Checklist for GDPR Compliance for HR

Step	Action/Task	Completed
1	Undertake an audit of all HR procedures, policies and processes that involve processing personal data.	
2	Document what data is being processed, for what reason, where it comes from, where it goes, how long it is held and how you dispose of it. If you have employees in countries outside the EU, note the special arrangements that may be required for sharing/sending data.	
3	Document the lawful reasons for processing each stream of data (if there is more than one reason for any stream then document it)	
4	Decide how you will provide Privacy Notices to employees. You may do this at different stages in the employment relationship, but review documents such as application forms, medical consent letters, and your data protection policy. Remember that as well as advising employees about what data you are processing and why and how, you must also advise them of the valid legal reason for processing. If processing 'special category data', you will have to provide the valid reason under ordinary and special category data.	
5	Update or develop a data protection policy including the requirements of privacy notices but also include information about what breaches of security look like and how they should be reported.	
6	Decide how you will advise employees of any changes to the data you are processing.	
7	Decide how you will ensure that employees' data is kept accurate and relevant.	
8	Review how data is disposed of to ensure it is done securely.	
9	If you have relied on 'consent' as a valid reason for processing in the past, review this in light of the ICOs advice that it may no longer be valid.	
10	Update your subject access request process and ensure all relevant staff are aware of what is required, by when, and what should not be provided.	
11	Develop a process for documenting and reporting data security breaches.	
12	Integrate Privacy Impact Assessments into the early stages of your project management processes.	
13	Review your contracts with third parties and update or draft a written contract confirming that they are aware of and meeting their data protection obligations.	
14	Consider whether to nominate a Data Protection lead or a designated Data Protection Officer.	
15	Undertake the ICO self-assessment to check your readiness.	

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/