

Key Considerations When Handling Employee Data

Reviewing what information your organisation collects and how it is used can help identify gaps in transparency, security and compliance.

 **The Information You Collect**
Identify the employee, worker and candidate information held by the organisation. Employers should collect only the information genuinely required for a clear employment or business purpose.

 **Your Lawful Basis**
Establish the lawful basis relied upon for each type of processing. Employers should not automatically rely on consent, as the imbalance within an employment relationship can make it difficult to show that consent was freely given.

 **Special Category Data**
Make sure employees and candidates understand what information is collected, why it is used, who it may be shared with and how long it will be kept. Privacy notices should be reviewed when practices or technology change.

 **Privacy Information**
Gather relevant documents, interview the individuals involved and give the person accused an opportunity to respond. The investigation should be impartial and proportionate to the seriousness of the allegation.

 **Workplace Monitoring**
Consider whether monitoring is necessary, proportionate and limited to a defined purpose. Employees should normally be told what is monitored and why, and less intrusive alternatives should be considered.

-  **Data Protection Impact Assessments**
Assess whether a data protection impact assessment is required before introducing high-risk monitoring or technology. The assessment should identify privacy risks and the measures that will be used to reduce them.
-  **Access and Security**
Limit access to workforce information to those who genuinely need it. Sensitive records, including medical information, should be stored securely and kept separate where appropriate.
-  **Retention and Deletion**
Establish how long different categories of employee information should be retained. Records should be deleted securely when there is no longer a legal or legitimate business need to keep them.
-  **Employee Rights**
Ensure managers can recognise subject access requests and other employee data rights. Requests do not need to use formal wording or specifically refer to data protection law to be valid.
-  **Employee Exits**
Review access permissions, devices, accounts and stored information when employment ends. Exit procedures should protect both personal information and the organisation's confidential business data.



Chester Office
Knights Court
1 Weaver Street
Chester, Cheshire
CH1 2BQ
01244 354 800



Liverpool Office
3rd Floor
No. 4 St Paul's Square
Liverpool
L3 9SJ
0151 321 0000