Comprehensive Pre-Filled Request For Information For Convert Experiences

Powered by Convert.com

Index

Download Empty RFI Template

convert®

Regulatory & Governance

FCA registration number
N/A

What FCA permissions do you rely on for the purpose of this agreement?
N/A

In the last 12 months, has your company (or Principle) or any persons associated been under investigation, sanctioned, prohibited or fined by the FCA, the ICO or the Advertising Standards Authority? If yes, please provide details including the activity and / or individual in question, the outcome and the current status.
No

In the last 12 months, has your company (or Principle) or any persons associated been under investigation, sanctioned, prohibited or fined by the FCA, the ICO or the Advertising Standards Authority? If yes, please provide details including the activity and / or individual in question, the outcome and the current status.
No

Can you describe how you meet the FCA's requirements of responsible lending, and what procedures you have in place in making an assessment of the creditworthiness of a customer?
No

Can you describe how you deal fairly with customers in arrears or default in accordance with the FCA's principles and consumer outcomes?
N/A

What procedures do you have in place to ensure that all customers are treated fairly and in accordance with the FCA's principles and consumer outcomes?
N/A

What procedures do you have in place to identify customers with vulnerability issues and where identified have procedures in place to provide customer with additional support to help them make an informed decision?
N/A

What systems and controls do you have in place to prevent your business from being used for the purposes of financial crime including fraud, bribery, tax evasion and money laundering?
N/A

How do you ensure your business is adequately protected from interruption and can effectively recover any loss or damage to property, software or loss of key personnel?
We have in place a Business Continuity policy

What processes do you have in place for the review and approval of marketing material in accordance with CONC 3 and other relevant regulation?
N/A

Please set out in detail what activity you will be doing with us?
We are an A/B testing software company so you will use the software to A/B test its websites

Customer Journey

Please provide all customer facing URL's
app.convert.com, convert.com, support.convert.com

Please outline of the type of product you will offer once we introduce a customer to your company?
A/B testing and optimization vendor

Please outline the end to end customer journey once we introduce a customer to your company (please also provide screenshots)
N/A

Do you trade off canvass? (for example, in a customer's home or in the street). If yes, please provide details of activities.
No

Do you intend to outsource any of the activity you undertake with us to a third party. If so, please state which activity and who it will be outsourced to, including the third party's legal entity and all registered trading names.
No

Do you charge any fees to customers? If yes, when are they introduced, what is the fee for and at which point is it payable?
convert.com/pricing

Policy Documentation

Please confirm if you have the following policies (or similar): Yes / No

Whistle-blowing Policy
No

Anti-Money Laundering & Financial Crime Policy
No

Anti-Bribery & Corruption Policy
No

Conflicts of Interest Policy
No

Modern Slavery Policy
No

Breach Policy
Yes

Corporate Governance & Risk Management Policy
Yes

Information Security/Data Protection Policy
Yes

Complaints Handling Policy
Yes

Business Continuity Policy
Yes

TCF Policy – Treating Customers Fairly
No

Vulnerable Customer Policy
No

Training & Competency Policy/Manual
Yes

Have all Policies been reviewed, revised and communicated to staff within the last 12 months?
Yes

Complaints

Do you have a complaints procedure in place which complies with DISP?
N/A

How many FOS complaints have you received in the last 12 months?
N/A

Of those, how many did the adjudicator or Ombudsman rule in favour of the customer?
None

What were the main reason for these complaints?
N/A

Application

Describe the system architecture/infrastructure – including hardware, operating systems and services – for all components, including external systems (application server, database server, etc.).
We rely on Amazon Web Services who is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services.

Describe your application and operating system patch methodology.
We rely on Amazon Web Services who is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services.

Describe where and how logging is performed, maintained and reviewed.
Live Logs in Convert track how end users are interacting with web pages and experiments on them at a project and experiment level in real time. They capture information like timestamp when a goal triggered, the event type that was triggered, variation displayed to the end user and many more details. Live logs are different from the logs that are kept here: logs.convertexperimetns.com. These are used for debugging purposes and are kept only for 7 days.

Is the system housed in a secure managed data center? If not, describe the security features of the location
We rely on Amazon Web Services who is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services.

Is the system located on a shared resource or on a dedicated resource? If it is shared, describe the processes in place to isolate different customer environments.
We rely on Amazon Web Services who is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services.

Describe disaster recovery/business continuity plans as they relate to the services provided to TNC.
Business Continuity is managed as part of the Emergency Management Plan to ensure seamless follow up of an emergency and continuity of services. This Plan takes into account several incidents that may be minor/localised (levels 1 or 2a) incidents or (levels 2b or 3) emergencies.
- Serious Staff Incident
- Utilities Failure - Pandemic / Serious Outbreak of Infectious Disease
- Data Network Failure
- IT Systems Failure
- Fraud
- Personal Data Security Breach
- Serious Blog/Social Network Incident
- Competitors move faster in technology
- Losing of connectivity between people because of a natural disaster
- Large lawsuit by customer
- DDOS attacks
- Financial disaster (Wall Street)
- Bus-Factor: One person does it all
- Free competitor comes in with similar standards
- Third parties that we rely on
These have been identified as the main incidents after a Pre-Mortem Analysis.

Describe the systems and processes in place for incident/intrusion prevention, detection and response.
Our Incident Management Program (network, computers and data) consists of:
- **Identify** the essential elements of what is required to attain compliance or successful cybersecurity resilience
- **Assess:** Gauge and evaluate Convert Insights state of protection mechanisms, gaps and opportunities for improvement.
- **Develop:** This step involves the set of activities required to draft and test the adoption of the cybersecurity strategy, policy and set of actions to manage cyber security. The overall set of documents include know-how, know-what knowledge on areas such as surveillance and monitoring of threats, security audits, vulnerability assessments, incident handling and reporting, risk management, business continuity and more.
- **Train:** After development, we create awareness of the Program by providing training to relevant stakeholders.
- Continuously **monitor** the internal and external environment for changes or developments.

How are system administrator access requests, changes, approvals, etc. submitted and documented?
Convert's Data Management Policy defines three roles for accessing data:
- Data Controller who has the responsibility to ensure that appropriate data management policies are in place so that the data owners can ensure they are compliant with legislation to the best of their ability.
- Data Owner who authorise the access and use of data, regularly review access privileges, assess the risks, ensure that appropriate contingency plans are in place to safeguard the data.
- Data Custodian to whom in some cases data will be entrusted (e.g. an individual or a third party company) for the purposes of storage and/or processing.

How do system administrators gain access to the system components?
Using VPN and AWS console

Are you accessing any TNC systems or systems on behalf of TNC? If so, describe the configuration of the computer and network environment used by your staff and/or systems which are accessing those TNC systems.
No

Describe any APIs, web services availability and the level of documentation that exists for them.
https://www.convert.com/features/ab-testing/api/, https://api.convert.com/doc/v2/

Does the platform provide the ability to integrate custom code for additional publishing functionality? If so, please describe how.
No

How do you integrate with 3rd-party development IDEs for the management of content external to the CMS platform?
We do not integrate with IDEs yet

Describe integration options for identity services to allow authentication and single sign-on integration.
https://support.convert.com/hc/en-us/articles/360044054271-How-to-enable-SSO-Login-feature-for-my-Convert-account-

Describe your platform's social media integration (to platforms like Facebook, YouTube, Twitter, and LinkedIn, as well as separate blog instances). Describe how "share" functionality works with those integrated platforms.
https://support.convert.com/hc/en-us/articles/204871655-Add-and-Track-Social-Sharing-Buttons

For enterprise systems of record (Marketing Automation, Web Analytics, CRM, Data Management Platforms, etc.), how may APIs or "connectors" does your platform support out-of-the-box?
We can integrate with many third party tools by using this:
https://support.convert.com/hc/en-us/articles/360042473452

Describe the level of effort required in building APIs or connectors for integration with a platform that is not supported.
Depends on the platform and what options they have for custom js tracking

Describe the level of effort required for a customer to get access to a newly released integration with a 3rd-party platform.
None to little as we usually integrate by a click of a button via the UI

Can the CMS can seamlessly display 3rd-party or custom web applications (embedded applications within a modifiable CMS page) that are hosted at other locations (i.e. line of business web applications that are hosted in our datacenters)? If so, describe how.
No

Does your platform support integration with Marketing Automation platforms? If so, please describe how.
Not yet but we can check if you are interested into this

What data sources are commonly supported (i.e. XML, DB integration capability)? Describe each.
Javascript and custom events, data layers

How does your platform support integration with code version control systems?
We do not integrate with those yet

Application

Technical Dependencies

Does managing your platform require training for a custom markup language?
No

Does your operation of your platform favor one particular technology environment or language? If no, please describe which one and why.
Javascript

How does your platform minimize the need for coding in all phases of digital experience creation/management (i.e. template configuration, template management, testing, targeting & personalization)?
By using the Visual and Code Editors

What steps do you take or features does your platform have that enables it to be technically agnostic towards whatever backend technology environments your customers may choose?
Convert is an A/B testing platform so does not interact with the backend

What technologies does the CMS support for published pages? In other words, what type of output templates can your platform support? (i.e. .NET, JSP, PHP, XML, etc.)
N/A

Platform Architecture

Does your platform provide a Software-as-a-Service (SaaS) option?
Yes

Is your platform delivery architecture true multi-tenant SaaS? If yes, please describe.
No

Is your platform delivery architecture single-tenant SaaS? If yes, please describe.
No

Are feature releases and updates to the platform instantly available to all customers?
Yes

Are new integrations with 3rd-party platforms or services instantly available to all customers?
Yes

If feature releases and updates are not instantly available to the platform, please provide details on the process required for a customer to update their instance to the new version.
N/A

If new integrations are not instantly available to the platform, please provide details on the process required for a customer to get access to the new integrations within their instance.
N/A

Is your platform a dynamic in nature, meaning it makes service calls to the CMS itself "at runtime" to power digital experiences? If so, please explain why your organization has chosen this approach.
No

Do you leverage a "Decoupled Architecture" in which the CMS is decoupled from the live hosted site? If your platform leverages a Decoupled Architecture, please explain how you deliver dynamic content and services.
N/A

If your platform leverages a Decoupled Architecture, please explain why your organization has chosen this approach.
N/A

How does the platform enable consistent performance and reliability through its architecture?
We rely on AWS

How does your platform architecture support rapid content delivery around the world?
We rely on Akamai

What is your hosting strategy? (For example: Do you offer hosting in multiple data-centers and geographies?)
Yes we rely AWS cloud services

What software—such as databases or runtime licenses—are required to run your software in a production environment?
None

Describe how you support Disaster Recovery.
Business Continuity is managed as part of the Emergency Management Plan to ensure seamless follow up of an emergency and continuity of services. This Plan takes into account several incidents that may be minor/localised (levels 1 or 2a) incidents or (levels 2b or 3) emergencies.
Serious Staff Incident
Utilities Failure
Pandemic / Serious Outbreak of Infectious Disease
Data Network Failure
IT Systems Failure
Fraud
Personal Data Security Breach
Serious Blog/Social Network Incident
Competitors move faster in technology
Losing of connectivity between people because of a natural disaster
Large lawsuit by customer
DDOS attacksFinancial disaster (Wall Street)
Bus-Factor: One person does it all
Free competitor comes in with similar standards
Third parties that we rely on
These have been identified as the main incidents after a Pre-Mortem Analysis.

Describe how you support High Availability. Are there extra charges for High Availability?
No extra costs, uptime is here: http://status.convert.com/

Implementation & Deployment

Given the size of our website, please describe a typical migration plan. How would it take for us to migrate our existing site content to the proposed solution? Please include: time frames (how long does a typical migration of this size take?), resources, and any software or technology needed to perform these tasks.
N/A

How does your platform ensure that implementation/agency partners can efficiently delivery digital experiences without excessive development effort and time?
With the Visual Editor

How does your platform enable multiple agency partners or internal dev teams to work on the platform while maintaining site stability and code unity?
Via the Collaborators and granural permission levels

How does your platform minimize the need for excessive agency / 3rd-party effort around managing updates to the platform and related site instances?
N/A

What are the general integration timelines with 3rd party systems and platforms?
There is no specific timeline, as we receive an integration request we work on this the soonest possible

Privacy & Data Protection

PII Collection, Processing, Storage

What data is being collected? (Not just personal data or PII data, but all data you are collecting in our relationship, your pixels, etc.) + What are you doing with the data you are accumulating?
Information We Collect When You Register and Create An Account
Visitors to our website (convert.com) (the "Site") may read information about us and our products and services without revealing any personally identifiable information. However, in order to become a customer, you must create an account and set up a profile. When you do this, we ask for your name, your organization's name, its street address and your e-mail address. We also require you to select a password. Once you are a registered user you can update your profile and you may elect to provide additional information (e.g. a nickname and certain user preferences).

Information We Collect When You Register for a Webinar
Visitors or Customers can register for a webinar. Here we store the email address to share the webinar details.Information We Collect When You Request the NewsletterVisitors or Customers can sign up to receive our Newsletter. Here we store the email address to share the Newsletter on a monthly basis.

Information We Collect From Your Websites
The Services we provide consist of tracking visits to your website and collecting information about the behavior of those visitors. The data we collect helps you optimize your website and to use it strategically. This data may include the web addresses (URLs) of pages visited, the URLs of web pages that referred your visitors to your website, details about the web browsers that visitors to your website use to browse your website, the operating systems used by those visitors, the number of screen colors and the screen resolution used by the visitors to view your websites, and external geodata elements connected to your visitors' ip address (including country, city, region, etc.). Our Services are organized so that our customers can specify the categories of data they wish to receive. The aforementioned categories of information do not necessarily enable us or others to identify you or the visitors to your website. However, if the URLs we collect contain information that in themselves identify personally identifiable information, such as a name or phone number, or if they link to pages that contain personally identifiable information, then we may collect that information as well.
Notes for transparency:
On by default
- Currently session cookie ID (timeout 20 minutes on cookie and server cache).- Currently falling under performance cookies in our interpretation of GDPR / ePrivacy Directive and ePrivacy Regulations.

Off by default
- When cross browser targeting is turned on by the customers we insert unique cookie in URL to pick-up on the other domain (could be interpreted by GDPR as personal data). This feature is off by default as part of our privacy by default policy.- When a unique visitor IDs are given by the customer to replace session IDs this could be interpreted as personal data This feature is off by default as part of our privacy by default policy.
- When geotargeting is used (not on my default) we could store country, region and city in CDN or server cache for correct targeting.

Other Information We Collect
Our Services allow our customers to transmit and store additional information on our servers. This additional information can be anything, including personally identifiable information, except that we don't permit URLs or internet addresses to be stored. We have no control over what information is transmitted by our customers to our servers. Our customers may also request that we receive personally identifiable information that has been rightfully obtained by those customers, such as the email addresses of those who visit their websites and the information that visitors to their websites choose to post.

Cookies
A "cookie" is a small data file that can be placed on your hard drive when you visit certain websites. We use cookies to identify visitors who browse our customers' websites. These cookies contain an identifier that identifies each such visitor anonymously in order to analyze his or her past behavior in relation to your website. None of our cookies contain or collect personally identifiable information.Infor below:
_conv_s
convert.com
This cookie contains an ID string on the current session. This contains non-personal information on what subpages the visitor enters – this information is used to optimize the visitor's experience.1 dayHTTP Cookie, 1st party cookie, Strictly Necessary_conv_vconvert.comThis cookie is used to identify the frequency of visits and how long the visitor is on the website. The cookie is also used to determine how many and which subpages the visitor visits on a website – this information can be used by the website to optimize the domain and its subpages.6 months (or 7 days if ITP 2.1 applies)HTTP Cookie, 1st party cookie, Strictly Necessary_conv_vconvert.comThis cookie is used to identify the frequency of visits and how long the visitor is on the website. The cookie is also used to determine how many and which subpages the visitor visits on a website – this information can be used by the website to optimize the domain and its subpages.6 months (or 7 days if ITP 2.1 applies)HTTP Cookie, 1st party cookie, Strictly Necessary

Where is Data stored?
We are using European carbon neutral servers on AWS Cloud based in Frankfurt so it is Europe based.

Do you have ISO 27k compliance?
We do not have such an official compliance certificate but we are planning to obtain one in the next 2 years. At the moment we rely on AWS ISO certificates since our servers are on their cloud infrastructure.

Transfer of data
For any transfer of personal data outside the European Economic Area to a country which is deemed by the EU to not have an "adequate" level of data protection, we have put in place with our affiliates, with our third party service providers, and with our customers, the necessary safeguards and mechanisms to ensure that such transfers comply with applicable data protection laws.These safeguards include the EU Standard Contractual Clauses (SCC) and E.U.-U.S. Privacy Shield and Swiss-U.S. Privacy Shield certification. In addition, we may institute in the future, in our discretion, other lawfully approved mechanisms such as Binding Corporate Rules and Codes of Conduct. For transfers to third party service providers, we ensure that such entity maintains appropriate safeguards and shall have in place required data protection terms to ensure protection of personal data to the same degree as required of Convert.

Can I sign a DPA?
We make it easy for our customers to formalize and share with their stakeholders, including employees, customers and potential auditors, that they use Convert Experiences in a way that meets GDPR data processing obligations.
The Data Processing Agreement (DPA) is an easy-to-execute document that only requires an electronic signature from the customer. For reference, please visit this https://www.convert.com/gdpr/dpa/.

User Authentication & Access

What method is used to authenticate end users to the system?
Yes, access to systems is based on specific roles and duties of each role and is reviewed frequently.

Is every user assigned a unique account?
Yes

How is the authentication session secured?
Our cloud infrastructure (AWS) takes care of it.

How are credentials of the user secured within the system?
Our cloud infrastructure (AWS) takes care of it.

Describe the password standards/options, including complexity, length, expiration, etc
- All passwords should be reasonably complex and difficult for unauthorized people to guess. members should choose passwords that are at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and punctuation marks and other special characters. These requirements will be enforced with software when possible.
- In addition to meeting those requirements, members should also use common sense when choosing passwords. They must avoid basic combinations that are easy to crack. For instance, choices like "password," "password1" and "Pa$$w0rd" are equally bad from a security perspective.
- A password should be unique, with meaning only to the members who choose it. That means dictionary words, common phrases and even names should be avoided. One recommended method to choosing a strong password that is still easy to remember: Pick a phrase, take its initials and replace some of those letters with numbers and other characters and mix up the capitalization. For example, the phrase "This may be one way to remember" can become "TmB0WTr!".
- Members must choose unique passwords for all of their company accounts, and may not use a password that they are already using for a personal account.
- All passwords must be changed annually, with a higher frequency varying based on the sensitivity of the account in question. This requirement will be enforced using software when possible.
- If the security of a password is in doubt– for example, if it appears that an unauthorized person has logged in to the account — the password must be changed immediately.
- Default passwords — such as those created for new members when they start or those that protect new systems when they're initially set up — must be changed as quickly as possible.

Describe authentication security measures such as inactive session timeouts, invalid login attempt lockouts, etc.
Our cloud infrastructure (AWS) takes care of it.

Does the system have role-based access control? If so, describe.
No

Security Specifics

Information Security Org

Is there an identified individual or group that is responsible for Information Security within your Organization?
Yes - Dionysia Kontotasiou, Head of Privacy & Security, dionysia@convert.com

Has an independent third party review of the information security program been conducted in the last 12 months?
Yes - Yes, penetration tests are being conducted every 12 months by an independent external third party.

Is there an independent audit function within the organization?
Yes

Is there a designated person or team with appropriate seniority with responsibility or accountability for data protection / privacy matters within your organization, e.g. a Chief Privacy Officer, a Data Protection Officer or a Privacy Team?
Yes - Dionysia Kontotasiou, Head of Privacy & Security, dionysia@convert.com

Is there a documented process to a) identify and escalate data breaches and security incidents, and b) notify customers of such data breaches or security incidents as soon as possible, and in accordance to contractual obligations?
If a member of Convert Insights considers that a security breach has occurred, this must be reported immediately. Part 1 of the Security Breach Report Form should be completed without delay. Part 1 of the Report Form will assist in conducting an initial assessment of the incident by establishing: if a security breach has taken place; if so: what data and systems are involved in the breach; the cause of the breach; the extent of the breach (how many individuals are affected); the harms to affected individuals that could potentially be caused by the breach; how the breach can be contained. Following this initial assessment of the incident, an appropriate Lead Investigator is appointed to investigate the incident and will decide if it is also necessary to appoint a group of relevant stakeholders to assist with the investigation. The Lead Investigator will determine the severity of the incident and by completing part 2 of the Security Breach Report Form (i.e. s/he will decide if the incident can be managed and controlled locally or if it is necessary to escalate the incident to the Emergency Management Team. The severity of the incident will be categorised as level 1, 2a, 2b or 3

Is there periodic internal monitoring for compliance with privacy policies and procedures?
Yes

Does your organization have a defined process for access management (i.e. - provisioning accounts for users, limiting user access based on the principle of least privilege, terminating access and periodic access certification)?
Yes we have a Data Management Policy in place

Are privileged accounts (i.e. - administrator, super-user, etc.) limited to select IT personnel and reviewed on an annual basis?
Yes

Is there a documented Records Retention Policy?
Yes - We have a Data Retention schedule written as a policy.

Are audits performed to ensure compliance to the records retention policy?
Yes

Does the Organization employ any third parties such as sub-contractors or vendors?
Yes

Are third parties required to adhere to your security policies and standards?
Yes

Does management require the use of confidentiality or non-disclosure agreements with external parties (including vendors or suppliers)?
Yes

Are third parties subject to due diligence checks, vetting and risk assessments which cover privacy and security?
Yes

Is there a process for ensuring contracts and agreements with sub-contractors contain appropriate privacy, confidentiality and security provisions relevant to the nature of the services and the data handling involved?
Yes

Are third party connections to your network monitored and reviewed to confirm only authorized access and appropriate usage (i.e. VPN logs, server event logs, system, application and data access logging, automated alerts, regular review of logs or reports)?
Yes

If you subcontract the processing/handling of personal information to an external party, do you have a process in place to periodically monitor and assess the external party's security practices?
Yes - For international data transfers we rely on Privacy Shield and EU Standard Contractual Clauses (SCCs)

If you send data for processing in another country (e.g. offshore outsourcing), do you have a governance framework and additional processes and controls in place to ensure secure and compliant processing?
No

Does your organization conduct background checks that include criminal, drug, credit, professional and academic screening?
Yes

Are employees and contractors joining your organization required to sign written confidentiality, non-disclosure, acceptable use of resources and ethics at the time of hire?
Yes

Are they required to acknowledge on an annual basis?
Yes

Does your organization have a disciplinary process for non-compliance with information security policies and standards?
Yes - Convert Insights operates a strict "notice and takedown" procedure. Users are encouraged to be vigilant and to report any suspected violations of the Data protection Policies immediately to support@convert.com. On receipt of notice (or where Convert Insights otherwise becomes aware) of any suspected breach of these Policies, Convert Insights reserves the following rights:to remove, or require the removal of, any content which is deemed to be in breach or potentially in breach of these Policies; and/orto disable any User and access to Convert Insights IT Resources. If any breach of these Policies is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff or contract termination in the case of third parties may be taken.

Are there periodic updates and communications to staff on key security/privacy messages, initiatives or issues?
Yes

Security Specifics

Security Policies

Who is responsible for information management and cyber security within your organisation?
Dionysia Kontotasiou

Do you have a formal Information Security Program in place? Please provide details of its structure if so.
Yes, our Information Security Program (data in any format) consists of:
Understanding the Data: to properly approach information security, Convert Insights first needs to understand the types of information it collects and stores.
Performing a Risk Assessment: A risk assessment is a key tool for determining where systems may be vulnerable to a security incident.
Determining Legal Requirements: our Information Security Program is developed by reference to our legal compliance obligations.
Developing Policies and Internal Controls: We created and maintain the policies and internal controls that ensure Convert Insights is complying with key laws and regulations on an ongoing basis. Key policies and internal controls are described in point 3.
Addressing Ongoing Compliance: Key components of ensuring ongoing compliance include: (i) Providing security training and awareness programs (ii) Monitoring and auditing compliance efforts and benchmarking against the security compliance plan (iii) Evaluating and revising program controls, policies and protocols.

What policies does your organisation have in place for managing information security? Please provide copies.
Generic Policy Framework
Acceptable Usage Policy
IT Security Policy
Web and Social Media Policy
Emergency Management Plan
Employee Password Policy
Open Source Software License Policy
Privacy and Security Checklist for GDPR Compliance when selecting third party software
Staff Information Security Training Policy

How frequently are your information security policies reviewed?
Convert Insights reserves the right to amend these Policies at any time in any manner in which sees fit at the absolute discretion of the Company. Any such revisions are noted in the revision history of each policy. Policies are reviewed at least annually, to determine whether it requires revision in light of new threats or technologies.

When were your information security policies last updated?
May 2018

What training do staff receive in relation to the information security policies and procedures? How frequently do they receive training?
Staff Information Security Training Policy sets out the training that Convert Insights staff will be provided with to ensure that all handling of information is compliant with the General Data Protection Regulation (GDPR). In general training for all data users cover these areas:IT Security awareness strategy is delivered through multiple methods with the aim of raising user awareness and highlighting end user responsibilities.Scheduled targeted Security Awareness Training sessions are available on demand in conjunction with Data Protection training. On staff induction new hires are briefed on the Data Protection Policy and the IT Security Policy.

What processes do you operate to ensure information security policies are complied with?
We use these processes to ensure that information security policies are in place:
There is someone with specific responsibility for Information Security in Convert Insights.
All staff receive annual awareness of the Information Security Regulations.
Everyone managing and handling information understands that they are directly and personally responsible for following good information security practice.
Only staff who need access to information as part of their duties are authorised to do so.
Everyone managing and handling information is appropriately supervised.Methods of handling information are clearly described.
An audit of information is conducted on an annual basis. This includes an assessment and evaluation to ensure that all information held is accurate and up to date and that adequate controls are in place to ensure information is managed and stored appropriately.
A copy of Information Security Policies are given to all new members of staff.
Procedures for selecting appropriate third-party service providers and obtaining written agreements from them to ensure that information receives adequate security and protection.
Reasonably up-to-date network firewall protection
Reasonably up-to-date virus and malware protection
Routine monitoring of computer systems for unauthorized access

Is there a formal disciplinary or sanction policy for staff who violate information security policies and procedures?
Convert Insights operates a strict "notice and takedown" procedure. Users are encouraged to be vigilant and to report any suspected violations of the Information Security Policies immediately to support@convert.com. On receipt of notice (or where Convert Insights otherwise becomes aware) of any suspected violation of these Policies, Convert Insights reserves the following rights:to remove, or require the removal of, any content which is deemed to be in breach or potentially in breach of these Policies; and/orto disable any User and access to Convert Insights IT Resources.If any breach of these Policies is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff or contract termination in the case of third parties may be taken.

Are your security and information management processes accredited to any official standard?
Convert Insights endeavours, at all times, to ensure consistent, high quality implementations and management of its IT resources, processes and practices. A comprehensive framework of well-defined policies, procedures and standards are required to facilitate and ensure this. In developing the IT policies, procedures and standards for Convert Insights, due regard and consideration has been given to the ISO 27000 series of standards which have been specifically reserved by ISO (International Standards Organisation) for information security matters. It is not intended that Convert Insights seeks to be compliant with all aspects of the relevant ISO information security standards as this would not be appropriate in all instances. However, it is intended that Convert Insights would aspire to implement policies, standards and procedures which are consistent with key aspects of the standards.

Security Measures

What physical security measures do you have in place at your premises? In particular, what restrictions govern access to facilities storing data? Identify processes and/or controls you have in place for physical access.
We rely on Amazon Web Services who is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. Regarding the physical security measures, AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.AWS only provides data center access and information to employees and contractors who have a legitimate businessneed for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely. Details from AWS are presented here: https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

Is access given to anyone outside the organization? Will any other parties have downstream access to our data? If so, who and for what purposes? What areyour processes for assessing and monitoring data security for any third-parties with access, for example, to provide IT support? If so, are appropriate security procedures in place to manage and oversee such access?
No, access is only restricted to Convert Insights members as defined in our IT Security Policy.

Are personnel permitted to work remotely? If so what security features are in place to secure remote connectivity?
Yes, Convert Insights is a remote distributed team. Several policies are in place to secure remote connectivity:

- Acceptable Usage Policy
- IT Security PolicyWeb and Social Media Policy
- Employee Password Policy
- Open Source Software License Policy
- Privacy and Security Checklist for GDPR Compliance when selecting and installing third party software

Do you have antivirus and anti-hacking measures in place to prevent the compromising of the integrity of data or systems? If so, please describe.
Yes, antivirus is compulsory pre-requisite for any computer joining the Convert Insights network as described in our IT Security Policy.

Is there a program for identifying IT system vulnerabilities and a program for applying security patches in a timely manner? Identify processes and/or controls you have in place for vulnerability management.
We rely on AWS tools for this.Amazon Inspector automatically assesses vulnerabilities and deviations from best practices.AWS Systems Manager and specifically Patch Manager automatically apply patches in a timely manner.

Do you perform network security testing? Identify processes and/or controls you have in place for building and maintaining secure networks and systems
We have requested a Vulnerability and Penetration testing from AWS

What encryption policies do you apply to data? For example do you encrypt: portable or removable media storage that store persona data/data at rest/data in transit? Identify processes and/or controls you have in place for protecting data.
All Convert Insights laptops must have their internal hard drive encrypted.
All Convert Insights mobile devices that host Convert Insights data (email) must be protected by encryption and layered authentication where appropriate.
Where sensitive information is transmitted through a public network to an external third party the information must be encrypted first and sent via secure channels (SFTP, SSH, HTTPS, VPN etc.)

Are authentication and logical access controls, including passwords, applied to control different levels of access to information depending upon requirements and roles? Identify processes and/or controls you have in place for passwords and permissions
Yes, access to systems is based on specific roles and duties of each role and is reviewed frequently.

Are unique IDs required for all personnel? Is a policy in place to manage IDs?
Yes, all individuals have a unique user ID (end users, DBA's, network admin, programmers) for their personal and sole use so that activities can be traced to the responsible person as indicated in our IT Security Policy.

What procedures do you operate for secure destruction of systems and media used for data storage before being reused for other purposes?
N/A

Is access to data restricted to a need to know basis?
To protect data from falling into the wrong hands, it's important that Data Controllers and Data Owners (as defined in Data Management Policy) understand which users have access and why these users need access to systems and data. The decision process for users to gain access to systems and data is based on the need-to-know principle, which is that access to data must be necessary for the conduct of the users' job functions.

Are your security measures subject to any form of independent review? Do you offer annual third-party verification of any of your data security processes and controls such as an SSAE 16 report, a Service Organization Control report (SOC 2 or SOC 3 report), PCI compliance reports or ISO review reports? If so, please forward us a copy
Yes, Convert Insights Inc. is PCI-DSS compliant. Convert Insights Inc. isn't itself SOC compliant, but our datacenter providers are (AWS/Hetzner). Customers interested in SOC reports concerning the cloud infrastructure providers utilized by our services can obtain the reports directly from the respective providers.

Security Specifics

Incident Management

Do you have a formal cyber security program?
Yes, our Cyber Security Program (network, computers and data) consists of:Identify the essential elements of what is required to attain compliance or successful cybersecurity resilienceAssess: Gauge and evaluate Convert Insights state of protection mechanisms, gaps and opportunities for improvement.Develop: This step involves the set of activities required to draft and test the adoption of the cybersecurity strategy, policy and set of actions to manage cyber security. The overall set of documents include know-how, know-what knowledge on areas such as surveillance and monitoring of threats, security audits, vulnerability assessments, incident handling and reporting, risk management, business continuity and more. Train: After development, we create awareness of the Program by providing training to relevant stakeholders.Continuously monitor the internal and external environment for changes or developments.

Have you identified the key cyber security risks your organisation faces? How often do you review and update these?
Yes, we have listed the key cyber security risks, just to name a few here:Data loss or theftCompliance/regulatory incidentsSocial engineering attacksImpersonationsLack of PoliciesHuman factorBring your Own Device (BYOD)Lack of training and awarenessLack of recovery planAging infrastructurePasswordsThird party service providersHacking (DDOS, Cookies theft)These risks are reviewed and updated twice annually.

When was the last time your cyber security incident response plan ("IRP") was reviewed and updated?
May 2018

When was the last time your IRP was tested through a tabletop or simulation exercise?
This is planned for Q4 2018.

How do you log and issue alerts on relevant security events?
If a member of Convert Insights considers that a security breach has occurred, this must be reported immediately. Part 1 of the Security Breach Report Form should be completed without delay. Part 1 of the Report Form will assist in conducting an initial assessment of the incident by establishing: if a security breach has taken place; if so: what data and systems are involved in the breach; the cause of the breach; the extent of the breach (how many individuals are affected); the harms to affected individuals that could potentially be caused by the breach; how the breach can be contained. Following this initial assessment of the incident, an appropriate Lead Investigator is appointed to investigate the incident and will decide if it is also necessary to appoint a group of relevant stakeholders to assist with the investigation. The Lead Investigator will determine the severity of the incident and by completing part 2 of the Security Breach Report Form (i.e. s/he will decide if the incident can be managed and controlled locally or if it is necessary to escalate the incident to the Emergency Management Team. The severity of the incident will be categorised as level 1, 2a, 2b or 3.

Does your IRP clearly define when a security event triggers its application?
Yes. security events are closely tied to the applications that are affected.

What stakeholders are involved in your IRP?
Our Incident Response Plan involves the Emergency Management Team [EMT].The Emergency Management Team [EMT] has full responsibility for the response to and management of a major emergency. In the event of the EMP being activated, all staff will work under the direction of the EMT. Members of the EMT and staff with specific responsibilities will receive appropriate formal training in Emergency Management and related responsibilities. It is the responsibility of senior managers to ensure that staff members are aware of their responsibilities. The Chair of EMT is responsible for the overall management of emergency coordination and response for Convert Insights. Core members of EMT have specific duties as outlined in our Emergency Management Plan.

Do you have formally defined criteria for notifying us of an incident that might impact the security of their data or systems?
On the basis of the evaluation of risks and consequences, the Lead Investigator, and others involved in the incident as appropriate, will determine whether it is necessary to notify the incident to others outside Convert Insights. For example: individuals (data subjects) affected by the incident; other bodies such as regulatory bodies, the press/media; external legal advisers.As well as deciding Who to notify, the Lead Investigator must consider: What is the message that needs to be put across? In each case, the notification should include as a minimum: a description of how and when the incident occurred; what data and IT assets were involved; what action has been taken to respond to the risks posed by the incident. How to communicate the message? What is the most appropriate method of notification (e.g. are there large numbers of people involved? Does the incident involve sensitive data? Is it necessary to write to each individual affected? Is it necessary to seek legal advice on the wording of the communication?). Why are we notifying? Notification should have a clear purpose, e.g. to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.

What are your service levels for notification?
Convert Insights is obliged under the General Data Protection Regulation Article 33 to keep personal data safe and secure and to respond promptly (within 72 hours) and appropriately to data security breaches.

Does your IRP identify how your workforce internally reports an incident?
Yes, we have an internal procedure on how to report the incidents and keep them in a central place for Policies' improvement.

Does your IRP define triggers for escalation to senior management in the event of a significant incident?
Yes, in the event of an Emergency incident, Senior Management is notified.

Does your IRP address obtaining forensics and other technology services in the event of an incident?
Yes, this lies under notification section and who to notify once the incident takes place.

Does your IRP address how to carry out large scale communication exercises with affected plan members?
Yes, responsibility for managing all aspects of external communication and contact with the media following an Emergency rests with the Content Crafter Role within Convert Insights. The Content Crafter will handle all information flow to print and broadcast media following early consultation with the Emergency Management Team (EMT). An early and clear response from Convert Insights is essential to set the tone for subsequent updates.Social media will be used as one of the key communication channels. Security around the incident will be crucial to the control of information flow and message management; therefore media access must be strictly curtailed unless agreed specifically by the EMT.

Has your organisation experienced any successful cyber security attacks? Have you had data breaches in the past two years? If so how timely were they identified, what was the cause, what data was taken and how have you remediated root cause issues
No

Does your IRP require post-incident debriefing and analysis, including lessons learned and potential revisions to the plan? Have any such reviews been conducted?
Subsequent to a cyber security breach, a review of the incident by the Lead Investigator will take place to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved. The Lead Investigator will send a copy of all cyber security breach reports to the whole team and will use these to compile a central record of incidents. Convert Insights will report on incidents at least on a quarterly basis in order to identify lessons to be learned, patterns of incidents and evidence of weakness and exposures that need to be addressed. For each serious incident, the Lead Investigator will conduct a review to consider and report on the following: What action needs to be taken to reduce the risk of future breaches and minimise their impact? Whether policies procedures or reporting lines need to be improved to increase the effectiveness of the response to the breach? Are there weak points in security controls that need to be strengthened? Are staff and users of services aware of their responsibilities for information security and adequately trained? Is additional investment required to reduce exposure and if so what are the resource implications? Since we did not face any cyber security attacks, there was no need to update the Policies by lessons learnt so far, however we have a standard annual review and the Policies and Procedures are adapted to the new trends whenever needed.

What training do your staff receive in relation to the IRP and cyber security issues?
Staff Information Security and Data Protection Training Policies set out the training that Convert Insights staff will be provided with to ensure that all handling of data and IT resources is compliant with the General Data Protection Regulation (GDPR). In general training for all users cover these areas:
Security
Data Protection Principles
Data Subject Rights
Security Breaches
Privacy Notices
Additional training is provided for the Development and HR teams.
Finally, a checklist is included in the Policies with quick references to what staff need to know regarding Data and Protection and IT resources security.

Do you have a Security Incident Management policy and plan for resolving security incidents that includes identification, severity assignment, communication, resolution and testing of the plan?
Yes, our Cyber Security Program (network, computers and data) consists of:Identify the essential elements of what is required to attain compliance or successful cybersecurity resilienceAssess: Gauge and evaluate Convert Insights state of protection mechanisms, gaps and opportunities for improvement.Develop: This step involves the set of activities required to draft and test the adoption of the cybersecurity strategy, policy and set of actions to manage cyber security. The overall set of documents include know-how, know-what knowledge on areas such as surveillance and monitoring of threats, security audits, vulnerability assessments, incident handling and reporting, risk management, business continuity and more. Train: After development, we create awareness of the Program by providing training to relevant stakeholders.Continuously monitor the internal and external environment for changes or developments

Is there an Incident / Event Response team with defined roles and responsibilities?
Yes, Dionysia Kontotasiou, dionysia@convert.com

Is that team available 24x7x365?
Yes

Does the plan include procedures for notifying us of data breaches that may involve our data, systems and/or applications?
Yes

Are audit trails and logs maintained for network/system/application events to support monitoring or incident research?
Yes

Security Specifics

Continuity and Disaster Recovery

Do you have a defined Disaster Recovery Plan and/or Business Continuity Plan (BCP)?
Yes - Business Continuity is managed as part of the Emergency Management Plan to ensure seamless follow up of an emergency and continuity of services. This Plan takes into account several incidents that may be minor/localised (levels 1 or 2a) incidents or (levels 2b or 3) emergencies.
- Serious Staff Incident
- Utilities Failure - Pandemic / Serious Outbreak of Infectious Disease
- Data Network Failure
- IT Systems Failure
- Fraud
- Personal Data Security Breach
- Serious Blog/Social Network Incident
- Competitors move faster in technology
- Losing of connectivity between people because of a natural disaster
- Large lawsuit by customer
- DDOS attacks
- Financial disaster (Wall Street)
- Bus-Factor: One person does it all
- Free competitor comes in with similar standards
- Third parties that we rely on

These have been identified as the main incidents after a Pre-Mortem Analysis.

Do you have recovery strategies that assure the continued maintenance of the service level agreements with us?
Yes

Has your organization performed a detailed Business Impact Analysis (BIA) relative to the services being provided?
Yes

Have you worked to define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for the services provided?
Yes

Are alternate facilities (i.e. - data centers, office locations, etc.) used?
No

Is the capacity at the recovery location reviewed on a regular basis to ensure that adequate capacity is available in the event of a disaster?
Yes

Do the Business Continuity and Disaster Recovery plans include notification when incidents occur?
Yes

Do you test your Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) on an annual basis?
Yes

What business continuity and disaster recovery plans do you have in place? Do they address risk of loss, damage, or corruption of information arising from:Human error, Computer virus, Network failure, Theft, Fire, Flood, and Other disasters?
Business Continuity is managed as part of the Emergency Management Plan to ensure seamless follow up of an emergency and continuity of services. This Plan takes into account several incidents that may be minor/localised (levels 1 or 2a) incidents or (levels 2b or 3) emergencies.
- Serious Staff Incident
- Utilities Failure
- Pandemic / Serious Outbreak of Infectious Disease
- Data Network Failure
- IT Systems Failure
- Fraud
- Personal Data Security Breach
- Serious Blog/Social Network Incident
- Competitors move faster in technology
- Losing of connectivity between people because of a natural disaster
- Large lawsuit by customer
- DDOS attacks
- Financial disaster (Wall Street)
- Bus-Factor: One person does it all
- Free competitor comes in with similar standards
- Third parties that we rely on

These have been identified as the main incidents after a Pre-Mortem Analysis.

Are the business continuity and disaster recovery plans regularly tested? When was the last test?
Yes, Emergency Management Plan and Business Continuity are reviewed and tested at least annually. Last update was in May 2018.

Do you have data backup and systems recovery operations that are independently tested?
Yes, our cloud infrastructure (AWS) takes care of it.

Do you have a named business continuity manager with defined responsibilities and supporting resource/procedures?
Yes, our DPO: dionysia@convert.com

Do you have a Business Continuity Management structure and procedures in place?
Business Continuity is managed as part of the Emergency Management Plan to ensure seamless follow up of an emergency and continuity of services. This Plan takes into account several incidents that may be minor/localised (levels 1 or 2a) incidents or (levels 2b or 3) emergencies.
- Utilities Failure
- Pandemic / Serious Outbreak of Infectious Disease
- Data Network Failure
- IT Systems Failure
- Fraud
- Personal Data Security Breach
- Serious Blog/Social Network Incident
- Competitors move faster in technology
- Losing of connectivity between people because of a natural disaster
- Large lawsuit by customer
- DDOS attacks
- Financial disaster (Wall Street)
- Bus-Factor: One person does it all
- Free competitor comes in with similar standards
- Third parties that we rely on

These have been identified as the main incidents after a Pre-Mortem Analysis

Do you have a current and valid Business Continuity Plan? If yes, are all its requirements currently met?
Yes

Do you have a dedicated relocation/Work Area Recovery site available to you?
Yes, managed through AWS

Do you have a dedicated IT Back up/Recovery site available to you?
Yes, managed through AWS

How are your business continuity plans/provisions tested?
Emergency Management Plan and Business Continuity are reviewed and tested at least annually. Last update was in March 2020.

Is there an agreed and documented business continuity stakeholder communications process in place?
Yes

PCI Compliance

Does your organization store, transmit, process or access cardholder and/or sensitive authentication data?
- Cardholder data includes Credit Card Number or Primary Account Number (PAN), Cardholder Name, Card Expiration Date and Service code.
- Sensitive Authentication Data includes Full Track Data, CAV2/CVC2/CVV2/CID and PIN"
No

Are you compliant with Payment Card Industry (PCI) Data Security Standards (DSS)?
Yes, via Stripe payment processor

Was compliance formally validated according to PCI DSS requirements based on the volume of cardholder data stored, transmitted, processed or accessed?
Yes