VikingCloud Privacy Notice

October 2024

This Privacy Notice describes how we collect, store, use, and share your personal information and explains your rights in relation to the personal information we hold about you. In this Privacy Notice, references to "you" and "your" are references to a user of **www.securetrust.com** that completes billing details, purchases SecureTrust PCI Manager (Cloud Compliance Direct) and / or purchases digital certificates services from us directly via such website. If you buy services from us via any other means, please read the VikingCloud Privacy Notice here **Privacy Policy | VikingCloud**.

If your payment processor (e.g. your bank) has contracted with us to provide you with Payment Card Industry Data Security Standard (**PCI DSS**) compliance services (rather than you contracting with us directly), the use of your information is determined by your payment processor. Please contact them for more information.

Some of the information listed in this notice will not be personal information, as it will apply to your organization. However, where you are a sole trader or a non-limited liability partnership, your business information could be classed as personal under the data protection / privacy laws in your location. Therefore, to ensure we are transparent, we have included our use of organization-level information in this notice.

As of the 31st January 2020, the United Kingdom (**UK**) is no longer part of the European Union. However, the UK government translated the majority of the EU General Data Protection Regulation into UK law. Therefore, all material requirements remain the same and all references to the General Data Protection Regulation (GDPR) in this Privacy Notice relate to both the UK and EU. Unless explicitly stated within this notice, references to the General Data Protection Regulation with relate to both the EU and the United Kingdom (UK).

If you are based in Mexico, the Ley Federal de Protección de Datos Personales en Posesión de los Particulares does not apply to people acting in a professional capacity. We are also not directly in scope for the Californian Consumer Privacy Act (**CCPA**). However, the collection and use of your information will remain the same so you can still review this Privacy Notice if you would like to know more.

Who we are.

When we say ‘we’ or ‘us’ in this Privacy Notice, we are referring to the legal entity applicable to your location as listed in the Subscriber Agreement, who we will refer to as VikingCloud in this document.

Where do we get your information from?

We collect information from you when you:

- Complete the form as part of the ‘Buy Now’ journey on our website.
- Enter bespoke contractual arrangements with us to receive digital certificates.
- Use the portal to complete your self-assessment services.
- Use our compliance tools which you install on your device(s).
- Contact us by phone, email, text message, physical mail as well as via our online chat service or social media (LinkedIn, Twitter, Facebook, or Instagram).
- Visit our website (we capture some information by way of cookies where you have consented to this).
- If you buy one of our identity-based digital certificates, we will also collect information from government records and / or from data and credit brokers to verify who you and/or your organisation are. A list of some of our sources be found here: **https://certs.securetrust.com/CA/registry-list.php**

What kinds of information do we collect about you?

- When you create an account:
    - Personal – your name, address, and country (and region, e.g. EU vs. US). Note region is only applicable once our mobile application is available to our direct clients.
    - Employment – your employer / company name.
    - Work contact details – your work email address and phone number.
    - Website server logs – we automatically collect server logs which contain your IP address and your approximate location (town / city level).
- Cookie information – see our Cookie Policy here for more information.
- Payment information – card number, expiry date, and security code. If you pay by check or bank transfer, we will receive your bank details.

- When you use the services:

    - The information you complete in your self-assessment questionnaire (designed to guide you through your compliance validation with the PCI DSS).
    - The IP addresses and / or domain names you ask us to scan or provide you a digital certificate and the results of the scans (i.e., any vulnerabilities identified).
    - Information relating to the device(s) you have installed our compliance tools on, along with the local area network the device(s) is connected to, the external IP address of this network, configuration details for the device(s), and results of scans for cardholder data.
    - Any document you may choose to upload, such as previously completed compliance questionnaires, vulnerabilities scans, attestations of compliance and / or identity documents.
    - Your feedback on our products and services.

- Application logs; records of when you use, attempt to use your access credentials, changes to your compliance status, your responses to the self-assessment questions, responses to the validation requirements and any alerts relating to errors identified (for example if you're unable to update a field).

How do we use your personal information, and what are our legal grounds?

Worldwide, several data protection and privacy laws require organizations to process personal information only where we have a 'lawful basis' (the legal justification for the processing of personal data, as outlined in your local law). This section will explain the legal basis/es applicable in your country.

Please read the 'Use of Your Information' column below regardless of your location. Please note the following:

- Australia – a legal basis is not required (as we do not process sensitive information).
- Brazil – refer to the table below, as the same reasons used in the EU also apply under your local law (Lei Geral de Proteção de Dados Pessoais, often referred to as "LGPD").
- Canada – consent is required.
- India – consent is required.
- South Africa – refer to the table below, as the same requirements under the GDPR also apply under your local law (the Protection of Personal Information Act or "POPIA").

Legal requirements and obligations for obtaining and managing consent

Under data protection and privacy laws, organizations must meet specific requirements to receive and manage consent, which varies in different jurisdictions.

Where we process your personal information based on consent under the GDPR (or similar laws such as the LGPD or the POPIA), the requirements for consent under the GDPR and similar laws mean consent can only be used in specific circumstances, i.e., where people have free choice, and their information can be deleted at any time.

Where we are using non-GDPR standard consent, such as within Canada and India, we imply your consent by way of you providing us with your personal information and we make sure you are informed by providing you with this Privacy Notice. However, please note that if you withdraw your consent then we may not delete your information if we have a good reason for keeping it.

Below you can see more detail on legal bases under the GDPR (broadly aligned to LGPD and POPIA).

Use of Your Information

Reason for using your personal information	Legal ground
Website Monitoring If you provide your consent via our cookie tool, we will set and access cookies when you visit our website. See our Cookie Notice for more information. **Sales & Marketing** Where you have provided your consent, most often in regions where this is required, we will send marketing messages relating to our products and services, including webinar invitations and white papers. **Call Recordings** We record calls for the purposes of customer support.	**Consent** Under applicable laws which apply to the use of cookie technologies, we can only use non-essential cookies (such as analytics cookies) if we receive your consent. We may need your consent to send marketing in some EU countries. You have the right to withdraw consent at any time. Depending on your region, we may require your consent to record calls.
Servicing To use the services, you do need to give us your name, contact information and work details to allow us to set up an account for you. **SecureTrust PCI Manager (Cloud Compliance Direct)** We use the information you enter into your self-assessment questionnaire to help guide you through the PCI DSS compliance process and enable you to report on and self-attest your compliance with the PCI DSS. We also need your IP address(es) to conduct vulnerability scans and device information to check if your device is compliant with the PCI DSS. These tools generate information as listed in the 'What kinds of information do we collect about you?' section above.	**Necessary for a contract** This relates to the necessary use of your information to allow us to deliver the services you have purchased from us.

We will use your contact details to send you essential notices; reminders that your subscription is due to expire, informing you of any changes to our products / services and applicable changes to PCI DSS itself.

Application logs are automatically reviewed to produce alerts for manual review, with alerts being generated if there are indications of errors or problems with the system. These logs are also used to provide you with an audit trail of changes which you can review within the portal.

SSL / Digital Certificates

Website certificates:

- When issuing a certificate, we use the requested domain name to validate you have control of that domain.
- If you procure one of our more identity-based certificates, we conduct additional checks on your organization to ensure it exists and the location matches publicly available records as well as ensuring you are authorized to obtain a certificate on behalf of your company.
- For our most rigorous certificates, we also check tax and company registration information.

Code-signing certificates:

- When issuing a certificate, we conduct checks on your organization to ensure it exists and the location matches publicly available records, ensure you are authorized to obtain a certificate on behalf of your company and your private key is generated and protected in a Hardware Crypto Module.

Secure email and MyIdentity certificates: • We use the email address provided to send the certificate. • For MyIdentity certificates you can also provide your title and name, but this is optional. **Finance** We will use account and payment information if we invoice you directly or if there is a dispute about a payment.	
Legal Duties We may disclose or share your personal information to comply with a legal obligation such as a court order. Where we do so we'll only provide the minimum information needed to comply.	**Necessary for compliance with a legal obligation** Your personal information may be processed to meet any legal obligations VikingCloud is subject to.
Protecting Life We may disclose your information to the police or other authorities if we have serious concerns about you or another's wellbeing.	**Necessary to protect vital interests** This will usually only apply to protect someone's life.

Necessary for legitimate interests

We also use your information when we have a 'legitimate interest' as long as this does not unfairly impact you or your privacy rights. Each activity is assessed, and your rights and freedoms are considered to make sure that we are not being intrusive or doing anything beyond your reasonable expectations.

We will assess the information we need, so we only use the minimum. If you want further information about processing under legitimate interests, you can contact us using the details in the Contact section of this Privacy Notice.
You also have the right to object to any use of your information where we use 'legitimate interests' as a lawful basis. We will re-assess our interests and yours, considering your particular circumstances. If we have a very strong reason for the use of your information, we may continue to use your information.
We use 'legitimate interests' in the following circumstances:

Reason for using your personal information	Legitimate interest(s)
Sales & Marketing Where your location does not require your opt-in consent, we will send marketing messages relating to our products and services, including webinar invitations and white papers. We may also use your feedback in our marketing materials - we will take steps to make sure you are not identifiable from any feedback we publish.	We need to promote our products and services to run a successful business.
Analysis and management reporting We analyze and report on our sales & marketing activities and our cashflow, as well as our service levels / how often our tools are used. We do this to produce aggregated reports - i.e., facts and figures, which no longer contain personal information. We analyze: • The success of our marketing campaigns to verify how many people respond to the campaign, how many led to discussions and how many resulted in sales. • The use of our products and services – how often the self-assessment portal is used, how often our scanning and endpoint tools are used, how many calls we received / dates and times of such calls, feedback on parts of our services that are difficult to use / could be improved. • The types and frequency of the vulnerabilities and malware we identify when providing you with the services, so we can help you avoid threats.	We need to analyze and assess our performance to ensure we provide a good service and to optimize our resources.

• The nature of the organizations we provide services to – the industry and size of such organizations as well as the number and types of devices. • How long invoices take to be paid, to help us manage our cashflow.	
Security Application logs are captured, automatically processed and alerts reviewed to identify and resolve potential security issues. If you are a digital certificates customer who uses our 'Trusted Commerce Seal' on your website, we also collect the IP address of your website users (their browser will make a call to our servers).	We need to maintain our Information / Cyber Security posture to ensure our information assets are protected.
Call Recordings Where we don't require your consent to record calls, we will still let you know the call will be recorded. You can tell us if you are not happy with this, and we will provide alternative options.	We need to retain and analyze calls with our clients to ensure we are providing a good level of customer service and to monitor the performance of our agents.
Certificate Consumers If we receive a notice suspecting a site is undertaking phishing, or that an application signed with one of our certificates is malware, after confirmation we will share information about the certificate, namely information as to the organization or the domain.	We need to maintain our Information / Cyber Security posture to ensure our information assets are protected.

Online Tracking

At present, we do **NOT** respond to **Do Not Track** signals your browser sends. But you can use our cookie tool to let us know your preferences.

Who do we share your personal information with?

We share your personal information with other organizations. The organizations we share personal information with are as follows:

- Sales and marketing software providers
- Platform providers
- Website providers and website tool providers
- Security tool / service providers
- Survey providers
- Telephone providers
- Cookie consent tools
- Government Bodies and Regulators
- Professional services providers and consultants, such as our bank, contractors, external auditors, and lawyers
- Certificate Consumers, if we receive a request in relation to threats such as malware / phishing
- As part of an actual or contemplated business sale, merger, consolidation, change in control, transfer of substantial assets or reorganization

We only share personal information where there is a requirement to do so, and where appropriate technical, organizational, and where necessary, contractual measures are in place in order to ensure its protection.

Overseas Transfers

The information that we process about you will be stored in the United States. It may also be stored or accessed by authorized individuals who operate in a variety of countries, or who work for us or for one of our suppliers.

If you are based in the EU or UK, we need to have specific protections in place to transfer your information to another country. We also need to let you know which methods we use.

- Some countries have been assessed by the relevant authorities as being ‘adequate’, which means their legal system offers a level of protection for your information which is equal to the level of protection in your country. **This applies to some of our suppliers, as well as some of the transfers of information within VikingCloud.**
- The EU Commissioner and the UK have also approved Binding Corporate Rules (**BCRs**) as a way to protect information shared within a group of companies. This requires the group to commit to meeting EU / UK standards across all regions. These rules need to be approved by all the EU supervisory authorities (or for the UK, the UK regulator) and require extensive monitoring and oversight. **Some of our suppliers have BCRs.**
- Where the country or mechanism has not been assessed as ‘adequate’, the method we use most frequently is Standard Contractual Clauses (SCCs). These contract terms place EU

standards onto companies in other jurisdictions. The European Commission approved standard contractual clauses are available via the link below, please contact us if you would like more information. **https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en**

- **We have SCCs in place to allow sharing between VikingCloud group entities globally.**
- **We have SCCs in place with some of our service providers - we carry out due diligence checks of their practices and where necessary agree additional controls to ensure that your information is treated securely and in accordance with this privacy policy.**

If you are based in a country outside of the countries above, there may be local obligations we have to meet. See below for details of the additional controls which we will apply to protect your information:

- Australia – contractual commitments to comply with the Privacy Principles under the Privacy Act.
- Brazil – LGPD contains the same requirements as the GDPR in relation to international transfers. However, the Brazilian Authority (ANPD) has yet to issue approved terms. We have extended the EU SCCs to cover your information.
- Canada – clear privacy notices explaining the transfer. We also need to tell you who to contact for more information. Please contact the Global Data Protection Manager using details in the 'Contact' section below.
- India – at present, no restrictions are in place unless sensitive personal information is involved (which does not apply here).
- South Africa – we must ensure a binding agreement is in place which ensures the POPIA principles are upheld including when further transferring personal information.

How long do we keep personal information for?

Your payment information is stored for sixty (60) days.
As an 'Approved Vulnerability Scanning Provider', the PCI Council requires us to keep scans and associated information for a minimum of 3 years.

As a 'Trusted Certification Authority', the Certification Authority /Browser ("CAB") Forum requires us to keep event records for a minimum of 2 years.

Any other information that we process about you (such as your log-in details and how you use our services) will be retained until we no longer need it for the purposes for which it was collected, as set out in this Privacy Notice. We will base that decision on the following criteria:

- Any legal or regulatory requirement to delete information within, or retain the information for, a specific timeframe;
- Our legitimate business reasons for keeping the information, such as to analyze and assess our activities;
- The likelihood of a claim arising where we would need to defend our conduct; and
- Whether the information is likely to remain up to date.

We will review and delete or destroy personal information on a regular basis. If we are unable to delete or destroy personal information, we will ensure that the personal information is encrypted or protected by security measures so that it is not readily available to or accessible by us.

Automated decisions/profiling

Automated decisions are where a computer makes a decision about you without a person being involved. Profiling is where information is used to infer information about you. We do not make any automated decisions or profile you.

Security

The payment service we use is owned by us, VikingCloud. Due to the number of transactions we process, we are annually audited by an external provider to make sure we also meet the PCI DSS. We can provide our 'Attestation of Compliance' on request.

Our digital certificates business is independently audited annually, to ensure we are meeting the requirements of the CA/Browser Forum and the root programs (our WebTrust audits). You can find a copy of the audit reports here - **Legal Repository | VikingCloud Certification Authority (securetrust.com)**.

We align to the International Standard for Information Security (ISO27001) as well as that relating to Privacy (ISO27701). This involves setting up a system to manage risks around both information security and data protection / privacy, as well as putting in place measures and objectives to keep improving.

An example of a measure we take is to enforce TLS1.2 (when transferring information externally / to our suppliers). TLS1.2 is a network protocol for encrypting information in transit.

Access to your information is only provided to our people who have a need to know. We implement role-based access control so only those with a relevant role are given permission. We audit access on a regular basis.

Your Rights

There are a number of rights available under the global data protection and privacy laws. These do not usually require any fee, and we must respond within one (1) calendar month in most circumstances.

Not all rights apply in all situations and some regions have different timeframes. If you require further details of timeframes and what applies in your jurisdiction, please use contact our Global Data Protection Manager using the Contact details below.

The easiest way to exercise any of your rights / enquire if a right is applicable in a specific circumstance or to check what timescales apply would be to contact our Global Data Protection Manager as set out below. If we need further information to comply with your request, we will let you know.

Right of access / right to know

You have the right to ask for access to and receive copies of your personal information. You can also ask us to provide a range of information relating to how we collect / use your information.

Right to rectification / right to correct

If you believe the personal information we hold about you is inaccurate or incomplete, you can ask us to correct that information.

Right of erasure / right to be forgotten / right to delete / right to anonymization

In some circumstances, you have the right to ask us to delete and / or anonymize personal information we hold about you.

Right to restrict processing / right to have information preserved

In some circumstances, you are entitled to ask us to restrict the processing of your personal information. This means we will stop using your personal information, but we will not delete it. Or you could ask us to NOT delete your information.

Data portability

You have the right to ask us to provide your personal information in a format that allows you to share your personal information with another provider.

Right to object

You are entitled to object to us processing your personal information if the processing is based on legitimate interests. You also always have the right to object to our use of your information for marketing purposes.

Changes to this Privacy Notice

Any changes we may make to the Privacy Notice in the future will be posted on this page and, where appropriate, notified to you by email. Please check back frequently to see any updates or changes.

Contact

Our Global Data Protection Manager can be contacted using the following email address: **dataprotectionprivacy@vikingcloud.com** or alternatively by writing to us at 1st Floor Block 71A, The Plaza, Park West Business Park, Dublin 12.

Questions, comments, and requests regarding the Privacy Notice are welcomed and should be addressed to: **dataprotectionprivacy@vikingcloud.com.**

If you have any concerns about the ways in which we process your personal information, we encourage you to contact us. In many countries you also have a right to complain to the relevant supervisory authority, however, most regulators require that you contact us first so that we can address your concerns.

Please see below for details of the relevant regulators:

- Australia
  - Office of the Australian Information Commissioner (OAIC)
    - **https://www.oaic.gov.au/about-us/contact-us**
- Brazil
  - Autoridade Nacional de Proteção de Dados (ANPD)
    - **https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/peticao-de-titular-contra-controlador-de-dados**
- Canada
  - Office of the Privacy Commissioner of Canada
    - **https://www.priv.gc.ca/en/report-a-concern/**
- European Economic Area
  - EU regulators, plus those from Iceland, Liechtenstein and Norway
    - **https://edpb.europa.eu/about-edpb/about-edpb/members_en**
- India
  - There is no regulator as such, the current law is overseen by the Ministry of Communication & Information Technology (Department of Technology)
- South Africa
  - Information Regulator (South Africa)
    - **https://inforegulator.org.za/complaints/**
- United Kingdom
  - Information Commissioner's Office (ICO)
    - **https://ico.org.uk/global/contact-us/contact-us-public/**