Vyne Technologies Ltd
+44 (0)20 7880 1700
hello@payvyne.com

4 Fulwood Place, Holborn,
London WC1V 6HG
United Kingdom

Who we are

We are Vyne Technologies Limited, a company registered in England and Wales under company number 11872778 and having our registered office at The Fulwood, 4-7 Fulwood Place, London WC1V 6AE. Our principal place of business is 10 Bloomsbury Way, London, WC1A 2SL. In this Privacy Policy, this is the company referred to as "we" or "us" or "our" or "Vyne".

We are a technology provider whose mission is to improve the way ecommerce retailers get paid online.

We connect business and consumers to their bank accounts to allow safe and secure payment for goods and services, instantaneously and at a low cost.

We do this by using a combination of direct bank connections and third party aggregators.

We are authorised and regulated by the Financial Conduct Authority (FCA) as an Authorised Payment Institution with reference number 925649.

About this policy

Vyne is committed to protecting and respecting your privacy. This policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us in accordance with applicable data protection laws.

We are the data controller of any personal data you provide to us which is covered by this privacy policy, and we are subject to applicable data protection laws.

In some situations as described below we also act as data processor on behalf of our merchants. See the section entitled "Where we act as Data Processor on behalf of a merchant" for more information.

If you have any questions please email info@payvyne.com.

This Policy was last updated on 26/04/2022. We may change this Policy from time to time, when we do we will publish the updated Policy on our website.

This Policy is provided in the German language to help German data subjects understand how we use, process and store their data. In the event of conflicts between this Privacy Policy and the Privacy Policy in the English language, the English language shall prevail.

If you are a payment service user, each time you give consent to initiate a payment, you will be deemed to have accepted the version of the Privacy Policy which is posted on our website at the time of making the consent.

If you are a merchant, we will contact you via email if we make a change to our Privacy Policy which affects how we process your personal data.

About you

This policy applies to:

- everybody who accesses our Website (www.payvyne.com) ("website visitors");
- people who use our services to make payments ("payment service users"); and
- businesses who contract with us to receive payments or access other merchant services, or potential business customers, including payment gateways or integrator partners ("merchants").

You must be 18 years old or over to use this Website or any of our services. We do not intend to process any data for persons under the age of 18. If we become aware that we are collecting data for under 18's we will investigate the issue and ensure that all such data is identified, processing is stopped immediately and all data is deleted following our security processes.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

What type of information do we collect from you?

The personal information we collect about you depends on the particular activities carried out through our Website or the services and/or products that we are or are planning to provide to you.

We will only collect the data that we need to collect in order to perform these activities.

We also collect, use and share aggregated data such as statistical or demographic data for business purposes ("Aggregated Data"). Aggregated Data may be derived from your personal data but is not considered personal data as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific Website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, this is then treated as personal data which will be used in accordance with this Policy.

If you are a website visitor

We currently collect and process the following information:

- Technical Data, which includes anonymised information about your browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our Website.
- Usage Data, which includes anonymous analytical data about how you use our Website.

- Contact data, which includes information submitted through any "contact us" form on our website or equivalent, or other methods of communicating with us that we display.

If you are a payment service user

The types of data we collect vary depending on how you interact with us, as explained below. We may collect and process the following types of data depending on the circumstances:

- **Transaction Data**, which includes the banking or financial institutions you make payments from via our services, dates, amounts, and beneficiary (merchant) details.
- **Technical Data**, which may include your internet protocol (IP) address, and other data necessary to direct you to your bank or financial institution to initiate a transaction;
- **Contact Data**, which may include your email address, in cases where a Merchant supplies this in order to deliver a Vyne "request to pay" email to you, where we are delivering a receipt or payment status update to you as part of a "request to pay" process, or where a Merchant includes this or other contact information in a payment description. We may also link Contact Data to any feedback you provide us on a payment.
- **Usage Data**, which includes anonymous analytical data about how you use our products and services; and
- **Financial Data**, which may include your bank account details (including sort code and account number and/or IBAN), your billing address, and your full name.
- **Login Data**, which may include the username or other customer identifier you use to log in to your online banking, your online banking password, and any security or authentication codes sent to you by your bank when you set up a payment with us. Note that we only collect this data in limited circumstances when you initiate a

payment from a bank in the EEA which requires this, and we never store this data, as described below.

When you initiate a payment from a UK bank

When you select your chosen banking app or banking provider and provide your consent for us to initiate a payment, we use "deeplinking" to securely direct you to your online banking environment where you can review the details of your payment and, if you wish to proceed, authenticate the payment directly with your bank. We do not require any Financial Data in order to do this.

We process limited Technical Data when you initiate a payment from a UK bank which is limited to your Internet Protocol (IP) address, (which we need in order to investigate any technical issues with a payment you have made and comply with our legal obligations to prevent fraud and other types of financial crime), and any other non-personal technical information necessary to direct you to your banking provider and initiate a payment. We also store Transaction Data when you have made a payment with us, which is limited to the name of your sending bank, the recipient, the time of the payment, and the amount. Unless we also act as the payment service provider for the merchant you are sending payments to, these data types are not considered personal data as they do not directly or indirectly reveal your identity.

Note that in some cases, we also act as the payment service provider for the merchant you are sending payments to. In this case, although we do not require personal data to initiate a payment, when a successful payment is received by us, we receive personal data sent with the payment by your banking provider (see below). In this situation, this also means that some of the data we use to initiate a payment (such as Transaction Data and Technical Data) may become personal data as it may be directly or indirectly coupled with the other personal data we receive.

Vyne Technologies Ltd
+44 (0)20 7880 1700
hello@payvyne.com

4 Fulwood Place, Holborn,
London WC1V 6HG
United Kingdom

When a Merchant sends you a request to pay via email

When a Merchant sends you a Vyne request to pay via email, we collect and process Contact Data (your email address) from the Merchant to direct the payment request to the right person, and to send you updates on the status of your payment, including payment receipts.

These emails may also ask you for feedback on the payment experience and / or provide an opportunity to provide further information where things went wrong. It's entirely voluntary to provide this feedback. When you do provide feedback to us in this way, this is processed on a "pseudo-anonymised" basis; we take steps to decouple this feedback from other personal information we may hold. However as the feedback is associated with a specific payment on our systems, it may be possible to link other data we hold in relation to this payment (including Contact Data, Transaction Data and Technical Data) to any feedback you choose to provide. As such, please do not include any additional personal data within your feedback unless this is necessary to investigate an issue.

When you use Account Information Services to verify your details before receiving a payment

When a Merchant wishes to make a payment to you, the Merchant may require you to verify you own the bank account they wish to pay, and to verify your details, before making this payment. This is referred to as a "Verified Payout".

When you go through a Verified Payout process, we collect and process your Contact Data (in order to send you request and update emails), and your Financial Data (in order to verify your details and ownership of the account you select during the verification process, and to allow the Merchant to pay your account). Your chosen bank will provide us with your Financial Data when you provide them with your explicit consent to share these details. The Merchant who

wishes to pay you may also provide your Financial Data and Contact Data to us, if you have separately provided these to the Merchant.

The Merchant who wishes to pay you may also provide further data in transaction reference fields which in some cases may be personal data if it is linked to your identity and could be used to identify you (such as a car registration plate). Where this is the case, we store this information for reference purposes, to enable Vyne and the Merchant to locate payments and resolve issues or disputes.

We also process limited Technical Data when you verify your ownership of an account during the Verified Payouts Process, which is limited to your Internet Protocol (IP) address, your "consent token" provided to us by your bank, and other non-personal technical data that is necessary to direct you to your bank and verify your details. The "consent token" we collect is deleted as soon as we receive the account information requested from your bank, to ensure that we only have access to your account information for as long as we need it. We may also use Technical Data to investigate and resolve issues with the account verification process and to gain insights in order to improve our products and services.

When we use Contact Data to send you receipts and status updates via email, these emails may also ask you for feedback on the Verified Payouts experience and / or provide an opportunity to provide further information where things went wrong. It's entirely voluntary to provide this feedback. When you do provide feedback to us in this way, this is processed on a "pseudo-anonymised" basis; we take steps to decouple this feedback from other personal information we may hold. However as the feedback is associated with specific activity on our systems, it may be possible to link other data we hold in relation to this payment (including Contact Data, Transaction Data and Technical Data) to any feedback you choose to provide. As such, please do not include any additional personal data within your feedback unless this is necessary to investigate an issue.

Vyne Technologies Ltd
+44 (0)20 7880 1700
hello@payvyne.com

4 Fulwood Place, Holborn,
London WC1V 6HG
United Kingdom

When you initiate a payment from a bank located in the European Economic Area (EEA)

Because of the way Payment Initiations currently work in the EEA, if your chosen banking provider is located in the EEA, it may be necessary for us to collect limited Financial Data (in most cases this is limited to your IBAN) so we can set up the payment that you have requested to make.

In some cases, where required by your bank and supplied by you, we also collect and securely send Login Data that you enter during the payment flow to your selected bank via our payment processing partners, in cases where your bank requires this to initiate a payment. When you enter Login Data as part of a payment, we send this information directly to the payment processing partner displayed on the payment consent screen, who sends this directly to your bank. It is not possible for us to view your Login Data and we never store this information.

We also process limited Technical Data when you initiate a payment from a bank located in the EEA which is limited to your Internet Protocol (IP) address, (which we need in order to investigate any technical issues with a payment you have made and comply with our legal obligations to prevent fraud and other types of financial crime), and any other non-personal technical information necessary to direct you to your banking provider and initiate a payment. We also store Transaction Data when you have made a payment with us, which is limited to the name of your sending bank, the recipient, the time of the payment, and the amount.

Note that in some cases, we also act as the payment service provider for the merchant you are sending payments to. In this case, although we only require limited personal data to initiate a payment, when a successful payment is received by us, we receive additional personal data sent with the payment by your banking provider (see below). In this situation, this also means that some of the data we use to initiate a payment (such as Transaction Data and Technical

Data) may become personal data as it may be directly or indirectly coupled with the other personal data we receive.

Where we act as the merchant's Payment Service Provider

In some cases we provide payment services to the merchants you make payments to by providing receiving accounts for the merchant's use.

Where this is the case, when you send a payment via Vyne to an account we operate on behalf of a merchant, we receive additional Financial Data alongside the Transaction Data sent by your banking provider with the payment. This is standard information included with bank transfers and normally includes your full name, your billing address, and your account details (sort code and account number and/or IBAN). As this data could directly or indirectly reveal your identity, this is considered personal data.

When this is the case, we employ additional security measures, such as storing the details on a separate access-controlled database and "pseudonymisation", to minimise the extent of processing activity on this personal data and to ensure the information is kept as secure as possible.

Where we act as Data Processor on behalf of a merchant

In some cases, we may securely share your Financial Data and/or Transaction Data with the merchant you have made a purchase from using our services. When we do this, we act as data "processor" to the merchant in question, as the purpose for sharing the data in this way is determined by the merchant as data controller (for example, some merchants require the name on the sending account for regulatory compliance or order fulfilment purposes). We

may send this information to other third parties when a merchant has specifically instructed us to, such as the payment gateway the merchant uses to manage payments.

If you require further details on the merchant's use of your data as data controller it's best to contact the merchant directly for information or consult their Privacy Policy.

If you are a merchant

We currently collect and process the following information:

- Contact Data, which includes the full names and contact details of key individuals within your organisation relevant to the service we provide;
- Identity and Screening Data, which includes information required to verify the identity of your organisation's representatives and beneficial owners and any other personal data which may be necessary for us to comply with our obligations under Anti Money Laundering (AML) legislation or other regulations;
- Financial Data, which includes the account details (account name, account number and sort code) of trading accounts you wish to receive payments into;
- Profile Data, which includes any username or passwords you use to log in to our services or administer your account(s) with us, interests, preferences, feedback and survey responses;
- Technical Data, which may include internet protocol (IP) addresses, and other data which is necessary to facilitate payments, administer your account, manage risk, and comply with our legal and regulatory obligations;
- Usage Data, which includes analytical data about how you use our products and services.

How do we collect data from you?

We use different methods to collect data from and about you including through:

A) Direct interactions. You may give us your Identity Data, Contact Data and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- apply for or use our products or services;
- subscribe to our services, products and/or publications;
- contact us using the contact us form on the Website;
- request marketing materials to be sent to you; or give us feedback.

B) Automated technologies or interactions. As you interact with our Website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our cookie policy for further details on how we use cookies and similar technologies which is available here.

C) Third parties or publicly available sources. We may receive personal data about you from various third parties and public sources as set out below:

(i) Technical Data from the following parties:

a) analytics providers based inside or outside the EU;

b) advertising networks based inside or outside the EU; and

c) search information providers based inside or outside the EU.

(ii) Contact Data, Financial Data and/or Transaction Data from:

a) providers of technical, payment and delivery services based inside or outside the EU;

b) Credit reference agencies;

c) Anti-fraud databases and other third party databases, including sanctions lists; and

d) Government agencies, such as tax authorities

(iii) Identity Data and Contact Data from data brokers or aggregators based inside or outside the EU.

(iv) Identity Data and Contact Data from publicly available sources such as Companies House and the Electoral Registers based inside the EU.

How we use your personal data

We will process your personal information lawfully, fairly and in a transparent manner. We collect and process information about you only where we have legal basis for doing so. The most appropriate legal basis will depend on how you use our Website, the services or products that we provide, and/or how you use our services and/or products. Most commonly, we will use your personal information in the following circumstances:

- Performance of a Contract: Where we need to perform the contract we have entered into with you or to take steps at your request before entering into such a contract (for example, when we provide a service you request from us).
- Legitimate Interests: Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Legal Obligation: Where we need to comply with a legal or regulatory obligation.
- Consent: you give us consent to do so for a specific purpose. Generally we rely on consent where:
- we send you direct marketing communications that require consent by law;

- where we place cookies or similar technologies on your device in accordance with our cookie policy (available here); and
- on other occasions where we ask you for consent, in which case we will use the data for the purposes we explain at that time.

We have set out below a description of all the ways we use your personal data and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific lawful ground we are relying on to process your personal data where more than one ground has been set out in the categories below.

Purposes/Activity

Type of data subject

Type of Personal Data

Legal Basis for Processing

To set up a payment initiation where you have requested this	Payment Service User	Financial Data (only collected when your bank requires this information) Technical Data (only becomes personal data if it is coupled with Financial Data) Login Data (never stored by Vyne, and only collected when it is necessary to initiate a payment) Contact Data (where a Merchant sends you a request	Performance of a Contract

		to pay via email)	
To verify your ownership of an account a Merchant wishes to pay	Payment Service User	Financial Data Technical Data Contact Data	Performance of a Contract Legitimate Interest (which include the provision of a "verified payouts" service to our Merchants)
To register you as a new customer and open an account on your behalf.	Merchant	Identity Data Contact Data	Performance of a Contract

To process and deliver your order and/or provide our services and products to you on an ongoing basis. This will include: • making our services and products available to you; • managing payments, fees and charges; • initiating refunds or payouts on behalf of payment service users or	Merchant Payment service user	Identity Data Contact Jo Data Financial Data Transaction Data	Performance of a Contract Legitimate Interests (which include the protection of our business to ensure we are paid for the services provided to you)

merchants; • collecting and recovering money owed to us from your use of our services and products.			

To manage our relationship with you which will include: • notifying you about changes to our terms or privacy policy; • notifying you about fee increases and/or renewal dates; • asking you to leave a review or take a survey; • dealing with queries	Merchant Website Visitor Payment service user	Identity Data Contact Data Transaction Data Account Data Profile Data	Identity Data Contact Data Transaction Data Account Data Profile Data

from you in relation to our services and/or products; • managing the relationship where notice to terminate an agreement is served.			
To administer and protect our business and our Website (including troubleshooting, data analysis, testing, system maintenance,	Merchant Website Visitor Payment service user	Identity Data Contact Data Technical Data	Legitimate Interests (e.g. for running our business, to enable the provision of administration and IT services, to support and maintain network security, to prevent fraud and in the context of a business

support, reporting and hosting of data)			reorganisation or group restructuring exercise) Legal Obligation
To maintain, run and improve the functionality of our Website including to: • enable you to customise or personalise your experience of our Website; • enable you to access and use our Website and	Website Visitor	Contact Data Technical Data	Legitimate Interests (e.g. to ensure the maintenance of our Website, to develop our Website, to respond to your queries about our service and product offerings.)

associated applications; • contact and communicate with you through our Website; • run competitions and/or offer additional benefits to you; • run analytics, market research and business			

development.			
To use data analytics to improve our products/services, marketing, customer relationships and experiences.	Merchant Website Visitor Payment service user	Identity Data Contact Data Profile Data Usage Data Technical Data	Legitimate Interests (e.g. to study how customers use our products / services in order to improve and to develop them, to grow our business and to inform our marketing strategy.)
To make suggestions and recommendations to you about services that may be of interest to you.	Merchant Website Visitor Payment service user	Identity Data Contact Data Technical Data Usage Data Profile Data	Legitimate Interests (e.g., to develop our products / services and grow our business)

To defend or initiate any legal claims that may arise from our service provision to you (e.g. recovery of unpaid fees)	Merchant Website Visitor Payment service user	Merchant Website Visitor Payment service user	Legitimate Interests (e.g., to protect our business interests)
For Operational reasons, such as improving efficiency, training and quality control	Merchant Website Visitor Payment service user	Identity Data Contact Data Technical Data Usage Data Profile Data Transaction Data	Legitimate Interests (e.g.to be as efficient as we can so we can deliver the best service for you at the best price). Legal Obligation

To monitor transactions for AML and fraud prevention purposes	Merchant Payment service user	Identity Data Contact Data Transaction Data Financial Data	Legal Obligation
To conduct checks to identify our customers and verify their identity, including where applicable, screening for financial and other sanctions or embargoes, credit reference checks, KYC checks etc.	Merchant Payment service user	Identity Data Contact Data Financial Data	Legal Obligation

To ensure the confidentiality of commercially sensitive information and to protect the security of our systems.	Merchant Website visitor Payment service user	Identity Data Contact Data Technical Data Transaction Data Usage Data Profile Data Financial Data	Legitimate Interests (e.g. to protect trade secrets and other commercially valuable information.) Legal Obligation
To market our products and services to you	Merchant Website visitor Payment service user	Identity Data Contact Data	Legitimate Interests (e.g. to promote our services and products to you). Consent (depending on the marketing activity).

To market our products and services to you	Merchant Website visitor Payment service user	Identity Data Contact Data	Legitimate Interests (e.g. to promote our services and products to you). Consent (depending on the marketing activity).
To collect feedback on the payment experience, including investigating any issues you have experienced with payments	Merchant Payment Service User	Technical Data Contact Data Transaction Data Usage Data	Legitimate Interests (to improve our products and services and investigate potential issues / incidents)
To monitor and manage risk and obtain insurance	Merchant Website visitor	Identity Data Contact Data Technical Data	Legitimate Interests (e.g. to obtain insurance policies and to manage our risks as a business)

	Payment service user	Transaction Data Account Data Usage Data	Legal Obligation

We have carried out balancing tests for all the data processing we carry out on the basis of our Legitimate Interests. You can obtain information on any of our balancing tests by contacting us at info@payvyne.com.

Automated decision-making

If you are a Merchant, we may use automated decision-making tools to assess your risk in line with our legal requirements and decide whether or not we can provide our services to you.

For example, we may conduct an automated check of your business' ownership structure, or financial history, during onboarding and automatically decide not to proceed with account opening.

If you are unhappy with a decision we have made using automated means, you can ask for a review of the decision by getting in touch with us (see the "Contact Details" section below).

"Soft" credit checks

If you are a Merchant, we may also conduct "soft" credit checks on your business and key individuals associated with it (including your business' representatives and beneficial owners) using third-party suppliers for the purpose of verifying your identity and managing risk.

We only use these checks for identity verification purposes and the searches are not visible to any other company or business that performs credit searches - they are only visible to you. Soft credit checks do not affect your credit score in any way.

Marketing and opting out

We aspire to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

You can ask us to stop sending you marketing messages at any time by following the unsubscribe links on any marketing message sent to you; or by contacting us at info@payvyne.com.

We will not pass your data on to third-party marketing companies.

Who has access to your information?

We may have to share your personal data with the parties set out below for the purposes set out in the table above:

- service providers who provide IT and system administration services;
- our payment processing partners (currently Token and Yapily) who help us to connect to your bank account and in some cases act as the entity which formally sets up the payment for you;

- our e-money provider Modulr who helps us to process payments for merchants, and facilitate refunds and payouts to payment service users;
- our customer support system Zendesk, who helps us deal with support requests and queries in relation to our products and services;
- professional advisers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services;
- HM Revenue & Customs, the Financial Conduct Authority, regulators and other authorities based in the United Kingdom or European Union who require reporting of processing activities in certain circumstances;
- third-party services providers which enable us to establish and validate your identity;
- credit reporting agencies, courts, tribunals and regulatory authorities, in the event you fail to pay for goods or services we have provided to you;
- courts, tribunals, regulatory authorities and law enforcement officers, as required by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise or defend our legal rights; and
- third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Policy.

International transfers

Whenever we transfer your personal data out of the UK, we ensure that a similar degree of protection is afforded to it by using specific contracts approved for use in the UK which give personal data the same protection it has in the UK.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

Vyne Technologies Ltd
+44 (0)20 7880 1700
hello@payvyne.com

4 Fulwood Place, Holborn,
London WC1V 6HG
United Kingdom

How long we keep your personal data

We don't keep personal information for longer than is necessary. We will only retain your personal information for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal information for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal information, we consider the amount, nature and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

While we retain this information, we will protect it within commercially acceptable means to prevent loss and theft, as well as unauthorised access, disclosure, copying, use or modification

Where we process personal data for marketing purposes or with your consent, we process the data until you ask us to stop and for a short period after this (to allow us to implement your requests). We also keep a record of the fact that you have asked us not to send you direct marketing or to process your data indefinitely so that we can respect your request in future.

Security

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it and those processing your

information will do so only in an authorised manner and are subject to a duty of confidentiality. Any sensitive information (such as name, address, email, mobile/cell number or bank details) is encrypted and we utilise secure web-based data collection technology, including industry standard SSL, with 2048-bit RSA keys, facilitating up to 256-bit AES encrypted sessions. We utilise appropriate measures to safeguard data against unauthorised access, disclosure, alteration, or destruction. These measures may include, among others, encryption, physical access security, auditing, and other appropriate technologies.

When you are on a secure page, a lock icon will appear on the web browsers such as Microsoft Internet Explorer or Safari. Once we receive your information, we make our best effort to ensure its security on our systems. Where we have given (or where you have chosen) a password which enables you to access certain parts of our websites, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

We also have procedures in place to deal with any suspected data security breach. we will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. You have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where:
    - you have successfully exercised your right to object to processing (see below); or
    - where we may have processed your information unlawfully; or
    - where we are required to erase your personal data to comply with local law.

However, we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- Object to processing of your personal data. You may object to our processing where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d)you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured,

commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

- Withdraw consent at any time. You may withdraw your consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, where they would infringe the rights of a third party (including our rights) or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping. Relevant exemptions are included in both the GDPR and in the Data Protection Act 2018. We will inform you of relevant exemptions we rely upon when responding to any request you make.

If you wish to exercise any of the rights set out above, please contact info@payvyne.com.

Contact details

Please contact us, if you have any questions about this Policy or the information we hold about you. If you wish to contact us, please use the contact details below. Our full details are:

Full name of legal entity: Vyne Technologies Limited Email: info@payvyne.comPostal address: 71-75 Shelton Street, London, United Kingdom, WC2H 9JQ

Vyne Technologies Ltd
+44 (0)20 7880 1700
hello@payvyne.com

4 Fulwood Place, Holborn,
London WC1V 6HG
United Kingdom

Making a complaint

Vyne Technologies Limited is registered as a data controller with the Information Commissioner's Office ("ICO"). You have the right to make a complaint at any time to the ICO who are the UK supervisory authority for data protection issues. The ICO may be contacted at https://ico.org.uk/make-a-complaint/ or by telephone: 0303 123 1113.

We would like the opportunity to deal with your concerns before you approach the ICO so please contact us in the first instance and we will do our best to resolve your complaint.