InfoCentric Pty Ltd
Ground Floor East,101 Collins Street
MELBOURNE VIC 3000 Australia
GPO Box 569, Collins St West
MELBOURNE VIC 8007 Australia
Telephone +61 3 9650 1000
ABN: 70 140 243 447

InfoCentric Privacy Statement

Revisions

Version	Date	Author	Comments
1.0	12/07/2017	Rainer Runge	First Release
1.1	17/05/2018	Revan Oluklu	First Revision

Contents

Privacy Statement, effective as of 12 July 2017

InfoCentric Pty Ltd (the "Company") is committed to protecting the privacy of individuals who visit the Company's Websites ("Visitors"), individuals who register to use the Services as defined below ("Customers"), and individuals who register to attend the Company's corporate events ("Attendees"). This Privacy Statement describes the Company's privacy practices in relation to the use of the Company's Websites and the related applications and services offered by the Company (collectively, the "Services").

The Company will comply with the Australian Privacy Principles (APP) set forth by the Office of the Australian Information Commissioner. For more information on the Australian privacy principles, please visit the Office of the Australian Information Commissioner website here.

1. Websites covered

This Privacy Statement covers the information practices of the InfoCentric web sites, including www.InfoCentric.com.au and sites over which InfoCentric provides services; collectively referred to "Company's Websites".

The Company's Websites may contain links to other websites. The information practices or the content of such other websites is governed by the privacy statements of those other websites. The Company encourages the review of the privacy statements of other websites to understand their information practices.

2. Information collected

When expressing an interest in obtaining additional information about the Services, or registering to use the Company's Websites or other Services, or registering for an event, the Company may require Visitors, Customers, and Attendees to provide the Company with personal contact information, such as name, company name, address, phone number, and email address ("Required Contact Information"). When purchasing the Services or registering for an event, the Company may also require Customers to provide the Company with financial qualification and billing information, such as billing name and address, and the number of employees within the organization that will be using the Services ("Billing Information"). The Company may also ask Visitors, Customers, and Attendees to provide additional information, such as company annual revenues, number of employees, or industry ("Optional Information"). When Visitors apply for a job with the Company, Visitors, Customers, and Attendees may also require applicants to submit additional personal information as well as a resume or curriculum vitae ("Applicant Information"). Required Contact Information, Billing Information, Applicant Information, Optional Information and any other information submitted to the Company to or through the Services is referred to collectively as "Data."

During navigation of the Company's Websites, the Company may also collect information through the use of commonly-used information-gathering tools, such as cookies and web beacons ("Website Navigational Information"). Website Navigational Information includes standard information from

your web browser (such as browser type and browser language), your Internet Protocol ("IP") address, and the actions you take on the Company's Websites (such as the web pages viewed and the links clicked). For additional information about the collection of Website Navigational Information by the Company and others, please see the table in Section 4 below.

Health Related Data We May Collect

The Company may collect health-related data with the following specifications in regards to its access, storage and utilisation:

Access: The Company may have access to your health-related data with either your express consent or at the direction of a third party that you have authorised to share your health-related data. To the extent your health-related data is protected health information ("PHI") or its regulated equivalent in other jurisdictions, the Company will handle such PHI in accordance with applicable laws and regulations.

De-identified, Anonymised, or Aggregated Data: The Company may de-identify, anonymise, or aggregate your health-related data in compliance with applicable laws and regulations. The Company will not use nor share such information in violation of applicable laws or regulations.

Security: The Company will provide appropriate physical, technical, and administrative safeguards with respect to your health-related data and in accordance with applicable security laws and regulations. The Company will encrypt your health-related data both in storage and in transit.

3. Use of information collected

The Company uses Data about Customers to perform the services requested.

The Company uses Website Navigational Information to operate and improve the Company's Websites. The Company may also use Website Navigational Information alone or in combination with Data about Customers and Data about Attendees to provide personalised information about the Company.

We may use personal information:

- To enroll you for and provide the Company Services to you, and to recognise you when you return to our sites as part of providing these services.
- To respond to your inquiries and fulfil your requests, such as activation services and troubleshooting issues.
- To personalise your experience on the Company Services.
- To complete and fulfil your purchase, for example, to process your payments, have your order delivered to you, communicate with you regarding your purchase and provide you with related customer service.
- For our business purposes, such as data analysis, audits, fraud monitoring and prevention, developing new products, testing, enhancing, improving or modifying our Company Services, identifying usage trends, operating and expanding our business activities.

- To send administrative information to you, for example, information regarding the Company Services and changes to our terms, conditions, and policies.

Personal information may be shared or disclosed:

- To our authorised third-party service providers and suppliers who provide services to us such as web site hosting, data analysis, payment processing, order fulfillment, information technology and related infrastructure provision, customer service, email delivery, credit card processing, auditing and other similar services.
- To a third party in the event of any reorganisation, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings).
- As we believe is required, necessary or appropriate: (a) under applicable law, including laws outside your country of residence; (b) to comply with legal process and/or to respond to requests from competent public and government authorities including public and government authorities outside your country of residence; (d) to enforce our terms and conditions; (e) to protect our operations and those of any of our affiliates; (f) to protect our rights, privacy, safety and physical and intellectual property, and/or that of our affiliates, you or others; and (g) to allow us to pursue available remedies or limit the damages that we may sustain.

4. Website Navigational Information

Cookies, web Beacons and IP Addresses

The Company uses commonly-used information-gathering tools, such as cookies and web beacons, to collect information during navigation of the Company's Websites ("Website Navigational Information"). This section describes the types of Website Navigational Information used on the Company's Websites and how this information may be used.

Cookies

The Company uses cookies to make interactions with the Company's Websites easy and meaningful. When visiting one of the Company's Websites, the Company's servers send a cookie to the client computer. Standing alone, cookies do not personally identify a user; they merely recognize the user's web browser. Unless the user chooses to identify themselves to the Company's Websites, either by responding to a promotional offer, opening an account, or filling out a web form (such as a "Contact Me" or a "Request a demo" web form), the user remains anonymous to the Company.

The Company uses cookies that are session-based and persistent-based. Session cookies exist only during one session. They disappear from the user's computer when the user closes their browser software or turn off their computer. Persistent cookies remain on the user's computer after the user closes their browser or turns off their computer.

IP Addresses

When users visit the Company's Websites, the Company collects user Internet Protocol ("IP") addresses to track and aggregate non-personal information. For example, the Company uses IP addresses to monitor the regions from which Customers and Visitors navigate the Company's Web sites.

The Company also collects IP addresses from Customers when they log into the Services as part of the Company's "Identity Confirmation" and "IP Range Restrictions" security features.

Data from the Services (Usage logs and Analytics Data). The Company also collects and processes usage data when Customers use the Services (e.g., ingest volume, search concurrency, number of unique user logins, operating system, internet protocol address, source type (count), session duration and other use data) ("Usage Data") in order to provide, maintain, and improve Services.

In addition, the Company collects and processes anonymised, aggregated data about a group or category of Services, features or users in order to improve the Services ("Analytics Data"). For example, Analytics Data may include anonymized Usage Data, information about the server environment (e.g., OS type/version, CPU type/version, database type/version, disk utilisation), information about the devices operating the Services (e.g., browser type/version, OS type/version, device type/version), or such other similar information about user configuration or operation of the Service features or functionality.

5. Customer testimonials

The Customer may post a list of Customers and testimonials on the Company's Web sites that contain information such as Customer names and titles. The Company always obtains the consent of each Customer prior to posting any information on such a list or posting testimonials.

6. Sharing of information collected

Service Providers

The Company will not share Data about Visitors, Customers and Attendees unless formal consent has been obtained beforehand. The Company does not share, sell, rent, or trade any information with third parties.

Affiliates

The Company will not share Data about Visitors, Customers and Attendees unless formal consent has been obtained beforehand. The Company does not share, sell, rent, or trade any information with third parties.

The Company will not share Data about Visitors, Customers and Attendees unless formal consent has been obtained beforehand. The Company does not share, sell, rent, or trade any information with third parties.

Compelled Disclosure

The Company reserves the right to use or disclose information provided if required by law or if the Company reasonably believes that use or disclosure is necessary to protect the Company's rights and/or to comply with a judicial proceeding, court order, or legal process.

7. Communications preferences

The Company offers Visitors, Customers, and Attendees who provide contact information a means to choose how the Company uses the information provided. Visitors, Customers, and Attendees may manage receipt of marketing and non-transactional communications by clicking on the "unsubscribe" link located on the bottom of the Company's marketing emails. Additionally, Visitors, Customers, and Attendees may send a request to info@InfoCentric.com.au.

8. Customer Data

Customers may electronically submit data or information to the Services for hosting and processing purposes ("Customer Data"). The Customer will not review, share, distribute, or reference any such Customer Data except as provided in the Company's Subscription Agreement, or as may be required by law. In accordance with the Customer's Master Subscription Agreement, the Customer may access Customer Data only for the purpose of providing the Services or preventing or addressing service or technical problems or as may be required by law. Additional information about the Company's privacy and security practices with respect to Customer Data is available upon request to info@InfoCentric.com.au.

9. How to Manage Your Customer Data

If you would like to access, correct, update, or delete the personal information that you have provided to us, you may contact us by: visiting the specific product or service web site; using support@InfoCentric.com.au email link; or sending a letter to the postal address below including your name, e-mail address, account identification, and purpose of the request.
For your protection, we will only implement requests with respect to personal information about you (not anyone else), and we may need to verify your identity before implementing your request.

We will comply with your request as soon as reasonably practicable and in accordance with applicable law. We may need to retain certain information for recordkeeping purposes, as required under applicable legal obligations, and/or to complete any transactions that you began prior to requesting

such change or deletion (e.g., when you make a purchase or enter a promotion, you may not be able to change or delete the personal information provided until after the completion of such a purchase or promotion). Some of your information may remain within our systems and other records, in compliance with applicable law.

10. Security

The Company uses robust security measures to protect Data about Visitors, Customers, and Attendees. The Company maintains Data about Visitors, Customers, and Attendees. This information, which is stored in the Services, is secured as follows:

Third-Party Architecture: The architecture used to host Customer Data submitted to the Services is typically provided by a third party provider, Amazon Web Services, Inc. ("AWS"). Currently, the architecture hosted by AWS in provisioning of the Services is located in Sydney, Australia.

Security Controls: The Services include a variety of security controls. These controls include:

Unique user identifiers (user IDs) to ensure that activities can be attributed to the responsible individual;

Password length controls;

Password complexity requirements for Web access to the Services.

Security Procedures, Policies and Logging: The Services are operated in accordance with the following procedures to enhance security:

User passwords are stored using a salted hash format, using a slow hashing algorithm that is always encrypted in transit;

User access log entries will be maintained, containing date, time, URL executed or entity ID operated on, operation performed (viewed, edited, etc.)

Logs are stored in a secure centralised host to prevent tampering

Passwords are not logged under any circumstances

User Authentication: Access to the Services, directly or via API, requires a valid user ID and password combination, or an API key/secret, both of which are encrypted via TLS while in transmission.

Physical Security: Production data centres used to provide the Services, where the Services are off-premise, have systems that control physical access to the data centre. These systems permit only authorised personnel to access secure areas. The facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, physical access screening and escort controlled access, and are also supported by on site back-up generators in the event of a power failure.

Reliability and Backup: All networking components, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Services is

stored on a primary database server that is clustered with a backup database server. All Customer Data submitted to the Services is backed up daily.

Patching: All networking components, load balancers, Web servers and application servers, used to host Customer Data, are patched in-line with AWS standard patching service levels.

11. Changes to this Privacy Statement

The Company reserves the right to change this Privacy Statement. The Company will provide notification of the material changes to this Privacy Statement through the Company's Websites at least thirty (30) business days prior to the change taking effect.

12. Contacting us

Questions regarding this Privacy Statement or the information practices of the Company's Web sites should be directed to InfoCentric Privacy by clicking here or by mailing InfoCentric, GPO Box 569, Collins St West, Melbourne, Victoria, 8007, Australia.