# Rail-tech and data protection

**Katie Hewson**, commercial, outsourcing and technology associate and **Darren Fodey**, rail partner at law firm Stephenson Harwood explore some consequences of the General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) has revolutionised customers' expectations of how service providers handle their personal data over the past year and a half. This applies across all industries – and the railway is no exception. Increasingly, personal data is being used to better tailor services to customers and we can expect this to continue with rail-tech projects. Big data and smart ticketing technology creates tremendous opportunities but it must come with a degree of caution: handling customers' data in compliance with data privacy rules poses complex challenges. This is something to which customers are increasingly alive, particularly with high profile breaches in other industries gaining prominence in the national headlines.

Facing large fines if they get it wrong, organisations in the rail industry need to consider GDPR compliance in all aspects of their passenger data handling, from the security they put in place around passenger data to their sharing of customers' contact and journey details with ticketing companies, Network Rail and service providers.

### Innovation with data

The rail industry is moving towards greater, and more novel, uses of personal data. Recently, industry submissions to the Williams Rail Review have emphasised the need to improve passenger experience and to innovate, perhaps with tailoring the passenger experience to each individual. The rail industry, and train operating companies (TOCs) in particular, are making use of increasing amounts of passenger data and new technologies. The industry is exploring novel methods of obtaining and analysing passenger data and train operations, for example through on-train sensors, trackside signals and smart ticketing apps.

Smart ticketing involves the collection of far more passenger data points than TOCs could previously access. Such data can be put to a wide variety of uses, from behavioural analysis to targeted marketing and profiling. Big data covering millions of customer journeys can also be used for purposes such as transport and infrastructure planning.

### Increased amounts of personal data

The development of technology has also allowed the industry to tie much of the data that they hold to identifiable individuals. This means that, from a legal perspective, more and more passenger data qualifies as 'personal data'.

The GDPR and related data protection laws regulate only personal data. These laws impose particular requirements for the protection of personal data, which do not apply to regular, non-personal data. Non-personal data may be covered by other requirements (such as information security and/or confidentiality), but it does not fall within the scope of data protection law.

This does not mean that GDPR obligations can simply be bypassed by removing people's names from a dataset: the Public Transport Victoria case study below demonstrates that removing individuals' names does not necessarily prevent data from being personal data. Even data that does not contain identifying information can be personal data, if there is more than a slight hypothetical possibility that it can be reconstructed in a way that identifies an individual.

Technological developments are allowing rail sector bodies to identify more and more people from pieces of data, thereby bringing increasing amounts of information under the tighter data protection regime. For example, cookies and online identifiers can be classed as personal data, since they often uniquely identify a person (whether by means of an ID number, code or otherwise). Biometric information such as fingerprint data used for payments also qualifies since it is unique to each passenger. Even information that a TOC only sees in aggregated form, but has someone process and strip out the raw data on its behalf, such as usage analytics, may be personal data for which the TOC is responsible, depending on the exact terms of the collection and handling of this data.

In the days of paper tickets, all that a TOC may have known about the purchase of a ticket was which machine it was issued from and when, and what the destination and ticket type was. However, now (particularly if a ticket was purchased online or through an app), the TOC may know the traveller's email and postal address, name, phone number and that customer's previous purchases and interactions with the TOC. They may even have built a profile of that customer, predicting their future

journeys and including information about their interests derived from their website browsing activities or interactions with adverts. All of this information is likely to be personal data and it will all need to be handled in compliance with the GDPR requirements.

### Increased risks

While many of these developments in technology have clear benefits to TOCs and others, including convenience and cost reduction, those using passenger data need to be aware of their responsibilities when innovating and the dangers of getting it wrong.

In particular, technological advancements bring increased risk and exposure to cyber-crime. With more personal data in use, there are greater risks of cyber criminals or commercial organisations misappropriating it.

The security landscape is constantly changing, with more complicated attacks being developed all the time and it is imperative that the rail industry keeps pace with these developments to protect their data and critical infrastructure. The more the industry relies on digitisation, the bigger the possibility of attack and the higher the risk to passenger safety and security of rail assets. Breakdowns, signal failures, software failures, and passenger data breaches are all potential consequences of a cyber-attack, let alone the possible reputational and financial damage. This is a very real risk for TOCs, as Great Western Railway discovered when its accounts were hacked a couple of years ago. No financial information was compromised in the attack but approximately 1,000 GWR accounts were accessed using an automated system, which harvested password details from other areas of the web.

For further thoughts on cyber security in the rail industry, please see our previous article in this series.

### Increased regulation

As the uses to which rail data can be put have grown, and the risks themselves have grown, regulation of those uses has also become more onerous, in an attempt to ensure that data is used and kept responsibly.

There is also far more scrutiny over whether companies are fulfilling their legal obligations in relation to data, both from regulators and from customers themselves, who have greater awareness of their data rights. The key area of legal regulation here is the GDPR. This applies throughout Europe (and beyond, where goods and services are supplied to Europeans, or they are monitored). It has also been incorporated into domestic UK law, so it will continue to apply, even after Brexit.

Key GDPR requirements that must be borne in mind in a rail-tech context are:

- scope
- accountability and design
- consent
- consent/direct marketing
- breach notification
- privacy notices
- rights of data subjects
- fines.

### Scope

The GDPR's definition of personal data includes pseudonymised personal data. This means data to which pseudonyms have been allocated to conceal the identity of the data subject. It also includes location data and online identifiers. For TOCs, this means that a wide range of data processed falls within the remit of the GDPR's obligations: many types of cookies and trackers, for example, will be personal data.

### Accountability and design

There is an emphasis on being able to evidence compliance with the GDPR, including by carrying out Privacy Impact Assessments for high risk projects to help assess and minimise their effect on privacy rights and keeping detailed records of consents obtained. TOCs must also implement so-called 'privacy by design and default' internal processes that embed data protection principles into every stage of a new rail-tech project.

### Consent

When a TOC is relying on obtaining consent to process data, the consent given must be a very clear and explicit statement, which must be separate from other terms and conditions. Consent also must be a positive opt-in and consent should not generally be a pre-condition of signing up to a service. TOCs must check that their consent practices are in line with this high standard.

### Consent/direct marketing

Under separate legislation, prior opt-in consent is required for the placing of any cookies (or similar technology) on a device, and for the sending of a direct marketing message. Any consent to receive cookies or direct marketing must also be to GDPR standard. Consent opt outs must be honoured. This can have a big impact on rail-tech projects, particularly as they often rely on the placing of cookies, pixels or similar.

### Breach notification

Organisations will need to report a personal data breach to the Information Commissioner's Office within 72 hours and inform data subjects of a high-risk breach. With TOCs increasingly using information of value to hackers in rail-tech projects – such as card and bank account details and journey information – security is of the utmost importance and security lapses are likely to be subject to enforcement action.

### Privacy notices

The requirements for the content of privacy notices are fairly lengthy and prescriptive, meaning that most rail-tech projects are likely to require a review of the existing privacy terms to make sure they give transparent information about the new project's use of personal data. New notices may need to be developed, or methods of giving 'just in time' fair processing notices at the point data is collected.

### Rights of data subjects

Data subjects have wide-ranging rights, including a more extensive 'right to be forgotten' and strengthened rights to object to processing. There is also a right of portability allowing for free transmission of data in commonly used formats. There have been a greater number of complaints about data protection since the GDPR was introduced and these broader rights were widely publicised. Companies undertaking a rail-tech project need to ensure that they comply with and help people exercise their rights, including by fully informing them of what those rights are and designing systems to make sure that requests are quickly acted upon.

#### Case study: Public Transport Victoria

Just because individuals' names are not included in a dataset does not mean that the data is not personal data, if there are unique identifiers or characteristics of individuals that can be ascertained from the data. The Australian train operator Public Transport Victoria discovered this to its cost when it released what it claimed was 'de-identified' travel history data (tap in and out information) from smart cards to assist with a data science company's big data "datathon". Although there were no names, addresses or similar obvious personal information included in the information published, the unique travel histories of particular individuals could be traced over time and could in theory have been used to re-identify people and to give insight into their movements and behaviours. Obviously, Australia is not subject to the GDPR, but the Australian test of 'identifiability' is similar to those used under the GDPR to consider whether information is personal data and therefore subject to the GDPR.

### Fines

Maximum fines are now up to four per cent of an organisation's worldwide turnover, or €20 million (£17 million). This represents a huge increase on the previous maximum sanction of £500,000 and provides a big incentive to comply.

### What next?

Rail companies need to carefully consider their privacy obligations before launching a rail-tech project. All this data protection regulation can sometimes be seen as putting the brakes on innovation. This need not be the case. In fact, rail-tech innovations can assist with embedding privacy rights into projects that can have real benefits for the public. This could include by providing data subjects with the ability to manage their consents and privacy settings on the go, through a TOC's app.

What the regulation around personal data does mean is that it is more important than ever to bear in mind the protection of personal data from the very start of a rail-tech project.

The Information Commissioner herself has frequently said that 'privacy does not have to be the price we pay for innovation. The two can sit side by side. They must sit side by side'.