Veritau Group

Data Protection Policy

Contents

Veritau Group

Data Protection Policy

POLICY STATEMENT

1 The Group processes a significant amount of personal data. This includes data it holds in its own right (for example employee records) and data held on behalf of its client organisations. The Group has a responsibility to ensure this data is adequately protected. This policy sets out guidance and measures to ensure the Group fulfils this responsibility.

PURPOSE AND OBJECTIVES

2 Data, including personal data, is a resource which must be effectively managed and protected like other resources. This policy aims to guide the Group in managing the personal data it holds, and in achieving the following objectives:

- protecting the rights of data subjects;
- fulfilling its obligations under data protection law

3 The UK GDPR and the Data Protection Act 2018 (DPA) provide the principal legal framework relating to personal data and this policy explains how their provisions will be applied by the Group.

4 This policy should be read in the context of the Group's overall information governance policy framework.

SCOPE

5 The companies comprising the Veritau Group are:

- Veritau Ltd
- Veritau North Yorkshire
- Veritau Tees Valley

6 Each is a separate legal entity and each is a data controller in its own right, registered as such with the Information Commissioner's Office (ICO). However the Group operates as much as possible as if it was a single business. This policy applies equally to all the companies in the Group and to disclosures and sharing of data between them.

7 This policy applies to all employees, contractors and agents of the Group who have any form of access to the Group's data and information systems.

ROLES AND RESPONSIBILITIES

8 All employees, temporary staff, contractors and agents using data on behalf of the Group should be 'risk aware'. They should understand the potential threats associated with personal and confidential data and be aware of the Group's information policies, including any specific measures introduced by the IAO of the personal data they process.

PRIVACY NOTICES

9 The Group will act for its constituent companies to provide a Privacy Notice to those individuals about whom it collects personal data setting out how it will be used.

10 A privacy notice need not be in writing although this is to be preferred. However this policy permits the inclusion of a few paragraphs detailing all the required privacy notice information within other written material. If a formal warning, given in special circumstances (such as an Interview under Caution), provides the individual with the necessary information then that is sufficient.

DATA PROCESSING

11 The Group, in order to fulfil its services to its clients, may process personal data obtained from them and act on their behalf. In this capacity it will be acting as a data processor. The Group and its employees must therefore comply with the relevant service agreement or contract in such circumstances, as well as this policy.

12 This will apply to the Group's Internal Audit service. The terms of an audit provide the necessary instruction to the Group. Usually no decision is made about any individual whose personal data is processed in the course of an audit; data subjects' identities are not relevant, except to ensure the validity of the testing being carried out. An exception to this is the need (under the accuracy principle) to correct any error which is found in personal data in an audit sample. This will be referred back to the client, ie the data controller, to carry out. It is also within the instructions to the Group to refer back to the data controller evidence of systematic error or fraud, which may be the personal data of one or more client staff members implicated by that evidence.

13 The Group will sometimes have data processed by a contractor which in certain circumstances may be acting as a 'data processor' for the Group. If so, in addition to the usual checks for technical competence and financial stability, the Contracts Checklist is to be satisfactorily completed.

14 Where appropriate, contracts should also include a right of audit allowing the company to inspect the contractor (including its premises and systems) and confirm that information risks are being appropriately managed.

15 Further advice and guidance in relation to data processing should be obtained from the AD Information.

DATA SHARING

16 The company should maintain appropriate arrangements for both ad hoc and routine data sharing with clients and other external bodies. Although data sharing is a reciprocal process, this policy is more concerned with the disclosure of personal data by the Group. Nevertheless the collection of personal data from another data controller must also be compliant.

17 Employees, contractors and agents must take account of the Information Commissioner's statutory 'Data Sharing Code of Practice' and of the North Yorkshire Multi-Agency Information Sharing Protocol.

18 Where repeated or routine data sharing with clients and other external bodies is taking place this should be codified in an agreement with the other party or parties. The company is a signatory to the Multi-Agency Information Sharing Protocol. This Protocol has been developed to ensure that information is being shared lawfully, appropriately and in compliance with best practice. The Protocol aims to establish consistent principles and practices to govern the sharing of personal and non-personal information within and between partner agencies. The presumption of the Protocol is that partner agencies will share information in all situations to improve service delivery, except where it would be unlawful to do so.

19 A template data sharing 'arrangement' with guidance on how it should be completed can be found annexed to the Protocol. Further advice and guidance in relation to the use of the template should be obtained from the relevant Information Governance Manager.

20 Data sharing agreements drafted and proposed by another party must only be entered into or agreed after considering advice from the relevant Information Governance Manager.

Internal Data Sharing

21 Employees, contractors and agents may be seconded to any of the Group's companies to provide its services to its clients. To the extent that the client has disclosed personal data to a Group company, either as a data processor or as a joint controller, that company is processing the personal data using Veritau Group staff. There is no disclosure of that personal data to another Veritau company, even if it is the employer of the individual concerned.

Transferring Data

22 Data held by the company may need to be transferred 'internally' between locations or from one information system to another. Data may also need to be transferred to other organisations for processing or to facilitate data sharing. Data should only be transferred using methods of transmission which take account of the need to maintain data integrity and security. Transmission includes data sent by post[1], e-mail and electronic file transfer[2]. It also includes the physical transfer of data using portable electronic devices.

23 Methods of data transmission and levels of protection will be kept under review by the Group. The risks to data integrity and security should be evaluated by individual managers and the most appropriate method for transmission chosen.

24 To minimise possible risks, the following measures should be taken:

[1] Including data sent in hard copy and on electronic storage devices (for example memory cards / data drives)
[2] Using file transfer protocol (FTP) or similar.

- data must not be transferred to any country outside the UK unless appropriate safeguards are in place;
- secure e-mail facilities or other secure data transfer arrangements (eg secure FTP server) must be used for communicating personal data;
- full disk encryption must be enabled on any mobile electronic device;
- mobile electronic devices used for business purposes should have the facility to be remotely disabled or for the data held on them to be wiped.

25 Sending personal or confidential data by post is the least secure method of transmission and therefore other more secure methods should be considered. If the post is the only option available then best practice is always to double check the address, ensure it is clearly written (typed if possible) and include a senders' address on the back of the envelope. All envelopes containing personal information should be marked 'private and confidential'.

26 Sensitive information should be sent by special delivery, or even hand delivered, and large amounts of information might need to be double enveloped. The intended recipient should be informed in such circumstances and confirmation of receipt obtained.

Requests to Disclose Data

27 For data that the Group holds on behalf of a client, requests must be referred to the client organisation and not be disclosed by Veritau unless instructed to. Unless there is no doubt about compliance, confirmation of the proposed disclosure should be sought from the relevant Information Governance Manager.

28 In some cases, the company can be legally obliged or compelled to disclose personal data which would not otherwise be disclosed[3]. Enquiries relying on such obligations should refer to the relevant legal provisions but in cases of doubt, officers should consult the relevant Information Governance Manager.

29 Once a request has been processed, the facts of the disclosure, and, if discretion has been applied, the reasoning behind a decision to disclose or refuse should be recorded.

30 Subject access requests in which a person asks for his or her own data, and the disclosure of personal data in FoI requests, are dealt with in the Information Access Policy.

DATA PROTECTION IMPACT ASSESSMENTS

31 A Data Protection Impact Assessment (DPIA) is a way to foresee possible risks to individual privacy when changes to services, systems or procedures are proposed, or where data sharing is being considered.

32 The company should therefore consider data protection issues as part of the planning stage for any change programme or project, or before data is shared with

[3] For example, various regulators often have a power to compel disclosure, as does HM Revenue & Customs. Similarly, the Department for Work and Pensions can compel disclosure of employee data if needed for benefit fraud investigations.

an external partner where it is anticipated that the data sharing will take place on a regular basis. A DPIA should be completed by the project manager, or anyone fulfilling that role where:

- a new service is being developed;
- there is a significant change to an existing service; or
- new or revised methods of data collection are being implemented.

33 Similarly, a DPIA should be completed by the relevant manager or Information Asset Owner (IAO) where data sharing is being considered which is significant in nature or likely to be repeated on a regular basis. But a is DPIA **not** required where the partner organisation is a signatory to the Multi-Agency Information Sharing Protocol as this provides a suitable framework for managing the risks to individual privacy.

34 Further advice including examples of completed Data Protection Impact Assessments can be obtained from the Information Governance Team.

COMPLAINTS

35 The Group's Complaints Policy will apply to any complaint about matters within the scope of this policy.

COMPLIANCE

36 Employees, apprentices, trainees, temporary staff, agency staff or volunteers are required to comply with this policy. Failure to do so could result in disciplinary action being taken against the member of staff concerned

REVIEW AND REVISION

37 This policy will be reviewed annually and/or whenever there is a change to a legal or regulatory requirement that affects this policy.

REFERENCES

38 This policy should be read in the context of the company's other information governance policies and guidelines, national legislation, codes of practice and accepted best practice. In particular, this policy should be read in the context of:

- The ICO's Data Sharing Code of Practice
- North Yorkshire Multi-Agency Information Sharing Protocol
- The ICO's Privacy Notices Code of Practice
- The General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018

39 The following policy documents are directly relevant to this policy:

- Data Breach Procedure
- Document and Records Management Policy
- Information Access Policy
- Information Governance Policy
- Information Security Policy

KEY MESSAGES

40 Individual managers are responsible for ensuring data protection compliance within their area. They will be supported in this by the SIRO and the Information Governance Managers. All employees, temporary staff and contractors (data users) should be 'risk aware'. They should understand the potential threats associated with personal and confidential data and be aware of the company's information policies.

41 Managers must ensure that third parties, including contractors and partner organisations, have adequate systems and procedures in place to protect personal data which they are processing on behalf of the company. Standard contract terms should always be applied to contracts involving the processing of personal data.

42 The Multi-Agency Information Sharing Protocol sets out the principles and practices governing the sharing of information with partner agencies. Specific data sharing agreements should be completed by all parties where the company routinely shares data.

43 Data Protection Impact Assessments should be completed before any significant change programme or project is instigated.