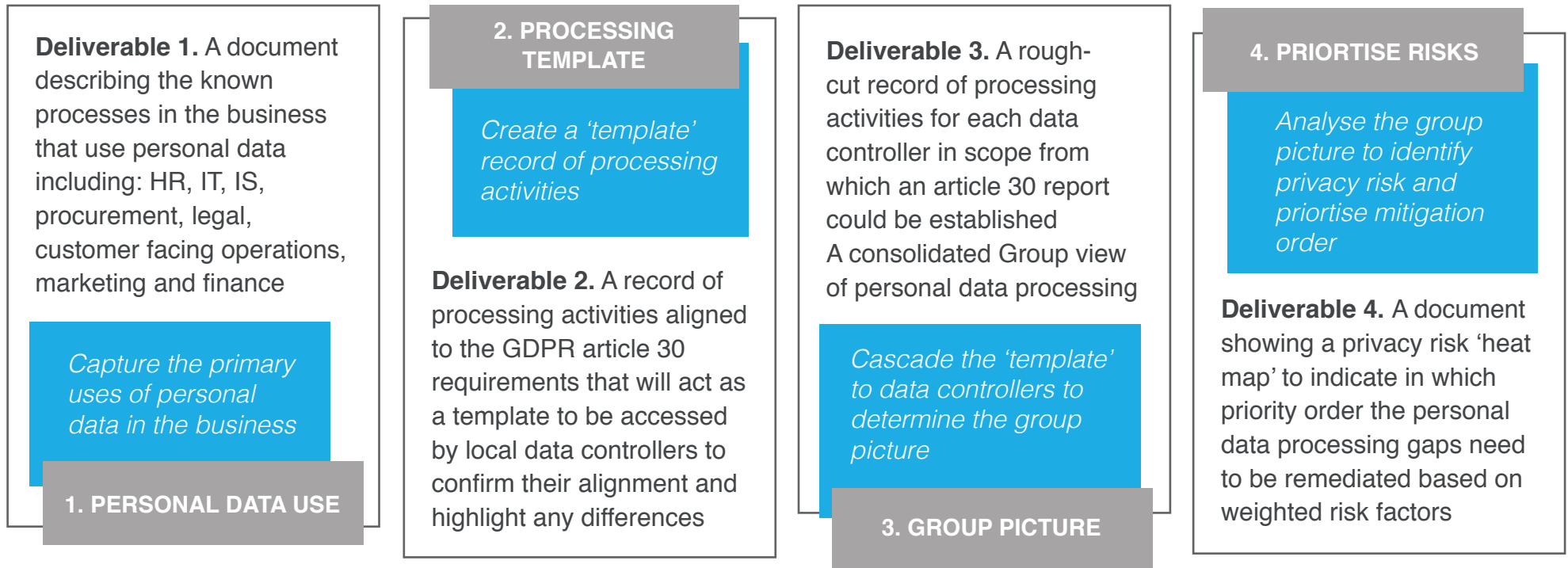
4 Identify legal basis for processing

5 Categorise the generic processes into high, medium and low risk

Deliverable

• A document showing the privacy risk 'heat map' to indicate in which priority order the personal data processing gaps need to be remediated based on weighted risk factors.

via resource
s e c u r i n g   s u c c e s s

VISIBILITY PHASE DELIVERABLE SUMMARY

Steps to quickly achieve
Personal data processing
risk visibility

Deliverable 1. A document describing the known processes in the business that use personal data including: HR, IT, IS, procurement, legal, customer facing operations, marketing and finance

Capture the primary uses of personal data in the business

1. PERSONAL DATA USE

2. PROCESSING TEMPLATE

Create a 'template' record of processing activities

Deliverable 2. A record of processing activities aligned to the GDPR article 30 requirements that will act as a template to be accessed by local data controllers to confirm their alignment and highlight any differences

Deliverable 3. A rough-cut record of processing activities for each data controller in scope from which an article 30 report could be established A consolidated Group view of personal data processing

Cascade the 'template' to data controllers to determine the group picture

3. GROUP PICTURE

4. PRIORTISE RISKS

Analyse the group picture to identify privacy risk and priortise mitigation order

Deliverable 4. A document showing a privacy risk 'heat map' to indicate in which priority order the personal data processing gaps need to be remediated based on weighted risk factors

'Ground Zero'

via resource

securing success

THANK YOU!

Please contact Torquil Macleod with any
questions.

tm@viaresource.com   +44 7967 802420   www.viaresource.com