Introduction

NY Highways (NYH) processes special category and criminal conviction data in the course of fulfilling its functions as a company. Schedule 1 of the Data Protection Act 2018 requires data controllers to have in place an 'appropriate policy document' where certain processing conditions apply for the processing of special categories of personal data and criminal convictions data. This policy fulfils this requirement.

This policy complements our existing records of processing as required by Article 30 of UK General Data Protection Regulation, which has been fulfilled by the creation and maintenance of an Information Asset Register. It also reinforces our existing retention and security policies, procedures and other documentation in relation to special category data.

Special categories and conditions of processing

We process the following special categories of data:

- racial or ethnic origin,
- religious or philosophical beliefs,
- trade union membership,
- health,
- sex life/orientation,

We also process criminal offence data under Article 10 of UK GDPR, including for pre-employment checks and declarations by employees in line with their contractual obligations.

We rely on the following processing conditions under Article 9 of UK GDPR and Schedule 1 of the Data Protection Act 2018 to lawfully process special category and criminal convictions data:

Article 9(2)(a) – explicit consent
We make 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. We regularly review consents to ensure they remain up to date.

Examples of such processing includes ethnicity information for equality monitoring.

Article 9(2)(b) – employment, social security or social protection
To comply with our legal requirements as an employer, we need to collect some special category data.

Examples include when we collect medical information to put in reasonable adjustments at work and monitor staff absence; and keep records of an employee's trade union membership.

When processing information under Article 9(2)(b), we also require a Schedule 1 condition under the Data Protection Act 2018. The condition we rely on for this processing is Schedule 1, Part 1, (1) - employment, social security and social protection.

Article 9(2)(g) – substantial public interest

To check relevant criminal history as required to determine suitability for the role.

When processing criminal offence data, we also must identity a Schedule 1 condition under the Data Protection Act 2018. The conditions we rely on for this processing are Schedule 1, Part 1, (6) – statutory and government purposes, and Schedule 1, Part 1, (10) – preventing or detecting unlawful acts.

Article 9(2)(h) – health or social care
We collect health data to provide staff with occupational health support where necessary.

When processing information under Article 9(2)(b), we also require a Schedule 1 condition under the Data Protection Act 2018. The condition we rely on for this processing is Schedule 1, Part 1, (2) – health or social care purposes.

Compliance with Data Protection Principles

We have several policies and procedures in place to ensure our compliance with the Article 5 Data Protection Principles and meet our accountability obligations, explained in more detail below:

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

- The appointment of a Data Protection Officer, Veritau, which provides reports to the Board of Directors.
- Taking a data protection by design and default approach to our processing activities, including the use of risk assessments.
- Maintaining documentation of our processing activities through an Information Asset Register.
- Adopting and implementing information governance policies and ensuring we have written contracts in place with data processors.
- Implementing appropriate security measures in relation to the personal data we process. More detail can be found in our Information Security Policy.

Principle (a): lawfulness, fairness and transparency
Processing personal data must be lawful, fair and transparent. We have identified an appropriate Article 6 condition and also, where processing SC or CO data, an Article 9 and Schedule 1 condition.

We consider how any processing may affect individuals concerned and provide clear and transparent information about why we process personal data, including our lawful bases, in our privacy notices and this policy document. All privacy notices provide details of data subject rights. Our privacy information is regularly reviewed and updated to ensure it accurately reflects our processing.

Principle (b): purpose limitation
NYH can only act in ways and for purposes it is empowered to do so by law. Personal data is therefore only processed to allow us to carry out the necessary functions and services we are required to provide in line with legislation. We clearly set out our purposes for processing in our privacy notices, policies and procedures, and in our IAR. If we plan to use personal data for a new purpose, other than a legal obligation

or function set out in law, we check that it is compatible with our original purpose, or we obtain specific consent for the new purpose.

Principle (c): data minimisation
We only collect the minimum personal data needed for the relevant purposes, ensuring it is necessary and proportionate. Any personal information that is no longer required, especially where it contains special category data, is anonymised or erased. Further information can be found in our Records Management Policy.

Principle (d): accuracy
Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is processed, we will take every reasonable step to ensure that data is erased or rectified without delay. Where we are unable to erase or rectify the data, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision. Where we have shared information with a third party, we will take all reasonable steps to inform them of the inaccuracies and rectification. We maintain a log of all data rights requests and have appropriate processes for handling such requests.

Principle (e): storage limitation
We have a Retention Schedule in place. Where there is no legislative or best practice guidance in place, the SIRO will decide how long the information should be retained based on the necessity to keep the information for a legitimate purpose or purposes. We also maintain a Destruction Log, which documents what information has been destroyed, the date it was destroyed and why it has been destroyed. Further information can be found in our Records Management Policy.

Principle (f): integrity and confidentiality (security)
We employ various technical and organisational security measures to protect the personal and special category data that we process. A full description of security measures can be found in our Information Security Policy.

In the event of a personal data breach the incident will be recorded in a log, investigated, and reported to our Data Protection Officer where necessary. High risk incidents are reported to the Information Commissioner's Office. This process is documented in greater detail in our Information Security Policy.

Retention of special category and criminal convictions data

The retention periods of special category and criminal convictions data are set out in our Retention Schedule. Retention periods of specific information assets are identified in our Information Asset Register, and we have in place a Records Management Policy.