GDPR CHECKLIST

For more information, check https://www.analyticsinhr.com/blog/general-data-protection-regulation-gdpr-impact-hr-analytics/

Full text of GDPR: https://gdpr-info.eu/

Note: we refer in this document to employees when we talk about data subjects. These can, however, also be contractors!

OVERVIEW OF DATA AND STORAGE	YES	NO	COMMENT
1) We have an overview of all types of personal data we store, the source of information, who we share it with, what we do with it, and how long we keep it			
2) We have an overview of the places where we store data			
3) We have an overview of the data flows between de places we store data			
PERSONAL DATA AND DATA TRANSFER			
1) We have communicated which data is processed			
2) We have communicated for which purpose data is processed			
3) We have communicated where the data is collected			
4) We have communicated with whom the data is shared			
5) The company's privacy policy is publicly available and easily accessible			
6) We have communicated which data is transferred abroad			
7) We have taken sufficient safety measures to transfer data			
8) We have taken special safety measures when data is transferred outside the European Economic Area			
9) We have communicated which safety measures we've taken to secure data			

COMMUNICATION OF EMPLOYEE RIGHTS			
1) We have communicated how employees can access their own data			
2) We have communicated how employees can enforce their right to erasure (a.k.a. ask for their data to be deleted)			
3) We have communicated how employees can rectify their own data			
4) We have communicated how employees can ask to receive his/her own personal data			
5) We have communicated how long we will keep employees data			
6) We have communicated all the purposes that we will use employee data for			
7) Employees can easily enforce the rights mentioned above			
8) **All purposes** that we use employee data for are communicated to the employees and explicitly agreed on by them			
ENFORMCEMENT OF EMPLOYEE RIGHTS			
1) We have procedures in place to give employees access to their own data when asked			
2) We have procedures in place to erase employee data when asked			
3) We have procedures in place to rectify employee data when asked			
4) We have procedures in place to transfer personal data of a subject when asked			
DPO			
1) We have a Data Protection Officer (DPO) in our company			
2) The DPO has a clear task description			

3) We have a procedure in place what to do when data is leaked/stolen/hacked/lost			
4) We have a procedure in place to contact the DPO in case of an emergency			
DATA PROTECTION IMPACT ASSESMENT AND DATA PROCESSING AGREEMENT			
1) When using new technologies or exploring possibilities of new analysis that is likely to pose a high risk for the rights and freedom of employees, we have procedures in place to conduct a data protection impact assessment (DPIA)			
2) All third parties that process or will process data have signed a Data Processing Agreement (DPA)			
3) All third party processors apply state-of-art security measures which are defined in the DPA			
4) The data processor is certified in conformity with ISO27001/2 standards or other, similar standards			
5)			