Checklist for employers on preparing for GDPR

		Yes/No/N/A
1	Educate your board and senior leadership team with a GDPR awareness session.	
2	Review whether you need to appoint a Data Protection Officer (DPO). DPOs are mandatory for public authorities, organisations whose activities involve the regular and systematic monitoring of data subjects on a large scale, or organisations who process sensitive personal data on a large scale. If you need one, get them appointed now.	
3	Set up a project team - this should be made up of all relevant departments and a project manager should be appointed. The DPO (if one is appointed) should be heavily involved in the project.	
4	Send data questionnaires to all departments requesting information on what personal data they hold and why. Set a deadline for the information to be returned.	
5	Compile the information returned by the departments to create a personal data life-cycle and inventory – this should set out: - the personal data the organisation collects and processes; - the reason that the organisation collects and processes the personal data; - how long the organisation retains the personal data and the reasons why; - how the organisation destroys the data; - the security measures the organisation uses to ensure the personal data is secure; and - what third parties it is shared with and why?	
6	Review the personal data life-cycle and consult with relevant departments over any proposed problem areas or areas of high risk. Create a project plan on how these particular risks are going to be managed and mitigated. If there are very high risks to personal data identified in your business then you will need to carry out a Privacy Impact Assessment.	
7	Review the personal data life-cycle to ascertain when and why personal data may be shared by the organisation with third parties and document the basis for this e.g. payroll providers, insurers. Review the contracts you have in place with these third-party processors and find out what security measures they have in place.	
8	Agree and implement a plan on how the organisation will handle data requests. Document the policy and train staff. Data access requests must be dealt with within 1 month under GDPR. This means you may need to put procedures and IT solutions in place so they can be dealt with quickly.	
9	Review all your privacy notices (to employees, customers/users as appropriate) to ensure they comply with GDPR requirements so that the data subjects are fully informed about how their data is used.	
10	Review and document the legal basis for which you collect and process data. If you are relying on consent this should be reviewed and another basis relied on where possible (especially when it comes to employees).	

	If you can only rely on consent then you need to consider if that consent complies with GDPR requirements and document how it does. It may need to be sought again to comply with GDPR. Under GDPR, consent must be explicit and unambiguous and capable of being withdrawn.	
11	Review or implement procedures to detect, report and investigate a data breach as generally these must now be reported to the Data Protection Commissioner within 72 hours. The process you need will depend on the type of personal date you hold and how it is held. Security measures and detecting breaches will require the input of your IT team or provider.	
12	Train your staff on GDPR and any processes and procedures you have brought in as a result of your GDPR readiness review. Build this into your annual training programmes.	
13	Make sure all new projects being considered and implemented by the organisation also consider any data protection issues that are relevant to the project.	
14	Document everything you have done to become GDPR compliant and put an audit plan in place to show continuous monitoring and improvement	