**General Data Protection Regulation:**

**Checklist and Audit Tool**

|  |  |
| --- | --- |
| **STEPS TO TAKE** | **✓ COMPLETED** |
| **AWARENESS** |  |
| 1. | Are decision makers and key people in the business aware that the law around data protection is changing? |  |
| 2. | Does the business understand and appreciate the impact GDPR is likely to have? |  |
| 3. | Has the business highlighted areas which could cause compliance issues under GDPR? |  |
| 4. | Has the organisation raised awareness across the whole business that the GDPR could impact business practices from May 2018? |  |
| 5. | Is the business aware of the potential resource implications of GDPR? |  |
| **STRATEGY** |  |
| 6. | Have you set out a strategy of the steps you will take to implement GDPR? |  |
| 7. | How will you measure how you are performing against your objectives? |  |
| **POLICIES, PROCEDURES AND PROCESSES** |  |
| 8. | Have you checked your existing data protection policy and related policies to ensure they are up to date with the requirements of GDPR? |  |
| **AUDIT** |
| 9. | Do you have a system in place that monitors compliance with the data protection policy? |  |
| 10. | Do you regularly review the effectiveness of data handling/processing activities and security controls? |  |
| **AWARENESS** |
| 11. | Do you have data protection training in place for staff? |  |
| **INFORMATION YOU HOLD** |  |
| 12. | Have you documented what personal data you hold, where the data has come from and who you share the data with? |  |
| 13. | Have you considered an information audit to help you understand the types of data you hold? |  |
| 14. | Have you identified where you may be operating as a ‘data processor’ as well as a ‘data controller’? |  |
| **LAWFUL BASIS FOR PROCESSING DATA** |  |
| 15. | Have you identified what types of processing you undertake and the reason for the processing? |  |
| 16. | Having identified the types of processing you carry out have you identified and documented the lawful basis on which you are processing data? |  |
| 17. | Have you explained the lawful basis in your privacy notices? |  |
| **PRIVACY NOTICES** |  |
| 18. | Have you reviewed and updated privacy notices in line with the requirements of GDPR in advance of the commencement of GDPR? |  |
| **CONSENT** |  |
| 19. | Have you checked how you seek, record and manage consent? |  |
| 20. | Can you confirm the following statements when considering the issue of consent as a legitimate reason for processing personal data?**Asking for consent**1. We have checked that consent is the most appropriate lawful basis for processing.
2. We have made the request for consent prominent and separate from our terms and conditions.
3. We ask people to positively opt in.
4. We don’t use pre-ticked boxes, or any other type of consent by default.
5. We use clear, plain language that is easy to understand.
6. We specify why we want the data and what we’re going to do with it.
7. We give individual options to consent to independent processing operations.
8. We have named our organisation and any third parties.
9. We tell individuals they can withdraw their consent.
10. We ensure that the individual can refuse to consent without detriment.
11. We don’t make consent a precondition of a service.
12. If we offer online services directly to children (i.e. work experience placements or recruitment), we only seek consent if we have age-verification and parental-consent measures in place.

**Recording consent** 1. We keep a record of when and how we obtain consent from the individual.
2. We keep a record of exactly what they were told at the time.

**Managing consent** 1. We regularly review consents to check that the relationship, the processing and the purposes have not changed.
2. We have processes in place to refresh consent at appropriate intervals, including any parental consents.
3. We consider using privacy dashboards or other preference management tools as a matter of good practice.
4. We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
5. We act on withdrawals of consent as soon as we can.
6. We don’t penalise individuals who wish to withdraw consent.
7. Post May 2015 we do not intend to rely on any consents that do not meet the requirements of the GDPR.
 |  |
| **THE RIGHTS OF INDIVIDUALS** |
| 21. | Have you checked and where necessary updated your procedures to ensure you can deliver the rights of individuals under the GDPR in relation to:-1. Right to be informed
2. Right of access
3. Right to rectification
4. Right to erasure
5. Right to restrict processing
6. Right to data portability
7. Right to object
8. Right not to be subject to automated decision making including profiling
 |  |
| **SUBJECT ACCESS REQUESTS** |  |
| 22. | Have you reviewed your procedures and processes to handle SARs under the new timescales? |  |
| 23. | Are business stakeholders appropriately trained on the changes to SARs and able to apply the new processes? |  |
| 24. | If your department currently handles a large number of SARs, have plans/resource been put in place to deal with the reduced timescale? |  |
| **DATA BREACHES** |  |
| 25. | Do you have procedures in place to detect and investigate personal data breaches? |  |
| 26. | Do you have procedures in place to report a data breach (if necessary under GDPR) to the ICO and (if necessary) to the individual(s) concerned? |  |
| 27. | Are colleagues appropriately trained on identifying when a data breach should be reported to the ICO and or the individual(s) concerned? |  |
| 28. | Do you have a procedure in place to keep a record of all data breaches (whether notifiable or not) containing:1. The facts of the data breach
2. The effects of the data breach
3. The action taken
 |  |
| **COMPLIANCE** |  |
| 29. | Is there someone within the HR team with responsibility for data protection? |  |
| 30. | Have you assessed under the GDPR whether you are formally required to appoint a data protection officer?1. Do you carry out large scale systematic monitoring?
2. Do you carry out large scale processing of special categories of data or data relating to criminal convictions and offences?
 |  |
| **CHILDREN** |  |
| 31. | Do you have systems in place to verify age? |  |
| 32. | Do you have a procedure in place to obtain parental or guardian consent for any child under 16? |  |
| **INTERNATIONAL ACTIVITIES** |  |
| 33. | If you operate in more than one EU member state have you determined who your lead data protection supervisory authority is and documented this? |  |
| **RECORDS OF PROCESSING ACTIVITIES** |  |
| 34. | If you have more than 250 employees have you been keeping suitable records of your processing activities including-1. The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection office.
2. The purposes of the processing.
3. A description of the categories of data subjects and of the categories of personal data.
4. The categories of recipients to whom the personal data have been or will be disclosed including recipients in non-EEA countries or international organisations.
5. Where applicable, transfers of personal data to a non-EEA country or an international organisation, including the identification of that country or international organisation and, in the case of transfers, the documentation of suitable safeguards.
6. Where possible, the envisaged time limits for erasure of the different categories of data.
7. Where possible, a general description of the technical and organisational security measures taken.

If you have less than 250 employees you do not need to keep the records above unless:* The processing you carry out is likely to result in a risk to the rights and freedoms of data subjects.
* The processing is not occasional.
* The processing which you carry out includes special categories of data or personal data relating to criminal convictions and offences.
 |  |
| **DATA PROTECTION BY DESIGN AND DEFAULT** |  |
| 35. | Have you implemented appropriate technical and organisational measures to show you have considered and integrated data protection into your processing activities? |  |
| **DATA PROTECTION IMPACT ASSESMENTS** |  |
| 36. | Have you established whether your processing activities fall under the requirement in the GDPR for you to have to undertake data protection impact assessments?1. Will you be using a new technology, and taking into account the nature, scope, context and purposes of the processing, is it likely to result in a high risk to the rights and freedoms of individuals?

**OR**1. Do you use systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects or significantly affect individuals?

**OR**1. Do you process on a large scale, special categories of data or of personal data relating to criminal convictions and offences?

**OR**1. Do you undertake systematic monitoring of a publicly accessible area on a large scale?
 |  |
| 37. | Do you have an individual appointed with responsibility to determine whether a DPIA is required? |  |
| 38. | If a DPIA is required, do you have a suitably experienced individual to carry out the DPIA? |  |
| 39. | If a DPIA indicates there is high risk, who in the organisation can help address these risks? |  |
| 40. | If any risks cannot be sufficiently addressed to the requirements of GDPR, is there a procedure in place to consult the ICO and who in the organisation will do this? |  |