Nopalaver Payroll Solutions Ltd – Data Protection Policy

Introduction

Nopalaver Payroll Solutions Ltd needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Nopalaver Payroll Solutions Ltd;

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 1998 describes how organisations – including Nopalaver Payroll Solutions Ltd must collect, handle and store personal information.

This Privacy Policy applies to the personal data of our Employees, Clients, Suppliers, Website Users and other people we may contact in connection with business.

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), the company responsible for your personal data is ("Nopalaver Payroll Solutions Ltd" or "us" or "we").

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes

- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

PEOPLE, RISKS AND RESPONSIBILITIES

Policy scope

This policy applies to:

- The office of Nopalaver Payroll Solutions Ltd
- All employees of Nopalaver Payroll Solutions Ltd
- All staff and volunteers of Nopalaver Payroll Solutions Ltd
- All contractors, suppliers and other people working on behalf of Nopalaver Payroll Solutions Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus, any other information relating to individuals including National Insurance details, PAYE details, Bank Information and Right to Work ID verification checks and documentation

Data protection risks

This policy helps to protect Nopalaver Payroll Solutions Ltd from some very real data security risks, including:

- **Breaches of confidentiality:** For instance, information being given out inappropriately.
- **Failing to offer choice:** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage:** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Nopalaver Payroll Solutions Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **board of directors** is ultimately responsible for ensuring that Nopalaver Payroll Solutions Ltd meets its legal obligations.

The **Data Protection Officer- Graham Jenner,** is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Nopalaver Payroll Solutions Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

The only people able to access data covered by this policy should be those who **need it for their work**.

- Nopalaver Payroll Solutions Ltd **will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used,** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Your Data

Where appropriate and in accordance with local laws and requirements, we may also use your personal data for things like marketing. Where appropriate, we will seek your consent to undertake some of these activities.

We generally use Employee data in two ways:

- For our main activity – Payroll Activities
- Marketing Activities

Payroll Activities

We've listed below various ways in which we may use and process your personal data for this purpose:

Collecting your data from you;

- Storing your details (and updating them when necessary) on our database, so that we can contact you in relation to payroll;
- Providing you with our payroll function and to facilitate the payroll process;
- Sending your information to specific suppliers, in order to comply with legislation for Pensions Auto Enrolment;
- Carrying out our obligations arising from any contracts entered into between us;

- Carrying out our obligations arising from any contracts entered into between Nopalaver Payroll Solutions Ltd and third parties in relation to your recruitment;
- Facilitating our administration, payment and invoicing processes;
- Verifying details, you have provided, using third party resources, or to request information (such as references, qualifications and potentially any criminal convictions, to the extent that this is appropriate and in accordance with local laws);
- Complying with our legal obligations in connection with the detection of crime or the collection of taxes or duties; and
- Processing your data to enable us to send you targeted, relevant communications, which we think, are likely to be of interest to you.
- We may use your personal data for the above purposes if we deem it necessary to do so for our legitimate interests. If you are not happy about this, in certain circumstances you have the right to object.

*Please note that this list is not exhaustive.

Marketing Activities

We may periodically send you information that we think you may find interesting, in particular, we may wish to use your data to enable us to market our full range of payroll functions and legislation / industry changes to you.

We would need your consent for some aspects of marketing activities which are not covered by our legitimate interests (in particular, the collection of data via cookies, and the delivery of direct marketing to you through digital channels) and, depending on the situation, we'll ask for this via an 'explicit opt-in' or 'soft-opt-in'.

'Soft opt-in' consent is a specific type of consent which applies where you have previously engaged with us and we are marketing other payroll-related services. Under 'soft opt-in' consent, we will take your consent as given unless or until you opt out. For most people, this is beneficial as it allows us to suggest other services to you alongside the specific one you applied for. For other types of e-marketing, we are required to obtain your explicit consent.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Operations Manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required. When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on **designated drives and servers** and should only be uploaded to an **approved cloud computing service**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data Use

Personal data is of no value to Nopalaver Payroll Solutions Ltd unless the business can make use of it.

However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never **be transferred outside of the European Economic Area** .
- Employees should **not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy

The law requires Nopalaver Payroll Solutions Ltd take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Nopalaver Payroll Solutions Ltd should put into ensuring its accuracy.

- It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject access requests

All individuals who are the subject of personal data held by Nopalaver Payroll Solutions Ltd are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**. If an individual contacts the company requesting this information; this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at gdpr@nopalaverumbrella.co.uk The

data controller can supply a standard request form, although individuals do not have to use this. Individuals will not normally be charged for a request, although a £10 per subject access request may be enforced if excessive requests are made to the business. The data controller will aim to provide the relevant data within 40 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Nopalaver Payroll Solutions Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Nopalaver Payroll Solutions Ltd aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used
- How to exercise their rights
- To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

HOW CAN YOU ACCESS, AMEND OR RETRACT YOUR PERSONAL DATA?

The main objectives of GDPR is to protect and clarify the rights of EU citizens and individuals in the EU with regards to data privacy.

You retain various rights in respect of your data, even after you have given it to us. To get in touch about these rights, detailed below, please contact us. We will seek to deal with your request without undue delay, and in any event within one month, subject to any lawful entitlement to extend this period.

We may keep a record of your communications to help us resolve any issues which you raise.

Right to object (Art. 21 GDPR)

The right to object enables you to object to us processing your personal data where we do so for one of the following three reasons:

- our legitimate interests;
- to send you direct marketing materials; and
- for scientific, historical, research, or statistical purposes.
- The "legitimate interests" and "direct marketing" categories above are the ones most likely to apply to our Employees, Clients and Suppliers. If your objection relates to us processing your personal data because we deem it necessary for your legitimate interests, we must act on your objection by ceasing the activity in question unless:

- we can show that we have compelling legitimate grounds for processing which overrides your interests; or
- we are processing your data for the establishment, exercise or defence of a legal claim.
- If your objection relates to direct marketing, we must act on your objection by ceasing this activity.

Right to withdraw consent (Art. 7 GDPR)

Where we have obtained your consent to process your personal data for certain activities (for example, for our marketing arrangements), you may withdraw this consent at any time and we will cease to carry out the particular activity that you previously consented to unless we consider that there is an alternative reason to justify our continued processing of your data for this purpose in which case we will inform you of this condition.

Data Subject Access Requests (Art. 15 GDPR)

You may ask us to confirm what information we hold about you at any time and request us to rectify or erasure of the information. We will ask you to verify your identity and for more information about your request. If we provide you with access to the information, we hold about you, we will not charge you for this unless your request is “manifestly unfounded or excessive”. If you request further copies of this information from us, we may charge you a reasonable administrative cost where legally permissible. We may refuse your request, where we are legally permitted to do so. If we refuse your request, we will always tell you the reasons for doing so.

Right to erasure (‘right to be forgotten’) (Art. 17 GDPR)

In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to “erase” your personal data. We will respond to your request within 30 days (subject to any lawful entitlement to extend this period) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will erase your data but will generally assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted in the future where your data is collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.
Normally, to enable us to agree your request to erasure, the information must meet one of the following criteria:

The data is no longer necessary for the purpose for which we originally collected and/or processed them;

- where previously given, you have withdrawn your consent to us processing your data, and there is no other valid reason for us to continue processing;
- the data has been processed unlawfully (i.e. in a manner which does not comply with the GDPR);
- it is necessary for the data to be erased in order for us to comply with our legal obligations as a data controller; or
- if we process the data because we believe it necessary to do so for our legitimate interests, you object to the processing and we are unable to demonstrate overriding legitimate grounds for our continued processing.

We would only be entitled to refuse to comply with your request for one of the following reasons:

- to exercise the right of freedom of expression and information;

- to comply with legal obligations, for the performance of a task carried out in the public interest or in the exercise of official authority;
- for public health reasons in the public interest;
- to exercise or defend a legal claim.
- When complying with a valid request for the erasure of data we will take all reasonably practicable steps to erase the relevant data.

Right to restriction of processing (Art. 18 GDPR)

You have the right to request that we restrict our processing of your personal data in certain circumstances. This means that we can only continue to store your data and will not be able to carry out any further processing activities with it until either:

One of the circumstances listed below is resolved;

You consent;

Or further processing is necessary for either the establishment, exercise or defence of legal claims, the protection of the rights of another individual, or reasons of important EU or Member State public interest.

The circumstances in which you are entitled to request that we restrict the processing of your personal data are:

- You contest the accuracy of the personal data that we are processing about you. In this case, our processing of your personal data will be restricted for the period during which the accuracy of the data is verified;
- You object to our processing of your personal data for our legitimate interests. Here, you can request that the data be restricted while we verify our grounds for processing your personal data;
- Where our processing of your data is unlawful, but you would prefer us to restrict our processing of it rather than erasing it; and
- Where we have no further need to process your personal data, but you require the data to establish, exercise, or defend legal claims.

If we have shared your personal data with third parties, we will notify them about the restricted processing unless this is impossible or involves a disproportionate effort. We will notify you before lifting any restriction on processing your personal data.

Right to rectification (Art. 16 GDPR)

You also have the right to request that we rectify any inaccurate or incomplete personal data that we hold about you. If we have shared this personal data with third parties, we will notify them about the rectification unless this is impossible or involves disproportionate effort. Where appropriate, we will also tell you which third parties we have disclosed the inaccurate or incomplete personal data to. Where we think that it is reasonable for us not to comply with your request, we will explain our reasons for this decision.

Right to lodge a complaint with a supervisory authority (Art 77. GDPR)

You also have the right to lodge a complaint with the supervisory authority.

Details of the supervisory authority: The Information Commissioner's Office, Wycliffe House,

Water Lane, Wilmslow, Cheshire, SK9 5AF Telephone : 0303 123 1113

LAWFUL REASONS FOR PROCESSING YOUR DATA LEGITIMATE INTERESTS

Article 6(1)(f) of the GDPR says that we can process your data where it "is necessary for the purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of you which require protection of personal data."

We don't believe that any of the following activities prejudice individuals in any way, we believe they help us to offer you a more tailored, efficient service. However, you do have the right to object to us processing your personal data on this basis. If you would like to know more about how to do so, please see the section entitled; "HOW CAN YOU ACCESS, AMEND OR RETRACT YOUR PERSONAL DATA?"

Employee Data

We believe it's reasonable to expect that if you are working under our employment that personal details must be stored to lawfully process payroll for you.

With regards to marketing material, we therefore think it's reasonable for us to process your data to make sure that we send you the most appropriate content. We must make sure our business runs smoothly, so that we can carry on providing services to Employees like yourself. We therefore also need to use your data for administrative activities, such as contract processing, payments and invoicing.

We have our own obligations under the law. If we believe in good faith that it is necessary, we may therefore share your data in connection with crime detection, tax collection or actual or anticipated litigation.

Client Data

To ensure that we provide you with the best service possible, we store your basic personal data and/or the personal data of individual contacts at your organisation as well as keeping records of our conversations, meetings, and assignments. From time to time, we may also ask you to undertake a customer satisfaction survey. We believe this to be reasonable – we deem these uses of your data to be necessary for our legitimate interests as an organisation providing a payroll function to you.

Supplier Data

We use and store the basic personal data of individuals within your organisation in order to facilitate the services from you as one of our Suppliers. We also hold your organisations financial details, so that we can pay

you for your services. We deem all such activities to be necessary within the range of our legitimate interests as a recipient of your services.

Other – such as Emergency Contacts

If an employee has given us your details as an emergency contact, we will use these details to contact you in the case of an accident or emergency. We believe this to be a vital element of our organisation, and so is necessary for our legitimate interests.

CONTRACT

Article 6(1)(b) of the GDPR gives us a lawful basis for processing where "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract".

Therefore, we are able to process personal data where:-

- We have a contract with you, and we need to process your personal data to comply with the obligations under the contract; or
- We haven't yet got a contract with you, but you have asked us to do something as the first step and we need to process your personal data to fulfil the request.

CONSENT

In certain circumstances, we are required to obtain your consent to the processing of your personal data in relation to certain activities. Depending on exactly what we are doing with your information, this consent will be opt-in consent or soft opt-in consent.

Article 4(11) of the GDPR states that (opt-in) consent is "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." This means that:

- you have to give us your consent freely, without us putting you under any type of pressure;
- you have to know what you are consenting to – so we'll make sure we give you enough information;
- you should have control over which processing activities you consent to and which you don't; and
- you need to take positive and affirmative action in giving us your consent – we're likely to provide a tick box for you to check so that this requirement is met in a clear and unambiguous fashion.

We will keep records of the consents that you have given in this way.

We have already mentioned that, in some cases, we will be able to rely on soft opt-in consent. We are allowed to market products or services to you which are related to the payroll function we provide as long as you do not actively opt-out from these communications.

As we have mentioned, you have the right to withdraw your consent to these activities. You can do so at any time.

COMPLIANCE WITH A LEGAL OBLIGATION

Article 6(1)(c) of the GDPR gives us a lawful basis for processing where “processing is necessary for compliance with a legal obligation to which the controller is subject”.

Therefore, we are able to process personal data where we have a contract with you, and we need to process your personal data to comply with our legal obligations under relevant law.

ESTABLISHING, EXERCISING OR DEFENDING LEGAL CLAIMS

Sometimes it may be necessary for us to process personal data and, where appropriate and in accordance with local laws and requirements, sensitive personal data in connection with exercising or defending legal claims. Article 9(2)(f) of the GDPR allows this where the processing “is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity”.

This may arise for example where we need to take legal advice in relation to legal proceedings or are required by law to preserve or disclose certain information as part of the legal process.

CONTACT US

For any matter relating to the processing of personal data, or this policy document, you can write to us at the following address:

1 South House, Bond Avenue, Bletchley, Milton Keynes, MK1 1SW

Alternatively, please send an email to: **gdpr@nopalaverumbrella.co.uk**

DIGITAL PRIVACY POLICY

Nopalaver Payroll Ltd is committed to respecting your privacy and the privacy of every visitor to our web site/person completing any online forms or signing up to this service. The information we collect about you will be used to fulfil the required services and enable us to improve how, as an organisation, we deal with you.

Should you have a question about the data we store, our contact details are:

Organisation: Nopalaver Payroll Solutions Ltd
Address: 1 South House, Bond Avenue, Bletchley, Milton Keynes
Post code: MK1 1SW
Email: gdpr@nopalaverumbrella.co.uk .
Phone number: 01908 370452
Data Protection Officer: Graham Jenner

The information that we collect about you will only be used lawfully (in accordance with the Data Protection Act 1998 and the General Data Protection Regulation 2018). All data is retained exclusively within the United Kingdom or transferred only to ‘third countries’ where ‘adequacy of protection’ or specific certification as defined by The GDPR has been confirmed.

This information will not be disclosed to anyone outside Nopalaver Payroll Solutions Ltd or its associated companies, partners, and other companies with which Nopalaver Payroll Solutions Ltd has arranged services for your benefit.

We expect the information we hold to be accurate and up to date. You have the right as an individual to find out what information we hold about you and make changes if necessary; you also have the right, assuming we are not obligated by law to refuse, to ask us to stop using the information. To have your information removed or rectified, please contact gdpr@nopalaverumbrella.co.uk
The type of information that we will collect on you, and you voluntarily provide to us on this website includes:

- Your name
- Telephone number(s)
- Email address
- IP address

We may, in further dealings with you, extend this information to include your address, purchases, services used, and subscriptions, records of conversations and agreements.

You are under no statutory or contractual requirement or obligation to provide us with your personal information; however, we require at least the information above in order for us to deal with you as a prospect in an efficient and effective manner.
The legal basis for processing your data is based on your specific consent/performance of a contract of employment/compliance with a legal obligation/your vital interest/ and/or our legitimate interest that we will have requested at the point the information was initially provided, therefore we will not store, process or transfer your data outside the parties detailed above unless we have an appropriate lawful reason to do so. Unless we are precluded from doing so by law, you have the right to remove your consent at any time by contacting us and requesting that processing of your details be restricted or deleted.

Unless otherwise required by law, your data will be stored for a period of 2 years after our last contact with you, at which point it will be deleted.

PROTECTION OF PERSONAL INFORMATION

Nopalaver Payroll Solutions Ltd takes precautions, including administrative, technical, and physical measures, to safeguard your Data against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.

Nopalaver Payroll Solutions Ltd uses industry-standard efforts to safeguard the confidentiality of Data, including encryption, firewalls and SSL (Secure Sockets Layer). We have implemented reasonable administrative, technical, and physical security controls to protect against the loss, misuse, or alteration of your Data.