LOGR

PRIVACY POLICY

EFFECTIVE DATE MARCH 1, 2024

This Privacy Policy explains what information LOGR collects about you and why, what we do with that information, how we share it, and how we handle the content you place in our products and services.

LOGR

DEFINITIONS

Authorised Person: means any person or entity, other than the Customer, that uses the Services with the authorisation of the Customer from time to time.

Commercial Information: means information: that is by its nature confidential; or is communicated by the disclosing party to the confidant as confidential; or the confidant knows or ought to know is confidential but excludes any information which the confidant can establish was in the public domain, unless it came into the public domain due to a breach of confidentiality by the confidant or another person, independently developed by the confidant or in the possession of the confidant without breach of confidentiality by the confidant or another other person; Confidential Information includes Content.

Content: any information or data that you upload, submit, post, create, transmit, store or display using our Services.

Customer: means the organisation that has registered to use LOGR, and, where the context permits, includes any entity on whose behalf that person registers to use LOGR.

Customer Account: means the LOGR Account of the Customer organization.

End Customer: means the end customer or purchasing customer of the hauled products.

Information: all of the different forms of data, content, and information collected by us as described in this Privacy Policy.

LOGR App: the mobile app for Truck Drivers.

LOGR Manager: means an Authorised Person who is registered as the dedicated LOGR Manager for any Customer from time to time.

Sensitive Information & Personal Information: as defined in the Privacy Act 1988 ("the Act"). For clarity, LOGR does collect nor endorse the collection of Sensitive Information such as racial or ethnic origin, political opinions and religious beliefs within the LOGR Service. Personal Information collected by LOGR also excludes the Prohibited Data of patient, medical or other protected health information, credit, debt or other payment data, or other information subject to laws governing child welfare and safety.

Services: means the services (including support services and the provision of any products, information, resources or other services) made available by Us on, from or through the Site and/or Application.

Truck Contractor: The Trucking Contractor supplier (trucking company or sole provider) to the Customer organisation.

Truck Driver: An authorised truck driver who is given access to the LOGR App to provide transport services on behalf of the Truck Contractor to the Customer.

Website: the LOGR website logr.com.au

Changes to our Privacy Policy

We may change this Privacy Policy from time to time. If we make any changes, we will notify you by revising the effective date at the top of this Privacy Policy. Where material changes are made, we will provide further notice by email to the LOGR Manager who can advise all Authorised Persons of the Customer of such changes. We encourage you to review our Privacy Policy whenever you use our Services to stay updated with our information practices and the ways you can help protect your privacy.

Should you continue to use our Services, you continue to agree to the terms of our Privacy Policy and any changes that are made and are in effect.

Information you provide to us

Account and Profile Information: We collect information about you and your company as you register for an account, create or modify your profile. We also collect information on you where you may have been registered or added by another user (such as LOGR Manager or other Administrator for a Customer). The LOGR Manager has added you as an employee, truck contractor, truck driver, and or client of the Customer, and you have been added so that you may have access to use the Services at their direction. If you have been added by a LOGR Manager and would no longer like us to process your information, please contact that LOGR Manager. If you are providing information (including Personal, Sensitive or Confidential Information) about someone else, you must have the authority to act for them and to consent to the collection and use of their Information as described in this Privacy Policy.

Content: We collect and store Content that You create, input, submit, post, upload, transmit, story or display in the process of using our Services or Website. This Content includes any

Personal Information, Sensitive Information or Confidential Information and other Commercially Information that you choose to include.

INFORMATION WE COLLECT FROM YOUR USE OF OUR SERVICES

Web Logs, Derived Data & Analytics: We may utilise logs, derived data from Content use to provide analytics on the use and operation of the LOGR Services. This data is used by Us to understand what is working and/or not working well and provides Us with insights in order for Us to improve the Service. Where Personal Information is captured during this process, We will treat the Personal Information in accordance with this privacy policy and anonymise the data first.

Cookies: We may utilise cookies which enable Us to monitor traffic patterns, user preferences and login sessions. If You do not want information collected through the use of cookies, there is a simple procedure in most browsers that allows You to deny or accept the cookie feature. But You should be aware that denying the cookie feature may prevent You from taking full advantage of LOGR.

HOW WE USE INFORMATION WE COLLECT

General Uses: We use the Information We collect about You (including Personal Information to the extent applicable) for a variety of purposes, including to:

- Provide, operate, maintain and improve LOGR Services;
- Enable You to access and use LOGR Services, including uploading, downloading, collaborating on and sharing Content.
- Enable You to communicate, collaborate, and share Content with users You designated
- Send You notifications as instigated by the LOGR Manager in relation to the unique needs or conditions of the operating environment.
- Investigate and prevent fraudulent tractions, unauthorised access to LOGR Services and other illegal activities;
- Process and complete transaction, and send You related information, including purchase confirmations and invoices; and
- For other purposes about which we obtain Your consent.

INFORMATION SHARING AND DISCLOSURE

We will not share or disclose any of your Personal Information, Sensitive Information, Confidential or other Content with third parties except as described in this policy.

In relation to information collected within LOGR that we have access to, We must:

- for any Personal Information (as defined in the Act) comply with the Act and all other laws, rules or regulations in Australia which relate to the privacy, protection and use or disclosure of Personal Information ("Privacy Laws") including only using and disclosing information in accordance with the Privacy Laws and not do anything that would put You in breach of the Privacy Laws and must ensure that Our officers, employees and sub-contractors also comply;

- keep all and any information, data, materials and other items belonging to or in the possession and control of You ("Your Data") secure and protect it from loss, deletion and the introduction of any errors or corruption; and

- if We become aware of any infringement of Our obligations under this clause, or unauthorised access to Your Data, we will promptly notify You and comply with any reasonable directions to remedy the infringement.

Access by Authorised Persons: Personal Information, limited to Name, ID or Licence Number, Contact Information, GPS location while logged in, or Content provided by You or an authorised authority on Your behalf may be disclosed to other Authorised Persons within the LOGR Account of that particular Customer. This could include LOGR Manager or other authorised Administrators, Truck Contractor or End Customer of the hauled product.

Your Sharing of Data to Others: You or an Authorised Person that You have given an administrative role to, have the ability to export data, provide API access to third party add-ons, to schedule data to be sent as email or email attachment, and to grant access to share Your data through the multi-party services of LOGR. Where data is Shared by You, it's Your responsibility to ensure the Privacy of data is ensured.

Law & Legal Requests: We may disclose Your Information (including Your Personal Information) to a third party where its disclosure is necessary to comply with any applicable law, legal process or government request. We will endeavour to redirect such requests of information to You.

Protection of Our Rights
In the event that You fall out of terms of services, e.g late payment of fees, We reserve the right to share Your Information with our Advisors to enforce our agreements and terms of service with you.

Aggregated and Anonymized Data: We may also share aggregated and anonymized information that does not directly identify you with the third parties. Where this aggregation is processed at a country level or higher.

LOGR Sharing With Your Consent. We will share your Personal Information with third parties when we have your consent to do so.

INFORMATION WE DO NOT SHARE

We do not share Personal Information about You with third parties for their marketing purposes (including direct marketing purposes) without Your permission.

DATA STORAGE, TRANSFER AND SECURITY

LOGR hosts data within Amazon Web Services and Google Cloud in a multi-regional service within Australia and the United States of America. We rely on the service providers and their security processes to safeguard the stored data in their controlled environment. We take all reasonable efforts in the design and development of the web and communication services using best security practices including data is encryption (AES256) at rest and in transit with active transport layer security (TLS 1.2)

Due to the inherent nature of the Internet as an open global communications system, We cannot guarantee absolute safety from intrusion by others, such as hackers. We will use all commercially reasonable efforts to ensure LOGR and Services remain highly available, recoverable, and secure, through effective governance, by practising DevSecOps, and use 3rd Party vulnerability detection services like Synopsys' Coverity And Black Duck, to continuously scan for vulnerabilities and where detected to promptly fix and patch.

Where You have data that You have exported or that You have transferred to an integrated third party app. The security of this data rests with You and not LOGR. We highly recommended that You have Your own policies governing data use and only integrate third party apps where You are comfortable with their policies and procedures.

LOGR

Updating or Removing your information

You may have access to update, amend, remove Your own Personal Information, or You may have to query the LOGR Manager or other authorised Administrators of the Customer Account to do so on your behalf.

Where You have deleted your Customer Account with LOGR. We will ensure deletion of Your Account & its Content within 30 days, other than Content that You have shared with other 3rd Parties or where LOGR is fairly using the data in aggregate and where responsibly anonymised.

Individual User's Data: Should You or an Authorised Person choose to delete Your User Account, Personal Information such as Name, Contact information and GPS data while logged into App, that has been captured to ensure Chain of Custody and Audit Change logs, may continue to survive user account deletion for a period of 7 years. The retention of such data for Chain of Custody and Audit should be agreed upon through contracts and agreements between those individuals and organisations conducting business, of which is outside of LOGR's scope of responsibility.

Notifications of Data Breaches

As per the Notifiable Data Breaches scheme, defined under the Privacy Amendment (Notifiable Data Breaches) Act 2017, LOGR will notify the affected individuals or parties if there's reasonable grounds to suspect there's been a breach or as directed to do so by the Commissioner. Where an eligible data breach is said to have happened if there is unauthorised access to, unauthorised disclosure of, or loss of personal information held by an entity; and the access disclosure or loss is likely to result in serious harm to any of the individuals, an agency or organisation, to whom the information relates.

Contact Us

LOGR Pty Ltd
176 Wattle Street,
Malvern, SA 5061

support@logr.com.au