FourNet®

Data Privacy Policy

4net Technologies Ltd Trading as FourNet
3 Scholar Green Road, Cobra Court, Manchester M32 0TR
Tel: 0845 055 6366

Table of Contents

Document Control

Document Title:	002 08 Data Privacy Notice PUBLIC VERSION
Owner:	Stuart Williams
Category:	Restricted
Classification:	ISO Controlled
Version:	5.1
Date:	11.10.24
Review Frequency:	Annually
Next Review Date:	11.10.25

Change History

Date	Version	Brief Description	Author
10.04.17	0.1	Initial Draft	Toni Hazlewood
23.06.17	0.2	For Board Review	Matt Dawe
21.07.17	0.3	Amendments Following Board Review	Toni Hazlewood
05.01.18	1.0	First Release	Matt Dawe
06.07.20	2.0	FourNet Branding/Updates	David O'Brien
24.08.20	3.0	Reformatting Post ISO 27001 Audit	David O'Brien
11.10.20	4.0	Renumbered in line with ISO Documentation Policy	David O'Brien
04.12.20	4.1	Information Security Incident Management	David O'Brien
05.03.21	4.2	Update to section 9	Mariam Jafri
11.03.21	4.3	General spellcheck update	David O'Brien
17.11.21	4.4	Annual Review	David O'Brien
15.09.22	4.5	Annual Review	Sarah-Jane Heber-Hall
10.10.22	4.6	Review of staff retention requirements	Sarah-Jane Heber-Hall
05.09.23	4.7	Annual Review	Sarah-Jane Heber-Hall
20.09.23	4.8	Annual Review and addition of DBS Certificate storage information retention and inclusion of Customer Processed Data to align with 002 66 Data Processing activities.	Sarah-Jane Heber-Hall
08.11.23	4.9	Review of staff email retention amendment to table 1	Sarah-Jane Heber-Hall
02.04.24	5.0	Amendment to include Marketing Information that we use.	Sarah-Jane Heber-Hall
11.10.24	5.1	Addition of call recording retention details added to the Policy	Sarah-Jane Heber-Hall

Document Information

This document is the property of 4net Technologies Limited, trading as FourNet. It must not be reproduced in whole or in part of otherwise disclosed without prior written consent from FourNet.

The official controlled copy of this manual is the digitally signed PDF document on the FourNet SharePoint® and visible to all authorised users. All printed copies and all electronic copies and versions except the ones described above, are considered uncontrolled copies used for reference only.

This document is controlled as a single entity, as any change, however slight, even a single character, to any part of the document by definition changes the entire document. For this reason, as well as the fact that the concept of "page" varies with the publication format, page-level revision is not practiced with this or any other FourNet document.

Authorisation

Document Prepared by:	Sarah-Jane Heber-Hall **Head of Compliance**
	Verified and Authorised by:
	
	Richard Pennington **Chief Executive Officer (CEO)**

1. Background

FourNet Technologies Limited ("**FourNet**") understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of all of our customers, suppliers and staff and will only collect and use personal data in ways that are described here and in a way that is consistent with our obligations and your rights under the law and current legislation.

2. Information About FourNet

Company Registration No.:	05448638
Registered Office:	3 Scholar Green Road Stretford Manchester M32 0TR
Data Protection Officer:	Stuart Williams
Email Address:	dpo@fournet.co.uk
Telephone Number:	0845 055 6366

3. What Does This Policy Cover?

This Privacy Policy explains how we use your personal data: how it is collected, how it is held and how it is processed. It also explains your rights under the law relating to your personal data.

4. Personal Data

Personal data is defined by the General Data Protection Regulation (EU Regulation 2016/679) (the "**GDPR**") and the Data Protection Act 2018 (the DPA) as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.

Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data and other online identifiers.

The personal data that we use is set out in Part 6 of this policy.

5. Your Rights

Under the GDPR and the DPA, you have the following rights, which we will always work to uphold:

- The right to be informed about our collection and use of your personal data. This Privacy Notice should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 12
- The right to access the personal data we hold about you. Part 11 will tell you how to do this;
- The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. Please contact us using the details in Part 12 to find out more;
- The right to be forgotten, i.e., the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please contact us using the details in Part 12 to find out more;
- The right to restrict, i.e., prevent the processing of your personal data;
- The right to object to us using your personal data for a particular purpose or purposes;
- The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases; and
- Rights relating to automated decision-making and profiling. We do not use your personal data in this way.

For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 12.

Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau (CAB).

If you have any cause for complaint about our use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.

6. Personal Data We Collect

We may collect some or all of the following personal data (this may vary according to your relationship with us):

- Name;
- Business Address;
- Business Email Address;
- Business Telephone Number;
- Business Name;

- Job Title;
- Payment Information; and
- Online activity related to our Website (please refer to our separate 002_36 Website Privacy Policy).
- Call Recordings for quality monitoring purposes and contractual service verification

We may obtain information from a trusted provider to help us make contact with key industry professionals, for marketing and sales purposes. We only purpose data that we believe is opted-In and always try to use business data that is accurate, actionable and data-privacy compliant.

7. How Do You Use My Personal Data?

Under the GDPR and the DPA, we must always have a lawful basis for using personal data. This may be because the data is necessary for our performance of a contract with you, because you have consented to our use of your personal data, or because it is in our legitimate business interests to use it. Your personal data may be used for one of the following purposes:

- Providing and managing your account;
- Supplying our products and services to you. Your personal details are required in order for us to enter into a contract with you;
- Personalising and tailoring our products and services for you;
- Ensuring that we are meeting our commitments and obligations to our clients and interested parties, by being able to measure and monitor conversational outcomes;
- Communicating with you. This may include responding to emails or calls from you;
- Supplying you with information by email and post, you may unsubscribe or opt-out at any time by replying to the sender of the email, or by contacting the data protection officer. Once an opt out notice has been received our systems will be updated to ensure that you are not contacted again; or
- With your permission and/or where permitted by law, we may also use your personal data for marketing purposes, which may include contacting you by email, telephone, text message and post with information, news and offers on our products and services. You will not be sent any unlawful marketing or spam. we will always work to fully protect your rights and comply with our obligations under the GDPR, the DPA and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and you will always have the opportunity to opt-out.

8. Data Retention and Disposal

We will not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected. Your personal data will therefore be kept for the periods laid out in table 1, shown below.

For Formal Documentation used within the Business, that may contain staff names, this is archived once superseded and then deleted after 24 months.,

Please note that financial data is held for a period of up to seven years, where practicable to do so. Personal data is removed from this type of data before it is archived.

When paper-based information is no longer required, or superseded, it is to be securely shredded and disposed of appropriately, and a certificate of destruction obtained from the shredding company, as proof of secure destruction.

Table 1 Data Retention Periods

Data Subject	Data Type	Retention Period
Customer	Contact Details	For the duration of the contract plus 24 months.
Customer Processed data	Cloud storage and call recordings, and any other contractually authorised data, instructed by a Data controller	In line with Controllers/Contractual requirements and obligations and Article 30 of Processing Activities of (UK) GDPR. Call recordings will be kept for 180 days, unless required for specific internal investigations or best practice training examples.
Supplier	Contact Details	For the duration that the supplier remains on the FourNet approved supplier list plus 24 months.
Staff	Personnel Records and Contact Details including H & S and First Aid training, as well as information required to authorise financial payments, like Business Travel and mileage claims and allowances. DBS Certificate Information	For the duration of employment plus 72 months, to cover the time limit for bringing any civil legal action. All emails and IM's will be deleted after 3 months from the date of leaving. Ongoing deletions of emails and IM's will be retained for 12 months only within backups. Only for the purpose for which it was obtained, and then destroyed within 6 months.
Accident Books , accident records / reports	Incident information	3 years from the date of last entry for all people over 18.
Subject Access requests and other GDPR requests	Data Protection Information	1 year following completion of the request.
Prospective Customer	Contact Details	24 months unless the Customer opts out, in which case the data will be deleted immediately.
Visitors	Contact Details	24 months

9. How and Where Do You Store or Transfer My Personal Data?

We use Salesforce to store your personal data. Privacy Policies, details of Binding Corporate Rules and Standard Contractual Clauses can be found here: https://www.salesforce.com/company/privacy/This system is used for Marketing, Sales, Project Management, Contract Management, and Service. This platform is accessed primarily by FourNet staff within the UK, and also our out of hours Service Team based in the Philippines.

We will only process your personal data in the Philippines if you have consented to the Standard Contractual clauses. All UK Government related contracts do not use this 3rd party service. For clients that do use this service, as data is processed outside the UK, we have increased our security procedures to counter any data breach. All access devices are monitored and are blocked from making large data transfers. This means that your data will be protected fully in line with GDPR and the all related Standard Contractual Clauses.

10. Do You Share My Personal Data?

We may sometimes contract with our approved third-party suppliers to supply products and services to you on our behalf. These may include payment processing and the delivery of goods and services to you. In some cases, those third-parties may require access to some of your personal data that we hold.

If any of your personal data is required by a third-party, as described above, we will take steps to ensure that your personal data is handled safely, securely and in accordance with your rights, our obligations, and the third-party's obligations under the law, as described above in Part 9.

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

11. How Can I Access My Personal Data?

If you want to know what personal data, we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a "subject access request."

All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 12. To make this as easy as possible for you, a Subject Access Request Form is available for you to use. You do not have to use this form, but it is the easiest way to tell us everything we need to know to respond to your request as quickly as possible.

There is not normally any charge for a subject access request. If your request is 'manifestly unfounded or excessive' (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your subject access request within 10 business days and, in any case, not more than one month of receiving it. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

12. How Do I Contact You?

To contact us about anything to do with your personal data and data protection, including to make a subject access request, please use the following contact details:

Data Protection Officer	Stuart Williams – Data Protection Officer
Email Address:	dpo@fournet.co.uk
Telephone Number:	0845 055 6366

13. Information Security incident Management

Staff must acquaint themselves with the Company's Information Security Incident Management Policy as detailed in document reference 002 39 Information Security Incident Management Policy. This is with regards to any information Security risk, weakness or event that may compromise this Data Privacy Notice.

14. Enforcement

Any member of staff found to have violated this Privacy Notice may be subject to disciplinary action, up to and including termination of employment. In certain circumstance, investigation by regulatory bodies and or the police may apply.

15. Changes to this Privacy Notice

We may change this Privacy Notice from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.

Any changes will be made available within 10 working days.

16. Communicating FourNet's Policies

Relevant training, bulletins, education materials, policies, procedures, and processes are provided on an ongoing basis to all employees to ensure they are fully aware of their responsibilities and are kept up-to-date of any new requirements. These are communicated in a number of ways, including, but not limited to:

- Induction sessions;
- PDR meetings;
- Company meetings;
- Atlas/Citation portal; and
- Regular company bulletins via Microsoft Teams.

17. Review and Ownership of This Policy

This policy will be reviewed and amended as required, and at least annually by the Data Protection Officer and Head of Compliance. This document is managed by the ISO review process and, as such any revisions will be authorised at Board Level prior to general release.

This policy document is ISO controlled and as such, the source document will be stored in the secure area of the FourNet ISO SharePoint® and a PDF version in FourNet Open Access ISO Documents PDFs folder, sub-folder 002 Policies.