VeriSmart GDPR Policy

And Risk Assessment

Definitions

GDPR : General Data Protection Regulations
PII : Personally Identifying Information
The Company : Inventoryclerkdotcom Ltd trading as VeriSmart Inventories
dCal : The VeriSmart online booking and booking management system
Iron : The VeriSmart online report generator
Clients : All customers who provide The Company with PII in the context of report fulfillment
Contractors : VeriSmart Licensees and or Team Clerks
Service : Inventory, Check-in, Mid-term, Check-out and Compliance reports,

GDPR

The Company has for the last year been developing secure systems that will ensure any person representing The Company meets that required within the GDPR; a legal requirement from the 25th May 2018.

GDPR applies to any organisation or entity which processes PII for any person (data subject) who is a resident of the EU, and as such, The Company complies with GDPR regulations.

The Company categorises the VeriSmart Inventories Head Office as a Data Controller and any Contractor processing Client information as a Data Processor.

Usage

Any PII provided to The Company by a Client will be used solely for any previously agreed upon Service to the Client and their customers (Landlords and Tenants) via VeriSmart Contractors.

PII provided to The Company in the form of Tenant and or Landlord details will only be used for the following purposes:

- To contact Tenants and Landlords to arrange meeting times
- To deliver reports to Tenants and Landlords
- To verify Tenants' feedback
- To supply Clients with delivery logs and other report verification and evidence.

Tenant's Portal

When tenants interact with The Company's online portal, they are sent and can view at any time The Tenant Privacy Policy - https://tenant.verismart.co.uk/gdpr.html
This contains all the information a Tenant may need to exercise any of their rights as a data subject.

Accountability

Any Client is welcome to copies of any detailed procedures and policy documents on request. Any Client is welcome to audit the security procedures and technical measures at The Company's Head Office providing it is at The Client's expense.

Where is the data and any applications stored?

All applications and data are stored in Telecity Groups Powergate Datacentre in London, UK. This Datacentre is ISO 27001 Information Security Management accredited - http://www.telecitygroup.com/uk-collateral/powergate_brochure.pdf

The application and database servers are hosted by www.linode.com, who are ISO 27001 Information Security Management accredited - https://www.linode.com/compliance
https://www.linode.com/security

Files, such as finished reports and photographs, are stored on Amazon Web Services S3 service. Amazon's data centres are in Ireland and remain within the EU or EEA.
https://aws.amazon.com/compliance/gdpr-center/
https://aws.amazon.com/compliance/iso-27018-faqs/

No data or files are moved outside of the EU or EEA. If however, in the future, there is a need to do so then all Clients will be informed prior to any move.

Data Protection Officer (DPO)

Whilst The Company has no legal requirement to appoint a DPO, The Company has chosen to do so in the interests of maintaining a commitment to data protection.

The contact details are:

In writing:
Data Protection Officer
Veri House 10A Chine Crescent Road
Bournemouth
BH2 5LQ

Or enquire via email at gdpr@verismart.co.uk or by phone on 0845 6123727.

Data Controls and Risk Management

The Company's data controls commence with the VeriSmart Information Asset Register. This register contains a list of all PII The Company controls and processes along with risk status and details of where it is stored.

When new PII is introduced to the The Company, the data is first assessed as to whether The Company needs to hold such information for any reason, and if it does, then the data is risk assessed as to its vulnerability to a potential breach.

Such assessments help The Company to decide how PII is stored, as well as under what circumstances, and for how long and how often it is assessed for retention. This information is then recorded in the Information Asset Register (IAR).

The Company's procedures keep in mind data protection and the rights of the data subjects. For example, The Company and or The Contractors will not communicate any information over the phone or by any other means without the requestor's identity and right to information verified.

All Data Processors as well as VeriSmart Head Office employees have training in data protection and data subject rights with procedures in place to handle any information requests The Company may receive.

Any supplied data marked as possibly containing PII is encrypted-at-rest (in storage) and can only be decrypted by The Company's application servers.

All system changes, updates, new features and bug fixes are reviewed for any risk of data leakage by The Company with appropriate testing before release. The Company's software change process refers to the IAR and treats all data or files accordingly.

Access and Tracking

All data, PII or otherwise, is accessible only through the VeriSmart secure and protected calendar booking system and is accessible only to those clients to whom the data belongs to via Clients' login details.

Similarly any data can also be seen by a Contractor who has the right to access such data for the purposes of fulfilling their contract with a Client.

Finally the same data can also be seen by VeriSmart Head Office employees for the purposes of Helpdesk assistance, statistical analysis and quality assurance.

PII and other data will never be used for any other purpose than for the reasons mentioned and will not be shared with any third-party except where a third-party has explicit permission.

The Company's VeriSmart booking system employs a variety of intrusion-detection and intrusion-prevention systems, including but not limited to automatic IP bans for suspicious behaviour, alerts to The Company's Helpdesk and the on-call engineer as well as any external intrusion-detection systems employed by The Company.

The Company's servers, applications and office-based computing devices are subject to a monthly security audit, which includes maintaining software versions up-to-date with the latest relevant security patches.

No system-generated transactional emails sent to any Contractor or The Company's head office contain PII.

All report downloads and booking actions are logged by IP address and unique identifiers. Suspicious actions are automatically logged out and prevented from connecting whilst alerting The Company's Helpdesk for further action.

Security Breach Procedure

The Company maintains procedures - should a breach occur - in order to ascertain what information has been accessed with an assessment of any likely risk to relevant individuals.

If a breach occurs, The Company has a process in place to notify the ICO of such a breach within 72 hours of becoming aware of it, even if all details are unknown at the time. In addition a process is available to inform any affected individual without delay about a breach should the breach result in a high risk to individuals' rights and freedoms. In addition, The Company can provide advice and help to an affected individual in order to limit or protect from any adverse effects caused by a breach.

All Company Employees and Contractors are mandated to inform The Company's Head Office of any potential security threat to the integrity of The Company's systems and data in addition to any potential PII breach; this to include the reporting of lost or stolen mobile phones, computers, tablets etc. which may have within them pre-stored access to The Company's systems.

Binding Corporate Rules

VeriSmart do not transfer information outside the EEA and therefore do not follow Binding Corporate Rules.