

Contextul Holdings Limited Privacy Policy

Throughout this policy Contextul, we and us, will refer to Contextul Holdings Limited and the services they provide via the website www.contextul.io including any subdomains that we may be employed to provide access to the products and services.

This document was last updated and approved by the Contextul Holdings Limited governance board on **June 28th 2024**.

1. Our Contact Details

Contact: The Data Protection Officer

E-mail: DataProtectionOfficer@contextul.io

Postal Address:

Data Protection Officer,
Contextual Holdings Limited,
The Old Workshop,
1 Ecclesall Road South,
Sheffield
S11 9PA
United Kingdom

Website: www.contextul.io

2. The Types of Personal Information we Collect

Due to the nature of this service, the Contextul DSAR processing services collect both personal information (this is information that can identify an individual, such as names, email addresses, and telephone numbers) and other types of data that you may provide to us in the documents that you ask us to process. This does not include any documents that are processed by PrivacyManager™, the documents processed by PrivacyManager™ are not shared with Contextul or any other third party.

We collect and process the following information:

Scenario	Type of data	The primary purpose and legal bases for processing
Customer information	We collect and process the names and contact information of all our customers.	We use this information as part of our contractual obligation to provide the services, provide support, and perform administrative tasks such as billing.
Payment information	<p>For our customers outside of any trial period, we will also collect payment information for use with our chosen payment provider.</p> <p>For clarity, Contextul does not collect or process credit or card information directly.</p>	We use this information as part of our contractual obligation to provide the services, provide support, and perform administrative tasks such as billing.
Website visitors	We collect information about visitors to our website.	We have a legitimate interest in understanding the number of visitors to our website. This includes monitoring for fraudulent access and potential cyberattacks.

Cookies and first-party tracking

We may use pixels, beacons, cookies, and clear GIFs. “Cookies” are small pieces of information that a website sends to a computer’s hard drive while a website is viewed.

We have a legitimate interest in making our website operate efficiently.

Feedback and support

We collect Personal Information from you contained in any support request that you submit to us.

We have a legitimate interest in receiving and acting upon, your feedback, issues, or inquiries.

When you communicate with us over the phone or a video-call platform, your calls may be recorded and sent to you as a support measure.

We may also analyse and/or use these calls for training, quality control, and sales and marketing purposes.

During such calls, we will notify you ahead of any recording starting if the call is to be recorded.

Mailing list

When you sign up for our mailing list, we will collect your email address and other information, such as your name.

We share information about our products and services with individuals who consent to receive such information.

Our mailing list is constructed based on consent by opting in, and you can opt-out at any time using the link in any of our mailing list communications, which is the unsubscribe button.

Web analytics

We use technology to monitor how you interact with our website. This may include which links you click on or information that you type into our online forms, as well as information about your device or browser.

We have a legitimate interest in understanding how you interact with our website to better improve it, and to understand your preferences and interests to select offerings that you might find most useful.

We also have a legitimate interest in detecting and preventing fraud.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing this information varies by scenario as detailed in the table above, but include the following:

- Your consent. You can remove your consent at any time. You can do this as described in the table above or by contacting us, using the information provided at the top of this policy document.
- We have a contractual obligation.
- We have a legitimate interest.

Sensitive Personal Data

The UK GDPR defines Sensitive Personal Information as a special category of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation.

Contextul does not knowingly collect any such data.

Children's Personal Data

As a company providing business services, Contextul does not knowingly collect any data relating to children.

3. How we get Personal Information and why we Have It

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- To identify you when using our products and services
- To create your account and provide access to our products and services
- To provide our services to you
- To improve our services to you
- To manage the security and smooth running of our products and services
- To provide support and answer questions or feedback provided to us
- To keep you updated with enhancements to existing or the release of new products and services
- To collect payment for the products and services that we provide
- To comply with our legal obligations in being a trust service provider
- To defend or exercise our rights in legal claims

In this and the previous sections, we describe the primary purposes for collecting your information. However, the same data may be collected and processed for several reasons.

4. Sharing of Personal Information

In addition to situations described elsewhere in this policy, we may share personal information in the following situations:

- Service Providers
 - We share your information with service providers. These providers may, among other things, provide hosting and cloud services, help us administer our website, send e-mail communications, provide technical support, detect fraud, process payments, and assist in the fulfilment of orders.
 - Our service providers will only be given access to your personal information if required and where it is required, and where required, they will only be provided with the minimum information required to provide the services that they are contracted to provide.
 - Our service providers are contractually obligated to use your personal information only at our direction and in accordance with our Privacy

Notice, to handle your personal information in confidence, and to not disclose your personal information to unauthorised third parties. Service providers who violate these obligations are subject to appropriate discipline including, but not limited to, termination as a service provider.

- Posting of Comments
 - Some parts of our website may allow users to post comments or reviews in a public forum. If you decide to submit information on these pages, that information may be publicly available.
- Other Disclosures with Your Consent
 - We may occasionally ask if you would like us to share your information with other unaffiliated third parties who are not described elsewhere in this policy.

5. Data Security and Retention

Your information (personal and otherwise) is securely stored both at rest (in the databases and other means of storage used by us to provide the products and services) and in transit using industry-recognised data encryption and protection technology and processes.

We keep all information (personal and otherwise) for only as long as necessary to provide the products and services you have requested.

When we dispose of your information, we do so in accordance with our data retention policy. Our disposal process is designed to securely dispose of your information, putting it beyond use and recovery.

6. Your Data Protection Rights

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us using the contact information at the beginning of this policy if you wish to make a request.

7. How to Complain

If you have any concerns about our use of your personal information, you can make a complaint to us using the contact information at the beginning of this policy.

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>

8. International Data Privacy

Contextul offers its services to companies all over the world and is proud to comply with data protection regulations where required or requested.

9. CCPA – The California Consumer Protection Act

This section applies only to California residents. Under California Civil Code Sections 1798.83-1798.84, California residents, including Contextul employees and contractors who reside in California, who are entitled to receive: (a) information identifying any third-party companies to whom Contextul may have disclosed Personal Information to for direct marketing, within the past year; and (b) a description of the categories of Personal Information disclosed.

Categories of Personal Information

Category	Description
Identifiers	Contextul collects and processes the following personal information. First name, last name, online identifier, internet protocol address, email address, and/or similar identifiers.
Sensitive Personal Information	Payment information, geolocation, account login.
Commercial information	Records of services purchased.
Sensory information	Records of services purchased.
Internet or similar network activity	Internet protocol address and information on a consumer's interaction with our website.
Geolocation data	An approximate physical location was obtained from the internet protocol address.

The Right Granted by CCPA

Right against Discrimination - You have the right not to be discriminated against for exercising any of the rights described in this section. We will not discriminate against you for exercising your rights.

Right to Access – See right to access in section 6.

Right to Delete – See right to erasure in section 6.

Right to Correct – See right to rectification in section 6.

Right to Opt-Out of Sale or Sharing of Your Personal Information - You have the right to opt out of having your Personal Information, including Sensitive Personal Information, sold or shared.

Context does not sell Personal Information or Sensitive Personal Information for monetary or other valuable consideration. We will only share your personal information as detailed in this policy.

If you wish to opt out of sharing your Personal Information, opt out of any sharing which you have consented to by following the instructions in section 2 or by contacting us using the contact information in section 1.

Right to Limit the Use and Disclosure of Sensitive Personal Information – You have the right to ask Contextul to limit our use of your Sensitive Personal Information to that information which is expected by an average individual as necessary to perform our Services by following the instructions in section 2 or by contacting us using the contact information in section 1.

10. VCDPA – The Virginia Consumer Data Protection Act

This section applies only to Virginia residents. If you are a Virginia resident, the Virginia Consumer Data Protection Act – Va. Code Ann. §§ 59.1-575 to 59.1-584 (“VCDPA”) provides you with specific rights regarding your personal data, subject to certain exceptions. We collect personal data and sensitive data, as defined by the VCDPA and process it as described in this policy.

The VCDPA defines “Personal Data” as any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal Data does not include de-identified data or publicly available information. Personal Data that is excluded from the scope of the VCDPA includes:

1. covered entities or business associates covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related federal laws and regulations, clinical trial data, or other qualifying research data;
2. personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA) or the Farm Credit Act, and the Driver’s Privacy Protection Act of 1994;
3. information collected from governmental organisations, non-profit organisations and higher education institutions; and
4. data processed or maintained for employment purposes including emergency contact information or benefits administration.

If you do not provide the information that we ask for, we may not be able to provide you with the requested services. Sensitive data is a category of Personal Data that requires greater security protections and standards of care in handling. “Sensitive Data” is defined by the VCDPA as (1) Personal Data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (2) the processing of genetic or biometric data for the purpose of uniquely identifying a natural person; (3) the personal data collected from a known child; or (4) precise geolocation data.

Contextul does not knowingly collect any Sensitive Data as defined by the VCDPA.

The Rights Granted by VCDPA

If you are a Virginia resident, the VCDPA provides you with specific rights regarding your Personal Data, subject to certain exceptions. These rights are explained below:

Right Against Retaliation or Discrimination - You have the right not to be retaliated or discriminated against for exercising any of the rights described in this section. We will not discriminate against you for exercising your rights.

Right to Access – See right to access in section 6.

Right to Delete – See right to erasure in section 6.

Right to Correct – See right to rectification in section 6.

Right to Opt-Out of Sale or Use of Your Personal Data for Targeted Advertisement – You have the right to opt out of having your Personal Information, including Sensitive Personal Information, sold and/ or used for targeted advertising.

Contextul does not sell Personal Information or Sensitive Personal Information for monetary or other valuable consideration. We will only share your personal information as detailed in this policy.

If you wish to opt out of sharing your Personal Information, opt out of any sharing which you have consented to by following the instructions in section 2 or by contacting us using the contact information in section 1.

Right to Data Portability – See your right to data portability in section 6.