Rail Delivery Group

National Rail

RDG-GN038

Issue Three

Date May 2019

Guidance Note –

Data Protection Requirements During and After Incidents

Synopsis

This document describes and explores the requirements of the General Data Protection Regulation and the Data Protection Act 2018 (together the "**Legislation**") within the context of personal data gathered as part of the Incident Care Team deployment to an incident. It is directed specifically at those with responsibilities for Incident Care Teams.

Applicability

This Guidance Note has been prepared for passenger train operating companies. However, its content may also be of use to others.

Authorised by

James Burt

Chair, RDG Incident Care Team Management Group

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. It had been understood that the Cabinet Office was drafting a revision to its 'Data Protection and Sharing – Guidance for Emergency Planners and Responders: Non-Statutory guidance to complement Emergency Preparedness and Emergency Response and Recovery', as first published in 2007, to encompass GDPR but with nothing further heard concerning this, the position regarding this is unclear.

In all cases of ICT deployment, it is strongly recommended that early contact be made with the TOC 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.

Issue record

Issue	Date	Comments
One	September 2016	Original version as an ATOC document.
Two	May 2018 (withdrawn September 2018)	Updated to reflect requirements of GDPR and reformatted as an RDG document. Withdrawn due to lack of consensus on best legal basis for compliance.
Three	May 2019	Following receipt of advice that 'legitimate interest' provides the best legal basis for compliance.

Contents

Part 1 About this document

1.1 Responsibilities

1.1.1 Copies of this Guidance Note should be distributed by RDG members to persons within their respective organisations for whom its content is relevant.

1.2 Explanatory note

1.2.1 RDG produces RDG Guidance Notes for the information of its members. RDG is not a regulatory body and compliance with RDG Guidance Notes is not mandatory.

1.2.2 RDG Guidance Notes are intended to reflect good practice. RDG members are recommended to evaluate the guidance against their own arrangements in a structured and systematic way. Some or all 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 to adopt) elements of the guidance should be documented.

1.3 Guidance Note status

1.3.1 This document is not intended to create legally binding obligations between railway duty holders and should be binding in honour only.

1.4 Supply

1.4.1 Copies of this Guidance Note may be obtained from the RDG members' web site.

Part 2 Introduction, purpose and scope

2.1 Introduction

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

2.1.2 This version (Version 3) of this Guidance Note has been updated and re-issued to reflect the introduction of revised data protection legislation in 2018.

2.1.3 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 should have already considered how ICT activities are affected by data protection regulations under the Data Protection Act 1998, but will now need to understand how the new Data Protection Act 2018 and the General Data Protection Regulation 2018 (hereafter referred to in this Guidance Note as the "**Legislation**") affect them.

2.1.4 The Legislation introduces a duty for organisations whose core activities require large scale, regular and systematic monitoring of individuals to appoint a Data Protection Officer (DPO) – it is expected that this will apply to TOCs. 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.

2.2 Context

2.2.1 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. 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 applicable legislation.

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

2.2.3 The intention of the Legislation is not to prevent the sharing of personal data but rather to ensure that this is done in a controlled way and only when it is in the best interests of the individual concerned. Although the following extract from the Cabinet Office's 2007 document Data Protection and Sharing in Emergencies[1] was written with the previous legislation in mind, the last sentence still applies.

"*Limitations on the initial collection and subsequent sharing of data between the police and humanitarian support agencies hampered the connection of survivors to support services like the Assistance Centre. The concern at the time was that the Data Protection Act might prevent the sharing of personal data without the explicit consent of those concerned. As a result, there were delays in information reaching survivors about the support services available. An over-zealous or incorrect interpretation of the duties imposed on public organisations by the Data Protection Act has been previously identified in the Bichard Inquiry as a cause for concern. That inquiry found no reason why, where the sharing of data was appropriate and for a good purpose, it should not be done*."

2.2.4 The above does not mean that any kind of data sharing is OK 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 before sharing any personal information in the course of ICT activities to determine what is appropriate and allowed. Sources of such advice will include the Information Commissioner's Office and the TOC's own DPO and legal advisers, who should be able to access additional advice if they are not in a position to provide the answer themselves.

2.2.5 A wealth of information exists online about the 2018 data protection legislation; this Guidance Note draws heavily on the Information Commissioner's Office Guide to the General Data Protection Regulation (GDPR) available online at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

[1] Full title: Data Protection and Sharing – Guidance for Emergency Planners and Responders: Non-Statutory guidance to complement Emergency Preparedness and Emergency Response and Recovery

2.2.6 The Cabinet Office's 2007 document 'Data Protection and Sharing During Emergencies'[2] is also of relevance, being particularly helpful in guiding organisations through this delicate balancing act, but as mentioned at the start of this Guidance Note, it is unclear whether and, if so, when a version of this updated to reflect the current legislation will be published. In the absence of this, in cases where there is any confusion over the right course of action, further advice should be sought from the ICO and the Cabinet Office.

2.3 Definitions used within this document

2.3.1 A glossary of terms is provided in Appendix B: Glossary.

Part 3 New Data Protection Legislation

3.1 Introduction

3.1.1 This Part explains the basics of the Legislation and is based on guidance from the Information Commissioner's Office (ICO), the UK's regulator for data protection.

3.2 What are the main differences between the new Legislation and the DPA 1998?

3.2.1 The new Legislation is very similar to the DPA 1998 in many aspects. Any railway undertaking already compliant with the DPA should therefore not face a significant challenge in meeting new requirements, however the main differences are provided here to assist.

Key area	Data Protection Act 1998	EU General Data Protection Act 2018; and the Data Protection Act 2018
Data breach	Businesses are under no obligation to report data breaches though they are encouraged to do so.	Any data breach must be reported to the Supervisory Authority within 72 hours of the incident. In the UK this is the ICO.

[2] Full title: Data Protection and Sharing – Guidance for Emergency Planners and Responders: Non-Statutory guidance to complement Emergency Preparedness and Emergency Response and Recovery

Data removal/Right to erasure	No requirement for an organisation to remove all data it holds on an individual.	An individual has the 'Right to erasure' – which includes all data including web records with all information being permanently deleted.
Reach	Only applicable to the UK.	Applies to the whole of the EU and, crucially, also to any global company which holds data on EU citizens.
Consent	Data collection does not necessarily require an opt-in.	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	Non-compliance could result in fines of up to £500,000 or 1% of annual turnover.	The potential penalties for non-compliance are much more severe with fines of up to €20 million or 4% of the business' annual global turnover.
Data Protection Officer	No need for any business to have a dedicated DPO.	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'. TOCs 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) not a legal requirement under DPA 1998 but have always been 'championed' by the ICO.	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 outlining differences between current legislation and the previous Data Protection Act 1998

3.3 Who does the new Legislation apply to?

3.3.1 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 controller determines the purposes and means of processing personal data.

ii) A processor is responsible for processing personal data on behalf of a controller.

3.3.2 The Legislation places specific legal obligations on 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.

3.3.3 A controller is not relieved of their obligations where a processor is involved – there is an obligation to ensure any contracts with processors comply with the Legislation as well.

3.3.4 The Legislation applies to processing carried out by organisations operating within the EU. 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?

3.4.1 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 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.

3.4.2 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.

3.4.3 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.

3.4.4 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" include: 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?

3.5.1 Article 5 of the GDPR, which has been translated into Chapter 2(34) of the Data Protection Act 2018, requires that personal data shall be[3]:

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.

3.5.2 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] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/

3.6 What are the lawful bases for processing data?

3.6.1 There are six lawful bases under which processing of personal data can happen. These are set out in Article 6 of the GDPR[4] and in Schedule 9 of the DPA 2018[5]. The lawful basis under which the Incident Car Teams should collect personal data is Legitimate Interest.

3.6.2 A legitimate Interest Assessment has been carried out and is provided in Appendix C: Legitimate Interest Assessment.

3.6.3 Under the new 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.

3.6.4 ICT members should always have a copy of the Privacy Notice available when engaging with Survivors[6] 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.

3.7 What rights do individuals have under the new Legislation?

3.7.1 Individuals have a number of new 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	If a Survivor (or any other data subject) asks for their personal data,

[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[5] http://www.legislation.gov.uk/ukpga/2018/12/schedule/9/enacted

[6] A copy is provided in the ICT Member Resource Kit dated March 2019

	supplementary information.	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

Part 4 Managing data collected by Incident Care Teams

4.1 Introduction

4.1.1 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.

4.1.2 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.

4.1.3 All companies should have an erasure policy in place which clearly sets out how long the data is held, along with corresponding procedures to ensure erasure of data that is no longer needed.

4.2 Gathering information

4.2.1 Information about persons involved 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.

4.2.2 At the point of collecting personal data from an individual a Privacy Notice should be provided. It is good practice to have the notice displayed on the form which is used to collect the data, whether that be online or via paper form.

4.2.3 An example Privacy Notice is provided in "Appendix D: Example Privacy Notice" of this Guidance Note.

4.3 How much information

4.3.1 One of the six principles of data protection is "Data Minimisation", which means only collecting the data that is relevant to the purpose for which you are using it.

4.3.2 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.

4.3.3 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 their loved ones to be treated if they have died. 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.

4.4 Sharing information

4.4.1 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.

4.4.2 The Cabinet Office's 2007 document Data Protection and Sharing in Emergencies states: '*Its [The DPA's] job is to balance individuals' rights to privacy with legitimate and proportionate use of personal information by organisations. In the context of emergency planning – and, in particular, in the aftermath of an emergency – it is important to look at this balance critically and realistically*[7]'. 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.

4.4.3 The Privacy Notice in Appendix D 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.

[7] Baroness Ashton of Upholland, 2007.

4.5 Storing and retaining information

4.5.1 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 from the moment the data has been obtained until the time when the data has been returned or erased.

4.5.2 The duties extend to the way the personal data is disposed of (erased) when it no longer needs to be kept – this must be done securely and in a way that does not prejudice the interests of the individuals concerned. 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.

4.5.3 Railway undertakings holding personal information will need to:

i) Review the length of time such data is kept.

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.

4.5.4 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.

4.5.5 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.

4.5.6 The railway undertaking's emergency management team and DPO should be able to advise ICT Champions on appropriate timescales and methods of retaining information. Particular care should also be given to how data is erased/destroyed to ensure that this is done in an appropriate way – this applies in respect of both electronic and paper records.

4.5.7 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 premise 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.

4.5.8 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.

4.5.9 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, but remains relevant for ICT activities.

Part 5 Summary of key recommendations

5.1 Introduction

5.1.1 This Part summarises key recommendations for railway undertakings as a result of the changes to data protection legislation.

5.2 Key recommendations

5.2.1 In advance of any deployment of the ICT, railway undertaking ICT Champions should **identify their organisation's designated DPO**[8] 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 to 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.

[8] It is assumed here that as organisations routinely handling large volumes of data about staff and travelling customers, they are required under the GDPR to have a DPO.

5.2.2 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.

5.2.3 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 C.

5.2.4 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 TOC 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).

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

5.2.6 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 under Part 5.2.1, 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.

5.2.7 The Legislation extends to the storage and eventual erasure of the information.

5.2.8 Compliance with the Legislation does not prevent the retention of information as potential evidence in subsequent legal proceedings.

Appendix A: Other sources of information

The Information Commissioner's Office

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

This is the website for the ICO's general information guide to the GDPR

https://ico.org.uk/for-organisations/

This is the link to the website for general data protection information and guides (including GDPR)

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

This has links to self-assessments for a variety of areas including:

a) Controllers Checklists
b) Processors Checklists
c) Records Management
d) Data Sharing and Subject Access

Cabinet Office

Cabinet Office (2007) *Data Protection and Sharing – Guidance for Emergency Planners and Responders: Non-statutory guidance to complement* Emergency Preparedness *and Emergency* Response & Recovery.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf

Note: It is unclear whether this is to be replaced by new guidance aligned to the GDPR.

Appendix B: Glossary

i) **'controller'** means 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;

ii) **'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

iii) **'enterprise'** means 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;

iv) '**filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

v) **'group of undertakings'** means a controlling undertaking and its controlled undertakings;

vi) **'Legislation'** means the Data Protection Act 2018 together with the EU General Data Protection Regulation 2018;

vii) **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

viii) **'personal data'** means 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;

ix) **'processing'** means 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;

x) **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

xi) **'pseudonymisation'** means 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;

xii) **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

xiii) **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;

xiv) **'supervisory authority'** means an independent public authority which is established by a Member State pursuant to Article 51;

xv) **'third party'** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Appendix C: Legitimate Interest Assessment

C1 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[9]). 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 specific needs of the individual.

C2 Basis for capturing, storing and processing personal data

[9] Note that the term RICT is used here as this section is intended for ext

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.
- **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.

C3 Legitimate Interests Assessment

C3.1 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.

C3.2 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 companies pick up the costs of e.g. travel and accommodation.

C3.3 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

C3.4 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 share the majority of or all data with 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 D: Example Privacy Notice

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 EU General Data Protection Regulation 2018 (the GDPR).

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.*