

# Getting ready for GDPR

## Part 1: Know Your Data Mapping the 5 W's

*The GDPR will “force companies to scrutinise  
how they process and handle customer data”*

Tony Pepper, Egress Software Technologies

The EU General Data Protection Regulation (GDPR) represents a significant change in the data protection compliance regime for data controllers and data processors.

Information is an important and valuable asset to any organisation. **Personal data** may be used for many different reasons, for example staff administration, the provision of goods or services to customers, marketing strategies, prevention of money laundering, a revenue stream etc.

## Transitioning to the new regime

The exercise of proper control and management of **personal data** is fundamental to ensure, and be able to demonstrate, compliance with the GDPR. Transitioning to the new regime will be challenging and require both personnel and financial resources. The level of existing compliance will affect the resources that are required.

However, taking a positive approach, and embracing the changes, will improve customer trust, records management and business opportunities, such as those associated with the digital economy.

## Using this resource

This resource is intended to be a non-legal tool to assist in the creation of an inventory of personal data processed, map the processing of personal data and analyse the legal basis of the processing.

Staff at all levels should be involved to establish what processing occurs – front line staff may well have a different experience to that of senior management.

**In-depth knowledge of the GDPR is not required to use this resource.**

However, an honest analysis is required and if the answer to a question is “Don’t know” or “Not sure” – write that down.

The more honest and comprehensive the analysis is, the easier it will subsequently be to identify processing that may require review and evaluation against the GDPR principles and whether/how the new accountability and risk-based security requirements are to be implemented. (Further resources on these areas will be released in due course)

### **NOTE:**

The GDPR (or the existing Data Protection Act) does not apply to data that is anonymised in such a way that an individual can no longer be identified from the information on its own, or “reconstituted” with other data to enable identification, as it is no longer “personal data”.

## **This resource is in two sections:**

|  |           |
|--|-----------|
| <i>Section 1 - A quick review – What is the current position</i> ..... | <b>4</b>  |
| <i>Section 2 - Mapping the 5W's</i> .....                              | <b>6</b>  |
| <b>WHY ... is personal data processed?</b> .....                       | <b>7</b>  |
| <b>WHOSE ... personal data is processed?</b> .....                     | <b>9</b>  |
| <b>WHAT ... personal data is processed?</b> .....                      | <b>11</b> |
| <b>WHEN ... is personal data processed?</b> .....                      | <b>13</b> |
| <b>WHERE ... is personal data processed?</b> .....                     | <b>15</b> |

## **Section 1 - A quick review – What is the current position**

To establish a base-line it may be necessary to assess current awareness and compliance with the existing Data Protection Act.

This is not intended to be an in-depth exercise.

In many cases it will be beneficial to ask various parts of the organisation, at different levels, for responses.

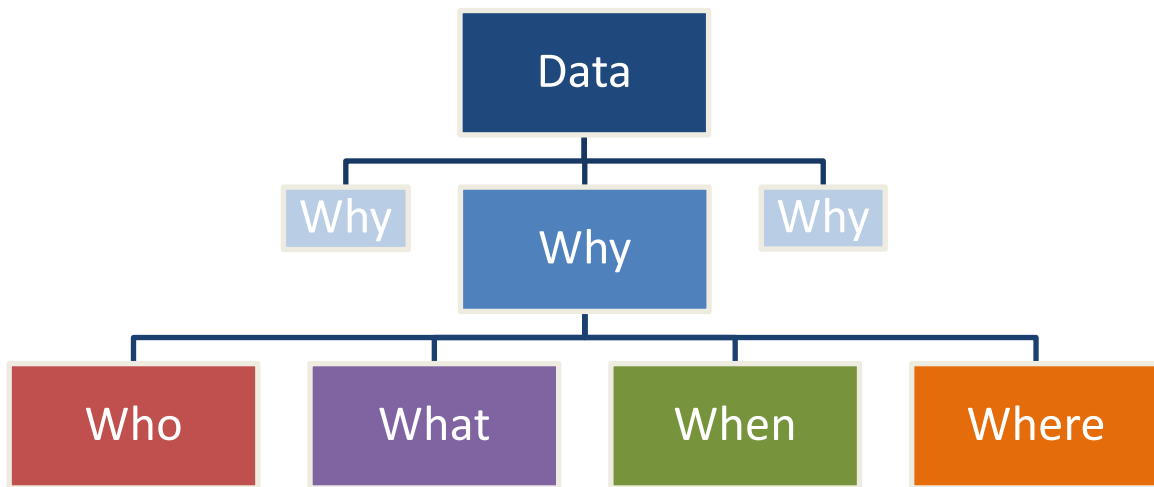
An honest appraisal will provide a good starting point for moving to compliance with the GDPR by establishing whether/what awareness-raising needs to occur and to consider existing policies and procedures.

| <b>A quick review – what is the current position</b>  | <b>Response</b><br>Yes/No/Being implemented |
|---|---|
| <b>Senior management awareness</b> <ul style="list-style-type: none"> <li>• Regularly discuss data protection</li> <li>• GDPR has been recognised as a challenge to the business</li> </ul>   |   |
| <b>Data protection policies and procedures (including retention and disposal schedules)</b> <ul style="list-style-type: none"> <li>• in place</li> <li>• compliance is monitored</li> <li>• compliance can be evidenced</li> <li>• regularly reviewed</li> <li>• communicated to staff</li> </ul>   |   |
| <b>Information security</b><br><br><b>Policies and procedures:</b> <ul style="list-style-type: none"> <li>• in place</li> <li>• compliance is monitored</li> <li>• compliance can be evidenced</li> <li>• regularly reviewed</li> <li>• communicated to staff</li> </ul> <b>Formal mechanisms in place to identify breaches and handle incidents</b> <ul style="list-style-type: none"> <li>• in place</li> <li>• compliance is monitored</li> <li>• compliance can be evidenced</li> <li>• regularly tested &amp; reviewed</li> <li>• communicated to staff</li> </ul> |   |
| <b>Clear and accessible fair processing information given to individuals</b>  |   |
| <b>New projects and initiatives</b> <ul style="list-style-type: none"> <li>• “privacy-proofed” at the planning stage</li> <li>• Reviewed during development, testing and delivery stage, i.e. pre- and post-implementation</li> <li>• ‘Privacy impact assessments’ are conducted when necessary</li> </ul>  |   |

## Section 2 - Mapping the 5W's

This section provides guidance for all controllers (and processors) in creating an inventory and map of data processing activities. In many cases, application/contact forms (hard copy or online) will often provide a good point from which to start to follow the data trail for customers and similarly for staff.

Whilst this resource follows the path below, it is only a guide to the basic thought-process. The type, complexity, volume, sensitivity or risk of the processing may require a more "in-depth" or sophisticated exercise.



The information collated will help inform the next steps – compliance with the principles and rights, and creating the "records of processing activities" required (in some cases) by Article 30 of the GDPR.

# WHY

## WHY ... is personal data processed?

**Personal data** is broadly defined in the GDPR and means any information relating to a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

**Consider all areas of the business and list all the reasons that personal data is used.**

Non-exhaustive examples of **why** personal data is used include:

- Staff administration
- Basic client administration
  - Examples of clients could be any one or more of:
    - account holder
    - customer
    - pupil
    - offender
    - patient
- Legal obligations (specify)
  - Examples include
    - AML/CFT/due diligence
    - Tax
    - Work permits
- Provision of goods or services
  - is this provided
    - Online
    - face to face
- Monitoring
  - Are any of the following used or recorded
    - CCTV
    - ANPR
    - IP address
    - Cookies
    - Apps
- Direct marketing activities
  - for self
  - for third party
  - creating/selling marketing lists
- Profiling
- Provision of processing services to a third party – but making no decisions that affect individuals
- Provision of processing services to a third party – but making decisions (alone or jointly) that affect individuals

**WHY is personal data processed?** List the reasons for processing

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |



# WHO

## WHOSE ... personal data is processed?

For **each of the reasons** identified list **all the different categories of persons** about whom personal data is processed.

Non-exhaustive examples of **categories of persons** include:

- Staff (specify: current/potential/former)
- Clients (specify: current/potential/former)
- Relatives/guardians
- Business contacts/suppliers
- Complainants, correspondents, enquirers
- Members or supporters
- Children
- Offenders and suspected offenders
- Other (describe)



# WHAT

## WHAT ... personal data is processed?

For **each reason** identified list all the different **types of personal data** recorded or used **and** identify the **source** **and** **legal basis** of the data.

### Non-exhaustive examples of types of personal data:

- Personal details - (specify - name, address, email, telephone, date of birth, emergency contact, sexual orientation, ethnicity, etc.)
- Financial details - (specify - bank account, credit card details, NI, Tax reference etc.)
- Health information
- Images/ Voice recordings
- 'Know your customer' or due diligence (specify – passport, tax reference, source of wealth etc.)
- Passport/driving licence/national ID card details
- IP address
- Criminal convictions/offences
- Biometrics - Finger print/retinal scan/DNA etc.
- Education & training
- Employment details (specify – CV, references, annual appraisals, employment status, work permit, leave, sickness etc.)

### Source of the data

- Individual themselves
- Third party individual
- Other sources – (specify)  
For example:
  - Credit reference agency
  - Criminal record check
  - Internet/Social media
  - Government departments/agencies
  - Private investigators
  - Due diligence/CDD checking companies

### Legal basis could be one or more of:

- Legal obligation (specify)
- Lawful function of public body (specify)
- Protection of vital interests of that person
- Performance of a contract
- Legitimate interests of the data controller (specify)
- Consent – (can you evidence that consent has been given?)

You will need to complete this page for each reason for processing

**WHAT personal data is processed?**

**Reason for Processing:**

| Type of personal data | Source | Legal basis |
|-----------------------|--------|-------------|
|                       |        |             |
|                       |        |             |
|                       |        |             |
|                       |        |             |
|                       |        |             |

# WHEN

## WHEN ... is personal data processed?

'Processing' includes the actions of obtaining, disclosing and deleting personal data.

For **each reason** identified establish:

- **when the personal data is obtained**
- **to whom, it may be disclosed and why**
- **how long it is retained for**

The retention period may be determined by:

### **A statutory requirement:**

- identify which particular section of law/regulation sets out the retention period
- is that a maximum or minimum period

**A business/professional practice** – what is it

**Other reason** - provide an explanation

### **NOTE:**

The GDPR does not apply to data that is anonymised in such a way that an individual can no longer be identified from the information on its own, or "reconstituted" with other data to enable identification, as it is no longer "personal data".

You will need to complete this page for each reason for processing

## WHEN is personal data processed?

**Reason for processing:**

**When is personal data obtained/updated:**

(This may be on more than one occasion)

**Disclosures:**

To whom:

In what circumstances:

**Retention period**

How long:

What determines the retention period:

# WHERE

## WHERE ... is personal data processed?

For each of the reasons for processing identified establish:

### Where processing occurs

*(may be more than one)*

- Manual records – location?
- Electronic records – format?
- In-house managed systems
- Bring your own device (BYOD)/remote working
- External hosted service – specify IOM/UK/EU/USA/another jurisdiction
- Cloud service – specify IOM/UK/EU/USA/another jurisdiction

You will need to complete this page for each reason for processing

## WHERE is personal data processed?

Reason for Processing:

Manual records location

Electronic records format(s)

Systems/services used



## Example of a personal data inventory

| WHY              | WHO                  | WHAT             |                           |   | WHEN                 |                |   |  | WHERE   |
|------------------|----------------------|------------------|---------------------------|---|----------------------|----------------|---|--|---|
|                  |                      | Type             | Source                    | Legal basis                             | Originally           | Updated        | Retention period  | Determined by:   |   |
| STAFF ADMIN      | Current staff member | Name             |                           |   |                      | As required    | Staff records retained for 6 yrs after termination unless ongoing litigation      | Employment/ limitation law                                 | Manual records - HR department/Spreadsheet held on Cloud server located IOM |
|                  |                      | Address          | Individual                | Contract                                | Appointment          | As required    |   |  |   |
|                  |                      | Contact details  |                           |   |                      | Regularly      |   |  |   |
|                  |                      | Health details   |                           |   |                      | As required    |   |  |   |
|                  |                      | CV               |                           |   | Pre-appointment      | No             |   |  |   |
|                  |                      | References       | third party               |   | Pre-appointment      | No             |   |  |   |
|                  |                      | CRB check        | third party               |   | ?                    | ?              | Copy not retained, record of number only  | CRB Code of Practice                                       |   |
|                  |                      | Passport details | Individual                | <b>Not sure - find out</b>              | ?                    | ?              |   |  |   |
|                  |                      | Work permit      | individual/ third party   |   | ?                    | ?              |   |  |   |
|                  |                      | Appraisals       |                           |   | Annually             | Regularly      | 3yrs after completion   | Standard practice  |   |
|                  |                      | Annual leave     | Individual                | Legitimate interests - staff management | At request           | As required    | <b>? Not sure - find out</b>  |  |   |
|                  |                      | Disciplinary     | individual/ third party   |   | At the time          | As required    | <b>? Not sure - find out</b>  |  |   |
|                  |                      | Tax/NI           | individual/ third party   |   |                      | As required    | <b>? Not sure - find out</b>  |  |   |
|                  | Bank account         | individual       | Contract                  | Appointment                             | As required          |                | Tax law   | <b>IOM Payroll company - not sure where data is held??</b> |   |
| Pension details  | Individual           |                  |                           | As required                             | until staff age 100  | Employment law |   |  |   |
|                  | Emergency contact    | Name             | Third party               | Vital interests                         | Appointment of staff | Regularly      | Untill staff leaves   | No business requirement                                    |   |
|                  |                      | Contact details  |                           |   |                      |                |   |  |   |
| DIRECT MARKETING | Existing customers   | Name             | Individual                | Consent of individual                   | First contact        | ?              | End of relationship (unless they still want to hear from us) or consent withdrawn | Data Protection Act  | Third party marketing provider held on cloud server in US                   |
|                  |                      | Address          |                           |   |                      | ?              |   |  |   |
|                  |                      | Email            |                           |   |                      | ?              |   |  |   |
|                  |                      | Mobile           |                           |   |                      | ?              |   |  |   |
|                  |                      | Phone            |                           |   |                      | ?              |   |  |   |
|                  | Former Customers     | Name             | Individual                | Consent of individual                   | First contact        | ?              | Relationship ended - consent still valid? <b>Find out more</b>                    | Data Protection Act  |   |
|                  |                      | Address          |                           |   |                      | ?              |   |  |   |
|                  |                      | Email            |                           |   |                      | ?              |   |  |   |
|                  |                      | Mobile           |                           |   |                      | ?              |   |  |   |
|                  |                      | Phone            |                           |   |                      | ?              |   |  |   |
|                  | Potential customers  | Name             | Third party list/internet | <b>Not sure - Find Out</b>              | ?                    | ?              | <b>? Not sure - find out</b>  |  |   |
|                  |                      | Email            |                           |   |                      | ?              |   |  |   |