

Infrabel General Privacy Policy

Last revised on 29 January 2024

1. SCOPE OF THIS PRIVACY POLICY

This privacy policy (the "**Policy**" or the "**Privacy Policy**") describes how Infrabel collects, uses, consults or otherwise processes a natural person's Personal Data. For the purposes of this Privacy Policy, any reference to "Infrabel", "we" or "us" refers to Infrabel SA, registered at the Crossroads Bank for Enterprises under number 0869.763.267, having its registered office at Place Marcel Broodthaers 2, B-1060 Brussels, telephone number +32 (0)2 525.22.11, email address internet@infrabel.be. In all situations described in this Policy, Infrabel will process your Personal Data as a DPO@infrabel.be.

TUC RAIL is a subsidiary of Infrabel. TUC Rail's privacy notice is similar to Infrabel's Privacy Policy. The latest version of TUC Rail's privacy notice can be found [here](#).

We are committed to protecting the privacy of our users and customers. The purpose of this Privacy Policy serves to inform you about how we collect, define and use information that would allow us to identify you, such as your name, email address or other contact information, online identifiers such as IP address or any other information you provide to us when using our website or our services.

We therefore ask you to take a moment to read this Privacy Policy carefully. It describes various data processing operations (including those related to your use of our website, your use of our contact forms and the use of our chatbot).

Our "website" means our main website www.infrabel.be and the sub-websites for which no specific privacy policy exists (such as www.info.infrabel.be or www.press.infrabel.be) or the external websites owned by us that link to this Privacy Policy (such as www.destrafsteploeg.be). If the website in question does contain a privacy policy, this privacy policy takes precedence over our "website" (e.g. www.jobs.infrabel.be and <https://opendata.infrabel.be>).

It will be updated periodically to reflect any changes in statutory requirements, processing or new features or services we may add. These changes will be announced through our information channels (including our website) and will take effect upon their announcement.

2. APPLICABLE LEGISLATION

"Data Protection Legislation" shall refer to Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), as well as any other legislation and/or regulation introduced pursuant to the GDPR and the e-Privacy legislation, or which implements, amends, replaces or consolidates them or any one of them, and any other applicable legislation relating to the processing of Personal Data and privacy.

Below are the details of the various types of processing of Personal Data.

3. WEBSITES, APPS AND SOCIAL MEDIA

Our websites and apps

When you visit the Infrabel website or download one of our apps, we collect a limited amount of Personal Data with a view to the management and proper functioning of this website or app.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: identification data: IP address (for the website via cookies and assimilated technologies), IP address and MAC address for the apps. For the apps, we also process some meta-data (date and time of your access to the server, type of operating system and quantity of data sent)

Retention period: with regard to cookies, see our Cookie Policy, with regard to other data: kept for purely technical reasons for the proper functioning of the app, with a maximum duration of 14 days

Source of data: Directly from you whenever you visit the website or install the app

Legal basis for processing: It is in Infrabel's legitimate interest as a company to be able to manage the website and apps it makes available, on the understanding that we always ensure in this regard that your interests are also safeguarded.

Recipients of data: IT service providers

Infrabel wishes to make your experience of the website and apps as informative and relevant as possible. To achieve this, we use cookies, with the intention both of protecting your privacy and providing you with a user-friendly online environment. If you would like to know more about how we use cookies, please read our [Cookie Policy](#).

Social media

We may process Personal Data obtained from social media platforms (including Facebook, LinkedIn, Instagram and/or Twitter) if something is Infrabel-related or addressed to Infrabel in order to (i) provide an initial response to questions or complaints, (ii) monitor our online reputation, (iii) integrate testimonials about Infrabel and our services which you publish into our internal and external communications and (iv) improve our services and identify opportunities on which Infrabel can focus.

Some of our web pages on these social media allow users to post their own material. Please remember that all material posted on our social media is accessible for – and therefore can be seen by – the public. You should therefore exercise caution with regard to disclosing certain personal information such as financial or address details through these platforms. We are not responsible for any action taken by third parties if you post personal information on any of our pages on these social media, for example Facebook or Instagram. We also refer to the privacy policies and cookie policies of the platforms you use.

In addition, our website may also contain integrated elements from third parties (plug-ins). These include videos stored and published by another party, but whose link we share, and which are distributed on, in or through our website. In addition, content from our website may be shared on social media via buttons ("share" and "like").

If you use these functions via these integrated elements, the actions taken on our website will be passed on to the company operating the relevant social media. The use of these integrated elements

and the data collected during your browsing are exclusively subject to the general terms and conditions and the privacy policies of the social media concerned. It is therefore important that, if you decide to make use of this function, you first consult the privacy policies of these parties on their own websites in order to know exactly what data is processed and how it is subsequently used. We do not receive personal data from these third parties, but we do receive anonymous statistical information, which enables us to improve our own services.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Any Personal Data relevant to the purposes described above that you decide to share with us or that you publish on social media; anonymised statistics

Source of data: Directly from you via publicly accessible pages on social media

Legal basis for processing: It is in Infrabel's legitimate interest as a company to process the Personal Data which you have chosen to communicate to us or which you have made publicly available via social media platforms, in order to improve our services, identify business opportunities and reinforce our internal and external communication, on the understanding that we always ensure in this regard that your interests are also safeguarded.

Recipients of data: IT service providers and social media, and recipients of our communications
Third party websites

When you click on a link from a Third Party website, you will be directed to a website over which we have no control and our Privacy Statement will no longer apply. Your browsing activities and interaction on any other website is subject to the terms of use and privacy and other statements of such third-party websites. We advise you to carefully read the privacy statements of other websites. We are not responsible or liable for the information on or the content of Third Party websites.

4. LOCAL RESIDENTS

1. Contact form

If you live near a railway line and would like more information about rail infrastructure or track work, would like to report a problem, make an enquiry or have any other rail-related question, you can contact us using the dedicated contact form for local residents. As part of this, we process your Personal Data for the purpose of correctly and smoothly processing your request and enabling feedback to you.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Gender, first name/surname, telephone number, email address, street, house number, municipality, images

Source of data: Directly from you upon completing the form

Legal basis of processing: necessary for fulfilling a task of public interest (Article 199, 1°, 2° of the Law of 21 March 1991, - 1° the acquisition, design, construction, renewal,

maintenance and management of railway infrastructure; and - 2° the management of the control and safety systems of this infrastructure)

Recipients of data: IT service providers

2. Complaint form to report noise and vibrations along the railway

If you live near a railway line and are experiencing nuisance from vibrations or noise along the railway tracks that are not being caused by Infrabel works, you can fill in the dedicated complaint form. In this context, we process your Personal Data for the purpose of opening a file, to have sufficient information to investigate your complaint and to enable feedback to you.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Gender, first name/surname, telephone number, email address, street, house number, municipality, images

Source of data: Directly from you upon completing the form

Legal basis of processing: necessary for fulfilling a task of public interest (Article 199, 1°, 2° of the Law of 21 March 1991, - 1° the acquisition, design, construction, renewal, maintenance and management of railway infrastructure; and - 2° the management of the control and safety systems of this infrastructure)

Recipients of data: IT service providers

3. Pruning request

You can request to have pruning work carried out with a view to ensuring safety on the rail network. This enables you to report situations that may pose a risk to the safety of local residents or train traffic, to enable us to investigate and act on as a priority. As part of this, we process your Personal Data for the purpose of correctly and smoothly processing your request and enabling feedback to you.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Gender, first name/surname, telephone number, email address, street, house number, municipality, images

Source of data: Directly from you upon completing the form

Legal basis of processing: necessary for fulfilling a task of public interest (Article 199, 1°, 2° of the Law of 21 March 1991, - 1° the acquisition, design, construction, renewal, maintenance and management of railway infrastructure; and - 2° the management of the control and safety systems of this infrastructure)

Recipients of data: IT service providers

4. Declaration of damage

Infrabel offers local residents the means to claim compensation for damage to a building that may have been caused by an Infrabel construction site nearby. As part of this, we process your Personal Data for the purpose of correctly and smoothly processing your request and enabling feedback to you. The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Gender, first name/surname, telephone number, email address, street, house number, municipality, fire insurance policy number, images

Source of data: Directly from you upon completing the form

Legal basis of processing: necessary for fulfilling a task of public interest (Article 199, 1°, 2° of the Law of 21 March 1991, - 1° the acquisition, design, construction, renewal, maintenance and management of railway infrastructure; and - 2° the management of the control and safety systems of this infrastructure)

Recipients of data: IT service providers

5. Application to purchase/rent a plot

If you wish to rent or purchase a site from Infrabel, please fill in the dedicated form. As part of this, we process your Personal Data for the purpose of correctly and smoothly processing your request and enabling feedback to you.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Gender, first name/surname, telephone number, email address, street, house number, municipality, images

Source of data: Directly from you upon completing the form

Legal basis for processing: execution of the contract (pre-contractual phase), to properly process your requests to purchase/rent plots from Infrabel.

Recipients of data: IT service providers

6. Chatbot for local residents

The Chatbot "Mia" is an automated helpdesk agent. It does not make any decision, and at no time is there an automated decision in the sense of the GDPR.

If you live near a railway line and would like more information about railway infrastructure or track work or would like to report a problem, submit a request or have any other rail-related question, you can contact us through the chatbot "Mia" provided for this purpose. "Mia" is an interactive and automated answering system controlled by artificial intelligence. We process your personal data in this regard in order to process your request quickly and

automatically and, if necessary, to contact you again and to improve Infrabel's automated responses to questions from the general public.

The list below describes the categories of data we process for these purposes, the source of the data, the legal basis for this processing activity and any parties with whom we may ultimately share the data.

- **Data categories processed:** email address

Data sources: your email address is only stored if you enter it. If the chatbot does not have an immediate answer to your question, it will ask you to enter your email address and contact you again later.

Legal basis for the processing: necessary for fulfilling a task of public interest (Article 199, 1°, 2° of the Law of 21 March 1991, - 1° the acquisition, design, construction, renewal, maintenance and management of railway infrastructure; and - 2° the management of the control and safety systems of this infrastructure)

- **Categories of data processed:** IP address

Sources of data: Directly from you when using the chatbot "Mia"

Legal basis for processing: It is in Infrabel's legitimate interest as a company to be able to collect the IP address so that we are technically able to communicate with you and provide you with a quick and efficient means of contacting us, on the understanding that we always ensure in this regard that your interests are also safeguarded.

Recipients of the processing: IT service providers

- **Categories of data processed:** conversations with the chatbot "Mia"
- **Sources of data:** Directly from you when using the chatbot "Mia"

Legal basis for the processing: It is in Infrabel's legitimate interest as a company to be able to use the conversations with Infrabel's chatbot in order to improve the automated answers and provide you with a quick and efficient means of contacting us, on the understanding that we always ensure in this regard that your interests are also safeguarded.

Recipients of the processing: IT service providers

5. CAMERAS

1. Technical and operational cameras

Infrabel has installed technical and operational cameras on its site, in closed areas not accessible to the public. These cameras are operated by Infrabel and are used particularly for the purpose of:

- the purchase, design, construction, upgrade, maintenance and management of railway infrastructure,
- the allocation of available railway infrastructure capacity (including studies, analysis and statistics and punctuality),

- managing the control and safety systems of this infrastructure (including operational safety),
- suicide prevention and anti-trespassing (warning the intruder that he/she is in a restricted area so that he/she can act accordingly).

They concern different types of cameras (such as dome cameras, linear cameras and pantographs). They are installed on assets that form part of the railway infrastructure, such as (1) level crossings, (2) maintenance service points (SPM), (3) signal boxes, tracks, catenaries and yards, and (4) locomotives and wagons.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: video and images

Categories of data subjects: (1) and (3) and (4): local residents, passers-by, railway personnel and contractor personnel (2): railway personnel and contractor personnel

Source of data: technical and operational cameras according to inventory

Retention period: maximum of 30 days: level crossings (30 days), SPM (30 days), punctuality (7 days), safety catenary (2 weeks), other: 30 days.

Legal basis for the processing: Necessary for fulfilling a task of public interest (Art. 199, 1°, 2°, 3° - 4° - 5° of the Law of 21 March 1991)

Access to data: Access to personal data is limited to staff members involved in such data processing. Access is granted only by the managers of Infrabel's access processes and is strictly controlled.

Recipients of data: /

2. Technical and operational cameras: drones

If you live near a railway line, you may see drones flying over the railway infrastructure and its immediate surroundings. The purpose of these drones is to take images of the tracks and associated infrastructure (bridges, tunnels, signalling boxes, etc.) at the request of Infrabel or its subsidiary TUC Rail. The drones are operated by a duly authorised pilot who holds the required licenses under the legislation on the use of unmanned aerial vehicles in Belgian airspace.

The drones are always visible when in use (at a distance of up to 90 m). They are always within sight of the pilot and the observer who are in close proximity.

Drones are deployed at Infrabel's request to verify the proper operation and condition of the rail infrastructure, install systems to ensure network safety and manage incidents or accidents on the network.

In its capacity as operator of such drones, Infrabel is, of course, obliged to process any personal data (such as images that could reveal information about anyone) it might acquire

in accordance with the legislation in force (see also Regulation (EU) 2019/947 and the Belgian Royal Decree of 8 November 2020 in this regard).

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed : video and images, but these are only processed in anonymised form in our IT Systems (so that no personal data is processed).

Categories of data subjects: before anonymisation: local residents, passers-by, railway personnel, after anonymisation: at most, railway personnel (*if they enter the railway site, this processing is subject to the employee privacy policy*).

Source of data: Drones (according to inventory)

Retention period: 2 weeks (during this time the personal data will be completely anonymised)

Legal basis for the processing: necessary for fulfilling a task of public interest (Article 199, 1°, 2° of the Law of 21 March 1991, - 1° the acquisition, design, construction, renewal, maintenance and management of railway infrastructure; and - 2° the management of the control and safety systems of this infrastructure)

Access to data: Access is granted only to persons who require it in order to process this data.

Recipients of data: /

3. Surveillance cameras

Infrabel has installed surveillance cameras on its site, in closed areas not accessible to the public.

Pursuant to Article 156 of the Law of 21 March 1991 and Article 24 of the SNCB management contract, SNCB has a Security Operations Centre (SOC) whose tasks include "ensuring the centralised management of camera surveillance and alarm processing".

The surveillance activities performed by the SOC of SNCB on behalf of Infrabel, using the cameras installed on Infrabel's premises, are carried out within the framework of this legal task.

SNCB is responsible for this data processing together with Infrabel. A declaration of these cameras has been submitted in application of the Law on surveillance cameras, and it also meets the requirements of that law (e.g. pictogram, contact with the police, real-time display of images).

Data processing for monitoring purposes, carried out by SNCB SOC on Infrabel's behalf, focuses on the evaluation of potential risks and hazards, and concerns

- railway track trespassers,

- prevention of theft, and criminal acts,
- whether or not to file a complaint with the police (calling the police, handing over images to the police, etc.).
- prevention and control of incidents and accidents, as well as prevention of suicide and anti-trespassing.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: video and images of individuals and car registration plates

Categories of individuals involved: local residents, passers-by, railway personnel and contractors

Source of data: Temporarily deployed (mobile) cameras

Retention period: 30 days

Legal basis for processing: Necessary for fulfilling a task of public interest (Art. 199, 1°, 2° of the Law of 21 March 1991)

Recipients of data: police, prosecutor's office, directly by SOC of SNCB

Access to data: Access is granted only to persons who require it in order to process this data.

Subcontractors: Service provider (Porteyes) and IT supplier (IT platform).

- The SNCB SOC manages all surveillance cameras for Infrabel through NICE / Milestone.
- Porteyes is the operator of the control room and the operator of the Porteyes cameras, on behalf of Infrabel.
- In the event of burglary and/or suicide alarm, the operator transmits the images to the SNCB SOC (location of the burglary, established facts, printout of the alarm screen/CCTV images) for further follow-up (including contact with the police).

Access to data: Access to personal data is limited to the personnel involved in this data processing, including control room (SNCB) operators, SNCB SOC operators, and police officers. Access is granted only by the managers of Infrabel's access processes and is strictly controlled. Infrabel does not have direct access to the camera images for surveillance purposes. In the event of an incident, the SNCB SOC checks the actual images upon request and, if necessary, stores them for the subsequent follow-up of these incidents.

4. Awareness-raising

The technical and operational cameras and surveillance cameras, may in certain cases be used for awareness-raising purposes, if identification of individuals is made impossible (anonymisation).

Since the anonymisation of these images also constitutes personal data processing, Infrabel, as the data controller, is of course also obliged to process the personal data in accordance with the applicable legislation.

The list below describes the categories of data we process for these purposes, the source of the data, the legal basis for this processing activity and any parties with whom we may ultimately share the data.

Categories of data processed: video and images (which are anonymised using a blurring technique)

Categories of data subjects: local residents, passers-by, railway personnel

Source of data: technical/operational and surveillance cameras

Retention period: during the anonymisation process and then deleted

Legal basis for the processing: Legitimate interest of Infrabel to raise awareness among local residents and the general public.

Access to data: Access to personal data is limited to staff members involved in this data processing, specifically individual members of Infrabel's Communication Department. The (non-anonymised) source images can only be accessed by these individuals. These anonymised images are not viewed in real time and only relevant images are communicated.

Access is granted only by the managers of Infrabel's access processes and is strictly controlled.

Recipients of the processing: /

5. Study & analysis

The technical and operational cameras, and surveillance cameras, may be used in certain cases for study and analysis purposes.

More specifically, this concerns various projects in which additional statistically relevant information is obtained, as an authorised (compatible) further use of camera images mentioned above, to obtain:

- Statistics for suicide prevention and anti-trespassing
- Study and Analysis of camera infrastructure for railway infrastructure optimisations and improvements.

The list below describes the categories of data we process for these purposes, the source of the data, the legal basis for this processing activity and any parties with whom we may ultimately share the data.

Categories of data processed: video and images (which are anonymised using a blurring technique)

Categories of data subjects: Before anonymisation: railway personnel, subcontractor employees, road users, local residents, passengers (e.g. at head of platform). After anonymisation: none.

Data source: The warning box at some sites (technical & operational cameras, at level crossings), at some locations of anti-trespass cameras and (limited to counts, with and without AI) of the surveillance cameras of Porteyes cameras for counting individuals and vehicles at level crossings.

Retention period: limited to the anonymisation process and then deleted

Legal basis for the processing: necessary for fulfilling a task of public interest (Article 199, 1°, 2° of the Law of 21 March 1991, - 1° the acquisition, design, construction, renewal, maintenance and management of railway infrastructure; and - 2° the management of the control and safety systems of this infrastructure)

Access to data: Access to personal data is limited to staff members involved in this data processing (specifically employees of I-CBE 131). The (non-anonymised) source images can only be accessed by these individuals. These anonymised images are not viewed in real time and only relevant images are communicated.

Access is granted only by the managers of Infrabel's access processes and is strictly controlled.

Recipients of the processing: IT service provider (assisting us in anonymising the data)

6. Technical management of the cameras

The technical management (including access management, calibration and parameter setting) of the various cameras mentioned above is strictly limited and controlled. Before access can be granted, the internal process is required and approved by the Infrabel access process manager. He will do so only after prior consultation with the Legal Department and the Data Protection Officer. This access is checked periodically by Infrabel's Compliance Department.

6. RAIL SAFETY

1. Certification

You may wish to contact us regarding the certification of your role as security personnel. This processing of your data is necessary for Infrabel, in application of the Belgian Royal Decree of 9 August 2020 determining the requirements applicable to security personnel, in order to certify that you are authorised to perform one or more critical security tasks for Infrabel. Specifically, the processing of personal data is necessary to verify your competency and identity, as provided for in this Royal Decree.

Verification of identity, age and skills: Infrabel is required to verify the identity, skills and competences of the individual applying for certification. Specifically, Infrabel is required to verify that the person is of age and verify and certify certain specific knowledge and confirm

certain data mentioned in the Royal Decree, such as (1) the surname, (2) the first name and (3) the date of birth of the person concerned.

Secure file: As the data controller, Infrabel ensures that the data processed within the scope of its powers are kept in a special secure file. The Infrabel staff members in charge of the certification mentioned above, as well as the specific employees of the Legal Department and the Compliance Department, have access to this file. The individuals concerned have the right to access and correct their data.

Retention period: Personal data processed in the exercising of powers referred to in this data processing are kept for five years from the end of the provision of services by the certified person (statutory limitation period). This period is necessary given the nature of the findings made by this type of staff member. After this period, the data will be destroyed or anonymised. If a copy of an identity document was communicated by the person to be certified, it will be kept only for the duration of the certification procedure.

Categories of data processed: the data necessary for the file are collected and processed (i.e. data relevant to the certification of the named security personnel, where appropriate, your full name, date of birth, number of the certificate, native language, data on the employer of the person to be certified (company number, VAT number, name, address), data on the person authorised to submit the request (name, first name, position, email address and telephone number), certificates demonstrating specific knowledge, attendance lists for in-service training days, proof of identity).

Categories of sensitive data: certificate of psychological fitness and medical fitness

Categories of data subjects: Security personnel from external firms. If you are an employee of Infrabel, the "Infrabel Employee Privacy Policy" applies to you.

Source of data: directly from you or from a third party (your employer, security service provider and our external service for prevention and protection at work.)

Legal basis for the processing: Statutory obligation, Art. 9, 13 and 14 of the Belgian Royal Decree of 9 August 2020.

Recipients of the processing: administrative authorities, police services, public prosecutors.

2. Violations

As part of the follow-up and processing of notifications and reports of violations of the Law of 27 April 2018 on the railway police, it is necessary for Infrabel to process data about you.

Specifically, the purpose of processing personal data in the exercising of the powers referred to in this Law is to ensure the management of reports of criminal offences, the penalties that may result from them and their enforcement, including the continuation of criminal or administrative proceedings.

The establishing officer must identify himself /herself by identification card. A copy of the fine or report is given to the perpetrator.

The establishing officer shall immediately notify the competent police services of any other criminal offence of which they have become aware in the performance of their duties.

Identity checks: the establishing officer may conduct identity checks to verify compliance with the railway's conditions of transport and the provisions of this Law. If persons who are asked to identify themselves by means of an official document that contains a photograph and enables their identity to be established, refuse or give a questionable identity, the establishing officer may request the assistance of the police. Within a reasonable time, the police shall provide the establishing officer in charge of the identification with the information necessary for the preparation of their report.

Members of the security service may carry out identity checks in accordance with Article 34, § 1, of the Law of 5 August 1992 on policing in the cases provided for in a cooperation protocol between the integrated police and the security service.

Access to the National Register and the Crossroads Bank for Vehicles: establishing officers whose functions require it and sanctioning officers have access to the data of the National Register, and security personnel and sanctioning officers have access to the Crossroads Bank for Vehicles.

Secure file: As the data controller, Infrabel ensures that the data processed within the scope of powers in the sense of the Law of 27 April 2018 are kept in a special secure file. Establishing officers, sanctioning officers and specialised Legal Department staff have access to this file.

Access to data: Access to the personal data is limited to the staff members involved in the follow-up and handling of the file in question, including the establishing officers, the sanctioning officer and the staff of Infrabel's Legal Department. Perpetrators have the right to access and correct their data.

Retention period: Personal data processed in the exercising of the powers referred to in this data processing is kept by law for five years from the day on which the administrative fine was imposed or the alternative measure was taken. After this period, the data will be destroyed or anonymised.

Categories of data processed: the data required for the case are collected and processed (i.e. information relevant to the management of the case such as, where applicable, name and first names, address and contact details, date and place of birth, gender, nationality, national registration number, vehicle registration number).

Categories of data subjects: Residents, passers-by, passengers

Source of data: Directly from you or by a third party (administrative authorities, police services, etc.), security service provider.

Legal basis for the processing: Statutory obligation, Law of 27 April 2018 on the railway police, including the follow-up of criminal and/or administrative proceedings.

Recipients of processing: administrative authorities, police services, prosecutors, security service provider.

7. COMMUNICATION

1. Satisfaction survey

A pop-up may appear on our website asking if you found the information you were looking for. If your answer is no, you will be directed to a form where you can submit your comments and/or suggestions. As part of this, we process your Personal Data to enable us to investigate your comment or suggestion for the purpose of improving the local residents section and to provide feedback to you.

However, you also have the option of submitting a comment or suggestion anonymously, by clicking the "I want to remain anonymous" box provided for that purpose. In that case, we will not process Personal Data about you. Please be aware that we will not be able to send you feedback on the handling of your comment or suggestion.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Gender, first name/surname, telephone number, email address, street, house number, municipality, images

Source of data: Directly from you upon completing the satisfaction survey **Legal basis for processing:** Ad hoc consent upon completing the form **Recipients of data:** IT service providers

2. Response to your requests and information mailings

You can send us an email or a letter or contact us by phone, or submit a form with a question, request, notification or response, for example, asking us to organise an awareness campaign on rail safety at a secondary school, ordering educational materials, a complaint or a request for reimbursement; we will respond to your individual query or, if necessary, by sending you a mailing. As part of this, we process certain Personal Data in order to manage various requests, including responding to your requests for information and enquiries, including whether or not to grant a particular request and following up on your responses. This processing also takes place for the purpose of planning our activities.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Address, email address, surname/ first name, phone number, gender, and if applicable (if necessary for the purpose of the request) photos and insurance policy number. With regard to a request to exercise your rights as a data subject in relation to personal data (GDPR), you might also need to identify yourself and therefore also provide a copy of an identity document.

Source of data: Directly from you via your email, letter, phone call or via the contact form on our website or via our web shop

Retention period: (a) [to be filled in] for the call centre and applications (b) either until after the webshop's products are shipped (if you register as a guest), or for as long as you decide to keep your profile (if you register as a returning customer).

Legal basis for processing: (a) regarding the help desk: It is in Infrabel's legitimate interest as a company to be able to properly follow up questions, requests and/or complaints in relation to which individuals contact Infrabel, in light of the fact that we always ensure in this regard that your interests are also safeguarded. We only send you information mailings if you have given your consent (e.g. via the designated form) (b) regarding the web shop: execution of the agreement with you.

Recipients of data: IT & call centre service providers

Access to data: Access to the personal data is limited to the staff members involved in this data processing: the external IT & call centre service providers as a first-line service and the employees of I-SCPA.323 Media (for the help desk) and I-ICT.513 (for the web shop) as a second-line service.

3. Competitions and events

From time to time, Infrabel organises competitions, events, and public events, such as within the context of awareness campaigns, for which you may register via the website and possibly via a form provided to you by one of our employees. In this context, we process your Personal Data for the purpose of organising and managing the competition or event, and to communicate further necessary information to you about it.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: Gender, first name/surname, telephone number, email address, street, house number, municipality, composition of households, images (photo and/or video), employee number

Source of data: Directly from you upon registration

Legal basis for processing: Ad hoc consent upon completing the competition form

Recipients of data: Third parties providing support for organising competitions or events and IT service providers

8. HUMAN RESOURCES

1. Employer branding

You may contact us with questions about Job Days and/or when we announce our job vacancies.

In this context, we process certain Personal Data to handle various requests, including answering your questions, deciding whether to grant a particular request and following up on your feedback, and to inform you about job vacancies and opportunities.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: address, email address, surname/first name, phone number, gender, CV

Retention period: strictly limited to the duration of the event, or, subject to your prior consent, for up to one year.

Source of data: Directly from you via email, on paper or contact form, or through third parties (such as the Job Days organiser and HR-Rail)

Legal basis for processing: Your consent

Recipients of data: HR Rail

Access to data: Access to personal data is limited to staff members involved in this data processing, including I-SCPA (event badging, surname and first name only) and I-HRO for employer branding (events).

2. Internships

You may contact us with questions related to an internship. In this context, we process certain Personal Data to assess your internship application.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: address, email address, surname/first name, phone number, gender, CV, studies and training, certificates and licences, hobbies and interests, cover letter

Retention period: strictly limited to the duration of the internship selection process, or, if applicable, the duration of the internship.

Source of data: Directly from you or through your school

Legal basis for processing: (a) during the stage of seeking an internship: your consent and (b) during the stage of negotiating and concluding an internship: the execution of the contract and necessary pre-contractual actions taken at your initiative.

Recipients of data: IT service providers, your school (internship contract) and HR-Rail

Access to data: Access to the personal data is limited to staff of Infrabel and HR-Rail involved in this data processing, including the hiring manager and I-HRO, HR-Rail staff responsible for the selection, the contractual part and administrative follow-up.

3. Headhunting

We may contact you regarding one of our job vacancies. In this context, we process certain Personal Data to manage the various stages of headhunting, including the compilation of our talent pool.

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: address, email address, surname/first name, phone number, gender, CV, studies and training, certificates and licences, hobbies and interests, cover letter

Retention period: for the duration of headhunting, up to a maximum of six months.

Source of data: Directly from you via email, on paper or contact form, or via jobs.infrabel.be, external recruitment websites (e.g. Jobat.be or Vacature.be), Forem/Actiris/VDAB (provided you have given your prior consent), LinkedIn (when you indicate your interest in a new position or via a direct message), your school (provided you have given your prior consent)

Legal basis for processing: Your consent

Recipients of the data: the Infrabel recruiter or, where appropriate, the HR-Rail recruiter

Access to data: Access to personal data is limited to staff members of Infrabel and, if applicable, HR-Rail, who are involved in such data processing.

4. Selection

HR Rail may contact us regarding a job vacancy and/or when you apply for one of our jobs. In this regard, we process certain Personal Data to assess or evaluate your suitability for the position for which you are applying

The list below describes the categories of data we process for these purposes, where your data comes from, the legal basis for this processing activity and with whom we may share the data.

Categories of data processed: address, email address, surname/first name, phone number, gender, CV, studies and training, certificates and licences, hobbies and interests, cover letter

Source of data: via HR-Rail

Legal basis for processing: Pursuant to the provisions of the Law of 23 July 1926 on SNCB and Belgian railway personnel, recruitment and selection activities are primarily the responsibility of HR Rail in its capacity as the lawful employer.

However, Infrabel also plays a role in the selection of candidates, in its capacity as de facto employer. Consequently, to be able to do this, Infrabel acts as a **separate** data controller **from** HR-Rail.

By applying for an open Infrabel vacancy, you consent to the processing of personal data by Infrabel for the purpose of selecting candidates.

If you would like to know more about this, we invite you to read the Privacy Policy on this topic, which can be found [here](#).

Recipients of data: IT service providers and HR-Rail.

5. Management of external service providers and interns

As soon as you carry out an assignment as an external service provider for Infrabel, or when you apply to carry out an assignment (*whether as a fixed-price assignment, or as a service provider under instruction, whether in execution of a public tender or outside of one, e.g. in execution of a framework agreement*), or when you undertake a traineeship with Infrabel, Infrabel processes a limited number of personal data in order to be able to correctly execute our agreement with you (or with the client). More specifically:

- To provide you with information on the practicalities of your assignment (where you need to be, at which work site, who will meet you, useful links and contacts, first meetings to be set),
- To provide you with information about what is expected of you, using applicable policies (including the security booklet, acceptable use policy and privacy policy), and logging of your use of our network resources.
- To provide you with the necessary equipment,
- To arrange the necessary access (applications, buildings, servers, etc.),
- For internships, to choose an internship supervisor and inform the team and other stakeholders which you will be assigned to, and training if necessary
- If necessary, to arrange invoicing and follow-up of your timesheets.

The list below describes the categories of data we process for these purposes, the source of your data, the legal basis for this processing activity and any parties with whom we may share the data:

Categories of data processed for onboarding: Personal identification (surname and first name, end of eID), demographic information (date of birth, gender, nationality, position), contact information (address, email).

Categories of data processed for execution of an agreement: Personal identification (surname and first name), demographic information (date and place of birth, gender, nationality, position), contact information (address, email, phone number), information on your education (studies and trainings / certificates / licences).

Source of data: directly from you or from your employer or the contractor of the public tender, in execution of the agreement, and/or from Infrabel's Procurement Department

Retention period: The onboarding information is stored in a central location in the Infrabel Onboarding application for 30 days. These are then included in Infrabel's IT systems throughout the duration of your assignment and then kept for 10 years for archiving purposes.

Legal basis for processing: execution of the agreement and necessary pre-contractual actions taken at your initiative.

Recipients of data: IT service providers

Access to data: Access to personal data is limited to Infrabel staff members involved in monitoring and handling the management of external employees and interns, such as the

local human resources offices, the HR admin, I-ICT (access), Infrabel Academy and the immediate supervisor (the latter, limited to their own new arrivals).

9. WHAT ARE YOUR RIGHTS?

Once you have provided us with your Personal Data, the Data Protection Legislation grants you several rights. Barring legal exceptions, you may, in principle, exercise them free of charge. These rights may be limited, for example, if granting a request would reveal Personal Data of another person, or if you ask us to delete information that we are required by law to keep or that we keep based on our legitimate interests.

To exercise your rights, you may submit a request by email to DPO@infrabel.be or by letter to the following address: Infrabel, for the attention of the Data Protection Officer, Place Marcel Broodthaers 2, B-1060 Brussels. In this case, please attach a copy of a proof of ID so that we can identify you.

Should you still have unanswered concerns, you have the right to file a complaint with the Data Protection Authority at any time. We of course encourage you to resolve any concern you have, with us, but, to the extent that this right applies to you, you are entitled to complain directly to the Data Protection Authority.

RIGHT TO WITHDRAW CONSENT

Wherever we rely on your consent, you will be able to choose to withdraw that consent at any time and on your own initiative by contacting us here. Withdrawing your consent does not affect the lawfulness of the processing based on your consent until the time of your withdrawal.

RIGHT TO ACCESS AND RECTIFY YOUR DATA

You have the right to access, evaluate and rectify your Personal Data. You may be entitled to ask us for a copy of your information in order to evaluate and/or correct it. If you wish to correct information such as your name, email address, address and/or any other data or preferences, you can easily do so by contacting us. You may also ask us for a copy of the Personal Data we process, as described in this Privacy Policy.

RIGHT TO ERASURE

In accordance with Data Protection Legislation, you have the right to have your Personal Data processed by us erased as described in this Privacy Policy, in case it is no longer necessary for the purposes for which it was initially collected or processed, or if you have withdrawn your consent or objected to any processing described in this Privacy Policy and no other basis for processing exists. If you wish your Personal Data to be erased, a request can be made by contacting us.

RIGHT TO RESTRICTION OF PROCESSING

Under certain circumstances, described in the Data Protection Legislation, you may ask us to restrict the processing of your Personal Data. This is the case, for example, if you dispute the accuracy of your Personal Data. In this case, we will restrict processing until we are able to verify the accuracy of your data.

RIGHT TO OBJECT TO PROCESSING

Under certain circumstances, described in the Data Protection Legislation, you may object to the processing of your Personal Data, including but not limited to when your Personal Data is processed for direct marketing purposes.

RIGHT TO DATA PORTABILITY

Where the processing of your Personal Data is carried out through automated processes and is based on your consent or the execution of a contract between you and us, you have the right to receive your Personal Data processed by us in a structured, common and machine-readable form and to transfer your Personal Data to another service provider.

10. SECURITY MEASURES

We have put in place appropriate technical and organisational measures to ensure an appropriate level of security for your Personal Data. These measures include (but are not limited to) encryption techniques, physical and IT system access controls, confidentiality obligations, and so forth.

In the event that Personal Data is compromised as a result of a Personal Data Breach, and where such a breach is likely to pose a risk or high risk to the rights and freedoms of individuals, we will make the necessary notifications as provided for in the Data Protection Legislation.

11. WHAT RULES APPLY TO CHILDREN?

We do not knowingly collect or solicit Personal Data from persons under the age of 16, except with the consent of a child's statutory representative, and in specific cases.

Should we become aware that we have collected Personal Data from a child under the age of 16, without verification of parental consent, we will take steps to ensure deletion of this data as soon as possible. If you believe we (may) have collected data from/about a child under the age of 16, please contact us.

12. HOW IS YOUR PERSONAL DATA SHARED WITH THIRD PARTIES?

We only share or disclose information, including to Third Parties, as described in this Privacy Policy.

In addition, your Personal Data will also be shared with government authorities and/or police officers when necessary for the purposes described above, if mandated by law or if required for the legal protection of the Data Controller's legitimate interests in accordance with applicable law.

13. ARE YOUR PERSONAL DATA TRANSFERRED TO A COUNTRY OUTSIDE THE EEA?

For the purposes described in this Privacy Policy, your data will generally be held within the European Economic Area ("**EEA**") and will only be transferred to a country or countries outside the EEA that is or are recognised by the European Commission as providing an adequate level of data protection. In the event that your data were to be nevertheless be transferred to or held in a country outside the EEA that is not recognised as providing an adequate level of protection, Infrabel will take appropriate security measures to ensure that the transfer complies with the requirements of the Data Protection Legislation.

If you would like more information on how Infrabel applies the above in relation to your Personal Data, please contact us.

14. HOW LONG WILL WE KEEP YOUR PERSONAL DATA?

We will retain your Personal Data for as long as necessary to fulfil the processing activities set out in this Privacy Policy, as long as you have otherwise been notified or as long as permitted by applicable law.

15. WHAT HAPPENS IF WE MAKE CHANGES TO THIS PRIVACY POLICY?

Infrabel reserves the right to occasionally update and/or make changes to this Privacy Policy. We will draw your attention to these changes where they involve a fundamental change to the processing or where the changes are relevant to the nature of the processing or are relevant to you and affect your data protection rights.

16. HOW TO CONTACT US

If you have questions, requests, comments or complaints regarding this Privacy Policy, please do not hesitate to contact us via:

DPO@infrabel.be

or

Infrabel SA Data Protection Officer
Place Marcel Broodthaers 2
B-1060 Brussels