

UK GDPR Checklist for HR Data

Overview – helpful guide thinking about HR data not all encompassing etc. for internal use

|  |  |
| --- | --- |
| Action | Completed |
| Data Protection |
| Audit your processing activities. |[ ]
| Ascertain what personal data your HR team processes. |[ ]
| In respect of each category of data: |
| * Identify a legal background for processing the data.
 |[ ]
| * Identify how this was obtained.
 |[ ]
| * Identify why this was originally gathered.
 |[ ]
| * Identify how long you will retain the information.
 |[ ]
| * Identify how secure it is in terms of encryption and accessibility.
 |[ ]
| * Identify whether it is shared with any third parties and on what basis you might do so.
 |[ ]
| * Give data subjects privacy notices about their rights.
 |[ ]
| * Consider whether a privacy impact assessment needs to be carried out before processing.
 |[ ]
| Review third party agreements if you transfer any personal data to third parties. |[ ]
| Data Protection Officers |
| Consider your requirements for a DPO. |[ ]
| Agree a job description/job tasks. |[ ]
| Appoint and train a DPO. |[ ]

|  |
| --- |
| Processes and Procedures |
| Ensure that the processing of all employee data falls within one of the stipulated processing conditions and document in writing. |[ ]
| Ensure you have processes and procedures in place for the following: |
| * Security of personal data
 |[ ]
| * Retention and destruction of personal data
 |[ ]
| * Electronic communications e.g. deletion of personal emails
 |[ ]
| * Other individual rights e.g. the right to be forgotten/have data removed
 |[ ]
| * Identification, recording and reporting of data handling breaches
 |[ ]
| * Response to Data Subject Access Requests
 |[ ]
| Data Transfers Inside and Outside the EEA |
| Identify whether personal data is transferred outside the EEA e.g. online service providers. If so: |
| * Justify each transfer using one of the conditions or exceptions.
 |[ ]
| * Record each transfer.
 |[ ]
| Data Subject Access Requests |
| Update DSAR policy with a comprehensive process; ensuring DSARs are dealt with in the required timeframe. |[ ]
| Agree what a “manifestly unfounded or excessive request” looks like for your School/MAT. |[ ]
| Review IT systems. |[ ]
| Train staff on the new requirements; ensuring they understand how to recognise a request, who it should be passed to and the urgency involved. |[ ]
| Handling Breaches |
| Have a robust procedure in place to detect, report and investigate breaches and communicate this to all employees. |[ ]
| Train appropriate colleagues on how to handle breaches. |[ ]
| Create a register to record breaches |[ ]
| Consider insurance cover, where required. |[ ]
| Privacy Notices |
| Review and revise privacy notices; ensuring all the rights individuals have are covered, including how to delete personal data or provide data electronically. |[ ]
| Review business procedures. |[ ]
| Familiarise yourself with ICO code of practice and identify high risk areas. |[ ]
| Determine who should conduct PIAs (Privacy Impact Assessment) and what resources they require. |[ ]
| Data Subject Rights |
| Train staff responsible for responding to requests relating to the rights of the new regime. |[ ]
| Ensure Line Managers and HR departments understand how to recognise a request from a data subject seeking to exercise their rights and how they should respond. |[ ]
| Ensure comprehensive processes are in place for dealing with each of the rights. |[ ]
| Training and Communication |
| Train Line Managers, HR department and any other individuals who regularly process personal data. |[ ]
| Raise awareness amongst staff about the importance of data protection and their responsibilities. |[ ]
| Review existing data privacy notices to inform individuals of the collection of their data. Identify gaps between the level of data collection and the processing undertaken by the School and how aware staff and service users are. |[ ]