Group Privacy Notice

As a member of the DNA Payments Group (the Company), First Payment Merchant Services take your privacy seriously. This Group Privacy Notice describes who we are and how and why we collect, store, use and share your personal data in accordance with the Data Protection Legislation. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event you have enquiries.

We collect, use and are responsible for certain personal data about you, which we process prior to, during and after your business relationship with us. This Group Privacy Notice is relevant to anyone who uses or makes enquiries our services, as well as website users. If you have signed an agreement with us, such as a Merchant Service Agreement, the agreement shall prevail and, as set out in the Data Protection Legislation, this notice shall be used for information purposes only.

We are subject to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We are also subject to the EU General Data Protection Regulation (EU GDPR) in relation to goods and services we offer to individuals and our wider operations in the European Economic Area (EEA).

In this notice, DNA Payments Group means DNA Payments Limited, a company incorporated under the laws of England and Wales, registration No 11154668, whose registered office is at 10 Lower Grosvenor Place, London SW1W 0EN, and its subsidiary companies (CR7 Services Limited, Optomany Ltd, Optomany KZ, Active Payments, First Payment Merchant Services, Card Cutters, Kwalitas, 123 Send Limited, 123 Hire Limited, EFT Solutions, Zash AB). Personal Data may also be processed by our Group companies, and so, in this notice, references to ‘we’ or ‘us’ mean DNA Payments Limited and its group companies.

The Company is the "Controller", as defined in the UK GDPR. This means that we are responsible for deciding how we hold and use Personal Data about you. We are required under the Data Protection Legislation to notify you of the information contained in this privacy notice.

We have appointed a Data Protection Officer (DPO) to oversee compliance with this Candidate Privacy Notice. Please see below for more information on how to contact the DPO if you would like to make some enquiries on how we process your personal data or related matters.

Key terms

It would be helpful to first clarify some key terms used in this policy:

Data Protection Legislation	Data Protection Act 2018 (EU) General Data Protection Regulation (GDPR) UK General Data Protection Regulation (UK GDPR) Privacy and Electronic Communications Regulations 2003 (PECR)
We, us, our, Controller	DNA Payments Group Ltd, which is made up of the following companies: DNA Payments Limited, CR7 Services Limited, 123 Send Limited, 123 Hire Limited, Optomany Limited, Optomany KZ, Active Payments, Card Cutters, Kwalitas, First Payment Merchant Service, EFT Solutions and Zash AB.
Our data protection officer	DPO@dnapaymentsgroup.com
Personal data	Any information relating to an identified or identifiable individual
Special category personal data	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership Genetic and biometric data (when processed to uniquely identify an individual) Data concerning health, sex life or sexual orientation
Data subject	The individual whose personal data is processed by a Controller or Processor

Personal data we collect about you

The personal data we collect about you depends on the particular products and services we offer you. We may collect and use the following personal data about you:

- your name and contact information, including email address, telephone number and company details
- information to check and verify your identity, eg your date of birth
- your gender, if you choose to give this to us
- location data
- your billing information, transaction and payment card information
- your professional online presence, eg LinkedIn profile
- your contact history
- upon your express consent, information to enable us to undertake credit or other financial checks on you
- information on how you use our website, IT, communication and other systems

We collect and use this personal data for the purposes described in the section '**How and why we use your personal data**' below. If you do not provide personal data we ask for, it may delay or prevent us from providing products and services to you.

How your personal data is collected

We collect most of this personal data directly from you—in person, by telephone, text or email and/or via our website and apps. However, we may also collect information:

- from publicly accessible sources, eg Companies House or HM Land Registry;
- directly from a third party, eg:
    - sanctions screening providers;
    - credit reference agencies;
    - customer due diligence providers;

- from a third party with your consent, eg your bank or building society;
- from cookies on our website—for more information on our use of cookies, please see our cookie policy
- via our IT systems, eg:

    — Entries made in our customer management platforms

How and why we use your personal data

Under the Data Protection Legislation, we can only use your personal data if we have a proper reason, eg:

- where you have given consent;
- to comply with our legal and regulatory obligations;
- for the performance of a contract with you or to take steps at your request before entering into a contract; or
- for our legitimate interests or those of a third party.

A legitimate interest is when we have a business or commercial reason to use your personal data, so long as this is not overridden by your own rights and interests. We will carry out an assessment when relying on legitimate interests, to balance our interests against your own.

The table below explains what we use your personal data for and why.

What we use your personal data for	Our reasons
Providing products and services to you	To perform our contract with you or to take steps at your request before entering into a contract
Preventing and detecting fraud against you or us	To meet out regulatory and legal obligations and to meet our legitimate interest, ie to minimise fraud that could be damaging for you and/or us
- Conducting checks to identify our customers and verify their identity - Screening for financial and other sanctions or embargoes - Other activities necessary to comply with professional, legal and regulatory obligations that apply to our business, eg under health and safety law or rules issued by our professional regulator	To comply with our legal and regulatory obligations
To enforce legal rights or defend or undertake legal proceedings	Depending on the circumstances: —to comply with our legal and regulatory obligations; —in other cases, for our legitimate interests, ie to protect our business, interests and rights
Gathering and providing information required by or relating to audits, enquiries or investigations by regulatory bodies	To comply with our legal and regulatory obligations
Ensuring business policies are adhered to, eg policies covering security and internet use	For our legitimate interests, ie to make sure we are following our own internal procedures so we can deliver the best service to you
Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests, ie to be as efficient as we can so we can deliver the best service to you at the best price
Ensuring the confidentiality of commercially sensitive information	Depending on the circumstances: —for our legitimate interests, ie to protect trade secrets and other commercially valuable information; —to comply with our legal and regulatory obligations
Statistical analysis to help us manage our business, eg in relation to *eg our financial performance, customer satisfaction, product range or other efficiency measures*	For our legitimate interests, ie to be as efficient as we can so we can deliver the best service to you at the best price

What we use your personal data for	Our reasons
Preventing unauthorised access and modifications to systems	Depending on the circumstances: —for our legitimate interests, ie to prevent and detect criminal activity that could be damaging for you and/or us; —to comply with our legal and regulatory obligations
Protecting the security of systems and data used to provide the goods and services	To comply with our legal and regulatory obligations. We may also use your personal data to ensure the security of systems and data to a standard that goes beyond our legal obligations, and in those cases our reasons are for our legitimate interests, ie to protect systems and data and to prevent and detect criminal activity that could be damaging for you and/or us.
Updating customer records	Depending on the circumstances: —to perform our contract with you or to take steps at your request before entering into a contract; —to comply with our legal and regulatory obligations; —making sure that we can keep in touch with our customers about existing orders and new products
Statutory returns	To comply with our legal and regulatory obligations
Ensuring safe working practices, staff administration and assessments	Depending on the circumstances: —to comply with our legal and regulatory obligations; —for our legitimate interests, eg to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you
Marketing our services and those of selected third parties to: —existing and former customers; —third parties who have previously expressed an interest in our services; —third parties with whom we have had no previous dealings where we have a lawful basis to do so.	For our legitimate interests, ie to promote our business to existing and former customers in compliance with the requirements of the Privacy and Electronic Communications Regulations (PECR).
Credit reference checks via external credit reference agencies	To meet our legal obligations and to reduce the risks to our business
External audits and quality checks, eg for ISO or PCI DSS requirements, to the extent not covered by ‘activities necessary to comply with legal and regulatory obligations	Depending on the circumstances: —for our legitimate interests, ie to maintain our accreditations so we can demonstrate we operate at the highest standards; —to comply with our legal and regulatory obligations
To share your personal data with members of our group and third parties that will or may take control or ownership of some or all of our business (and professional advisors acting on our or their behalf) in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale, initial public offering or in the event of our insolvencyIn such cases information will be anonymised where possible and only shared where necessary	Depending on the circumstances: —to comply with our legal and regulatory obligations; —in other cases, for our legitimate interests, ie to protect, realise or grow the value in our business and assets

How and why we use your personal data—in more detail

More details about how we use your personal data and why are set out in the table below

Purpose	Processing operation	Lawful basis relied on under the UK GDPR and EU GDPR	Relevant categories of personal data
Communications with you not related to marketing, including information	Addressing and sending communications to you as	Processing is necessary for compliance with a legal obligation to which	—your name, address and contact information, including email address

Purpose	Processing operation	Lawful basis relied on under the UK GDPR and EU GDPR	Relevant categories of personal data
about the services we are providing you with, about changes to our terms or policies or changes to the products or other important notices (other than those addressed above)	required by data protection laws, ie: —the UK GDPR or Data Protection Act 2018; **[**—the EU GDPR**]**	we are subject (Article 6(1)(b))	and telephone number and company details; —your account details (username)
	Providing you with information about your agreement and relevant payment services activities		
	Handling enquiries and complaints		
	Addressing and sending communications to you about changes to our terms or policies or changes to the products or other important notices	Our legitimate interests (Article 6(1)(f)), which is to be as efficient as we can so we can deliver the best service to you	—your name, address and contact information, including email address and telephone number and company details — your account details (username)
Assessing any application you make, including checking for fraud and money laundering, confirming your identity, and carrying out any other regulatory checks. We may compare your details with the details of countries, organisations and individuals who sanctions apply to, to decide whether we are prevented from doing business with you or processing a transaction under sanctions law.	Carrying out background checks and credit checks to meet our regulatory and legal obligations and to protect our legitimate business interests using information you provided us with and information made public by you.	Processing is necessary for compliance with a legal obligation to which we are subject (Article 1 (b))	— your name, address and contact information, including email address, postal address, telephone number and company details — Your date and place of birth — Your nationality — Identification details (e.g. passport or driving licence details) — Bank statements or utility bills
Meeting our contractual obligations, including those set by the card schemes	Negotiation and/or performance of a contract, including facilitating the provision of services by the card schemes; Executing financial settlements.	Processing is necessary to meet out contractual obligations or in the negotiation in anticipation of a contractual relationship Article 6 (1) (c)	— your name, address and contact information, including email address, postal address, telephone number and company details — Your bank account details
We might share your information with UK or other relevant tax authorities, credit reference agencies, fraud prevention agencies, and UK and overseas regulators and authorities.	Pursuing a legitimate interest in carrying out certain checks so that we can make responsible business decisions. As a responsible group of companies, making sure that we only provide certain products to	Processing is based on our legitimate business interests to ensure we protect our business and all of our customers Article 6 (1) (f)	— your name, address and contact information, including email address, postal address, telephone number and company details — Your bank account details

Purpose	Processing operation	Lawful basis relied on under the UK GDPR and EU GDPR	Relevant categories of personal data
	companies and individuals if the products are appropriate, and continuing to manage the services we provide, for example if we believe that you may have difficulties making a payment to us.		
We might share your information with our group companies, partners and service providers.	Sharing your details within our fully owned group companies to deliver customer support function.	Legitimate interest to execute the provision of products and services provided by the group companies. Article 6 (1) (f)	— your name, address and contact information, including email address, postal address, telephone number and company details — Information about the contract you have signed with us and the services and products you receive — Notes and call recordings in relation to the products and services you receive — Notes and call recordings in relation to enquiries and complaints you might make
	Using third-party service and software providers to carry out certain activities related to the service or product you are receiving from us, who may have access to your personal data from time to time. These providers have signed contracts to ensure your data is protected by them the same way as it is by us, in line with the requirements of the EU and UK GDPR and Data Protection Act 2018. These contracts are reviewed annually.	Legitimate Interest (Article 6 (1) (f)) Performance of a contract Article 6 (1) (c)	— your name, address and contact information, including email address, postal address, telephone number and company details — Your date and place of birth — Your nationality — Identification details (e.g. passport or driving licence details) — Bank statements or utility bills
We may need to collect debt you owe to us	Taking the required steps to recover monies owed to us.	A right to pursue payments owed to us under a contractual	— your name, address and contact information, including

Purpose	Processing operation	Lawful basis relied on under the UK GDPR and EU GDPR	Relevant categories of personal data
		agreement (Article 6(1)(c))	email address, postal address, telephone number and company details
Where applicable, to prevent, detect, investigate and prosecute fraud and alleged fraud, money laundering and other crimes	The law requires us to carry out these checks. It is in our legitimate interests to prevent and investigate fraud, money laundering and other crimes, and to check your identity in order to protect our business and to keep to any laws that apply to us. We must process your personal data under the contract for the services you have asked us to provide.	Processing is necessary for compliance with a legal obligation to which we are subject (Article 6(1)(b)) Our legitimate interests (Article 6(1)(f)), which is to be as efficient as we can so we can deliver the best service to you	— your name, address and contact information, including email address, postal address, telephone number and company details — Your bank account details — Transaction details
Marketing purposes	To provide you with information about related products and services (either as you have consented to this or because you made a sales enquiry with us) We may share your personal data with trusted partners who offer supplementary products and services which are of relevance to your business activities.	Article 6 (1) (a) Article 6 (1) (f)	— your name, address and contact information, potentially including email address, postal address, telephone number
Monitoring, recording and analysing any communications between you and us, including phone calls.	Check your instructions to us where required, to prevent and detect fraud and other crime, to analyse, assess and improve our services to customers, and for training purposes, to improve the services we provide to our customers and to protect our business interests.	Our legitimate interests (Article 6(1)(f)), which is to be as efficient as we can so we can deliver the best service to you and to ensure that we protect our business and other connected businesses.	— your name, address and contact information — your account details (username) — recordings of phone calls — logs of other correspondence (eg email)

How and why we use your personal data—Special category personal data

Certain personal data we collect is treated as a special category to which additional protections apply under data protection law:

- Personal data revealing nationality in so far it is necessary for us to comply with out legal and regulatory obligations when carrying out background checks.
- Personal data revealing health information in so far it is related to us communicating with you in a certain way.
- Personal data revealing health information in so far it is related to us providing you with support or assistance if you experience difficulties in making payments to us.
- Personal data revealing racial or ethnic origin, religious beliefs and health information in so far it is related to a complaint you may make about us.
- Personal data revealing health information in so far as it may be necessary to protect you or another person from harm.

Where we process special category personal data, we will also ensure we are permitted to do so under data protection laws, eg:

- we have your explicit consent;
- the processing is necessary to protect your (or someone else's) vital interests where you are physically or legally incapable of giving consent; or
- the processing is necessary to establish, exercise or defend legal claims.

How and why we use your personal data—sharing

See '**Who we share your personal data with**' for further information on the steps we will take to protect your personal data where we need to share it with others.

Marketing

We will use your personal data to send you updates (by email, text message, telephone or post) about our products and services, including exclusive offers, promotions or new products and services.

We will contact you for marketing purposes only if you have given you explicit consent for doing so, or you contract with us to receive products or services or make a sales and/or product enquiry with us, and we believe that you might be interested in hearing about related products and services (either provided by us or one of our trusted partners).

You have the right to opt out of receiving marketing communications, either from us or our partners, at any time and we will always ensure that we make this clear and easy to do by:

- contacting us at support@dnapaymentsgroup.com;

We may ask you to confirm or update your marketing preferences if you ask us to provide further products and services in the future, or if there are changes in the law, regulation, or the structure of our business.

We will always treat your personal data with the utmost respect and never sell it to other organisations for marketing purposes. As stated, we might share your personal data with carefully selected third parties who offer products and services that are supplementary to our products and services, such as cash advance providers. In such circumstances, we will only share the minimum amount of personal data required to contact you and we will enter into contractual agreements with our partners to ensure that your personal data is kept secure, only used for the purpose of offering a related product or service and that it is deleted within a set period of time if you do not take up their offer.

Who we share your personal data with

We routinely share personal data with:

- companies within DNAP Payments Group
- third parties we use to help deliver our products and services to you, eg warehouses and delivery companies;
- other third parties we use to help us run our business, eg credit referencing agencies, Software as a Service providers or website hosts;
- third parties approved by you, eg third party payment providers;
- credit reference agencies;

- our bank**;**
- our auditors
- card schemes and our regulators
- law enforcement agencies as may be required.

We only allow those organisations to handle your personal data if we are satisfied they take appropriate measures to protect your personal data. We also impose contractual obligations on them to ensure they can only use your personal data to provide services to us and to you.

We or the third parties mentioned above occasionally also share personal data with:

- our and their external auditors, eg in relation to the audit of our or their accounts, in which case the recipient of the information will be bound by confidentiality obligations;
- our and their professional advisors (such as lawyers and other advisors), in which case the recipient of the information will be bound by confidentiality obligations;
- law enforcement agencies, courts, tribunals and regulatory bodies to comply with our legal and regulatory obligations;
- other parties that have or may acquire control or ownership of our business (and our or their professional advisers) in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale, initial public offering or in the event of our insolvency. The recipient of any of your personal data will be bound by confidentiality obligations.

Who we share your personal data with—further information

If you would like more information about who we share our data with and why, please contact us (see '**How to contact us**' below).

Where your personal data is held

Personal data may be held at our offices and those of our group companies, on our Microsoft Azure and Oracle instances, third party agencies, service providers, representatives and agents as described above.

Some of these third parties may be based outside the UK/EEA. For more information, including on how we safeguard your personal data when this happens, see below: '**Transferring your personal data out of the UK and EEA**'.

How long your personal data will be kept

We will not keep your personal data for longer than we need it for the purpose for which it is used. Different retention periods apply for different types of personal data. Some of our retention periods are stated below but you may also contact us for a copy of our Data Retention Schedule.

EFT records (Transactions)	5
SARs	5
KYC data including all records and images	5
Call recordings	1
Customer records related to a product or services	6

Personal data of those who make an enquiry/marketing leads who do not become customers	

If you no longer have an account with us or we are no longer providing products and services to you, we will delete or anonymise your account data after six years.

Following the end of the of the relevant retention period, we will permanently delete or anonymise your personal data.

Transferring your personal data out of the UK and EEA

The UK and EEA and other, third countries, have differing data protection laws, some of which may provide lower levels of protection of privacy.

It is sometimes necessary for us to transfer your personal data to organisations based in countries outside the UK and EEA. In those cases we will comply with applicable UK and EEA laws designed to ensure the privacy of your personal data.

As we are based in the UK we will also transfer your personal data from the EEA to the UK.

Under data protection laws, we can only transfer your personal data to a country outside the UK/EEA where:

- in the case of transfers subject to UK data protection law, the UK government has decided the particular country ensures an adequate level of protection of personal data (known as an '**adequacy regulation**') further to Article 45 of the UK GDPR. A list of countries the UK currently has adequacy regulations in relation to is available here. We rely on adequacy regulations for transfers to the following countries: countries in the EEA.
- in the case of transfers subject to EEA data protection laws, the European Commission has decided that the particular country ensures an adequate level of protection of personal data (known as an '**adequacy decision**') further to Article 45 of the EU GDPR. A list of countries the European Commission has currently made adequacy decisions in relation to is available here. We rely on adequacy decisions for transfers to the following countries: UK.
- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for you; or
- a specific exception applies under relevant data protection law.

Where we transfer your personal data outside the UK, we do so on the basis of an adequacy regulation or (where this is not available) on the basis of legally-approved standard data protection clauses recognised or issued further to Article 46(2) of the UK GDPR. In the event we cannot or choose not to continue to rely on either of those mechanisms at any time, we will not transfer your personal data outside the UK unless we can do so on the basis of an alternative mechanism or exception provided by UK data protection law and reflected in an update to this policy.

Where we transfer your personal data outside the EEA we do so on the basis of an adequacy decision or (where this is not available) legally-approved standard data protection clauses issued further to Article 46(2) of the EU GDPR. In the event we cannot or choose not to continue to rely on either of those mechanisms at any time we will not transfer your personal data outside the EEA unless we can do so on the basis of an alternative mechanism or exception provided by applicable data protection law and reflected in an update to this policy.

Any changes to the destinations to which we send personal data or in the transfer mechanisms we rely on to transfer personal data internationally will be notified to you in accordance with the section on '**Changes to this privacy policy**' below.

Your rights

You have the following rights, which you can exercise free of charge:

Access	The right to be provided with a copy of your personal data
Rectification	The right to require us to correct any mistakes in your personal data
Erasure (also known as the right to be forgotten)	The right to require us to delete your personal data—in certain situations
Restriction of processing	The right to require us to restrict processing of your personal data in certain circumstances, eg if you contest the accuracy of the data
Data portability	The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations
To object	The right to object: —at any time to your personal data being processed for direct marketing (including profiling); —in certain other situations to our continued processing of your personal data, eg processing carried out for the purpose of our legitimate interests unless there are compelling legitimate grounds for the processing to continue or the processing is required for the establishment, exercise or defence of legal claims
Not to be subject to automated individual decision making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you
The right to withdraw consents	If you have provided us with a consent to use your personal data you have a right to withdraw that consent easily at any time You may withdraw consents by [*insert details as relevant depending on consents*] Withdrawing a consent will not affect the lawfulness of our use of your personal data in reliance on that consent before it was withdrawn

For more information on each of those rights, including the circumstances in which they apply, please contact us (see '**How to contact us**' below) or see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights.

If you would like to exercise any of those rights, please:

- email, call or write to us—see below: '**How to contact us**'; and
- provide enough information to identify yourself *(eg your full name, address and merchant ID or customer or matter reference number)* and any additional identity information we may reasonably request from you;
- let us know what right you want to exercise and the information to which your request relates.

Keeping your personal data secure

We have appropriate security measures to prevent personal data from being accidentally lost, or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access it. Those processing your personal data will do so only in an authorised manner and are subject to a duty of confidentiality. We continually test our systems and are PCI DSS compliant, which means we follow top industry standards for information security.

We also have policies and procedures 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.

If you want detailed information from Get Safe Online on how to protect your personal data and other information and your computers and devices against fraud, identity theft, viruses and many other online problems, please visit www.getsafeonline.org. Get Safe Online is supported by HM Government and leading businesses.

How to make enquiries about your personal data and how we use it, or to complain

Please contact us if you have any queries or concerns about our use of your personal data (see below '**How to contact us**'). We hope we will be able to resolve any issues you may have.

You also have the right to lodge a complaint with:

- the Information Commissioner
- a relevant data protection supervisory authority in the EEA state of your habitual residence, place of work or of an alleged infringement of data protection laws in the EEA

The Information Commissioner may be contacted using the details at https://ico.org.uk/make-a-complaint or by telephone: 0303 123 1113.

For a list of EEA data protection supervisory authorities and their contact details see here.

Changes to this privacy policy

This privacy notice was last updated on 25 July 2022.

We may change this privacy notice from time to time—when we do we will inform you via our website.

How to contact us

Individuals in the UK

You can contact our Data Protection Officer**]** by email if you have any questions about this privacy policy or the information we hold about you, to exercise a right under data protection law or to make a complaint.

Our contact details are shown below:

Our contact details	Our Data Protection Officer's contact details
DNA Payments Group Ltd 10 Lower Grosvenor Place, London, SW1W 0EN 0208 102 8100	Data Protection Officer DPO@dnapaymentsgroup.com

Individuals in the EEA

Individuals within the EEA can contact us direct (see above).

Do you need extra help?

If you would like this notice in another format (for example audio, large print, braille) please contact us (see 'How to contact us' above).