Rail Delivery Group

National Rail

RDG Guidance Note: Data Protection Requirements During and After Incidents

RDG-OPS-GN-038
Issue 4– February 2023

Important note

The content of this Guidance Note reflects the best information and advice available. However, as of the date of its publication, application of the General Data Protection Regulation (GDPR) effective from May 2018 within the context of provision of humanitarian assistance in response to an emergency remains untested, both practically and legally.

This Guidance Note assumes that railway undertakings already have in place all measures necessary to comply with GDPR requirements on a routine, business as usual basis and therefore focuses on the specific additional or different considerations and requirements applicable to post incident deployment of the Incident Care Team (ICT).

In all cases of ICT deployment, it is strongly recommended that early contact be made with the railway undertaking Data Protection Officer to make them aware of the circumstances and seek their guidance on meeting the requirements of the GDPR within that specific context.

About this document

Explanatory note

The Rail Delivery Group is not a regulatory body and compliance with Guidance Notes or Approved Codes of Practice is not mandatory; they reflect good practice and are advisory only. Users are recommended to evaluate the guidance against their own arrangements in a structured and systematic way, noting that parts of the guidance may not be appropriate to their operations. It is recommended that this process of evaluation and any subsequent decision to adopt (or not adopt) elements of the guidance should be documented. Compliance with any or all of the contents herein, is entirely at an organisation's own discretion.

Other Guidance Notes or Approved Codes of Practice are available on the Rail Delivery Group (RDG) website.

Executive summary:

While this document to some extent describes and explores the requirements of GDPR in general, its particular focus is on how these may be complied with within the context of personal data gathered as part of the Incident Care Team (ICT) deployment to an incident. It is therefore directed specifically at those with responsibilities for ICTs.

Issue record

Issue 1 of this document was published as ATOC/GN038 and Issues 2 and 3 were published as RDG-GN038.

Issue	Date	Comments
1	September 2016	Original version as an ATOCdocument.
2	May 2018 (withdrawn September 2018)	Updated to reflect requirements of GDPR and reformatted as an RDG document. Withdrawn due tolack of consensus on best legal basis for compliance.
3	May 2019	Following receipt of advice that 'legitimate interest' provides the best legal basis for compliance.
4	February 2023	Following periodic review. Takes into account and reflects the content of the Information Commission's Office's (ICO) Data Sharing Code of Practice, published in October 2021. Reformatted to comply with latest RDG template.

This document is reviewed on a regular 3 year cycle.

Document owner:

Peter Lovegrove
Operational Resilience Manager
Rail Delivery Group

Authorised by:

James Burt
Chair of RDG Incident Care Team Management Group

Contents

1 Purpose, scope and context

1.1 Purpose

This Guidance Note is designed to help railway undertakings understand the basics about data protection considerations in relation to ICT and incident response activities.

The primary audience for this Guidance Note is intended to be ICT Champions and their respective teams. Railway undertaking data protection and emergency management specialists may also find the document of interest, as the work of the ICT will link in with their own scope of work. ICT Champions need to understand how the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)[1] (hereafter referred to in this Guidance Note as the "Legislation") affect them within the context of an ICT deployment.

The Legislation places a duty on organisations whose core activities require largescale, regular and systematic monitoring of individuals to appoint a Data Protection Officer (DPO) and railway undertakings have these in place. However, it should not be expected that the DPO will be familiar with the activities undertaken by the ICT and so this document will assist them in understanding some of the implications for this specific element of their organisation's business.

1.2 Scope and context

During emergency response activities, railway undertaking ICT members will collect and use information about individuals in order to provide humanitarian assistance to them. It is important that railway undertakings consider how this information is both initially captured and collated and subsequently handled. In the context of ICT activities, information will need to be managed appropriately, not only because there is a legislative need to do so, but also because it may be required by the railway undertaking itself during post incident investigations or by other organisations, e.g. in connection with inquiries. It is important therefore that data is managed, stored, shared and destroyed appropriately, in order to protect the individuals to whom it relates and comply with the Legislation.

When it comes to sharing information about individuals, organisations may be cautious in their interpretation of the Legislation and may be unwilling to share any information at all, in case this contravenes the individual's rights.

2 Definitions

Key definitions applicable to this Guidance Note are as follows:

Term	Definition in the context of this document
Data concerning health	Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status.
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (as per Article 4 of the UK GDPR and Section 32 of the DPA 2018).
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller.
Data Protection Office (DPO)	Person responsible for ensuring that the organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

[1] Following Brexit, the EU General Data Protection Regulation (EU GDPR) has been kept in UK law as the UK General Data Protection Regulation (UK GDPR). This came into effect on and from 1 January 2021. There are only minor differences between the two.

Data sharing	The disclosure of personal data by transmission, dissemination or otherwise making it available.
Enterprise	A natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.
Filing system	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Group of undertakings	A controlling undertaking and its controlled undertakings.
Information Commissioner's Office (ICO)	The UK's independent authority set up by the Government to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. Also acts as the UK's Supervisory Authority.
Legislation	The Data Protection Act 2018 together with the UK General Data Protection Regulation.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Recipient	A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not
Supervisory authority	An independent public authority with overall responsibility for data protection. Within the UK, this is the Information Commissioner's Office.
Third Party	A natural or legal person, public authority, agency or body other than the data subject, Data Controller, Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorised to process personal data.

3 Data protection legislation

3.1 Introduction

This section explains the basics of the Legislation and is based on guidance from the ICO.

3.2 Key areas covered by the Legislation

Key area	EU General Data Protection Act 2018; and the Data Protection Act 2018
Data breach	Any data breach must be reported to the Supervisory Authority within 72 hours of the incident. In the UK this is the ICO.
Data removal/Right to erasure	An individual has the 'Right to erasure' – which includes all data including web records with all information being permanently deleted.
Reach	Applies to the whole of the EU and, crucially, also to any global company which holds data on EU citizens.
Consent	The need for consent underpins the Legislation. Individuals must knowingly opt-in whenever data is collected and there must be clear Privacy Notices. Those notices must be concise and transparent, and consent must be able to be withdrawn at any time.
Penalties	The potential penalties for non-compliance are much more severe with fines of up to £17.5 million or 4% of the business' annual global turnover.
Data Protection Officer	A DPO is mandatory for any public authority or body or where an organisation's core activities consist of regular processing of data subjects on a large scale or where the core activities process on a large scale 'special categories of data'. Railway undertakings are assumed to require a DPO because of the large volume of data processing that they undertake for their daily business.
Data Protection Impact Assessments	Data Protection Impact Assessments (DPIA) are mandatory and must be carried out when there is a high risk to the rights and freedoms of the individual. A DPIA helps an organisation to ensure they comply with the six data protection principles and meet an individual's expectation of privacy.

Table 1: Table summarising the key requirements of the Legislation

3.3 Who does the Legislation apply to?

The Legislation applies to 'Data Controllers' and 'Data Processors'; a railway undertaking could reasonably be both during a response to a rail incident and indeed is likely to be both during the course of its day-to-day business activities, handling, as it does, personal information on customers and staff.

i. A Data Controller determines the purposes and means of processing personal data.
ii. A Data Processor is responsible for processing personal data on behalf of a Data Controller.

Article 28 of the UK GDPR lays down requirements that must be in place between a Data Controller and a Data Processor, in order to protect the rights of the data subject. These requirements include a written contract and guarantees about security.

The Legislation places specific legal obligations on Data Processors; they are, for example, required to maintain records of personal data and processing activities and will have legal liability if responsible for a breach.

A Data Controller is not relieved of their obligations where a Data Processor is involved – there is an obligation to ensure any contracts with Data Processors comply with the Legislation as well.

The Legislation applies to processing carried out by organisations operating within the UK. It also applies to all companies who process the data of individuals who reside in an EU country or who are citizens of an EU country.

3.4 What information does the Legislation apply to?

Personal data:

i. The Legislation applies to 'personal data', meaning any information relating to a person who can be directly or indirectly identified, in particular by reference to an identifier.
ii. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data, facial recognition or online identifier, reflecting changes in technology and the way organisations collect information about people.
iii. The Legislation applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
iv. Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the Legislation depending on how difficult it is to attribute the pseudonym to a particular individual.

This means that a lot of the information a railway undertaking might collect relating specifically to individuals who have been involved in a rail incident comes under the Legislation.

This could be information about who they are, where they live, their medical needs, their age, what they were doing at the time of the incident, etc. The fact that the information could be collected through a variety of means, including railway undertaking ICT-specific forms, on electronic devices or on ad hoc pieces of paper, does not negate this as it must be expected that the railway undertaking will collate it and capture it electronically at a later date, both to support the continuing humanitarian support effort and provide a record of what has taken place.

Sensitive personal data:

i. The Legislation refers to sensitive personal data as "special categories of personal data" (see Article 9 of the GDPR, translated into Chapters 10 and 11 of the Data Protection Act 2018).
ii. "Special categories of personal data" includes: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.
iii. The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
iv. Specifically, in relation to the work of the ICT, the prohibition against the processing of sensitive personal data shall not apply if:

    a) There is a specific legitimate interest in obtaining and processing the data. For example, different cultures or religions may observe specific medical practices in the event of injury and/or customs in the event of bereavement which need to be identified and respected.
    b) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
    c) Processing is necessary for the performance of a task carried out in the public interest.

3.5 What are the responsibilities of organisations under the Legislation?

Article 5 of the GDPR, which has been translated into Chapter 2(34) of the Data Protection Act 2018, sets out the following six key principles which lie at the heart of the general data protection regime and which require that personal data shall be:

i. Processed lawfully, fairly and in a transparent manner in relation to individuals.

ii. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

iv. Accurate and kept up to date.

v. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

vi. Processed 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.

Article 5(2) of the GDPR, which has been translated into Chapter 4(57) of the Data Protection Act 2018, requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles". For the purposes of this Guidance Note, the controller is the company on whose behalf the personal data is being collected from the affected individuals.

3.6 What are the lawful bases for processing data?

There are six lawful bases under which processing of personal data can happen. These are set out in Article 6 of the GDPR[2] and in Schedule 9 of the DPA 2018[3]. The lawful basis under which ICTs should collect personal data is Legitimate Interest.

A Legitimate Interest assessment has been carried out and is provided in Appendix A.

Under the Legislation, organisations should inform people upfront about the lawful basis for collecting and processing their personal data, by way of a Privacy Notice at the point of data capture. However, where the situation does not allow for this to happen, such as in the event of a major incident, a Privacy Notice may be provided retrospectively.

ICT members should always have a copy of the Privacy Notice available when engaging with Survivors[4] but should use their discretion to assess whether the situation is such that it is either not feasible or not appropriate to provide it at that point. They are not breaking the law if they choose not to, however, the Survivor must still be provided with the Privacy Notice as soon as practically possible.

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
[3] http://www.legislation.gov.uk/ukpga/2018/12/schedule/9/enacted
[4] A copy is provided in the Rail Care Team Member Resource Kit

3.7 What rights do individuals have under the Legislation?

Individuals have a number of rights in relation to their personal information and this is relevant to the work of the ICT and is therefore of particular note.

Right	At a glance	What does this mean for the ICT?
The right to be informed	A right to be informed of how their personal data will be used.	The ICT must tell individuals how they are using their personal data.
The right of access	A right to access their personal data and supplementary information.	If a Survivor (or any other data subject) asks for their personal data, the ICT is required to and must be able to provide it to them if they have such data.
The right to rectification	A right to personal data being rectified if it is inaccurate or incomplete.	The ICT must be able to correct any erroneous information held about a person.
The right to erasure	A right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.	Unless there is a specific reason for continuing to hold information (further details on the ICO website on this), data must be erased if requested by the individual.
The right to restrict processing	A right to 'block' or suppress processing of personal data (can still be stored).	The ICT may be asked not to process information held about them.
The right to data portability	A right to obtain and reuse their personal data for their own purposes across different services.	The ICT must provide individuals with a copy of their personal data for use elsewhere if required – this could relate potentially to sharing with other emergency services, at the request of the individual.
The right to object	A right to object to their information being processed.	The individual can object formally to their information being processed by the ICT.
Rights in relation to automated decision making and profiling.	Not deemed relevant to ICT as no automated profiling or decision-making takes place.	N/A

4 ICO Data Sharing Code of Practice

4.1 Introduction

The Information Commission's Office's (ICO) Data Sharing Code of Practice,[5] published in October 2021 and available online at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice-1-0.pdf, provides a definitive source of information. It runs to 76 pages (plus appendices) – the remainder of this section comprises a summary of its key points within the context of an ICT deployment.

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

4.2 Description and purpose

Essentially, the ICI Code of Practice is intended to assist organisations in interpreting and complying with the legislation.

Describing itself as a practical guide for organisations about how to share personal data in compliance with data protection law and accountability obligations, the Code of Practice also contains some optional good practice recommendations. These do not have the status of legal requirements but aim to help with the adoption of an effective approach to data protection compliance. Its stated aim is to give individuals, businesses and organisations the confidence to share data in a fair, safe and transparent way. It also seeks to dispel myths and misconceptions about data sharing. It emphasises that data protection law is an enabler for fair and proportionate data sharing, rather than a blocker, and notes that sometimes it can be more harmful not to share data.

4.3 Sharing data in an emergency

It also makes it clear that data can be shared in an urgent or emergency situation as necessary and proportionate and that in such cases a decision about data sharing may need to be taken quickly – its advice is that '*in an urgent situation you should assess the risk and do what is necessary and proportionate*'. An example of an emergency situation is the risk of serious harm to human life.

4.4 Transparency

The key requirement for sharing of personal data is that it should be done fairly and in a transparent manner:

i. Individuals must be treated fairly and their data must not be used in ways that would have unjustified adverse effects on them.
ii. When you share personal data, you must ensure it is reasonable and proportionate.
iii. You must ensure that individuals know what is happening to their data.
iv. Before sharing data, you must tell individuals about what you propose to do with their personal data in a way that is accessible and easy to understand.

As an organisation, you must also ensure that the recipient of shared data understands the nature and sensitivity of the information and takes reasonable steps to be certain that security measures are in place.

Annex A to the Code is a checklist to help determine whether or not to share data.

4.5 Limitations

The above does not mean that any kind of data sharing is acceptable as long as it is in the interests of the individual. In some cases, some sharing may be appropriate and allowable whereas in other circumstances this will not be the case. Specialist advice should be sought from the undertaking's own DPO and legal advisers before any personal information is shared in the course of ICT activities to determine what is appropriate and allowed. They should be able to access additional advice if they are not in a position to provide the answer themselves.

5 Managing data collected by Incident Care Teams

5.1 Introduction

Data collected by ICTs must be handled safely and securely using appropriate organisational and technical security measures. This is the responsibility of the company on whose behalf the data is being collected. The security measures must be "appropriate" to the nature, scope, context and purpose of the processing and the risks posed to the rights and freedoms of individuals.

All companies should carry out a Data Protection Impact Assessment (DPIA) to identify risks with how the data is handled from the point to collection to the point of erasure.

The ICO Data Sharing Code of Practice strongly advocates use of DPIAs for the following reasons:

i. Some or all of the DPIA questions are likely to assist when assessing whether it is appropriate to share data, and whether it would be in compliance with the law.
ii. They are an invaluable tool to help assess and risks in any proposed data sharing and work out how such risks may be mitigates.
iii. DPIAs are a means of building in openness and transparency.
iv. They serve to demonstrate that such matters have been considered and documented.

Further information on DPIAs is available from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/.

5.2 Gathering information

Information about persons involved in or affected by a rail incident could be collected by a number of people and departments within a railway undertaking. This document does not describe what means are used to collect data, as these will be determined by each railway undertaking.

Subject to the caveats included in Section 3.6, a Privacy Notice should be provided at the point of collecting personal data from an individual. It is good practice to have the notice displayed on the form used to collect the data, whether that be online or paper-based.

An example Privacy Notice is provided in Appendix B. With one minor exception, the same wording is used for the Privacy Notice provided within the Rail Care Team Member Resource Kit.

5.3 How much information?

One of the six principles (see Section 3.5) of data protection is “Data Minimisation”, which means only collecting the data that is relevant to the purpose for which you are using it.

When asking for personal information, consideration should always be given as to whether there is a valid reason for requesting it in the context of providing humanitarian assistance to a person.

For example, asking for information about someone’s religious beliefs may not be necessary in normal circumstances (i.e. in the context of providing a rail service), but may be very important in an emergency situation. It may help identify dietary requirements, affect the medical treatment they wish to have, or how they wish a deceased loved one to be treated. In this case, it is acceptable for the ICT member to ask for and collect this information as it is in the person’s interest for this to be done.

5.4 Sharing information

The Privacy Notice covers sharing information with other agencies. Although data protection legislation is in place to avoid the inappropriate sharing of information, many people would expect emergency responders to share information when it is in their interest or that of the individual concerned to do so.

For example, it would be reasonable to expect that the police or health authorities may need access to some of the information held by railway undertakings about individuals in order to investigate the incident and/or to provide appropriate healthcare in the aftermath.

As noted in Section 4.3, the ICO Data Sharing Code of Practice clearly states that data can be shared in an urgent or emergency situation as necessary and proportionate and that in such cases a decision about data sharing may need to be taken quickly, also in some circumstances it can be more harmful not to share data.

The Privacy Notice in Appendix B sets out clearly that there is a legitimate lawful basis for such information to be shared. The ICT member must, at the earliest opportunity, inform the individual that the information has been and/or is being shared with a third party and for what reason – ideally this should be before any such sharing has taken place.

The ICO Data Sharing Code of Practice referred to above applies equally to the sharing of data by external agencies – such as the police and hospitals - with the railway undertaking. However, beyond noting that any such data must be treated in the same manner as data captured directly from the data subject by the railway undertaking, this falls outside the scope of this Guidance Note.

5.5 Data sharing agreements

The ICO Data Sharing Code of Practice advocates use of data sharing agreements for the purposes of explaining the specific aims, why the data sharing is necessary to achieve those aims and the benefits it is hoped to bring to individuals or to society more widely. However, data sharing agreements are not mandatory and are rather more practical to put in place where data is regularly and routinely shared between organisations than in an emergency situation.

5.6 Storing, retaining and erasing information

A railway undertaking's duties under the Legislation apply throughout the period of processing personal data – as do the rights of individuals in respect of that personal data. Railway undertakings must comply with the Legislation and recognise that this extends from the moment the data has been obtained, through its storage and up to the point of its eventual erasure.

The duties extend to the disposal (erasure) of personal data when it no longer needs to be kept. There are no specific minimum or maximum periods for retaining personal data. Instead, the principle is that personal data should not be retained longer than necessary, in relation to the purpose for which such data is required/processed.

Railway undertakings holding personal information will need to:

i) Review the length of time such data is kept. Compliance with the Legislation does not prevent the retention of information as potential evidence in subsequent legal proceedings

ii) Consider the lawful basis and purpose or purposes the information is being held for in deciding whether (and for how long) to retain it.

iii) Securely delete/erase/destroy information that is no longer needed for the purposes for which it was collected. This applies to any printed copies of electronically stored information and equally to handwritten notes that have subsequently been digitised.

iv) Update, archive or securely delete/erase information if it goes out of date. This is less likely to affect railway undertakings as the information stored relates to a specific period in time (i.e. when the incident happened). However, it may be relevant for some information if this needs to be updated in order to continue to provide assistance to individuals and their families in the months and years after the incident.

It is worth bearing in mind that inquiries into major incidents may only begin years after the event and could continue for many years after that. In an inquiry, any and all information may be called upon as evidence. Therefore, all records, even scraps of paper that may seem insignificant, may be needed.

ICT Champions should ensure their organisations have an appropriate data retention policy in place which sets out how long personal data should be retained and for what reason. Organisations will have different retention periods for different kinds of information or depending on the scale of the incident. There is no specific precedent, as this is up to each organisation to determine for themselves.

The railway undertaking's emergency management team and DPO should be able to advise ICT Champions on appropriate timescales for and methods of retaining information. Particular care should also be given to how data is erased/destroyed - this must be done securely and in a way that does not prejudice the interests of the individuals concerned. This applies in respect of both electronic and paper records.

In the unlikely event that there is nothing formal in place within a particular railway undertaking, it is a good idea to start thinking about how long information should be kept, balancing the principle that personal data should only be kept for as long as is necessary with the fact that information and notes may be needed for a trial, inquest or inquiry which could be years away. During the time that the information is kept, it will need to be stored properly so that access to it is controlled.

All information relating to an incident response will need to be stored in an appropriate way. This means that it will need to be kept securely, i.e. in a place where access is only provided to those who need to see it. Physical records could, for example, be kept in a locked storage area, bearing in mind that over a period of years, boxes and physical files may need to be moved from one storage location to another or that the organisation may move premises.

Digital records should be kept in an encrypted and password protected folder on the organisation's computer servers and again appropriate steps should be taken to ensure the continued security of that information. Access to information should be limited only to those who need it. It is also good practice to consider how to ensure data integrity and availability. Many organisations utilise storage which has fire and flood protection, and this is then also backed up electronically. This is general good practice for data management and remains relevant for ICT activities.

6 Recommendations for ICT Champions

6.1 Introduction

This Section pulls together the key recommendations for ICT Champions – working with their organisation's DPO and legal team - to ensure compliance with the Legislation.

6.2 Recommendations

Recommendation 1

In advance of any deployment of the ICT, railway undertaking ICT Champions should familiarise themselves with

- What constitutes 'personal data' and 'sensitive personal data' (see Section 3.4)
- The key requirements for sharing of personal data (see Section 4.2)
- The six key GDPR principles (see Section 3.5)

and assure themselves that the above can and will be respected in the event of an ICT deployment.

Recommendation 2

In advance of any deployment of the ICT, railway undertaking ICT Champions should identify their organisation's designated DPO and make contact with them to discuss the nature of information that is being collected through the ICT and how it is being used, managed, and retained or destroyed. If the ICT function is separate from the Emergency Management and or Business Continuity Team, then those individuals should also be part of any ICT related discussions.

The DPO should be asked about:

i. Any organisational policies or procedures relevant to data protection.

ii. Any organisational policies and procedures relating to data management, storage, retention and erasure/destruction.

iii. How best to handle any requests from Data Subjects in respect of their personal data.

iv. How best to manage specific requests for data sharing from other organisations during incidents.

v. How best to manage any personal information already held on file from previous incidents.

Recommendation 3

As any other than the most generic of ICT support is likely to be focussed on the individual Survivor, it follows that personal data will need to be collected and processed. Having a legal basis for this is therefore an absolute pre-requirement and without one such support must not be offered.

The legal basis which is recommended in this Guidance Note is that of Legitimate Interest. The rationale for this legal basis is set out in the Legitimate Interest Assessment in Appendix A.

Recommendation 4

Railway undertaking ICT Champions and RDG should ensure that any information collection methods (forms, etc.) contain a statement providing the following:

i. Why the information is being collected.

ii. The lawful basis for data collection and processing.

iii. How the information will be used.

iv. With whom the information might be shared.

v. The contact details for the DPO (of the railway undertaking whose train is involved).

vi. How to request rectification of any errors in the data held.

vii. Who to complain to (for the UK this is the Information Commissioner's Office).

This statement is known as a Privacy Notice and an example has been provided in Appendix B.

Recommendation 5

In the event of an ICT deployment, the appointed Deployment Manager should make urgent contact with the DPO advising them of the circumstances. They should seek re-assurance from the DPO in respect of the points referred to above, both as an aide-mémoire and to confirm that understanding of the Legislation in the context of an ICT deployment on the part of the Deployment Manager remains up to date and sufficient.

7 Other sources of information

The Information Commissioner's Office:

The ICO's website can be found at: https://ico.org.uk/

That part of the website which is 'For organisations' is at https://ico.org.uk/for-organisations/

This then provides links to a variety of documents, the most relevant of which to this Guidance Note are:

i. Guide to Data Protection: https://ico.org.uk/for-organisations/guide-to-data-protection/.

   This is described as being aimed at small and medium-sized organisations, but potentially also being of use to larger organisations.

ii. Guide to the UK General Data Protection Regulation (UK GDPR): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

   Described as 'The GDPR, as it applies in the UK. It applies to most UK businesses and organisations'.

iii. Data sharing information hub: https://ico.org.uk/for-organisations/data-sharing-information-hub/ .

This in turn has links to a number of other resources, the most relevant of which to this Guidance Note are:

a. Data Sharing: a code of practice: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/ – see under Section 4.

b. Data sharing myths busted: https://ico.org.uk/for-organisations/data-sharing-information-hub/data-sharing-myths-busted/.

Appendix A – Legitimate Interest Assessment

A1 Background and context

The UK's Passenger Train Operating Companies have a Duty of Care – this applies not only to their passengers and staff but also extends to others affected by their activities. In respect of passengers, the train operator is responsible for their safety, security and general well-being for the duration of the rail element of their journey.

In the vast majority of cases the journey is completed uneventfully and specifically without any of these being compromised. But occasionally incidents may impact on one or more of these elements. On very rare occasions, such incidents may be serious enough to result in significant injuries or even fatalities and will be life-changing events not only for those directly involved but also for their family members, friends and colleagues.

To provide an appropriate humanitarian response in such cases, the Train Operating Companies deploy what are known as Rail Incident Care Teams (RICTs[6]). Made up of specially selected volunteers who have been trained in how to respond to the needs of those involved in or affected by major incidents, these Teams will be sent to emergency reception centres, hospitals, stations and other locations where those in need of such support congregate. Their purpose is to offer practical (including financial) and emotional support. In doing so, they work alongside and complement other responding agencies – most obviously local authorities, health services and police Family Liaison Officers (where deployed) – as part of the overall multi-agency response. Clearly those offered RICT help and support are not obliged to accept it, but experience shows that the majority will do so.

To provide this help and support, it is necessary to collect, store and process personal data. At its most basic this includes names and contact details for the person involved and their family/friends. However, for this help to be most effective, it is also beneficial to capture sensitive personal data. This includes religion (as failure on the part of the RICT member to respect particular religious protocols/rites may cause offense and/or further trauma), physical disabilities (as these will need to be taken into account when arranging transport or overnight accommodation) and mental impairments. Sharing such information with partner agencies will in turn allow their responses to be specifically tailored to the needs of the individual.

A2 Basis for capturing, storing and processing personal data

Of the various legal bases for capturing, storing and processing personal data available to comply with the GDPR we believe the most appropriate to apply in respect of RICT work – which is specific to the provision of humanitarian response in the immediate aftermath of a major rail incident – is '**legitimate interest**'. Other options have been considered but rejected on the following bases:

- **Contractual obligation**: While a contract exists between a passenger and the Train Operating Company, this is not the case for family members/friends of the passenger who may not have and may never have had any relationship with the rail industry.
- **Legal obligation**: Not applicable as there is no legal obligation on the part of a train operator or the rail industry as a whole to provide RICT support – rather, it is something that train operators choose to do.
- **Vital interests**: Not applicable – RICT work will rarely, if ever, involve 'life and death' situations/decisions.
- **Public task**: RICT work is focused on individuals and does not impact in any direct way on the public at large.

[6] Note that the term RICT is used here as this section is intended for an external audience. It has the same meaning as ICT.

- **Consent**: RICT work involves engaging with individuals in what is a particularly traumatic and challenging situation for them and therefore one in which it is unreasonable to ask them to understand and give due consideration to what giving consent to their personal data being shared means. It is therefore doubtful that 'consent' given in such circumstances could be regarded as 'freely given' and having provided 'real choice and control'. An additional practical consideration is that those without sufficient understanding of English would need any consent notice translated which would inevitably create a delay in providing them with support.

A3 Assessment of Legitimate Interest

A3.1 Context

The following applies only to the specific circumstance of provision of Train Operating Company humanitarian response through Rail Incident Care Teams in the event of a rail incident requiring such a response.

A3.2 Legitimate interest

The UK's passenger Train Operating Companies have a legitimate interest in providing humanitarian support, i.e. practical and emotional support, to those whose lives are affected by rail incidents, either because they themselves have been involved or because they are family members/friends/colleagues of someone directly involved.

This forms part both of the Duty of Care that Train Operating Companies have for their passengers and their moral responsibilities.

It also allows Train Operating Companies to meet societal expectations that they will respond appropriately to such incidents as far as those involved/affected are concerned.

It demonstrates and allows them to meet corporate social responsibility.

The humanitarian response provided to the individual benefits them in a number of ways. Fundamentally, it allows them to focus on what is important at the time. For those directly involved, this will include such aspects as getting/keeping in contact with family/friends, replacement of lost or damaged personal items and taking responsibility for caring for pets. For their family members and friends it means they can focus on supporting their loved ones and removes the burden of arranging (and paying for) transport and accommodation and organising/funding meals, etc. For both, it also provides information and sign-posting which in turn help to promote choice and regaining of control.

Those with statutory responsibilities for responding to emergencies – in particular local authorities and health and police services – also benefit from rail industry provision of humanitarian response as it removes some of the burden (including financial) they might otherwise have to bear if Train Operating Companies pick up the costs of e.g. travel and accommodation.

A3.3 Why processing of personal data is necessary

For the post-incident humanitarian response provided by the Train Operating Companies to be most effective, it must be made available as a matter of urgency and must be tailored to the specific needs of the individual. This requires processing of personal sensitive data, including (but not limited to) age, physical or mental impairments and religious/beliefs. Without this information, those charged with providing the response may be poorly prepared to do so and cause further distress to those they are trying to help, or the provision of suitable help may be delayed.

Individuals will be given full choice in what personal information they choose to provide or withhold, with the RICT member able to provide an explanation as to why they are being asked for it and the consequences of them not providing it (e.g. declining to share their religion will mean that it will not be possible to allocate them an RICT member with an understanding of it).

The humanitarian response is targeted at the individual – there is no means of achieving this without the processing of personal data applicable to each such individual.

A3.4 Use of data

Where an individual declines the Train Operating Company's offer of humanitarian assistance there is no requirement to capture or process any personal data (other than to record this declining).

In all cases where the offer is accepted, then the data captured is what the individual would reasonably expect to be needed to provide that support.

This extends to the sharing of personal data with third parties – this will only be done where it facilitates the provision of support from such parties to the individual concerned and only within the context of the response to the incident. Examples include providing the name, contact details and any specific needs of an individual for whom overnight hotel accommodation is being arranged to the local authority in which the individual is resident in order that they can assume responsibility for the individual's longer-term care and support.

Overall, the benefits of processing personal data to the individual concerned are very significant in that it enables them to receive targeted support and assistance at a particularly critical time in their lives. Such data will be shared with third parties on the very strict understanding that it be used only in respect of the wider support being provided to the individual concerned within the context of the rail incident concerned.

Appendix B – Example Privacy Notice

The following wording is that included in the Rail Care Team Member Resource Kit with the single exception that the wording below has been updated to refer to the UK rather than the EU General Data Protection Regulation in the first sentence.

Privacy Notice

The purpose of this notice is to inform you how we will use your personal data and keep it safe, in compliance with the Data Protection Act 2018 (DPA18) and the UK General Data Protection Regulation.

Who we are
[INSERT COMPANY NAME HERE] is the name of our legal entity whose address is [INSERT ADDRESS HERE]. We are the Data Controller for all the personal data that you provide. To contact us regarding our use of your data can e-mail us at [INSERT EMAIL ADDRESS]. We provide a Rail Care Team ("RCT") to provide support to individuals in the event of an incident occurring on the railway.

Our lawful basis for collecting your data
We collect and store your personal data on the lawful basis of Legitimate Interest. It is necessary for us to hold your personal data in order that we can exercise our duty of care to you in respect of an incident that occurred on the railway.

What data we collect
We adhere to the principle of "data minimisation" and only collect the personal data that we may require in order to provide you with appropriate support in response to the incident.

Sharing information with third parties
To provide you with the right support and assistance, we may need to share your information with partner organisations. Depending on your needs, these may include the police, NHS organisations, local authorities, Kenyon International Emergency Services, Faith Communities, the British Red Cross and animal welfare organisations. Where information sharing does happen, we will inform you that it has taken place and let you know what has been shared. Where we do share your data with a third party, it will be on the basis that it is used for the purposes which it was collected.

Keeping it safe
We protect your privacy by ensuring we have the appropriate technical and organisational security measures in place to process your data in an appropriate, lawful, and safe manner.

What we do with your data
Your personal information will be used by the RCT to provide you with practical and emotional support that matches your needs and requirements. We will not use your personal data for any other purposes.

Storage and retention of your data
We will retain your data for as long as it is needed for its original purposes. In the event of a major incident, we may determine that we need to hold on to your personal data until after the incident investigation is complete and legal action has been taken.

Your rights regarding our use of your data
You have certain rights regarding how we use your data, and we are committed to upholding those rights, which are set out below.

- **Right of Access** - to request that we give you a copy of all the data we hold about you, this is called a 'Data Subject Access Request'.
- **Right to rectification** - to request that we update your personal data.
- **Right to complain** - If you believe at any time that we have acted outside the terms of this Privacy Notice you have the right to lodge a complaint with the Information Commissioner's Office. They can be contacted via https://ico.org.uk/, or by telephone at 0303 123 1113.

How to contact us

To exercise any of your rights set out above you can e-mail us directly at the email address shown at the start of this Privacy Notice.

Alternatively, you can write to us at the company name and address shown at the start of this Privacy Notice.

NOTE: *To process any request, we must first verify your identity before your data can be changed or released to you.*

Rail Delivery Group

National Rail

Rail Delivery Group Limited Registered Office, 2nd Floor, 200 Aldersgate Street, London EC1A 4HD
www.raildeliverygroup.com 020 7841 8000 Registered in England and Wales No. 08176197