



PRIVACY POLICY

[version date: 16-10-2024]

This Privacy Policy details how we, **e4 Strategic (UK) Ltd** (“we” / “e4”), use personal data collected by or in relation to the VERSA platforms, the VERSA Customer Portal, any optional VERSA services which you use and any related e4 websites or mobile apps (together referred to in this policy as “**VERSA**”)

e4 is committed to protecting the privacy and security of your personal information. This privacy policy describes how we collect and use personal information about you in accordance with data protection law. Please read it carefully.

Data protection law says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

If you have any questions about this policy or how we collect and use personal information about you please contact us at legal@e4strategic.co.uk.

1. **SCOPE OF THIS POLICY**

This privacy policy only applies to personal data which we process as a controller (meaning that we determine the purposes and means of the processing of the personal data). Where VERSA contains personal data for which a third party (such as a law firm, licensed conveyancer or mortgage lender) is the controller, we will act as a processor of that data and this privacy policy will not apply. In order to understand how the law firms, licensed conveyancers or mortgage lenders use personal data, please see their own privacy policies.

2. **INFORMATION ABOUT US**

We are e4 Strategic (UK) Ltd. We are registered in England and Wales under company number 13668841 and have our registered office at The Octagon, Suite E2, 2nd Floor, Colchester, Essex, United Kingdom, CO1 1TG.

3. **PERSONAL INFORMATION WE COLLECT**

Personal information which we collect may include the following:

- 3.1. **Account information.** If you register for and use VERSA we may collect personal information about you and your company relating to that registration such as your name*, your email* and other contact details* (including your mobile number), company details* (including company name, various registration numbers, website

address, contact details, address details and VAT number), VERSA usage history and correspondence with us about VERSA.

We need certain information to carry out our contract with you (or your firm) and you must provide this in order to enter into a contract with us (or as required under that contract), if you do not, we may not be able to carry out our contract with you. Mandatory information fields are marked above and on our registration form with an * asterisk.

- 3.2. **User authentication information.** We will collect personal data from you when you apply to be onboarded to VERSA and undertake our onboarding process. This process (together with the ID Verification process, see below) are to enable us to issue you with, and for you to create secure login credentials. Onboarding requires us to compare the personal data submitted by you in your onboarding application with information known to various third parties (e.g. your website to check and compare company and other information, the Law Society/CILEX/CLC and the like).
- 3.3. **User ID verification.** When you apply to be onboarded to VERSA, we also require that you undertake an ID verification process and a KYB (Know-your-business) check with our chosen third-party provider. We currently use Thirdfort Limited. Any personal data that you provide to such provider is done so in accordance with their Privacy Policy (please see Thirdfort's Privacy Policy at <https://www.thirdfort.com/privacy/> which describes their collection and use of your personal data and that of their service providers). We do not process any of this data directly but we will have access to reports from the provider which summarise the outcomes of your ID verification and/or KYB check and which contain the following data:
- 3.3.1. The **ID verification report** contains the following personal information: your name, date of birth, address, country of birth, phone number and an image of your passport. Note that Thirdfort also provide us with certain continuous background checks on you, for a period of 24 months from date of verification, and notify us of any material changes to the ID verification checks that Thirdfort carried out; and
- 3.3.2. The **KYB report** contains the following information relating to you and / or your company: company name, company registration number, address details, persons of significant control (names), ultimate beneficial owner/s (names), officers (including names, date of birth, address), ownership structure (including individual/entity name and address, country, shareholding), PEPs & sanctions screening and adverse media screening.
- 3.3.3. We access the above reports via our third-party provider and we may store these reports ourselves (for the duration of our contract period with you and for 12 months thereafter).
- 3.4. **Issue and creation of login credentials.** We use the information from the onboarding and ID verification and KYB processes to verify and confirm your identity before you are issued with and can create your user credentials. This helps us to prevent identity theft, keep data secure and to maintain the overall integrity of VERSA and its community of users.
- 3.5. **Payment information.** When you apply to be onboarded to VERSA, we also require that you register with our chosen third-party payment's provider. We currently use GoCardLess Limited. Any personal data that you provide to such provider will be handled by them as a data controller in accordance with their Privacy Policy

(please see GoCardLess's Privacy information at <https://gocardless.com/privacy/>). We do not process any of this data directly. However, we may gather information and reports back from this provider relating to payments due or paid to us and that those reports may include personal information relating to you.

- 3.6. **Professional information.** If you work for one of our customers, suppliers or business partners, the information we collect about you may include your contact information, details of your employment, your professional qualifications/registrations and our relationship with you. This information may be collected directly from you, or provided by your organisation. We use this as necessary for our legitimate interests in managing our relationship with your organisation. If we have a business relationship with you or your organisation, we may receive information about you from your organisation.
- 3.7. **Voluntary surveys and conference feedback.** We may contact you to obtain feedback or to participate in a business or individual customer survey. We do so to obtain important information that helps us to improve our product and service offerings to you. Any personal data and responses submitted are kept private and confidential. Participation in these surveys is voluntary. You decide (i) whether you wish to participate, and (ii) the nature of the information you choose to disclose. Survey information is used for statistical purposes and to improve our product and service offerings to you.
- 3.8. **Other correspondence or interaction** (for example by email, telephone, post, SMS, live chat, video calls, online forums, polls or via VERSA) between you and us, will include personal information (such as names and contact details) in that correspondence. This may include case related information, enquiries, reviews, follow-up comments or complaints lodged by or against you and disputes with you or your firm.
- 3.9. **Technical usage information.** We may collect information about your use of VERSA via technical means such as webpage counters and other analytics and reporting tools. This may include your IP address, login data, 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 VERSA as well as the date and time of your access and what you interact with on VERSA. We use this as necessary for our legitimate interests in administering and improving VERSA and our services, to ensure VERSA operates effectively and securely, to develop our business and inform our product, client and marketing strategies, and for other administrative purposes. We may also create aggregate statistical data from that information (for instance, overall numbers of use) which is not personal information about you.

We only use the following cookies which are strictly necessary for the provision of VERSA:

<p>Session cookies – Name/code available on written request.</p>	<p>These cookies provide security that is essential to comply with data protection security requirements as an online service provider.</p>
<p>Load-balancing cookies - ARRAffinity</p>	<p>These cookies ensure the content of any VERSA webpage loads quickly and effectively by distributing the workload.</p>

- 3.10. **LinkedIn or other social media.** If we engage with you on LinkedIn or other social media, we may use information you share with us (including your social media handle or profile) or which is available from your account to inform our correspondence and engagements with you.

3.11. Call information. We may also collect details of your user information (for live chat or video calls) or your phone numbers used to call our organisation and the date, time and duration of any such interactions or calls. We may also keep a log of the issues discussed on these interactions or calls. Please note that if we record your video calls or phone calls to or from us, we will inform you of this via the system informing you of this.

We will keep and use the information described above:

- to carry out our contract with you or your organisation (if applicable),
- to comply with any legal requirements for us to maintain certain records or carry out certain verifications and money laundering checks,
- to respond to your enquiries and send you quotes for our services;
- to verify your identity and provide you with our services;
- to invite you to attend events we hold and send you updates on the latest developments regarding our products and services; and
- for our legitimate interests in preventing fraud, dealing with a complaint or enquiry and administering your (or your organisation's) VERSA account and any services we offer, as well as to support you, review and improve our offerings, including troubleshooting, data analysis, testing, research, statistical and survey purposes.

Where personal information relates to your VERSA account or other correspondence or interaction between you and us, it is kept for a period of up to six years after the date on which your account is closed.

Where personal information is collected by us it is retained for a period of up to six years after the date of payment or our payment processing provider in accordance with their data policies.

If your information is on social media, including LinkedIn, it will be retained in accordance with the relevant social media platform's policies.

Any other information set out above such as initial enquiries or correspondence which does not relate to a VERSA account is typically kept for up to 2 years.

4. INFORMATION WE RECEIVE FROM THIRD PARTIES

In addition to the information collected by us as set out above, we may also receive information about you from the following sources:

- 4.1. **Our service providers.** We work closely with third parties (including, for example, business partners, sub-contractors in IT, technical, payment and delivery services, advertising networks, analytics providers, search information providers and credit reference agencies) who may provide us with information about you, to be used as set out in this privacy policy.
- 4.2. **Businesses we have bought.** If we have acquired another business, or substantially all of its assets, which originally held your information, we will hold and use the information you provided to them, or which they otherwise held about you, in accordance with this privacy policy. If we are reviewing whether to acquire a business, or substantially all of its assets, which holds your personal data (whether you are a customer or employee of that business or otherwise) we may receive limited personal data about you from that business or

professional advisors involved in the transaction, as necessary for our legitimate interests in making decisions about that acquisition. If we do not acquire that business, any information we receive about you will be deleted as soon as practicable following the decision not to acquire.

4.3. **Publicly available sources.** If relevant as part of our relationship with you, we may obtain information from publicly available sources such as Companies House.

5. **MARKETING**

We may collect your name and contact details (such as your email address, phone number or address) for our legitimate interests in marketing to you (by various channels) and maintaining a list of potential customers and in order to send you information about our products and services which you might be interested in.

You always have the right to "opt out" of receiving our marketing. You can exercise the right at any time by contacting us. If we send you any marketing emails, we will always provide an unsubscribe option to allow you to opt out of any further marketing emails. If you "opt-out" of our marketing materials you will be added to our suppression list to ensure we do not accidentally send you further marketing. We may still need to contact you for administrative or operational purposes, but we will make sure that those communications do not include direct marketing.

We never share your name or contact details with third parties (except for our group companies) for marketing purposes other than as part of a sale, merger, amalgamation or other transfer of our business. We may use third party service providers to send out our marketing, but we will only allow them to use that information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We may retain your details on our marketing list until you "opt-out" at which point we add you to our suppression list. We keep that suppression list indefinitely to comply with our legal obligations to ensure we do not accidentally send you any more marketing.

6. **THIRD PARTY WEBSITES, SERVICES AND APPLICATIONS**

VERSA contain links and interfaces to third party websites, products, services and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third parties and are not responsible for their privacy statements. When you leave VERSA, we encourage you to read the privacy policies relating to any third-party websites, services and applications you access.

7. **JOB APPLICATIONS**

We will collect and hold information on job applicants (including applications for work experience or internships), including information you provide to us in your application and/or curriculum vitae, or provided to us by recruitment agencies, as well as information on you from any referees you provide. We may also collect information about your professional history which you make available on LinkedIn, or which are on your organisation's website or other organisation's websites that you have been employed by or engaged with or which may regulate your profession.



We use this as necessary to enter into an employment contract with you, and for our legitimate interests in evaluating candidates and recording our recruitment activities, and as necessary to exercise and perform our employment law obligations and rights. Where you voluntarily provide us with special categories of data, such as information about your race, health or sexuality, we will store this as part of your application on the basis that you have decided to make it public to us for this purpose, and to ensure that our record of your application is accurate so we can comply with (and demonstrate our compliance with) our obligations under employment law.

We may operate an equal opportunities monitoring process as part of some of our application rounds, in which you may provide details of your gender, age, marital status, health, ethnicity, and other relevant details as set out on our monitoring form. If applicable, we use these forms and the information you provide as necessary for our legitimate interests in monitoring aggregate recruitment statistics and complying with our legal obligations regarding equal opportunities. The forms do not contain any information which allows us to directly identify you, and are detached from your application, stored separately, and only used to create aggregate statistics. Providing information in these forms is entirely voluntary, and the information you provide in those forms (or your decision not to provide any information) will not affect the handling of your application in any way. The individual forms are stored for 12 months and the aggregate statistical data (which you cannot be identified from) is stored indefinitely.

If you are successful in your application, your information will be used and kept in accordance with our internal privacy policy. If you currently work for us, or used to work for us, you can request a copy of this from us. If you are not successful in your application, your information will be held for up to twenty-four months after the relevant round of recruitment has finished.

8. LEGAL CLAIMS

Where we consider there to be a risk that we may need to defend or bring legal claims, we may retain your personal information as necessary for our legitimate interests in ensuring that we can properly bring or defend legal claims. We may also need to share this information with our insurers or internal and external legal advisers. How long we keep this information for will depend on the nature of the claim and how long we consider there to be a risk that we will need to defend or bring a claim.

9. OTHER USES OF YOUR INFORMATION

We will only use your personal information when the law allows us to do so. Although in limited circumstances we may use your information because you have specifically consented to it, we generally use your information in the ways set out in this policy because:

- 9.1. we need to perform a contract we have entered into;
- 9.2. we need to comply with a legal obligation;
- 9.3. it is necessary for our legitimate interests (or those of a third party) and your interests and rights do not override those interests; or

- 9.4. we need to protect your interests (or someone else's interests) or where it is needed in the public interest (although these circumstances are likely to be rare).

We will only use your personal information for the purposes for which we collected it as set out in this policy, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

10. SHARING YOUR INFORMATION

We may need to share your information with users of VERSA and other third parties, including third-party service providers and other entities in our group. Examples of where we may share your personal information with third parties include:

- 10.1. if we are under a duty to disclose or share your personal information in order to comply with any legal obligation, or in order to enforce or apply our agreements with you, or to protect the rights, property, or safety of us, our customers, or others or where we have another legitimate interest in doing so. This may include exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction;
- 10.2. where we use third-party service providers (including contractors and designated agents) and they need the personal information so that they can carry out their services. Third-party service providers may include those providing us with legal advice, ID verification, contract administration services, hosting and other IT services and payment processing;
- 10.3. where we share personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, and for system maintenance support and hosting of data;
- 10.4. in the event of a possible sale or restructuring of our business, we may share your personal information with third parties, for example with potential buyers and professional advisers where necessary in connection with the purposes which your information was collected for; and
- 10.5. where we need to share your personal information with a regulator or to otherwise comply with the law.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information. Where third parties process your personal information on our behalf as "data processors" they must do so only on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have attached our current "**List of data processors and data sub-processors**" as **Schedule 1**.

11. STORAGE OF YOUR INFORMATION

Our office headquarters are based in London and our main data centres are located in London and Cardiff. However, where required to perform our contract with you (or your organisation) or for our wider business purposes, the information

that we hold about you may be transferred to, and stored at, a destination outside the UK and the EU. It may also be processed by staff operating outside the UK and EU who work for us or for one of our service providers.

We will take all steps reasonably necessary to ensure that your personal information is treated securely and in accordance with this privacy policy.

Some countries or organisations outside of the UK and the EU which we may transfer your information to, will have an "adequacy decision" in place, meaning the EU or UK data protection authorities consider them to have an adequate data protection regime in place.

If we transfer data to countries or organisations outside of the UK and the EU which the EU or UK data protection authorities do not consider to have an adequate data protection regime in place, we will ensure that appropriate safeguards (typically we use model clauses approved by the EU or UK data protection authorities) are put in place where required. To obtain more details of these safeguards, please contact us.

12. DATA SECURITY

We select industry leading hosting providers which hold ISO 27001 accreditations to host VERSA. Our current hosting provider is Microsoft Azure (with information on their ISO 27001 accreditation available at <https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27001>).

As well as the measures set out above in relation to sharing of your information, we have put in place appropriate internal security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where necessary.

13. INFORMATION RETENTION

We have set out above indications of how long we generally keep your information. In some circumstances, it may be necessary to keep your information for longer than that in order to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

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 requirements. We have an internal policy which informs our retention periods for various record categories.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

14. YOUR RIGHTS

Data protection law gives you a number of rights when it comes to personal information we hold about you. The key rights are set out below. More information about your rights can be obtained from the Information Commissioner's Office (ICO). Under certain circumstances, by law you have the right to:

- 14.1. **Be informed** in a clear, transparent and easily understandable way about how we use your personal information and about your rights. This is why we are providing you with the information in this policy. If you require any further information about how we use your personal information, please let us know.
- 14.2. **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- 14.3. **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- 14.4. **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it (for instance, we may need to continue using your personal data to comply with our legal obligations). You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- 14.5. **Object to processing** of your personal information 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 us using your information on this basis and we do not have a compelling legitimate basis for doing so which overrides your rights, interests and freedoms (for instance, we may need it to defend a legal claim). You also have the right to object where we are processing your personal information for direct marketing purposes.
- 14.6. **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- 14.7. **Request the transfer** of your personal information to another party where you provided it to us and we are using it based on your consent, or to carry out a contract with you, and we process it using automated means.
- 14.8. **Withdraw consent**. In the limited circumstances where we are relying on your consent (as opposed to the other bases set out above) to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another compelling legitimate interest in doing so.
- 14.9. **Lodge a complaint**. If you think that we are using your information in a way which breaches data protection law, you have the right to lodge a complaint with your national data protection supervisory authority (if you are in the UK, this will be the ICO).



If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal information, withdraw your consent to the processing of your personal information or request that we transfer a copy of your personal information to another party, please contact us.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us understand the nature of your request, to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is an appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it. If we request any identification from you for this purpose, it is on the basis that it is necessary to comply with our legal obligations, and we will only keep and use this until your identity has been verified.

Please consider your request responsibly before submitting it. We will acknowledge your request and will then respond to your request as soon as we can. Generally, this response will be within one month from when we receive your request but, if the request is going to take longer to deal with, we will let you know.

15. CHANGES TO THIS PRIVACY POLICY

Any changes we make to this privacy policy in the future will be posted on this page and flagged via the VERSA Customer Portal for VERSA clients and users.

Such changes will also be summarised in the “**Changes Log**” attached as **Schedule 2**.

Schedule 1 - List of data processors and data sub-processors

			Type of data and whether e4 is the Controller and uses a Processor ('P') OR whether e4 is the Processor and uses a Sub-processor ('SP')			
Name	Services provided	Purpose of data processing	Customer Data	Consumer Data	Country (location of control)	Transfer mechanism
Assimilated Information Systems	Document generation	For web application access to their services, and VERSA Document Management	SP	SP	South Africa	UK Standard Contractual Clauses in the Agreement / Data Processing Addendum
Direct contractors - Mid or Back office	Mid-office & back-office services provided by individuals to e4 (on a full-time or part-time)	To enable them to provide mid-office & back-office services to e4	P	SP	United Kingdom / South Africa	UK Standard Contractual Clauses in the Agreement / Data Processing Addendum
Direct contractors - Production	Production services provided by individuals to e4 (on a full-time or part-time)	To enable them to provide production services to e4	P		South Africa / Mauritius	UK Standard Contractual Clauses in the Agreement / Data Processing Addendum
e4 Strategic (Ltd) Pty	Accounting, HR, Legal, IT/Technical Service	To provide accounting, HR, legal, IT/technical service	P		South Africa	UK Standard Contractual Clauses in the Agreement / Data Processing Addendum
Freshworks Inc	Customer service desk, Business Communications, Customer account management	To provide customer service desk, business communications, and customer account management	P		United States	Opted in to US/UK Data Privacy Framework.
GoCardless	Customer payments	For web application access to their services, and Customer payments	P		United Kingdom	n/a
GoTo Group Inc.	Online customer webinar training services	For web application access to their services, and Online customer webinar training services	P		United States	Opted in to US/UK Data Privacy Framework.
LB Group Limited	Accounting, Company secretarial	To enable them to provide accounting, company secretarial	P		United Kingdom	n/a

Microsoft Limited	Cloud services (Azure), website hosting, and data centre services	For web application access to their services, and Cloud services (Azure), website hosting, and data centre services	P	SP	United States / United Kingdom / Ireland	Opted in to US/UK Data Privacy Framework.
Thirdfort	ID verification, anti-money laundering and Source of Funds checks	To perform ID verification and anti-money laundering checks on our potential customers (and their customers/clients)	P		United Kingdom	n/a
Xero Limited	Online accounting system & services	To enable them to provide online accounting system & services	P		United Kingdom	n/a

Definitions:

1. Customer Data

Customer data refers to personal information collected from individuals and/or corporates in their role as customers or clients of e4/the company.

2. Consumer Data

Consumer data refers to personal information about individuals and/or corporates who are customers or clients of an e4 customer and is normally processed as a result of a property case transaction.

Schedule 2 - Changes log

Change #	Version	Date	Changes
0	v09-09-2024	9 September 2024	Not applicable. First version of e4Uk Privacy Policy.
1	V16-10-2024	16 October 2024	<ol style="list-style-type: none">1. Fixed error in date in footer on page 1, from 2022 to 2024.2. Updated clause 10, to add reference to our current "List of data processors and data sub-processors" being attached as Schedule 1.3. Updated clause 15, to add reference to the "Changes Log", attached as Schedule 2.4. Added Schedules 1 and 2.5. Minor formatting changes.