digimune
LIVE FREE

Website Privacy Policy

Welcome to our privacy notice, and thank you for taking the time to read it. We hope it provides the information you're looking for, but if you need any further details, please reach out to us at legal@digimunegroup.com or any other local email address provided.

We understand how important privacy and the security of your personal data are to you – they are just as important to us. That's why we adopt a *privacy by design* approach in everything we do. This means we develop our business strategies, products, services, websites, and applications with your privacy in mind. From time to time, we may update this privacy notice and will publish revised versions on our website.

This privacy notice aims to provide you with useful information about how we process your personal data and applies to you if you are:

- A visitor to any of our websites
- A customer who has ordered or requested a product or service we provide (including in the context of a trial)
- An end-user of our products or services (including in the context of a trial)
- An employee, customer, or supplier of one of our customers, where our customers use our products or services
- A vendor, or an employee of a vendor, that provides services to us
- An individual whose personal data has been collected by us, including for marketing purposes.

1. Definitions

There are some terms we use in this privacy notice to be concise, and this is what they mean:
"Solutions" means our software products, features, services, and applications, including in the context of a trial.
"Websites" means www.Digimunegroup.com, any linked pages and any other website controlled by Digimune.
"You or your "means you (the person reading this) or the individual whose personal data is processed by us.
"We, us, our, or Digimune" means Digimune Group and its affiliate companies (the Group) as Digimune is made up of several group companies operating worldwide. This privacy notice is issued on behalf of all Digimune entities within the Group and provides information about how each entity uses personal data. Depending on your location, a specific Digimune company – or multiple companies – may be responsible for processing your personal data. Additionally, other Digimune companies may process your data depending on the company you contract with or engage with as part of your relationship with Digimune.

2. Our Data Protection Officers and how to contact us

We have appointed a Chief Data Protection Officer for the Group. For any privacy related request contact: legal@digimunegroup.com.

3. Are you providing us with personal data about someone else?

If you provide us with personal data about someone else, you are responsible for ensuring that you have the right to share that data and that you comply with any applicable legal obligations. This may include explaining to the individual why you are collecting their personal data, how you intend to use it, and obtaining their consent if required under applicable law. We also recommend directing them to read this privacy notice.

4. When do we collect personal data?

To the extent permitted under applicable law, we may collect personal data about you and any other individual either directly or indirectly, if that data is provided to us by another party.
We collect your personal data when:

5. How do you interact with us?

You interact with you:

- directly through our Websites, solutions, guarantees, warranties and insurance products where we are the official distributors, forms (including where you only complete them partially, in which case we may use your personal data to contact you to remind you to complete any outstanding information and/or for marketing purposes), surveys, competitions, use social media, or contact us by phone, email, chatbots, fax or post;
- by using cookies or similar technologies;
- when You or your organisation provide(s) services to us and we collect basic personal data about you (mainly professional contact details);
- when third parties provide us with personal data about you. This can happen where:
  - we work with a business partner that has an existing relationship with you;
  - someone who uses our Solutions, or has interacted with us in another way, has given your personal data to us;
  - you use our Solutions, including services and features incorporated into those Solutions, which may require us to obtain your personal data from a third party from whom you have instructed us to obtain it;
  - you are an employee of a customer of ours, and your employer provides us with your contact details or other personal data in connection with your use of our Solutions;
  - personal data is provided to us by government agencies or credit reporting agencies;
  - personal data is provided to us by marketing / lead-generation companies, or information service providers ("Prospect data");
  - you have a social media account, and that social media company provides us with access to certain personal data for marketing purposes; or
  - where we acquire a business that had an existing relationship with you.
- when you participate in events organised by us. This happens where you attend seminars, learning, training or other events organised by Digimune virtually or in person, or where you attend our premises for an event.

6. What personal data do we collect?

We collect the following categories of personal data:
(1) Contact Information: name, address (business or personal), email address (business or personal), phone number (business or personal);
(2) Billing and payment information: payment details, including amounts, frequency, date and time, location, the individual or business making or receiving the payment, transaction history, bank details, business accounts and taxation data, authorised user details, identification details or documents;
(3) Online usage, metadata and web information: information on the services you viewed and searched for, response times, errors, duration of access; visit and page interaction (such as scrolling clicks and hovering the mouse over content), username, IP address, browsing time and history, passwords and logging data, device type, time zone, browser plug-in types and versions, social media profile photo or profile information, web log information, device identification number , device type, location information, connection information, operating system and platform;
(4) Communication preferences: marketing preferences, areas of interest, preferred contact method and details, correspondence relating to marketing, consent records, business information, such as name and number of employees;
(5) Organisation details: place of work, job title and organisation contact information;
(6) Physical access data: details of your visit to our premises, CCTV moving or still images and recordings, car registration data, event registration data, dietary requirements, access requirements; images taken when attending Digimune events;
(7) Voice recordings: where you contact us and speak to us, such as by telephone or other verbal communication platform;
(8) Correspondence: where you contact us for any reason (for example, requests for technical or operational support, where you have a question, or where you exercise your data protection rights), we will collect personal data contained in this correspondence;
(9) Data processed using solutions.
(10) Data collected from you: any information you voluntarily provide to us.
(11) Data collected from your device ("Raw data"): email data (recipient, email address, subject line, date sent, email filing information such as labels, metadata like email record creation and last update date, user id and thread id), calendar data (event location, and date and time, other information about the event including recipients and their email addresses, recurrence of the event, and other metadata like calendar record creation and last update date original start time, event iD and calendar iD, and whether the event is deleted), browsing data (name of active applications, title of window in currently active application, website URL of open browser, device type and operating system, activity data).

7. Why do we process personal data?

This section describes the purposes for which Digimune processes your personal data and the corresponding lawful basis for that processing. The lawful basis is our legal justification to process your data for the purposes of data privacy laws applicable in the European Economic Area ("EEA"), the United Kingdom, Republic of Ireland, Australia, Indonesia and South Africa. We process your personal data (Customers and/or their main contacts, their vendors and customers (or their main contacts and Websites:

- a. To deliver our Solutions - establishing you as a customer on our systems, providing you with any information or Solutions that you have requested or purchased and sending you updates or service-related communications about these Solutions.

Purpose Category of
Individual

b. Managing and administering your account - your billing and payments, and our relationship with you (for example, customer service and support activity, including troubleshooting or managing complaints).

c. Providing third party services - facilitating the processing orders for Solutions, provisioning solutions you have purchased, answering customer service requests, displaying reviews, images and other content and media you submit, maintaining and administering your account. We share your personal data with various service providers which hosts this data on our behalf. These service providers are independent data controllers in respect of personal data and processes such personal data pursuant to their own privacy notices.

d. Providing you with services - provide Solutions involving the use of Artificial Intelligence and Machine Learning. See section 8 hereunder.

e. Providing a service to Create and administer your Digimune ID - If you create a Digimune ID to access our Solutions, it is attached and relates to you. If you use it to access your Digimune Solution, it will exist regardless of that Solution, and you may be able to use it with another of our Solutions.

f. Data collected within the Digimune ID is used for audit, access, service improvement, and support purposes, but it is not available for any marketing, surveys or other outreach to you, unless you consent specifically to same. When you use your Digimune ID, Digimune will authenticate you by sending the product containing your personal data in the form of a ' JWT Token'. This is a technically necessary piece of information which includes your first name, last name, current email address and a unique ID (which is how we can track users and authenticate users) i.e. this ID will not change, but you might change your Digimune ID credentials. We may also capture the region selected so we can provide the Solution in the appropriate language and our Solutions need this personal data to correctly address you and communicate with you.

g. Providing a service to improve our Solutions and our security - Monitoring, measuring, improving, and protecting our content, undertaking internal testing of our Website, Solutions, systems and associated services to test and improve their security, provision and performance Websites, Solutions, and providing you with an enhanced, personalised user experience.

h. Carry out research and develop activities to improve and develop new Solutions including by seeking and obtaining your feedback.

i. Monitoring and carrying out statistical analysis and benchmarking regarding the use of our Websites, platforms, and Solutions, as permitted by applicable law.

j. Maintaining, checking, and improving the security and integrity of our Websites, Solutions, systems, platforms, and communications (and detecting and preventing actual or potential threats to the same).

k. Communicate with you or provide marketing Conducting surveys for customer research, benchmarking, improvement and marketing purposes, which may involve us sharing your personal data with trusted third parties who assist us with these activities.

l. Providing any information as required to comply with our legal or regulatory obligations.

m. Obligation Sending newsletters to you - if you have requested the newsletter or your consent if not posting testimonials or reviews in relation to our Solutions which you have supplied to us.

n. Sending you electronic direct marketing communications, analysing how you engage with our electronic marketing communications (including whether you open them and click through to access their contents).

o. Organising and managing events or contacting you if you have attended a Digimune event or an event partnered by Digimune. We may share personal data about your attendance with trusted third parties.

p. We, or a trusted third party, may also contact you after an event to get some feedback about the event to help us improve our future events.

q. Solutions and Websites users Delivering joint content and services with third parties with which you have a separate relationship, for example, social media providers including LinkedIn or Instagram.

r. Monitoring and carrying out statistical analysis and benchmarking regarding the use of our Websites, platforms, and Solutions, as permitted by applicable law.

s. We may use your personal data to contact you with details about our business, our Solutions or other offers which we feel may be of interest to you or which you have asked for. We may also share your personal data with other companies in our Group and carefully selected third parties so that they (or we) may contact you with information about their products or services which we feel may be of interest to you. We or they may wish to contact you for this purpose by telephone, within a Solution, by post, SMS message or email, or other communication platform. We will only contact you by email or SMS message in line with your marketing preferences. You can unsubscribe from email marketing using the links provided in the emails we send to you.

t. Performing due diligence reviews to operate our business - Our legitimate interests or legal obligation Detecting, preventing, investigating, reporting, or remediating any criminal, illegal or prohibited activities (including fraud and money laundering), or to otherwise protect our legal rights (including liaison with official bodies, regulators, and law enforcement agencies for these purposes).
u. Our legitimate interests Obtaining legal or other professional advice and establishing, defending, and enforcing our legal rights and obligations in connection with, any legal proceedings (including prospective legal proceedings).

v. Our legitimate interests Managing, planning, and delivering our global business and marketing strategies (including collating management information and recording Customers, Solutions and Websites users.

w. Purchasing, maintaining, and claiming against our insurance policies. Training our staff, supporting their learning, development, and performance.

x. Managing any proposed sale, purchase, restructuring, transfer or merging of any or all part(s) of our business or another business, including to respond to queries from the prospective buyer or merging organisation.

y. Managing, publicising, and participating in corporate social responsibility and Environmental Social and Governance (ESG) initiatives. For example, we may anonymise and/or aggregate your personal data to create reports or dashboards and share those with trusted third parties or on our Websites, to raise awareness on topics that are important to us, such as supporting the growth of small and medium businesses.

z. Comparing information for accuracy, to categorise it, and to verify it with our systems or third parties.

aa. Complying with any of our legal or regulatory obligations (including our responsibilities under codes of conduct and anti-bribery laws).

bb. Complying with instructions, orders and requests from law enforcement agencies, regulatory bodies, supervisory authorities, any court or otherwise as required by law.

cc. Monitoring and recording communications with you, including e-mails, webchats and phone and other voice or video conversations (after informing you of the monitoring and/or recording during that call and before the recording starts), for training purposes.

dd. Protecting our assets, our customers, and their assets, and protecting our employees and other workers from unacceptable behaviour, fraudulent or other harmful communications or actions by using CCTV video surveillance, monitoring and recording in or around our premises.

ee. Enhancing personal data we collect from you with data we obtain from third parties that are entitled to share that data; for example, data from credit agencies, search information providers or public sources (e.g., for customer due diligence purposes, or to improve accuracy of our records), but in each case as permitted by applicable law.

ff. We may also enhance personal data we collect from you with data which we already hold about you in our systems through your use of our Solutions or other interactions with us (including as a free trial) or by combining data where you use a multiple Solutions.

gg. Carry out analytics and digital advertising - Delivering targeted advertising and marketing campaigns (which may include in-Solution messaging) or sharing information with which may be useful to you, based on your use of our Website, Solutions, or any other data we hold about you.

hh. Providing you with location-based services, for example, targeted advertising and other personalised content, where we collect geo-location data.

ii. Ensuring our advertisements match the potential interest of users, tracking the efficiency of ads and optimising the effectiveness of our campaigns. We use Conversion APIs provided by Meta, Google and LinkedIn. An API is a software intermediary allowing two applications to talk to each other, when using a conversion API, we allow our server to communicate with these third-party servers. Where you consent to "Targeting technologies" on our website, we collect information about your usage of our website from our server logs and share this information with these third parties for the abovementioned purposes. We also share what we call "offline" data, which is information we collected from our interactions with you that took place outside of our website and can help us understanding your entire experience with Digimune. This data includes your hashed contact details, as well as information about your organisation and information about your interactions with Digimune (e.g. whether you are interested in a product, which product it is, how interested you are).

jj. Profiling and automated decision making - Profiling activities consist of using personal data of individuals to predict their interests and likely behaviours. This is usually carried out using behavioural information and, amongst other uses, helps us to inform our decisions about marketing audiences. This allows us to send the right message to the right audience.

kk. We may use personal data generated when you use our Solutions and Websites to improve them and give you the best service and experience. This means that we may use personal data
(including data collected using cookies and similar technologies) to evaluate and predict your personal preferences and interests. Please note that this is subject to your consent where required by applicable law. We may conduct profiling activities to:

- support you and personalise the communications we send in relation to our Solutions where permitted by applicable law and in line with your preferences;
- deliver advertising, marketing (including in-Solution messaging) or information which may be useful to you, based on your use of Solutions (considering your preferences as required); and
- provide you with location-based services (for example location relevant content) where we collect geo-location data.

Please be aware that, in connection with the purposes above, we may use the personal data of your customers, suppliers, employees, and other individuals, whose personal data you input into our Websites or Solutions.

ll. Automated decision-making - We do not conduct any automated decision-making with a significant or legal effect, or otherwise, about you or any individuals.

8. Artificial Intelligence and Machine Learning

Digimune is committed to innovation and is constantly evaluating new ways to improve its Solutions and develop new ones. Using Artificial Intelligence ("AI") and Machine Learning ("ML") allows us to improve our Solutions, giving you access to new, functionalities and automated features (e.g. automatic processing of invoices).

8.1 What is ML?

ML is a type of AI which uses data and algorithms to recognise patterns, drawing inspiration from the way humans learn. It provides systems the ability to automatically learn and improve from experience, without being explicitly programmed. It usually works with ML models, which are programs trained to recognise patterns in previously unseen data sets.

8.2 How do we use ML?

Digimune uses ML in some Solutions and may process personal data.

"Data processed using Solutions", to deliver these ML powered services. For the purposes of delivering ML powered services, personal data is generally used for the purpose of:

a. Building an ML model, and continuously training it

We build and train ML models using data including personal data, so they can perform the task they have been designed to perform. For example, to design a service allowing the automatic processing of invoices, we would create an ML model designed to recognise specific data fields in an invoice and train this ML model on a number of invoices so it can learn where these fields are located and what they are likely to contain. This ML model would then continually be updated and

trained based on new invoices. The purpose of this processing is to create an accurate ML model and continuously ensure its accuracy.

b. Providing the Solution

Personal data entered in the Solution is consumed by the ML model to deliver the service it has been programmed to deliver . For example, an ML model designed to automatically process invoices would, once trained, be applied to new invoices to automatically recognise fields and populate them into a Digimune Solution.

The purpose of our use of AI and ML at Digimune is not to make decisions about individuals. Our purpose is to automate manual and time-consuming processes for the benefit of our customers and other parties.

9. The Digimune Network

Digimune has created a trusted network with its partners, with the purpose of interconnecting our Solutions, as well as our partner solutions. The aim of the Network is to provide additional, innovative and integrated Solutions to you, to help automate your workflows and improve your customer/user experience. For this purpose, data inputted into our Solutions may be shared with other Solutions and platforms to facilitate provision of the Network Services.

Digimune is mostly acting on behalf of its customers in the context of the Network (as a data processor under European Union, the United Kingdom, Republic of Ireland, Australia, Indonesia and South Africa data protection laws), and the processing of personal data to provide the Network Services is covered by agreement.

Data processed in the Network may however be processed by Digimune for the following purposes (as a data controller under European Union, the United Kingdom, Republic of Ireland, Australia, Indonesia and South Africa data protection laws):

- To build and feed ML models ;
- To provide ML powered services;
- To purchase data sets from third parties, in order to improve accuracy of data held in the Digimune Network;
- To carry out research and development activities to improve our Solutions based on data ingested by the Network.

Processing of personal data by Digimune as a data controller under European Union, UK, Australian, South African and Indonesian data protection laws in the context of the Network will be carried out in accordance with this privacy notice.

10. Mobile data

We may obtain personal data through mobile applications that you or your users install on mobile devices to access and use our Websites or Solutions, or which you or your users use to provide other services related to that mobile application (for example, to sync information from our Solution with that mobile application).

These mobile applications may be our own Solutions or be provided by third parties. Where the mobile application is operated by a third party, you must read that third party's own privacy notice which applies to your use of that third party mobile application. We are not responsible for those third-party mobile applications or the use of your personal data by those third parties.

Mobile applications may provide us with personal data related to your use of that mobile application and / or our Websites or Solutions accessed through that mobile application. We may use this personal data to provide and improve the mobile application or our own Website or Solution. For example, activity undertaken within a mobile application may be logged for review.

You can configure application privacy settings on your mobile device, but this may affect the performance the application and the way it interacts with our Websites and Solutions.

11. How long do we keep personal data for?

We retain personal data about you during and after termination of your relationship with us. This data is held and used for as long as permitted for legal, regulatory, fraud prevention and legitimate business purposes, in accordance with our internal Digimune policies. For more information on the retention of personal data, please contact the Digimune at:

legal@digimunegroup.com

12. How is personal data shared?

Sometimes we may need to share your personal data with third parties. This will usually be because you have asked us to, we are required to by law, or because a third party integrates with our Solution or provides us or you with a service.

Third parties Reason

Our service providers and agents (including their sub-contractors) or third parties which process personal data on our behalf (e.g., internet service, cloud storage and platform providers, payment processing providers and those organisations we engage to help us send communications to you); third parties with which you request that we share personal data with for your own or their purposes. Helping us to provide you with the Solutions and information you have requested or which we believe is of interest to you. Partners, including system implementers, resellers, value-added resellers, independent software vendors and developers.

Allowing partners to provide you the Solutions, services, and information you have requested or which they believe is of interest to you.
Helping us to provide you with the Solutions and information you have requested or which we believe is of interest to you, or in the context of a restructuring.
Third parties used to facilitate payment transactions, for example clearing houses, clearing systems, financial institutions, and transaction beneficiaries.

13. Helping us to ensure payment for Solutions.

Other parties who may also be controllers of the data we share with them, for example, academic or research organisations. Research necessary for our own or another organisation's legitimate interests (e.g., to deliver valuable insights to our customers or enable us to improve the service we offer you). In these circumstances, we will take additional steps to protect your personal data, for example pseudonymisation (defined in Article 4(5) GDPR) means replacing any information which could be used to identify an individual with a pseudonym, or, in other words, a value which does not allow the individual to be directly identified), or anonymisation (Data can be considered 'anonymised' when individuals are no longer identifiable. It is important to note that a person does not have to be named in order to be identifiable) and aggregation (the formation of a number of things into a cluster) prior to sharing the data, to protect your privacy and the confidentiality of your data.
Third parties where you have a relationship with that third party, such as social media providers, partners, and other third parties with which we work and whose products or services we think will interest Marketing and targeting purposes.
Credit reference and fraud prevention agencies; government bodies and departments, regulators and any other third party necessary to meet your or Digimune Group's legal, regulatory, and reporting obligations; law enforcement agencies so that they may detect or prevent crime including fraud or prosecute offenders including to comply with applicable laws and regulations and to protect our business.
Statutory or regulatory reporting or the detection or prevention of unlawful acts; any third party in the context of actual or threatened legal proceedings; professional advisors and auditors for the purpose of seeking professional advice or to meet our audit responsibilities.
Another organisation if we sell or buy (or negotiate to sell or buy) any business or assets, another organisation to whom we may transfer our agreement with you.

In the context of an acquisition, sale or restructure. When we share personal data with third parties which are providing us with services, or providing services to you on our behalf, we always have an agreement in place to ensure protection of your personal data i.e., that it is only used for agreed purposes and in accordance with applicable laws.

14. Do we use cookies and similar technologies?

More information can be found in our specific cookie policies relating to Websites and Solutions, but it is worth mentioning here that our Website and Solutions may contain technology that enables us to:
• check specific information from your device or systems directly relevant to your use of our Websites and Solutions against our records to make sure they are being used in accordance with our agreements and to troubleshoot any problems you may be experiencing;
• obtain information relating to any technical errors or other issues with our Website, and Solutions;
• comply with our legal or regulatory obligations;
• collect information about how you use the functions and features of our Website and Solutions; and
• gather statistical information about the operating system and environment from which you access our Solutions including web traffic data.
For those Solutions using cookies and similar technologies, a cookie policy will be made available to you directly in the Solution, usually in the Solution Help Centre.
If you follow a link which takes you away from our Website or Solutions, our privacy notice does not apply when you arrive at your new online destination, and we are not responsible for the handling of your personal data after you have left our Website or Solution. Please read the privacy information of the third party responsible for the new online location which you have linked to.

15. What data privacy rights do you have?

Data privacy rights differ from one region to another. Please consult the relevant part of Section 20 below dealing with data privacy rights to obtain more information on your local rights.

16. How is your personal data kept secure?

We will keep your personal data secure by applying appropriate technical and organisational measures against its unauthorised or unlawful access or use and against its accidental loss, destruction, or damage.

We will do our best to protect your personal data, but we cannot guarantee the security of your personal data while it is being transmitted to our Website or Solutions or to other websites, applications and services via an internet or similar connection. If we have given you (or you have chosen) a password to access certain areas of our Websites or Solutions, please keep this password safe, and when choosing your own password please ensure it is strong and do not use variations of previously used passwords, and with all passwords, do not write them down or leave them accessible to unauthorised persons.
If you believe your personal data has been compromised in connection with your use of Solutions or Websites or otherwise in connection with Digimune, please contact us
at legal@digimunegroup.com .

17. If you are based in the United Kingdom or the Republic of Ireland Key data protection laws

The key data protection laws in the United Kingdom are the UK General Data Protection Regulation ("UK GDPR"), UK Data Protection Act 2018 and the Privacy and Electronic Communications Regulations.
The key data protection laws in the Republic of Ireland are the General Data Protection Regulation, the Data Protection Act 2018 and the S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.

18. If you are based in South Africa Key data protection laws

The key data protection law in South Africa is the Protection of Personal Information Act (POPIA), which regulates the collection, use, and processing of personal information from identifiable individuals within the country; it is considered the most comprehensive data protection law in South Africa and shares similarities with the EU's GDPR with the major difference that it's applicable to individuals and entities. Whereas the EU's GDPR and UK Data Protection Act 2018 is only applicable to living individuals.

19. If you are based in Australia Key data protection laws

The key data protection law in Australia is the Privacy Act 1988 which outlines the Australian Privacy Principles (APPs), governing how organizations collect, use, store, and disclose personal information, applying to both the private sector (with certain turnover thresholds) and most Australian government agencies; the Office of the Australian Information Commissioner (OAIC) enforces this legislation and investigates breaches of the APPs.

20. If you are based in Indonesia Key data protection laws

The main data protection law in Indonesia is the Personal Data Protection Law No. 27 of 2022 on (PDP) Law, which was passed in 2022. Other relevant laws include the Electronic Information and Transaction (EIT) Law and various regulations.

21. If you are based anywhere else in the world

The key data protection laws of each country should be identified and studied to ensure that the data subject fully understands the protection of their personal information. If there is any uncertainty, legal advice should be sought. other countries do not necessarily protect your personal data in the same way. You can google the countries that the European Commission considers provide an equivalent level of data protection to that which exists within the European Economic Area (EEA).

22. Controllers and processors

This privacy notice describes our processing of your personal data in our capacity as a "data controller" under applicable laws in the the United Kingdom, Republic of Ireland, Australia, Indonesia and South Africa. A data controller decides how and why your personal data is processed. Depending on the country in which you are located, a different Digimune company may be the data controller of your personal data.
Where we process personal data on behalf of another individual, for example our customers, partners, or other parties, we do not decide how and why to process that personal data. In those instances, we are a "data processor" under applicable law rather than a data controller. Where we are a data processor of your personal data, we use it in accordance with the data controller's instructions to us. Those instructions include the terms and conditions applicable to the product or service you or your employer are using, and our Data Processing Agreement which forms part of those terms.
If we are a data processor of your personal data, then you should also read the relevant data controller's privacy notice. Make sure that you familiarise yourself with the privacy notice of your own employer, accountant, business, or other organisation that you have a direct relationship with, and which may share your personal data with Digimune.

23. Your data protection rights

If you are based within the the United Kingdom, Republic of Ireland, Australia, Indonesia and South Africa, you have the following data protection rights:

• the right to be informed about the processing of your personal data;
• the right to obtain access to your personal data;
• the right to have your personal data rectified or erased, or to place restrictions on processing your personal data;
• the right to object to the processing of your personal data e.g., for direct marketing purposes or where the processing is based on our legitimate interests;
• the right to have any personal data you provided to us electronically returned to you in a structured, commonly used and machine-readable format, or sent directly to another company, where technically feasible (this is known as 'data portability');
• where the processing of your personal data is based on your consent, the right to withdraw that consent subject to legal or contractual restrictions;
• the right to object to any decisions based solely on the automated processing of your personal data, including profiling; and
• the right to lodge a complaint with the data protection supervisory authority responsible for data protection matters in your location.

Please note that in some circumstances the exercise of the above rights may be limited by legal restrictions and exemptions. If relevant, we will explain this when responding to a request to exercise data protection rights. If you think we hold any personal data about you which is incorrect or if there are any changes to your personal data, please let us know so that we can keep our records accurate and up to date.

If you wish to exercise your data protection rights as an individual, please contact us at
legal@digimunegroup.com
If you do not want us to use your personal data for purposes set out in our privacy notice, we may not be able to provide you with access to all or parts of our Website or Solutions.

24. International transfer of personal data

Personal data in EU member states and the UK is protected by data protection laws, but other countries do not necessarily protect your personal data in the same way. You can google the countries that the European Commission considers provide an equivalent level of data protection to that which exists within the European Economic Area (EEA).
Our Website and some of our Solutions, or parts of them, may be hosted outside the EEA or UK, or Australia or Indonesia or South Africa which means that we may transfer personal data to third countries which do not have adequacy determination in some circumstances. In addition, we may use service providers located outside the the abovementioned regions to help us provide our Websites, Solutions or other services to you and this means that we may transfer your personal data to these regions. We take steps to ensure that where your personal data is transferred outside of these regions, appropriate measures and controls are in place to protect that data in accordance with applicable data protection laws. In each case, such transfers are made in accordance with applicable data protection laws and may be based on the use of (i) the European Commission's Standard Contractual Clauses for transfers of personal data outside the EEA, or (ii) the UK's International Data Transfer Agreement and/or the European Commission's Standard Contractual Clauses and/or the UK Addendum for transfers of personal data outside the UK.

For more information on international transfer of personal data, please contact:
legal@digimunegroup.com.

25. How can you contact us?

If you have any question about this privacy notice, or wish to exercise your data privacy rights as an individual, you can contact us by sending an email to:
legal@digimunegroup.com.