Veritau Group Appropriate Policy Document

The Veritau Group comprises Veritau Ltd, Veritau North Yorkshire Ltd, and Veritau Tees Valley Ltd. The Veritau Group, and each of its members as appropriate, are referred to below as Veritau.

This document demonstrates that the processing of personal data falling into the special categories (SC), and of criminal offence (CO) data, by Veritau, is compliant with the Article 5 principles of the UK General Data Protection Regulation (UK GDPR), and with the Data Protection Act 2018 (DPA 2018).

The DPA 2018 includes the requirement for Veritau to have an Appropriate Policy Document (APD) in place when processing SC or CO data under certain conditions. This document incorporates Veritau's APD and includes an outline of Veritau's retention policies with respect to this data. In addition it provides information about Veritau's processing of special category and criminal offence data where a policy document is not required. The information supplements Veritau's various privacy notices, including its employee privacy notice.

Veritau processes data, including personal data and SC and CO data, on behalf of its clients, acting as a data processor. Such processing does not require Veritau to have an APD in place and is not within the scope of this document. Veritau also processes such data in its own right, whether as an employer or in its roles as an independent internal auditor, fraud investigator, and as Data Protection Officer for its clients. As such it is a data controller, either solely or jointly with its client, and under these circumstances this APD is applicable.

Veritau

Conditions for processing special category and criminal offence data

Veritau processes special categories of personal data under the following UK GDPR Articles:

Article 9(2)(a) – explicit consent
Veritau makes sure that consent given by any person is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of such processing include health information Veritau receives from disabled employees who require a reasonable adjustment to perform their duties; and salary deductions for trade union subscriptions or charitable donations.

Use of biometric data (ie fingerprint or face recognition) by employees to authorise the use of a mobile phone provided to them is optional and, to the extent that this amounts to processing of that data by Veritau, relies on consent[1].

Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on Veritau or the data subject in connection with **employment**.

Examples of such processing include managing sickness absences; declarations concerning political activity or potential conflicts of interest; salary deductions for trade union membership; and potentially data from any category, if relevant to a grievance or disciplinary procedure.

Article 9(2)(c) – where processing is necessary to protect the **vital interests** of the data subject or of another natural person.

This would be very unusual; an example of such processing would be using health information about a member of staff in a medical emergency.

Article 9(2)(g) - reasons of **substantial public interest**

Veritau as a public authority

As a public authority Veritau may be required to respond to a Freedom of Information request, or to test or demonstrate that it conforms to equalities and other duties imposed on public authorities. It may need to process SC or CO data to do so (although it would be unlikely to be disclosed).

By definition, there is a clear basis in law for such processing.

[1] The provision of the fingerprint or image when setting up the phone is the required explicit indication of consent. It can be withdrawn by the user without notice at any time through the phone's settings. The biometric data cannot processed by Veritau for any other purpose or in any other way

Internal audit

Veritau provides internal audit services for many of its clients. Its auditors will agree with the client which service areas are to be reviewed, and what records or samples will be examined in the course of the review. In such circumstances Veritau will be a data processor for the client, as that agreement amounts to an instruction to process. Such records or other information may include both SC and CO data.

Since the client (data controller) has a legitimate legal basis for processing, no additional legal basis is required by Veritau.

Veritau imposes on all its employees a duty of confidence such that the requirement at S 11(1)(b) of DPA 2018 is fulfilled and they can review SC or CO data

Fraud investigation

Veritau's fraud investigation function includes investigating allegations and suspicions of wrong-doing by employees of the client, or by members of the public in relation to services provided by it. Veritau carries out data matching and statistical analysis in order to locate or identify errors in service delivery or in other internal processes. Apart from correcting such errors, if fraud or other wrong-doing is indicated, then further investigation may be carried out, perhaps leading to disciplinary or legal action, including prosecution.

The conduct of such analysis, and of an investigation (including abandoning it), are determined by Veritau, which is therefore a controller, jointly with its client, of the personal data processed in the course of such analysis or investigation.
In the course of any such analysis or investigation, SC data may be collected and processed.

Preventing and detecting fraud or other wrong-doing are an integral feature of the management of those clients and their services, such that the purpose of Veritau's processing is identical to the purpose for which the joint controller processes it. However Veritau does not rely on any Article 9 provision, regardless of what the joint controller relies on, except this one; that it is in the substantial public interest for its clients, especially those which are public authorities, to be supported and assisted in the prevention and detection of fraud.

Veritau imposes on all its employees a duty of confidence such that the requirement at S 11(1)(b) of DPA 2018 is fulfilled and they can review SC data.

Veritau recommends to its clients that their privacy notices should inform data subjects that data may be processed by joint controllers such as Veritau.

Information Governance

Veritau acts as Data Protection Officer for many of its clients, a role requiring it to be independent and not unduly influenced – ie not instructed – by them.

For some, it also carries out tasks associated with their obligations under information law, including subject access requests, Freedom of information requests, and others.

The conduct of information rights requests (including decisions about whether to disclose or not), and of DPO matters, is determined by Veritau, which is therefore a joint controller with each client of the personal data processed in the course of such work. In both roles, Veritau may access or collect SC or CO data.

Employing a DPO is an integral feature of the management of those organisations, as is the provision (or withholding, or rectification, restriction or deletion) of personal data in response to requests, such that the purpose of Veritau's processing is identical to the purpose for which the joint controller processes it, or would have done. However Veritau does not rely on any Article 9 provision, regardless of what the joint controller relies on, except this one; that it is in the substantial public interest for its clients, especially those which are public authorities, to comply with all their data protection obligations.

Veritau imposes on all its employees a duty of confidence such that the requirement at S 11(1)(b) of DPA 2018 is fulfilled and they can review SC data.

Veritau recommends to its clients that their privacy notices should inform data subjects that data may be processed by joint controllers such as Veritau.

Criminal Offence (CO) data

Veritau processes criminal offence data under Article 10 of the UK GDPR
Examples of its processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Veritau's fraud investigation function includes investigating allegations and suspicions of wrong-doing by employees of the client, or by members of the public in relation to services provided by it. Veritau carries out data matching and statistical analysis in order to locate or identify errors in service delivery or in other internal processes. Apart from correcting such errors, if fraud or other criminal acts are indicated, then further investigation may be carried out, perhaps leading to prosecution. In the course of any such analysis or investigation, CO data may be collected and processed.

When processing CO data for these purposes Veritau relies on the conditions at paragraphs 6 (Statutory etc and government purposes) and 10 (preventing and detecting unlawful acts) of Schedule 1 of DPA 2018.

Veritau may also from time to time rely on paragraph 12 of Schedule 1 (Regulatory requirements relating to unlawful acts and dishonesty etc).

Veritau imposes on all its employees a duty of confidence such that the requirement at S 11(1)(b) of DPA 2018 is fulfilled and they can review CO data.

Veritau recommends to its clients that their privacy notices should inform data subjects that data may be processed by joint controllers such as Veritau.

Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD (see Schedule 1 paragraphs 1 and 5).
The remainder of this policy is the APD for Veritau. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines Veritau's retention policies with respect to this data.

Description of data processed

Veritau processes, or may from time to time process, personal data falling into all the special categories listed below[2]:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Data concerning health;
- Data concerning a natural person's sex life or sexual orientation
- Biometric (eg fingerprint or face) for the purpose of identification

Veritau also processes criminal offence data.

Schedule 1 conditions for processing

Below is the name and paragraph number of each of the Schedule 1 conditions on which Veritau relies for processing.

Special category data
Veritau processes special category data for the following purposes in Part 1 of Schedule 1:

- **Paragraph 1(1)** employment

Veritau processes special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- **Paragraph 6(1) and (2)(a)** statutory, etc. purpose**s**
- **Paragraph 10(1)** preventing or detecting unlawful acts
- **Paragraph 12(1) and (2)** regulatory requirements relating to unlawful acts and dishonesty

Criminal offence data
Veritau may from time to time process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- **Paragraph 1(1)** employment
- **Paragraph 6(2)(a)** – statutory, etc. purposes
- **Paragraph 10(1)** preventing or detecting unlawful acts

[2] all of these? Yes, although only rarely. But any might be the subject of a grievance claiming discrimination, or if a conflict of interest is declared or otherwise emerges

- **Paragraph 12(1) and (2)** regulatory requirements relating to unlawful acts and dishonesty

Procedures for ensuring compliance with the principles

Accountability principle
Veritau has put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer, who reports directly to Veritau's highest management level.
- Taking a 'data protection by design and default' approach to its activities including the use of data protection impact assessments (DPIAs)
- Maintaining documentation of its processing activities through its Information Asset Register
- Adopting and implementing data protection policies and ensuring it has written contracts in place with its data processors and sub-processors
- Implementing appropriate security measures in relation to the personal data it processes.
- Carrying out DPIAs for its high risk processing.

Veritau regularly reviews its accountability measures and updates or amends them when required.

Principle (a): lawfulness, fairness and transparency
Processing SC or CO data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

Veritau provides clear and transparent information about why it processes personal data including its lawful basis for processing in its staff privacy notices and this policy document.

Veritau's processing for the purposes of employment relates to its obligations as an employer.

Veritau also processes special category personal data to comply with other obligations imposed on it in its capacity as a public authority e.g. the Equality Act.

Principle (b): purpose limitation
Veritau will not process personal data for purposes incompatible with the original purpose for which it was collected.

Veritau is a signatory to the North Yorkshire Multi-agency Information Sharing Protocol, which is applied all its routine personal data sharing even if the recipient is not itself a signatory. This requires that Veritau must be satisfied that any recipient of personal data has a legal basis to process it.

Principle (c): data minimisation
Veritau collects personal data necessary for the relevant purposes and ensures it is not excessive. The information it processes is necessary for and proportionate to its purposes. Where personal data is provided to Veritau or obtained by it, but is not relevant to its stated purposes, it is to be erased.

Principle (d): accuracy
Where Veritau becomes aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, it will take every reasonable step to ensure that data is erased or rectified without delay. If Veritau decides not to either erase or rectify it, for example because the lawful basis it relies on to process the data means these rights don't apply, it will document its decision.

Principle (e): storage limitation
All special category data processed by Veritau for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in its Records Management Policy. Veritau determines the retention period for this data based on its legal obligations, and the necessity of its retention for its business needs. Veritau's retention schedule is reviewed from time to time and updated when necessary.

Principle (f): integrity and confidentiality (security)
Electronic information is processed within the secure network provided to Veritau by City of York Council. Hard copy information is processed in line with its security procedures.

Veritau's electronic systems and physical storage have appropriate access controls applied.

The systems Veritau uses to process personal data allow it to erase or update personal data at any point in time where appropriate.

Retention and erasure policies

Veritau's retention and erasure policies are based on the purpose for which records are created and used. They do not identify categories of data and therefore do not explicitly state how long any of the special categories of data will be retained. There is no retention period specific to any of the special categories. Data falling into any of the special categories will be retained according to its purpose, not its category.
However the Information Asset Registers do identify what SC data is included in each asset, and indicate how long it will be retained. The assets relate to all of Veritau's services, including its internal management.
The Records Management Policy sets out retention periods for the types of records that Veritau uses to provide all of those services and internal management.

Review Date

April 2023