NetworkRail

Fair, accountable and safe: our data protection handbook

Contents

An introduction from our Chief Executive

Information is one of our greatest assets; it's critical that we know how to look after it. To deliver as a high-performing organisation, we must know what information we have and where, we must keep it safely, and we must ensure fairness, transparency and accountability.

We have some challenges ahead. As we handle such vast amounts of personal information across the organisation every day, changes to data protection legislation, for example, mean big changes. The General Data Protection Regulation (GDPR) is one such new data protection law which will come into effect in May 2018, and this will mean different regulations for handling personal information.

This handbook outlines the types of things we should all be thinking about when we're dealing with personal information. Protecting information, whether through an improvement in our day to day processes or ensuring the right controls at the outset of a new project, is an essential step in not only helping us comply with our legislative duties, but also in being better every day.

Mark Carne,
Chief Executive

What is personal information?

Personal information (or personal data as it's sometimes called) is any information relating to someone you can or could identify.

It's important to remember that someone can be identified not just by their name, but also by things like reference numbers and location data. Personal information includes a wide variety of information – for example a rota, next of kin details, a list of birthdays that you hold for your team, HR records, or contact details of your customers and suppliers.

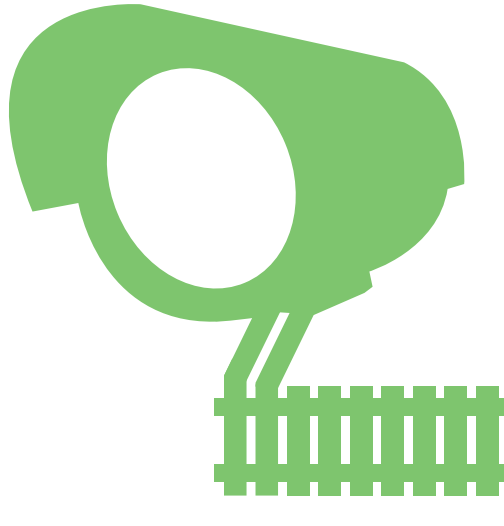
Sensitive personal information can include information about people's ethnicity, sexuality, physical and mental health and whether they have been convicted of a crime.

Anonymised information is information which has had all identifiers removed. It's the opposite of personal information because it's no longer possible to identify someone from it.

A car registration number, matched with DVLA records of who the registered keeper is.

A surname and a town of residence alone, matched with electoral register data.

CCTV footage, matched with a register of attendees at an event.

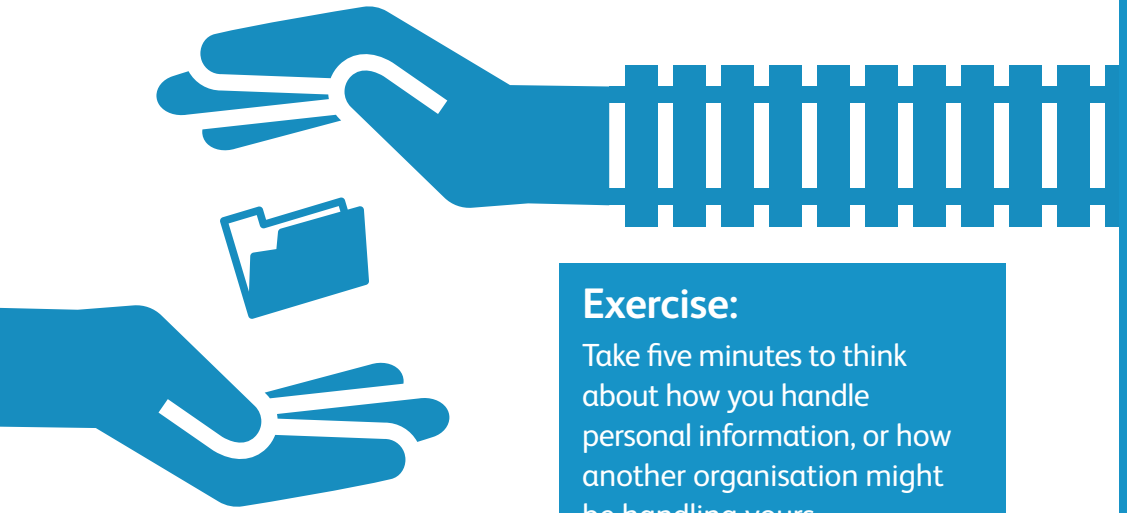


What is data protection?

Data protection helps us handle people's personal information fairly and safely.

It's not just about data stored on computers – it's about people's right to respect for their personal information. It can also cover paper records, video and audio recordings, phone calls, text messages and social media.

Network Rail has a duty to comply with data protection laws. Activities covered by these laws aren't limited to collecting or disclosure of the information, but also cover recording, organising, storing, altering and transferring the information.



Exercise:

Take five minutes to think about how you handle personal information, or how another organisation might be handling yours.

Question:

Do you know how you should be treating the information you deal with, or how another organisation should be treating your information?

Key terms – Data protection legislation uses some key terms, which explain our different responsibilities throughout Network Rail.

Definitions…

Processing

Anything done to the information. That might be collecting or recording the information. It could be how it's organised, stored or adapted. It also covers how we retrieve, use and make the information available, and how we delete it when we're finished with it.

Data subject

The person who the personal information relates to.

A data subject might include:

- A passenger in a station
- An employee
- A visitor to our premises.

Data controller

The person or organisation which decides why and how personal information should be processed – normally, at work, this will be Network Rail.

Data processor

A person or organisation who processes personal information on behalf of a data controller.

A data processor might include:

- A records management company, holding our old paper records
- A cloud service provider, holding HR records
- A third party parking provider, holding records of our staff with entitlement to park.

Network Rail has responsibilities. As a data controller we must...

- Tell the regulator (the Information Commissioner's Office) if we suffer a data breach
- Have appropriate security measures in place
- Consider the privacy of others in everything that we do
- Know what personal information we have, and where we keep it
- Make sure people know their rights
- Put in place a data protection officer and relevant policies
- Make sure our partners work within the law
- Tell people what we are doing with their personal information
- Make sure people know the law is changing

A CLOSER LOOK...

Stefan applies for a role in Network Rail. His CV is sent to Karen, the interviewing manager, who decides to progress his application. Karen records their interview using handwritten notes, which she transcribes into an electronic document and sends to HR. She then places the handwritten notes in the confidential waste container. A third party contractor collects and safely destroys the confidential waste in line with our procedures.

In this case Stefan is the **data subject**, because his personal information is included in both his CV and the interview notes. The **data controller** is Network Rail, because we have organisational rules on how long Karen should be keeping the information for, and how it should be destroyed. The contractor is the **data processor**, because it is acting on our instructions.

Why is data protection important?

The General Data Protection Regulation is a legal requirement, but we can all benefit from good data protection practice – it means that our own personal information is given the respect it deserves, and gives us control over how it is handled.

Business Benefits – If we do data protection well it is a great opportunity to ensure we keep only the information we require.

High quality data – If we look after our information well, it will be more accurate and will help us make more informed decisions.

Trust and privacy – Trust builds reputation and can be easily lost when we suffer data breaches. Being open and honest around how we use data will help us build integrity.

Compliance – We all have a responsibility to comply with the law. If we don't, we risk being fined by the regulator.

The regulator has the power to issue fines for breaches of data protection law. Under the General Data Protection Regulation this is up to 4% of global annual turnover. For Network Rail this could be hundreds of millions of pounds.

Did you know?

In the past the regulator has fined:

- Talk Talk **£400,000** for security failings that allowed a cyber attacker to access customer data
- Greater Manchester Police **£150,000** for having a system in place which permitted the sending of unencrypted DVDs of witness interviews (some of which were then lost)
- 13 charities **£181,000** in total, for trading personal information and profiling donors' wealth without telling them

The regulator also has the power to serve enforcement notices. These notices can require data controllers to i) stop doing things the ICO thinks are in breach of the law or ii) do things to make sure they comply with the law. Failure to comply with an enforcement notice can be a criminal offence.

Imagine the potential cost if the regulator decided that a huge IT project had to be stopped for data protection reasons?

If we don't get data protection right, and we suffer data breaches or fines, it could have a significant reputational impact for Network Rail.

2017
'Wannacry' ransomware affects multiple NHS systems

2017
Cyber attack compromises accounts of 245,000 customers of payday loan company Wonga

2014
Millions of Yahoo user accounts accessed using 'forged cookies'

What does it mean for me?

We expect all our people to maintain the highest standards of data protection compliance.

Our reputation depends on us all maintaining the highest standards of business behaviour and acting with integrity in everything we do. That includes handling personal information fairly, with accountability, and safely.

So everyone should complete the relevant training, and comply with our policies and guidance which are designed to support the business. These can be found on our Connect community page.

Accountable

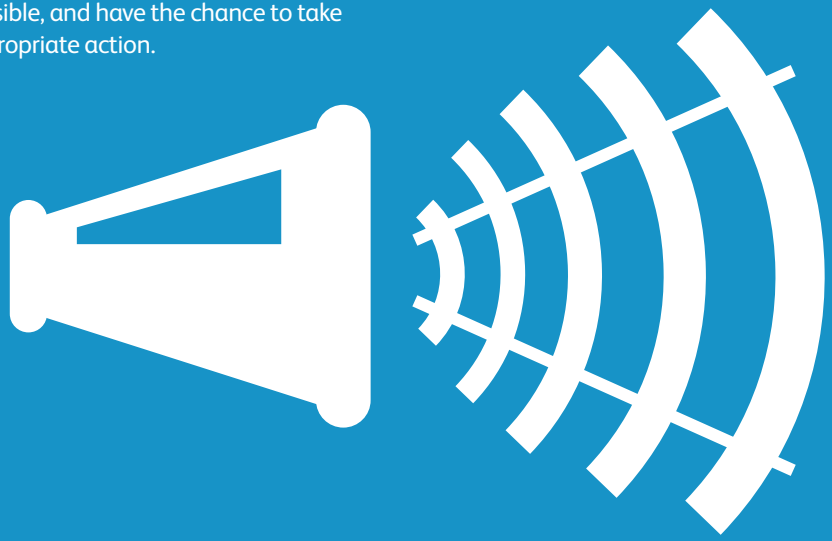
We are all accountable for how we handle people's personal information.

It's everyone's responsibility to keep personal information safe and to make sure that people's rights are respected. That includes understanding the risks when handling that information and taking appropriate steps to mitigate those risks.

Mistakes can happen, but it's important that we're open about them. **A data breach** – a breach of security leading to, for example, accidental loss, destruction or damage of personal information – can be contained, and harm avoided, but only if we know about it as soon as possible, and have the chance to take appropriate action.

Under the General Data Protection Regulation we are required to report serious breaches to the regulator within 72 hours, and in some cases to let the people whose information has been compromised know what has happened.

If you become aware of a data breach you should contact the data protection team immediately: data.protection@networkrail.co.uk.



Accountable

Personal information should be handled in line with the following principles:

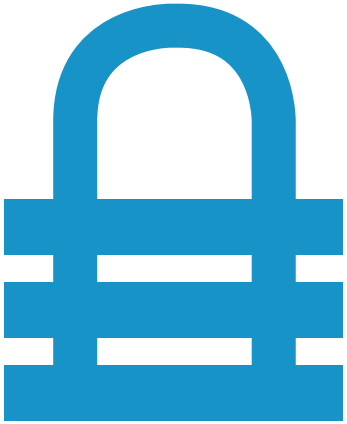
Lawfulness, fairness and transparency
We should treat all personal information fairly, in line with the law, and in a way that is clearly understood.

Purpose limitation
When we collect personal information we should only use it for the purposes for which we originally collected it, unless we inform people about a change in use.

Data minimisation
We should aim to use personal information as little as possible, and avoid using it at all if we can.

Accuracy
We should aim to keep the personal information we do hold accurate and up to date.

Storage limitation
When we have to store personal information, we should try to do so in a way which doesn't allow individuals to be identified for any longer than is necessary.



Fair

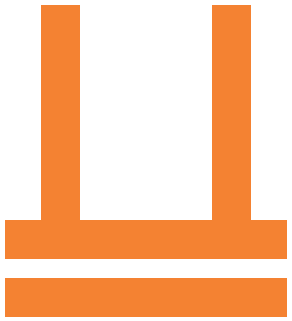
Everyone has rights under data protection law. One of the most important is the right of subject access - which helps individuals know what is happening with their personal information.

Anyone has the right to ask Network Rail whether we are handling their personal information and why we're doing so.

It also allows that person to ask for a copy of the information itself, so they can, for example, check that it is accurate and being handled fairly. By law we have to respond within certain timeframes.

If you receive a subject access request, contact the data protection team immediately:

data.protection@networkrail.co.uk



Keeping us all safe and secure

It's important that we all treat personal information in a safe way.

That means we should protect it from uses which haven't been authorised or might be against the law. We should also keep it safe from accidental loss, destruction or damage.

We can do that by following our policies and guidance, making sure we understand the risks, and thinking about data protection from the start of a project, process or as we begin a new piece of work.

You can find more information on our Security Connect community page.

Better every day

One requirement of the General Data Protection Regulation is 'privacy by design'. This means making sure we have the best technical and organisational measures in place to look after personal information.

If we get it right, privacy by design can help us be better every day. If we think about privacy as we plan a programme or piece of work, we will better manage the information we handle. As part of this we should document how our actions and plans might affect people's personal information.

In some circumstances, you may need to complete a data protection impact assessment. This helps us identify and reduce risks to privacy.

You can find out more about how to complete a data protection impact assessment on our Connect community page.

Ask yourself these questions…

Q1 Do I need to store this information?

Q2 Have I thought about where it should be stored?

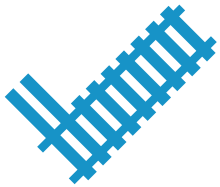
Q3 Do I restrict access only to those who need it?

Q4 Do I tell people why I require their information and what I will use it for?

Q5 Do I understand other people's right to privacy?

Checklist: What should we do differently?

Using common sense rules will mean personal information is less likely to fall into the wrong hands or get damaged.



- Only keep personal information for the purpose for which you have collected it, don't use it for anything else.
- Keep it in a safe place, and make sure only those people who need it can access it. That might mean restricting file access or locking it away.
- Keep it up to date and dispose of the information securely when it's no longer required, using confidential waste bins for paper copies.
- Keep it safe from misuse, accidental loss, destruction or damage. That might mean using an encrypted memory stick or making sure papers are not left lying around.
- If you are dealing with our suppliers, contractors and third parties make sure they are complying with current and future legislation.
- Document the personal information you hold in a personal information asset register, so we're clear about who is accountable for it. For an example, see our Connect community page.
- Anyone can ask for the information we hold about them, so make sure we can access it easily, and be prepared to rectify or erase it completely if it is incorrect.
- Contact the data protection team if you become aware of a data breach.

For more information
See our Connect community page, which includes the most up to date guidance, tools and other information to help you make the right decision when it comes to data protection.

You can also find more information about data protection on the website of the regulator – the Information Commissioner – at ico.org.uk

Your rights…

The General Data Protection Regulation creates some new rights for individuals and strengthens some existing rights.

The right to access - to be told whether your personal information is being handled, and to get a copy of it

The right to rectification - to have errors in your personal information put right

The right to restrict or object - in some circumstances, you can ask for the handling of your personal information to be put on hold or stopped, for instance where it is inaccurate

Rights regarding automated decision making - you can ask for computer decisions to be reviewed by a person

The right to be informed - when you give someone your personal information, they should be clear what they will do with it and why

GDPR

General Data Protection Regulation - some key terms

- Data Protection Impact Assessment - a tool to help identify data protection risk
- Personal data breach notification - we need to let the regulator know about serious breaches
- Privacy by design - thinking about people's privacy in everything we do
- The right to be forgotten - the right to ask an organisation to erase personal information when it's no longer needed
- Consent - when we rely on someone's consent it must have been given freely and unambiguously
- Personal information - any information relating to an identified or identifiable living individual
- Data portability - allows someone to transfer their personal information between different services and providers
- Data Protection Officer - first point of contact on data protection issues

Notes...

To find out more about data protection
get in contact with the team
data.protection@networkrail.co.uk