|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **GDPR Checklist**  | **V2 2.2018** |  |
| Priority (**C**HML) | Item | Action | Next Steps | Owner | Review Date | Completed Date |
|  | GovernanceG1 | Decision whether to appoint a formal Data Protection Officer or non-statutory responsible person. Necessary or optional?Article 37-39 |  |  |  |  |
|  | G2 | Completion of DPO (or equivalent) training and job specification and authority level  |  |  |  |  |
| C | G3 | Project Team in place for implementation of GDPR.Should privacy be a standing item on the board agenda? Process for escalating privacy issue appropriately |  |  |  |  |
|  | G4 | GDPR Record Keeping process in place (250 employees or more or processing particular types of data only) Article 30 |  |  |  |  |
|  | G5 | Records for decision making process of GDPR implementation e.g. project plans, meeting minutes, board minutes |  |  |  |  |
| H | G6 | Process in place for using data protection impact assessments (PIA) Article 35 when assessing privacy impact and risks to individuals |  |  |  |  |
| H | Lawful Processing L1 | Data audit complete – reviewed and signed off by board |  |  |  |  |
| H | L2 | Legitimate Business Interest Assessment(s) completed and signed off by board |  |  |  |  |
| H | L3 | Decisions taken on appropriate grounds for lawful processing (Article 6-11) |  |  |  |  |
| H | L4 | Retention Policy reviewed and signed off by board – Candidates, Clients Contacts, Employees, Suppliers, Others |  |  |  |  |
|  | L5 | Decision taken on when consent is necessary or appropriate ground for lawful processing. Process reviewed and agreed on how consent should be obtained and process if withdrawn or not given (Article 7 and 8) |  |  |  |  |
|  | L6 | Review marketing policy and define what marketing is within your group |  |  |  |  |
| C | Security S1 | Review IT system data security – engage with your suppliers, IT team and system experts -  |  |  |  |  |
| H | S2 | Review personnel system security e.g. passwords, confidentiality, use of BYOD, remote access controls |  |  |  |  |
| C | S3 | Crisis Management: Ownership, policy and process for handling security of personal data, breach notification (within time limits) to supervisory authority and to data subject if high risk breach. |  |  |  |  |
| H | S4 | Segregation of Data – special categories of data or confidential data e.g. passport details, segregated and with limited access. |  |  |  |  |
|  | S5 | Review of storage of data hard copy/soft copy and use of email |  |  |  |  |
|  | Third Parties TP1 | Clarity around controller, processor and joint controller relationships with third parties |  |  |  |  |
|  | TP2 | Review business contracts – own terms, client own terms - controller/joint controller clauses as appropriate |  |  |  |  |
|  | TP3 | Intra group data sharing agreements in place– controller/processor and/or joint controllers |  |  |  |  |
|  | TP4 | Controller-Processor terms in place with suppliers (and companies you supply to as processor) |  |  |  |  |
|  | TP5 | Analysis completed of third party processing of your personal data outside EEA – legitimacy of processing assessed. Model terms, Binding Corporate Rules or adequacy in place. |  |  |  |  |
|  | Employees Emp1 | Employee Privacy Notice drafted, approved and communicated |  |  |  |  |
|  | Emp 2  | Review of internal policies including employee, internet and IP policies completed and communicated |  |  |  |  |
|  | Emp 3 | Employee code of practice around use of personal data and behaviour completed and communicated |  |  |  |  |
|  | Emp 4  | Staff Training Programme  |  |  |  |  |
|  | Data Subject Rights DS1 | Subject Access Request Process in place |  |  |  |  |
|  | DS2 | General Complaints Process in place  |  |  |  |  |
|  | DS3 | General Data Management Process in place – handling data corrections and setting DS preferences e.g. no mailshots |  |  |  |  |
|  | DS4 | Policy and Process for handling GDPR Right requests within 30 day time limits: deletion, removal, objection to processing, suspension and restriction of processing, request to transfer data to another party.  |  |  |  |  |