

SELF-ASSESSMENT QUESTIONNAIRE: COMPLIANCE WITH DATA PROTECTION OBLIGATIONS WHEN PROCESSING PERSONAL DATA.

This Questionnaire is aimed at those who have responsibilities for data protection, and should be answered (i.e. by the nominated person who is responsible for data protection in your organisation); it will also help managers and administrators understand the full range of data protection issues which are faced whenever personal data are processed. The Questionnaire also seeks to identify weaknesses in compliance procedures.

If a question is not relevant to your particular processing circumstances, please enter N/R. Since each question is based on a statutory obligation which the Controller or Processor has towards the protection of personal data and the Data Subjects involved, it is important to double check that you are not overlooking something which could make your processing unlawful. If the answer remains `N/R`, you are advised to consult an authorised officer of the Data Protection Office.

The Data Protection Office advises data controllers and data processors to implement the requirements found in the questionnaire. This Office may also request you to fill in the questionnaire before carrying out security checks on your premises under sections 14 and 27 of the DPA.

A. GENERAL MANAGEMENT

- ✓ Do you have a Policy on data protection in your organisation?

- ✓ If yes, how do you judge the policy?

- ✓ If yes, when was the policy last reviewed?

- ✓ Is the policy adequately resourced, and supported by a management infrastructure that can sustain, monitor and review the Policy and generate reports on its effectiveness?

- ✓ If the answer to the above question is 'Yes', how well do you think the Policy is promoted and supported by management?

- ✓ Is there an identifiable person responsible for data protection within your organisation?

- ✓ If the answer to the above question is 'Yes', how is that person supported by management for data protection matters?

- ✓ Do all individuals who are authorised to process personal data (e.g. staff) receive appropriate training, instruction or guidance on data protection?

- ✓ If the answer to the above question is 'Yes', how do you judge the training given?

- ✓ Are you confident that all individuals (e.g. staff) who process personal data understand their data protection obligations associated with that processing?

- ✓ If there are contracts, associated with the processing of personal data, which allow third parties access to personal data, for example data processors, do these contracts specify data protection requirements?

- ✓ If the answer to the above question is 'Yes', how well do you judge the effectiveness of the monitoring/auditing of contractual controls?

- ✓ Is there a folder of documents, or other documentation, which will help to manage and demonstrate compliance with data protection obligations?

- ✓ If the answer to the above question is 'Yes', what is your view on the quality of the information in the folder or in other documentation?

B. LAWFULNESS OF PROCESSING

- ✓ Has the full extent of the processing, which is authorised by law and/ or regulations, been identified?

- ✓ Has proof of lawful processing been retained?

C. TRANSPARENCY OF PROCESSING

- ✓ Are Data Subjects made aware, before they provide personal data, of why personal data is being collected and which organisations will use their data?

- ✓ Are there significant practical or technical difficulties in providing the details identified above?

- ✓ Are there reasons (e.g. in the public interest) for not providing such information?

- ✓ When personal data about Data Subjects are provided by other organisations or individuals, are these Data Subjects made aware of why personal data is collected and which organisations will use the data?

- ✓ Is there a significant technical or practical difficulty in providing the details identified above?

- ✓ Are there reasons (e.g. in the public interest) for not providing such information?

D. QUALITY OF PERSONAL DATA

- ✓ Is personal data assessed as to whether it is 'adequate, relevant and not excessive' in the context of each particular purpose?

- ✓ Are there significant practical or technical difficulties in meeting these criteria in all circumstances?

- ✓ Are there reasons (e.g. in the public interest) for retaining the personal data since the personal data might become relevant in the future?

- ✓ Is personal data assessed for accuracy and checked whether up to date?

- ✓ Are there significant practical or technical difficulties in carrying out such assessments?

- ✓ Before action is taken against a data subject, is the accuracy of the personal data checked?

- ✓ Are there significant practical or technical difficulties in carrying out such checks?

- ✓ Do formal criteria/procedures for the deletion of personal data exist?

- ✓ Are there significant practical or technical difficulties in deleting personal data?

- ✓ Are there reasons (e.g. in the public interest) for not deleting some or all of the personal data?

E. SECURITY OF PERSONAL DATA

- ✓ Is there a security policy that covers all aspects of the processing of personal data?

- ✓ If the answer to the above question is 'Yes', how do you judge the security policy?

- ✓ If the answer to the above question is 'Yes', how well is the security policy supported and promoted by management?

- ✓ Do security controls or procedures include measures to ensure the integrity of the personal data and of its processing?

- ✓ How effective do you consider the controls/procedures to be?

- ✓ Do security controls or procedures include measures to permit user identification, authentication and authorisation for processing?

- ✓ How effective do you consider the controls/procedures to be for the above question?

- ✓ Do security controls include measures to safeguard operating procedures?

- ✓ How effective do you consider the controls/procedures to be for the above question?

- ✓ Do security controls or procedures include measures to facilitate the use of encryption?

- ✓ Do security controls or procedures include measures to invoke a business continuity/ disaster recovery plan?

- ✓ Are there significant practical or technical difficulties in forming such a plan?

- ✓ Do security controls or procedures include measures to establish adequate audit and monitoring arrangements?

- ✓ How effective do you consider these arrangements to be?

- ✓ Do security controls or procedures include measures to safeguard the physical

security of the processing environment?

- ✓ How physically secure do you consider your processing of personal data to be?
- ✓ Are staff trained in the necessary security controls and procedures?
- ✓ If the answer to the above question is 'Yes', how do you judge the training given?
- ✓ When did you last receive training/instruction on IT security requirements?

F. DATA SUBJECTS' RIGHTS

- ✓ Do procedures allow for Data Subjects to be informed of the nature of the processing of personal data, and to receive confirmation as to whether or not personal data about them is processed?
- ✓ Are there significant practical or technical difficulties in providing such information?
- ✓ Are there reasons (e.g. in the public interest) for not providing such information?
- ✓ Do procedures allow Data Subjects to exercise their right of access to personal data which relate to them?
- ✓ Are there significant practical or technical difficulties in providing such information?

- ✓ Are there reasons (e.g. in the public interest) for not providing such data?

- ✓ Do procedures allow Data Subjects to be informed of the logic underpinning any decision-making processing which significantly impacts on them and to challenge such decisions?

- ✓ Are there significant practical or technical difficulties in providing such information?

- ✓ Are there reasons (e.g. in the public interest) for not providing such data?

- ✓ Do procedures have the capability to correct, block or erase personal data (e.g. . in compliance with requests from Data Subjects and/or from the Data Protection Office or Courts), and to notify Third Parties who have received the Data Subject's personal data?

- ✓ Are there significant practical or technical difficulties in providing such information?

- ✓ Do procedures allow Data Subjects to object to the processing of personal data?

- ✓ Are there reasons (e.g. in the public interest) for not allowing such objections?

G. NOTIFICATION

- ✓ Has a comprehensive census of the processing of personal data been carried out?

- ✓ When was the census carried out?

- ✓ Do procedures anticipate the need to notify details of the processing to the Data Protection Office?

- ✓ Are there practical or technical difficulties in providing such notification?

- ✓ Are there reasons (e.g. in the public interest) for not providing such a notification?

H. SYSTEM DESIGN

- ✓ Are data protection considerations taken into account during the development, purchase or acquisition of hardware and software?

- ✓ Are changes to the software or processing environment considered in the context of data protection obligations?