Data Protection Responsibilities for accessing and using Sentinel

Version 1.3

Published Date: 27 October 2022

Document Control

Date	Version	Author Role	Author Name	Change Details
27/10/2022	V1.3	Data Protection Specialist	Sandy Gilchrist	Updated with links to forms

Contents

Introduction

These instructions explain how we work together for the smooth running of Sentinel and protection of personal data. It covers our data protection obligations to provide a designated point of contact, and to address data protection principles, legal basis, security measures, data breach communications, data protection impact assessments, the use of processors, and international transfers of personal data.

The appendices set out the template to be completed when parties need to correspond about these matters, and a personal data sharing agreement to comply with.

1. Definitions

Term	Description
Parties	Any organisation that uses Sentinel, e.g. Sponsors, training providers, medical providers, providers of site-access control services, NSAR, and Network Rail, including Technical Authority (the Sentinel custodian that sets out the rules, undertakes assurance assessments, and conducts investigations where required)
Means	The joint processing of personal data on Sentinel.
Purpose	to establish an 'authority to work decision'.

2. General

The section describes general data protection requirements when parties jointly process personal data on Sentinel, and to demonstrate compliance to the Network Rail designated contact through the assurance process.

2.1 The parties acknowledge they have jointly determined the means and purpose in their legitimate interests. In order to preserve the integrity of the personal data, each party acknowledges their part in ensuring access to the system, processes and organisational set-up are fit-for-purpose.

2.2 Each party accepts their respective roles and responsibilities, as laid out here, to minimise the risk of unauthorised or unlawful processing of the personal data.

2.3 Each party shall be accountable for their respective data protection obligations.

2.4 Each party shall define their respective data protection obligations precisely.

2.5 At the time of the determination of the means and at the time of the joint processing itself, each party shall be responsible for demonstrating compliance with data protection by design by implementing appropriate technical and organisational measures designed to support the data protection principles effectively and maintain an appropriate level of security proportionate to the risks presented by the processing.

2.6 Any pre- and post-processing shall be separate from the joint processing, except as specified here, and subject to other arrangements and legal bases where applicable.

3. Contact and Communications Between Parties

This section describes the requirement for parties to designate a point of contact for communications with each other, regulators, and card holders, and to demonstrate compliance to the Network Rail designated contact through the assurance process.

3.1 Each party shall designate a point of contact for data protection matters, such as (but not limited to) rights requests by individuals, personal data breaches or other incidents, and enquiries from regulators.

3.2 Where individuals bypass their designated contact, and contact another party, they shall be referred back to the designated contact without undue delay, and in any case within 24 hours.

4. General Principles of Data Protection

This section describes the requirements for parties to comply with the data protection principles and to demonstrate compliance to the Network Rail designated contact through the assurance process.

4.1 Each party shall observe the general principles of data protection.

4.2 Regarding the principle of lawfulness, fairness and transparency, each party shall:

a) have in place adequate policies and training outlining the principles to be followed by its employees and workers to ensure personal data is processed fairly, lawfully, transparently and in a manner consistent with its legitimate business interests.

b) provide in its privacy notice the essence of these arrangements including at least:

i. personal data is jointly processed with other parties in our legitimate interests for the stated purposes, including profiling;

ii. individuals may exercise their right to request further details at any time; and

iii. contact details to correspond with regarding data protection matters.

4.3 Regarding the principle of purpose limitation, each party shall:

b) process personal data for the stated purposes, including profiling;

c) respect the limitations of the stated purposes before processing the personal data for further purpose(s), by conducting a compatibility test for any new purpose(s) and

i. where not compatible with current purposes, undertake not to process personal data for that new purpose without authority to do so;

ii. where compatible, further consider additional technical and organisational measures as required, and inform the other parties of the intention to do so.

d) respect the limitations of processing the personal data for any prior purpose(s).

4.4 Regarding the principle of data minimisation, each party shall only process personal data that is adequate, relevant and limited to what is necessary for the stated purposes or as obligated to do so by law.

4.5 Regarding the principle of accuracy, each party shall:

a) ensure that processing remains accurate, and, where necessary, kept up to date; and

b) take every reasonable step to ensure that any inaccurate personal data, having regard to the stated purposes, are erased or rectified without delay.

4.6 Regarding the principle of storage limitation, each party shall:

a) keep such personal data in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed.

b) specify in its policy documentation procedures for the tracking and deletion of personal data according to their retention schedules.

c) retain personal data for the duration of the business relationship between the parties or until instructed to delete personal data under the terms of a contract, except where lawfully required to retain the personal data for longer.

4.7 Regarding the principle of integrity and confidentiality, each party shall:

a) process in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
b) have in place adequate documentation including, but not limited to, policies and employee or worker contracts, clearly designating any personal data as confidential to allow its legitimate, authorised processing of personal data.
c) only introduce a new party to the processing with the appropriate authority.

4.8 Regarding the principle of accountability, each party shall:

a) manage risk adequately including, but not limited to, necessity, proportionality and legitimacy tests, data protection impact assessments, legitimate interest assessments, and transfers tests, as required.
b) make any risk assessment available to the other parties upon reasonable request.
c) maintain a record of processing activities including, but not limited to, in particular a list of recipients of the personal data, which must be provided to the other parties upon reasonable request as required without undue delay.
d) log all individuals' rights requests as per data protection obligations.
e) be responsible for, and be able to demonstrate compliance with, the principles set out in this clause.

5. Legal Basis of Processing

This section describes the requirements for parties to only process personal data when there is a legal basis to do so, and to demonstrate compliance to the Network Rail designated contact through the assurance process.

5.1 Each party acknowledge that personal data is shared and processed in relation to the stated purposes including profiling based on:

a) public and legitimate interests for general processing, whilst
b) for special categories of personal data, the processing is necessary for
    i. the purposes of carrying out the obligations and exercising specific rights of the party or of the individual in the field of employment and social security and social protection law, including, and
    ii. reasons of substantial public interest as laid down by the Health and Safety at Work Act 1974 as well as in relation to the Sentinel Scheme Rules as referred to in the Railways and Other Guided Transport Systems (Safety) Regulations (ROGS) 2006. This clause also requires that the conditions of Schedule 1 of the Data Protection Act 2018 are met.

5.2 Each party shall state the legal bases it relies upon for any additional specified, explicit and legitimate purposes that it processes personal data for, which shall be proportionate to the legitimate aim pursued, and, in particular, refer to:

a) the types of data which are subject to the processing;
b) the individuals concerned;
c) the entities to, and the purposes for which, the personal data may be disclosed;
d) purpose limitation;
e) storage periods; and
a) processing activities and processing procedures, including measures to ensure lawful and fair processing.

5.3 Each party shall be responsible for undertaking its own necessity, proportionality and legitimacy tests to justify further processing, taking upmost account that such purposes are not incompatible with the stated purposes by undertaking a compatibility test taking into account, inter alia:

a) any link between the stated purpose and the intended further purposes;
b) the context in which the personal data have been collected, in particular regarding the relationship between individuals and the respective party as well as other parties that may be involved with the processing activities;
c) the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed;
d) the possible consequences of the intended further processing for individuals;
e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

5.4 The legal basis for all processing, including general processing as well as processing of special categories of personal data, shall be documented appropriately, supported by appropriate policies where required, and made available upon reasonable request to other parties involved with the joint processing.

6. Data Protection Impact Assessments

This section describes the requirement for parties to complete their own data protection impact assessments and by gaining approval from the Network Rail designated contact by completing the appropriate form.

6.1 Each party shall be responsible for its own data protection impact assessment ("DPIA") with regards to the joint processing and include which party is responsible for the various measures designed to manage or mitigate any identified risks, in particular regarding automated decision-making, special categories of personal data, or where the individual is a child.

6.2 Each party shall provide practical assistance upon reasonable request to another party undertaking its DPIA.

6.3 Each party shall consider completing a DPIA for any stated or further planned processing activities and associated purpose(s):

a) that is large scale.
b) involves profiling or monitoring.
c) decides on access to services or opportunities; or
d) involves sensitive data or vulnerable individuals.

6.4 Each party shall undertake DPIAs for any stated or further planned processing activities and associated purpose(s) involving:

a) the use of systematic and extensive profiling or automated decision-making to make significant decisions about individuals.
b) special categories of personal data or criminal offence data on a large scale.
c) systematically monitoring a publicly accessible place on a large scale.
d) the use of new technologies.
e) the use of profiling, automated decision-making, or special category data to help make decisions on someone's access to a service, opportunity, or benefit.
f) profiling on a large scale.
g) the processing of biometric or genetic data.
h) combining, comparing, or matching data from multiple sources.
i) processing personal data without providing a privacy notice directly to the individual.

j) processing personal data in a way which involves tracking individuals' online or offline location or behaviour.

k) processing children's information for profiling or automated decision-making or for marketing purposes or offer online services directly to them.

l) processing personal data which could result in the risk of physical harm in the event of a security breach. This clause applies unless the party has already done a substantially similar data protection impact assessment.

6.5 When undertaking a DPIA, the party shall take utmost account of applicable statutory data protection and other relevant codes including (but not limited to):

a) Age-appropriate design code (also known as the Children's code).

b) Data sharing code.

c) the Network Rail Code of Conduct which requires compliance with the:

i. Sentinel Scheme Rules.

ii. Life Saving Rules.

iii. Code of Business Ethics.

iv. Network Rail Code of Conduct itself.

6.6 When undertaking a DPIA, the party shall take utmost account of risks caused by the nature, scope, context and intended purpose(s) of the processing.

6.7 When undertaking a DPIA, the party shall take utmost account of any:

a) concerns affected individuals may have.

b) impact that stakeholders may have including on other parties involved with the processing activities such as processors, controllers, and joint controllers.

c) any concerns the data protection officer may have, if appointed.

7. Security Measures

This section describes the requirements for parties to have appropriate security measures in place to protect personal data and by gaining approval from the Network Rail designated contact by completing the appropriate form.

7.1 For personal data that is processed for the stated purposes or any further processing activities and associated purpose(s), each party shall have in place appropriate technical and organisational measures so that personal data shall be processed in a manner that ensures a level of security appropriate to the personal data being processed, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7.2 Each party shall be able to demonstrate the ability to:

a) manage their respective security risk

b) taking appropriate steps to identify, assess and understand security risks to personal data and the systems that process such data;

i. implement appropriate organisational structures, policies, and processes to systematically manage security risks to personal data;

ii. in particular risks relating to processing activities that may arise as a result of engaging other parties such as controllers, joint controllers, and / or processors, including ensuring that they employ appropriate security measures, such as, in the case of processors, requiring sufficient guarantees about their technical and organisational measures.

c) protect personal data against cyber-attack with proportionate security measures in place which cover the personal data processed as well as the systems that process such data, these

measures to include compliance with Network Rail's Information Security policies in order to manage:

i. the security of data by implementing technical controls (such as appropriate encryption) to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest or accessing data that might remain in memory when technology is sent for repair or disposal.

ii. the security of systems by implementing appropriate technical and organisational measures to protect systems, technologies and digital services that process personal data from cyber-attack;

iii. training staff by giving appropriate support to help them manage personal data securely, including the technology they use;

iv. monitoring authorised user access to that data, including anomalous user activity, recording user access to personal data.

v. having processes in place, where unexpected events or indications of a personal data breach are detected, to act upon those events as necessary in an appropriate timeframe.

7.3 minimise the impact of a personal data breach, restore systems and services, including the availability and access to personal data in a timely manner in the event of a physical or technical incident, manage incidents appropriately, and learn lessons for the future, by:

d) effective response and recovery planning;

e) taking steps, when a personal data breach occurs, to understand the root cause, take appropriate action, including, documenting lessons learned, and, where required, reporting the breach to the ICO, the National Cyber Security Centre, other relevant bodies, and affected individuals.

8. Personal Data Breach Notifications

This section describes the requirement for parties to notify other affected parties when there is a personal data breach by completing the appropriate form and to follow any instructions from the Network Rail designated contact.

8.1 For personal data that is processed for the stated purposes or any further processing activities and associated purpose(s), when identifying a personal data breach referred to in the sub-paragraph of this clause, each party shall without undue delay, and in any case within 24 hours of becoming aware of the personal data breach, inform other parties about the nature, scope and context of the personal data breach where required, and agree which party

a) is the source of the personal data breach, and

b) shall take the lead in managing the personal data breach including investigating it, undertaking appropriate risk assessments, and managing any remediation, including providing any required notifications.

A personal data breach is as defined by the UK GDPR, noting that in particular 'unauthorised or unlawful processing may include disclosure of personal data to recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the UK GDPR – the consequence of such a breach being that the parties will be unable to ensure compliance with the principles relating to the processing of personal data.'

8.2 Where a party is required to inform other parties of a personal data breach, such notification should include the likely consequences of the breach, as well as the measures taken or proposed

to be taken by the party if applicable to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects, such consequences including:

a) the inability to comply with data protection obligations; and
b) the realistic identification of the potential range of significant adverse effects on individuals, which can result in physical, material, or non-material damage, such as loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy, as well as any other significant economic or social disadvantage to those individuals, in particular where such adverse effects on individuals may wholly or partially, directly or indirectly, lead to a further event or incident because of or as well as, for example, a further breach of legal obligations which the parties are beholden to – e.g. Health and Safety at Work Act 1974, ROGS 2006, Railways Act, etc.

8.3 Each party shall ensure for their respective part that a description of the nature, scope and context of the personal data breach are recorded and logged, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records.

8.4 Each party shall assist the other party in notifying the personal data breach to the ICO where required, including providing the information in the preceding paragraphs upon reasonable request. The parties shall define all the elements to be provided by the party identifying a personal data breach when assisting each other in the notification of a personal data breach to the ICO.

9. The Use of Processors

This section describes the requirements for parties to only use processors with an appropriate contract and by gaining approval from the Network Rail designated contact by completing the appropriate form.

Each party shall ensure, by way of a binding contract or other legal act, that any processors it relies upon:

9.1 9.1 only process personal data in line with the party's written instructions within the terms (unless it is required to do otherwise by law), which set out the extent of the processing that the processor is contracted, including (but not limited to):

a) the subject matter and duration of the processing;
b) the nature and purpose of the processing;
c) the type of personal data and categories of affected individuals; and
d) the party's obligations and rights.

9.2 9.2 provide sufficient guarantees, in particular in terms of its expert knowledge, resources and reliability, that they will implement appropriate technical and organisational measures to ensure the security of personal data, such as using encryption and pseudonymisation.

9.3 9.3 ensure their processing meets data protection obligations, including:

a) protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access, through (but not limited to):
    i. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    ii. the ability to restore access to personal data in the event of an incident; and
    iii. processes for regularly testing and assessing the effectiveness of the measures.

b) demonstrating they are competent to process the personal data in line with those data protection obligations, such as maintaining records, appointing a data protection officer, and allowing the party to conduct timely audits, inspections or assessments, to demonstrate the processor's data protection obligations have been met, taking into account the nature of the processing and the risks to the data subjects.

c) obtaining a commitment of confidentiality from anyone it allows to process the personal data, unless that person is already under such a duty by statute, covering their employees as well as any temporary workers and agency workers who have access to the personal data.

9.4 shall not engage another processor (i.e. a sub-processor)

a) without the party's prior specific or general written authorisation

b) where such authorisation is given, the processor shall demonstrate it has in place a contract with the sub-processor with terms that offer an equivalent level of protection for the personal data as those in the contract between the processor and the party.

9.5 inform the party without undue delay if:

a) any of party's instructions would lead to a breach of data protection obligations; or

b) they become aware of a personal data breach, taking utmost care to notify, the party within 24 hours, and assist the party in complying with its obligations regarding personal data breaches.

9.6 only transfer outside the UK when authorised by the party and ensure that such transfers comply with the transfer provisions as laid down by data protection obligations

9.7 assist the party where required in meeting its obligations to keep personal data secure, notify, where required, the ICO and affected individuals, and carry out DPIAs.

9.8 cooperate with supervisory authorities (such as the ICO) to help them perform their duties as required.

9.9 take appropriate technical and organisational measures to help the party respond to requests from individuals to exercise their rights.

9.10 at the end of the contract, in a secure manner, and, at the party's choice, delete or return to the party all the personal data it has been processing for it unless UK law requires it to be stored.

10. International Transfers of Personal Data

This section describes the requirements for parties to only transfer personal data outside of the UK where legally permitted to do so and by gaining approval from the Network Rail designated contact by completing the appropriate form.

In relation to a party exporting personal data to a recipient in a third country, and including onward transfers by that recipient, where the recipient is not covered by an adequacy decision, the party shall check that enforceable data subject rights and effective legal remedies for affected individuals are available, in addition to documenting one of the required appropriate safeguards or exceptions as stipulated by data protection obligations, where:

10.1 any routine restricted international personal data transfer that relies on an international data transfer agreement (IDTA) is subject to an international transfer risk assessment (TRA) prior to the transfer.

10.2 any more complex restricted international personal data transfer (such as where the recipient is based in more than one country) is, in addition to completing a TRA, subject to a DPIA, and the implementation of any necessary further contractual, technical and organisational measures to sufficiently mitigate risks, including relying on another appropriate safeguard or exception or not proceeding where there is an enhanced risk.

10.3 any unrestricted international personal data transfer Is subject to contractual clauses that commit the recipient to their data protection obligations to facilitate the exercising of data subject rights as well as the ability of data subjects to seek administrative and judicial redress and to claim compensation in the UK and the destination country, including where the recipient is a:

a) controller, their responsibilities, DPIAs, security measures, and transfers or disclosures not authorised by UK law.
b) processor (or sub-processor), their processor contract, security measures, and transfers or disclosures not authorised by UK law.

11. Individuals' Right to Exercise Their Rights

This section describes the requirements by parties to deal with requests from cardholders to access, modify or erase their personal data by gaining approval from the Network Rail designated contact by completing the appropriate form.

11.1 Each party shall provide any individual wishing to exercise their rights directly another party the details of the other party's designated point of contact.

11.2 Each party shall handle any rights requests without prejudice and act to respond or otherwise provide for these requests without undue delay, and in any case within 1 month, or as required by data protection obligations.

11.3 Each party shall validate any rights request received against their record of processing activities.

11.4 Each party shall fulfil any rights requests in a secure manner, including but not limited to, security of communications and transmission of personal data.

11.5 In relation to right of access, each party shall

a) respond as to whether or not personal data is being processed; and
b) provide the individual with information as laid down by data protection legislation including with regards to the purpose(s) and legal basis for the processing;
c) provide a copy of the personal data being processed; and
d) take into utmost account that the right to obtain a copy of the personal data shall not adversely affect the rights and freedoms of others.

11.6 In relation to right to data portability, where relevant, each party shall refer the individual to the party that provided the personal data, who shall resolve any referred or direct data portability requests.

11.7 In relation to right to rectification, each party shall

a) rectify any inaccurate personal data upon request by individual; and
b) refer the individual to the other party for any data rectification requests concerning personal data entered by the other party, and the other party shall resolve any referred or direct right to data rectification requests.

11.8 In relation to right to erasure, each party shall

a) determine if any of the applicable grounds for erasure as laid out by the data protection legislation apply;
b) if grounds do not apply inform individual that the request may not be fulfilled.
c) if grounds apply immediately erase any personal data as per data protection obligation; and
d) inform any recipient of the valid erasure request; and
e) inform the individual of these recipients if requested by the individual.

11.9 In relation to right to restriction of processing,

a) if the relevant party no longer needs the personal data for the purposes of the processing, but they are required by the individual for the establishment, exercise or defence of legal claims

restrict processing immediately, then the party shall inform the other party without undue delay, and in any case within 24 hours.

b) if the individual requests restriction pending the verification of the legitimate grounds of either party overriding those of the individual in connection to a right to object request, then the party shall
   i. restrict processing immediately, and
   ii. inform the other party without undue delay, and in any case within 24 hours.

11.10 In relation to right to object, if the individual objects to the legitimate interest of either party in processing or sharing their personal data the respective party shall demonstrate compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims, and, if unable to do so, cease processing immediately and notify the other party of valid objection request without undue delay, and in any case within 24 hours.

12. Designated Points of Contact

Responsibility	Network Rail Infrastructure Limited	Contact in party that Network Rail and Sentinel rely upon
Matters relating to these written arrangements	Sentinel Help Desk sentinel@mitie.com	Primary Sentinel contact (unless stated otherwise)
Requests by individuals exercising their rights	Sentinel Help Desk sentinel@mitie.com	Primary Sentinel contact (unless stated otherwise)
Personal data breaches and similar security incidents	Sentinel Help Desk sentinel@mitie.com	Primary Sentinel contact (unless stated otherwise)
Authorisation of designated points of contact	Network Rail Sentinel Operations Team	Primary Sentinel contact (unless stated otherwise)
Date of authorisation	Effective 31 October 2022	Effective 31 October 2022

13. Appendices

Appendices #	Document
1	Data Protection Matters Request Form
2	Data Protection Assistance Request Decision Tree
3	Data Protection Matters Decision Form
4	Personal Data Sharing Agreement between parties
5	Information Sharing Request Form
6	Information Sharing Decision Tree
7	Information Sharing Decision Form