Preparing for GDPR Exercise

Work through the key aspects of the "12 Steps" below and make notes where applicable.

Step	In place already?	What actions do you need to take next?	Who should do this?
Awareness			
Engage the support of senior management. Are they aware of the GDPR requirements?			
Train/update your staff			
Information you hold			
Map data flows through your system/ organisation. Where did it come from? Who do you share it with? Make a note of access permissions and all processing purposes.			
Create an Information Asset Register and identify retention periods			
Communicating Privacy Notices			
Review/update your current privacy notices – do they reflect the new requirements of the GDPR?			

Step	In place already?	What actions do you need to take next?	Who should do this?
Individual Rights including Subject Access Requests			
Do your systems help you to locate an individual's personal information?			
Is it easy to correct inaccurate information about an individual in your systems / records?			
Can individual's personal data be easily deleted on request or at the end of its retention period?			
Have you considered updating your SAR procedures and planning how you will handle requests within the new timescales (and provide any additional information)?			

Step	Do you have this in place already?	What actions do need to take next?	Who should do this?
Legal basis including Consent			
Have you identified a legal basis for processing data and can this be easily documented using existing systems?			
Are existing systems able to record consent to ensure you have an effective audit trail?			
Can consent be withdrawn easily (and logged) by an individual using your current systems?			
Children			
Do you have systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity for children under the age of 13?			

Step	Do you have this in place already?	What actions do you need to take next?	Who should do this?
Data Breaches			
Do you have the right procedures in place to detect, report and investigate a personal data breach?			
Data Protection by Design and DPIAs (Data Protection Impact Assessments)			
Do you already have a Privacy Impact Assessment (PIA) process in place?			
Data Protection Officers			
Is there someone who takes formal responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively?			
International			
Do you operate in more than one member state? If so you will need to determine where your main establishment is and identify your lead supervisory authority.			