Functional checklist

This checklist is prepared to assist InterManager members in mapping the roles, responsibilities and reporting lines of those given responsibility for preparing for GDPR. It should be noted that this checklist:

- is not an exhaustive list and each individual member of InterManager should consult the GDPR throughout the process of preparing for compliance with the Regulation to ensure that all requirements are covered;
- does not address the provision of goods and services or the monitoring of individuals; and
- does not address the GDPR requirement with respect to children.

Although the first part of this checklist is broadly sequential, and the output of some tasks will be necessary to commence work on other tasks, many of the listed issues, which are divided by functional responsibility, are likely to be performed concurrently and possibly by the same teams.		
1.	**Preliminary awareness training:** • senior management, key decision makers and line managers trained in the requirements of GDPR and the consequences of failure to comply; and • allocate budget and resources for implementation programme.	
2.	**Identify line management responsibility:** • identify and appoint the senior individual with functional responsibility responsible for compliance and reporting to the highest levels of management and establish reporting protocols including scope and frequency of reporting; and • nominate those with management responsibility for the change of management that will be necessary, including the managers/team leaders/supervisors of all areas of the business that receive, hold, process, transmit or have access to personal data.	
3.	**Produce project management timeline for compliance.**	
4.	**Identify and appoint a data protection officer (DPO):** • if large scale monitoring of individuals is performed or large scale processing of special categories of data or data relating to criminal convictions and offences is undertaken, it will be necessary to appoint a DPO; • even if not mandatory, consider whether the appointment of a DPO is beneficial; • if the DPO appointed is a 'formal DPO' ensure procedures are in place to comply with the requirements of the Regulation; and • notify the relevant supervisor authority.	
5.	**Support the data protection leads:** • provide appropriate training for (a) implementation of GDPR and (b) the management of GDPR once enforced; and • document and implement reporting procedures to senior management.	
6.	**Training:** Identify needs based training for staff. It may be necessary to conduct the training in phases as preparation for compliance with the GDPR progresses. By way of example, a standalone module may be desirable addressing only an introduction to GDPR and the initial information data audit (see below). Once the procedures have been finalised and implemented, training will be necessary in following the procedures for existing staff (with refresher training as necessary) for new joiners and those that change role and ensure training is recorded.	

7.	**Commence initial information data audit:** Each team that (a) has access to; (b) processes; and/or (c) has control over personal data, should categorise each item of personal data and identify: • what the personal data is; • where it comes from; • where it is held; • how long it is held for; • who has access to it and why; • whether the data subject has provided consent to that data being held and if so how; • how the consent records are maintained and accessed; and • who the data is provided to and if so why.	
8.	**Map the data flows:** From the information data audit, map the flow of data (a) within each business unit, (b) between business units, (c) to entities outside of the business, and (d) from entities outside the business (identifying whether the data flow is cross border).	
9.	**Undertake a risk assessment based on the output of the initial information data audit and the mapped data flows:** Based on the information obtained for each item of data, ascertain what procedures and security measures you need to put in place to comply with the legal requirements of the GDPR in respect of: • why each item of data is required; • confirm and record the lawful basis for (a) holding each item of data and (b) the processing activities that you subject that data to; • how informed and lawful consent is obtained from the data subject to hold the data; • how the data is held securely; • who has access to the data and why; • who processes the data and why; • the length of time that you hold the data; • the circumstances under which the data may be passed on and how the personal data is protected (a) during transfer and (b) once held by any party outside of the business; • how you record the movement of data; • how you identify and manage cross border movement of data; and • how you rectify data that is incorrect, including data that was incorrect when transferred.	
10.	**Draft the company's data protection compliance policy.**	
11.	**Review systems, services and equipment used for storing data and upgrade if necessary to meet acceptable security standards. Document:** • procedures for ensuring effectiveness of security software; • systems reviews; and • ascertaining integrity of externally provided services.	

The remaining tasks can for the most part be run concurrently with the teams responsible for each task co-ordinating and providing feedback to other teams as necessary. A supervisor/co-ordinator should be appointed to set project management time lines and monitor/manage slippage.		
12.	**Prepare privacy notices:** • these explain the lawful basis for processing personal data in your privacy notices; and • has your business reviewed your current privacy notices and does it have a plan in place to make any necessary changes in time for the GDPR implementation?	
13.	**Review and if necessary update consent procedures:** • how is consent sought, recorded and managed; • how can data subjects withdraw consent (should be as easy as providing it); and • implementation of an effective audit trail that can be used to demonstrate compliance with the consent procedures.	
14.	**Identify and document the procedures you need in order to provide the data subject with the mandated information:** • contacts; • purpose and legal basis for processing the personal data; • identity of the recipients of the data; • where applicable the cross border transfer of the personal data and safeguards employed; • the period the personal data will be held for, or the criteria to determine that period; and • the right to lodge a complaint with a supervisory body.	
15.	**Identify and document the procedures and contact points you need to ensure you can address the rights of individuals under GDPR:** • provision of information to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language; • handling requests from individuals for access to their personal data within the new timescales mandated in the GDPR; • mechanisms in place to notify affected individuals when a breach is likely to result in a high risk to their rights and freedoms; • correcting data errors; • ensuring errors in data that has been passed on has been rectified; and • provision of information within required timescale relating to access to data, rectification; erasure, restriction of processing and objection to the holding and/or processing of data.	
16.	**Identify and document the procedures you need to deal with breaches:** • implement appropriate procedures to ensure personal data breaches are detected, reported and investigated effectively; and • does your business have mechanisms in place to assess and then report relevant breaches to the ICO where the individual is likely to suffer from some form of damage e.g. through identity theft or confidentiality breach?	
17.	**Prepare data compliance procedure methodology:** Commence mapping the procedures necessary to comply with the GDPR and manage the risks identified in the risk assessment. This may include, though not necessarily be limited to: • identifying the lawful basis for (a) holding each item of data and (b) the processing of that data; • security measures;	

	• consent procedures; • determining the length of time that personal data can be held for; • recording the handling and movement of personal data; and • procedures when data is provided to entities outside of the business.	
18.	**Document the data management and processing procedures:** Based on the mapping exercise above; prepare your core documented procedures. These should demonstrate that you have implemented appropriate technical and organisational measures to ensure data protection in respect of your data collection, holding and processing activities.	
19.	**Identify and document the general management procedures required by GDPR:** In addition to documenting the data management and processing procedures, you will need to put in place overarching management procedures either to comply with specific requirements of GDPR or to ensure proper implementation and governance of GDPR. • the responsibilities, reporting lines, authorities and permissions of all those accessing, involved in handling, processing, controlling and managing personal data as well as those tasked with ensuring compliance with the GDPR; • when to conduct a data protection impact audit (DPIA) and the processes necessary to action this; • training requirements; and • monitoring and audit.	
20.	**Supervisory authority:** If your business operates in more than one EU member state, you will need to identify and document the lead supervisory authority.	
21.	**Consider cyber insurance.**	

Maria Pittordis/Ian MacLean
Hill Dickinson