PromoNow™

Secure, fast and agile solutions

for promotional deployments and consumer data safeguarding

PROMO**NOW**™

1. Service policy statement

PromoNow™ offers a secure single place of record for all aspects of promotional related activity. Campaigns are initiated, customized, monitored, fulfilled and evaluated all within the PromoNow™ enterprise cloud eco-system. Consumer data is securely segregated, need-to-know restricted and fully auditable for GDPR. Data centres are ISO27001 certified, PCI-compliant with security capability to UK government IL4 standards with Cisco ASA Firewall protection and web application firewall. Threat monitoring and vulnerability scanning with real-person experts to keep your data safe. Super-fast top tier hosting network guarantees 99.9% uptime, backed by a 24/7/365 support level agreement.

2. Collaborate and serve in real-time

Roles and privileges are defined, assigned and secured to each specific group; whether client side, agency or fulfilment partner - facilitating privacy by design whilst benefiting users to focus in on straightforward dashboard views and task actions in real-time. Campaign Managers configure promotions transparently for Campaign Clients who assess and chart performance on demand. Step-by-step screens guide Fulfilment & Handling Users to efficiently validate, dispatch, query, reject and communicate case-by-case or by-select-group functions increasing service standards and efficiency.

3. Dedicated cluster team

Each PromoNow™ instance is supported by a tri-team; named Technical Director, named Client Director and a named Service Delivery Manager. Personnel are HR Security Standard Policy vetted. All staff complete security awareness training and hold certificates in Information Security Awareness - ISO 27001:2013 (updated March 2020). Data centre staff are DBS checked. Comprehensive access logs are readily auditable. 24/7/365 Duty Manager Support comes as standard.

4. GDPR privacy by design

The seven key principles of GDPR are fundamental to PromoNow™:

- Lawfulness, fairness, transparency – privacy policy content, opt-in auditing.

- Purpose limitation – defined at setup, links privacy policy version to each PII record.

- Data minimisation – cross-check mechanic vs fields, (eg no postal = no address needed). Utilises IDs in data transfer.

- Accuracy – updateable consumer records via rectification

- Storage limitation – retention defined at setup, defaults as latest date + 6months to data-purge, right of erasure.

- Integrity & confidentiality – 'need to know' settings restrict PII data views, secure logins, database records zoned and protected to each campaign, Sql injection defences, captcha barriers, cross-site scripting protection, anti-abuse widget, tokenized unique user identifiers, multiple entry controls, IP whitelisted access restrictions, HTTPS SHA-256 TLS (Transport Layer Security). Encryption at rest of PII data. Web application firewall.

- Accountability – Auditable record of compliance, named DPO.

Registered ICO Data Controller Number: ZA720375

Special Category Data / Client Scoped Privacy Data Policy:

Sorry, we do not work on projects requiring the capture of special category personally identifiable information such as; health, race religion, sexual orientation, criminal records and trade union membership.

5. FMIT pioneers

Fast moving information technology (FMIT) practices are brand reputation critical, and an essential component of successful promotional campaigns. Change requests, from copy to mechanic configuration are tasked, actioned and completed with auditable dashboard ticketing. Continual end-to-end testing techniques throughout the development stage ensure defects are resolved early and timely. Development side tools, test browser compatibility and the UX (user experience) for device and screen resolution variants – all deployments are responsive as standard on PromoNow™.

6. L A M P web service stack

The Linux operating system, Apache HTTP server, MySQL relational database management system and PHP programming, alongside node.js, offer a proven and robust architecture with continual open-source scrutiny and improvements. You're in good company, with a proven stack that has been powering the majority of web applications for over 20 years. Used by; Facebook, Wikipedia, Slack, Yahoo! to Mailchimp and Amazon.

7. UKFast tier 3 hosting environment

PromoNow™ is hosted at UKFast's data centers, with 99.982% uptime with Redundancy N+1 - including UPS and standby diesel generators to make sure your service is always online. Purpose built environments protect PromoNow™ users to exceptional levels of both physical and virtual security at all times. You're in good company, with a proven environment provider, used by; National Rail, Metropolitan Police, Manchester City Council, LateRooms.com to the MOD and the Cabinet Office.

Tier Standards (poor to best):
T1 = 99.671% uptime, T2 = 99.749%, **T3 = 99.982% uptime**, T4 = 99.99% uptime

- PCI Compliance - commitment to safe and secure card payments and to protect you from credit card fraud, hacking. Regularly tested and constantly monitored, and to maintain a strong information security policy to protect your data.

- 100% Carbon Neutral – PromoNow™ believes in taking responsibility for our environmental impact. PAS 2060 – as a power-hungry industry, UKFast are committed to reducing their impact on the environment.

- Cyber Essentials – Government endorsed standard helping to protect PromoNow™.

- G Cloud 10 - UKFast are government approved suppliers through the G-Cloud 10 framework, with OJEU compliant hosting solutions with ease, speed and confidence.

- ISO 27001:2013 - UKFast secure web hosting to clients worldwide, offering hosting services certified to the ISO 27001:2013 standard - ensuring the security of all data. ISO27001:2013 certifies information security is taken seriously across all business operations.

- ISO 27018:2014 – provision of secure public cloud computing environments for the protection of Personally Identifiable Information (PII), certified to ISO 27018:2014 standards. ISO 27018:2014 complements much of the data processing responsibilities set out by the GDPR in its aims to protect personal data in addition to EU requirements.

- ISO 22301:2012 – provides a framework for the continual maintenance and improvement of a business continuity management system.

- ISO 9001:2015 – internal Quality Management System (QMS) - certified to ISO 9001:2015 standards - which is maintained and improved to ensure we meet the expectations of our clients.

- ISO 14001:2015 - As part of a commitment to managing operational carbon footprint, environmental standards are certified to ISO 14001:2015.

- NICEIC Electrical Contractor - This accreditation enables UKFast not only to guarantee the highest quality of electrical work, but to increase the speed in which it is carried out by having engineers onsite at data centres and across the property portfolio. UKFast take power seriously - only data centre owner and operator in the UK that is an approved NICEIC electrical contractor.

- 24/7 Automated Threat Monitoring – monitoring and defending against network threats.

- 24/7 Dedicated Linux Support – Real person monitoring and defending against network threats.

- 24/7 Managed Server – Systematic and immediate patching and application updates.

- 2 Hour Hardware Replacement SLA - In the unlikely event of unfixable server hardware failure, we guarantee that hardware will be replaced within two hours of the problem's diagnosis. Hardware is defined as the processor(s), RAM, hard disk(s), motherboard, NIC card and other related hardware included with the server.

ENDS.

Ready to get started?

Contact your agency partner,
or speak with a PromoNow™ SaaS advisor +44 20 380 555 40.

We look forward to helping and supporting your next promotional deployment.

Sincerely,

The PromoNow™ Team

Legal

PromoNow™ is a trading style of PROMOTIONS iNTERACTIVE

The team at Pi (aka PROMOTIONS iNTERACTIVE) have over 40 years of expertise in providing specialist campaign support and technology platforms within the promotions sector in the UK, Europe and beyond. World famous brands and their marketing agencies know they can call upon us to deliver with trust and integrity.

©2020 PROMOTIONS iNTERACTIVE LTD, Hersham Place Technology Park, Molesey Road, Surrey, KT12 4RZ, UK

Appendix 1: Technology SLA & Policies

Our SLA promise

24 Hour Emergency Telephone Support

We guarantee that our level-three qualified technical support team is available 24/7/365 for emergency telephone support. Whatever the time of day, we are at the end of the phone to help resolve any issues. Out of hours Duty Director on 07976 835173.

2 Hour Response and Full Report Promise

Should there be a problem with server services, rest assured that a qualified engineer will be working on the problem within 2 hours of being notified. In the rare event that your problem cannot be solved within 2 hours, we ensure that you're kept up to date by telephone until the problem is resolved.

We also provide a detailed overview of the issue and let you know when it will be resolved. Once the issue is resolved we make sure you have a full picture of what's happened. An engineer's report with full details of the issue and resolution is sent to you within 12 hours of completion.

24/7 Server Reboot

We ensure our qualified engineers are on-site at our data centres 24/7 to manage and maintain servers. So, should the need arise, we will reboot servers, physical or remote, 24-hours a day, 365 days.

Two Hour Hardware Replacement

In the unlikely event of unfixable server hardware failure, we guarantee that hardware will be replaced within two hours of the problem's diagnosis. Hardware is defined as the processor(s), RAM, hard disk(s), motherboard, NIC card and other related hardware included with the server. This guarantee excludes the time required to rebuild a RAID array and the reload of certain operating systems, processors and applications. It does not include any bespoke server hosting solutions.

Threat Monitoring and Intrusion Detection System

Built to meet high compliance standards, Threat Monitoring detects all activity across your solution, including servers, VMs and applications, providing you with an overview of any threats and vulnerabilities that put your business at risk. Secarma security engineers take actions to tackle threats 24/7.

By combining host-based intrusion detection, file integrity monitoring, intelligent blacklisting and vulnerability scanning and remediation from our in-house team, we improve the security of your infrastructure to mitigate the impact of a devastating cyber-attack.

Anti-DDoS Hosting & Protection

Every year, 17 million businesses are compromised by a Distributed Denial of Service (DDoS) attack, with 91% of those targeted experiencing downtime as a result.

Included as standard, UKFast's DDoS protection - DDoSX® - investigates attacks and generates a unique fingerprint for each attack, identifying and redirecting this traffic away from your webserver, keeping your business online and functional.

DDoS protection specialists analyse behaviour to predict DDoS attack patterns using algorithms to ensure we defeat the latest and most sophisticated attacks.

What does DDoS protection do?

- Maintained uptime, even during a DDoS attack
- An accelerated website, web application and more with our global CDN
- Create new DDoS rules, decreasing the likelihood of another attack
- Increased defence for your data and web applications

Web Application Firewall

A Web Application Firewall (WAF) is designed to protect data from hackers as they try to exploit weaknesses in application code.

These targeted attacks are disguised as genuine requests made to forms on websites - to a traditional firewall or Intrusion Detection System/Intrusion Prevention System they will appear authentic and so allow them to proceed; making them either unable to guard against these attacks or unable to offer comprehensive protection.

Once these requests get through to your application, the hacker can send a special request through your website form that will in turn release sensitive data stored on your database.

WAFs are designed to proactively protect the application layer against attempted fraud or data theft; blocking any suspicious activity. Inspecting every web request for cross-site scripting, SQL injection, path traversal and 400+ other types of attack, this protective layer aims to keep your data secure.

By combining host-based intrusion detection, file integrity monitoring, intelligent blacklisting and vulnerability scanning and remediation from our in-house team, we improve the security of your infrastructure to mitigate the impact of a devastating cyber-attack.

- Safeguard against application layer (layer 7) attacks
- Safeguard from all inbound and outbound traffic, for all web applications, by examining traffic from both directions to ensure that your database doesn't release any information that it shouldn't

- Inbound traffic monitoring and report production, illustrating the level of suspicious traffic targeting your site
- Reduced financial and reputational risk, ensuring that your business offers the highest level of security for your clients
- A specialised team of security experts overseeing your WAF and continually identifying new rules to better protect your application
- 24/7/365 UK-based support from a dedicated team of experts

Sitting directly on the application layer your WAF examines every HTTP request/conversation that comes through to your database server - and applies a set of bespoke rules set to filter out illegitimate traffic.

Custom rule sets are managed by security experts and exist for a wide range of applications. New rules can continually be applied to keep pace with new and emerging threats. Our WAF also proactively observes your genuine traffic, creating bespoke rules to ensure that any legitimate traffic is not blocked.

With no changes to your existing set up and an additional layer or protection, WAFs ensure that your site provides the upmost protection for your clients and also allows you to comply with PCI 6.6.

Our high performance WAF solution is designed to safeguard against a number of vulnerabilities, including:

- Cross-site scripting (XSS)
- Injection flaws (SQL injection)
- Malicious file execution
- Insecure direct object reference
- Cross-site request forgery (CSRF)
- OS command injections
- Information leakage

- Improper error handling
- Application denial of service
- Broken authentication
- Session management
- Insecure cryptographic storage
- Insecure communications
- Failure to restrict URL access

Risk Assessment of Problems, Privacy and Security (RAPPS) Traffic Lighting

Our unique RAPPS traffic light system provides a recognizable framework to work through known risks and discover new ones. A simple and easily understandable traffic light signal is applied from inception.

Secure Software Development Lifecycle (SDLC)

To meet the demands of FMIT we adopt an agile approach to development from inception to decommission. The project timeline allocates resource, time and quality assurance through each phase:

1. Planning & Requirements + RAPPS
2. Architecture & Design + RAPPS
3. Test Concept Planning + RAPPS
4. Coding + RAPPS
5. User Testing, Security Testing & Results + RAPPS
6. Release & Maintenance + RAPPS
7. Close & Data Purge
8. Decommissioning

Our RAPPS (Risk Assessment of Problems, Privacy and Security) overlay is an ever-present traffic light signal throughout each stage. At stage 5 testing each deployment is subjected to Secarma vulnerability scanning and other third party assessment tools.

100% UKFast Connectivity Guarantee

We know how essential uptime is to your business, which is why we offer you a 100% connectivity guarantee.

- Because each circuit in every regional POP (internet access point) is connected to a different router, we guarantee continuous service, even in the event of a total loss of a router and/or circuit.
- Each POP has a redundant UPS (uninterruptable power supply) system, so should either UPS fail or be taken out of service for maintenance, your connection remains unaffected.
- Ensuring maximum network performance and reliability, we operate on the main hub between Manchester and London, and with significant duplication of connectivity, we promise to always deliver a resilient, constant route to the internet.
- We carry out comprehensive round-the-clock monitoring of our network routers, circuits and power. So, if there's a network issue, we can act immediately to resolve it without disrupting your business.

Fair scope

We understand quotes are often required prior to supply of complete visuals, in 'quoting blind' we promise to make our best efforts to meet and interpret visuals to industry best practice, and within the constraints of the shifting sands involved in mobile responsiveness web design. Designs should contain consistent headers and footers across the page templates. For effective responsiveness to mobile first, key elements work best centralized and with the flex in the design for them to be 'stacked' in portrait views.

Supplying artwork?

We work with Adobe Photoshop, XD, and Illustrator. Files must contain all layers, with assets and elements cleanly cut and isolated. For online production we recommend pages are based upon a **typical width of 1920pixels, with a screen height / fold / scroll guide of 1080px**. Where possible save and downsize assets accordingly, particularly if using art-boards. We will optimize assets if necessary to ensure online speed usability, but as a rule of thumb a we are talking KBs, not MBs and certainly not GBs.

We're happy to work with whatever your preference for file transfers, **please prefix file names with a version control number**; WeTransfer, YouSendIt, DropBox. GoogleDrive, etc.

If your design includes custom / proprietary fonts these need to be packaged, licensed and supplied to us appropriately with a full webfonts kits (all browser file types are required: .ttf, .otf, .woff, .woff2, .eot). We are licensed for Adobe Fonts, and of course any Google Fonts.

We know there will be final copy changes and edits, no problem we're happy to do those, working with a copy-deck is a great idea and **please label and prefix the file with a Version control number**, eg V2 – XXXX – approved copy terms.

If your scope includes email templates, as a general rule we are happy to design and develop these based upon the web design assets. If you are designing them width is all important, we recommend a vertical layout, with a width between 500 to 650 pixels. With the key message high up the design, and text copy areas to explain the content if the user has chosen not to download and view images within the email. Many email client browsers are very old, as such fonts used must be web-safe standard fonts Arial, Arial Black, Arial Narrow, Comic Sans, Courier New, Georgia, Impact, Tahoma, Times New Roman, and Verdana. Play it safe with a body copy font size of 14 pixels and 22 pixels for title.

*By supplying any assets, imagery, photography and video you are expressly indemnifying us against any copyright infringements and/or liability.

*Agreed timelines to LIVE deployment are based upon production commencing upon receipt of all approved deigns and layouts.

*Any custom/proprietary fonts required but not supplied will be re-charged at cost + £40 admin per font.

Fair scope

Privacy Policy Notice

This statement discloses the privacy practices for Promotions Interactive Ltd, our website, and how we safeguard user data.

We take your privacy and security very seriously. Users agree to their information being held and processed in accordance with GDPR. Specifically; personally identifiable data will only be used for the purposes of this platform by us and any appointed Data Sub-Processor. Data may be transferred out of the EEA, data will be safely deleted within a reasonable time once our relationship with you has come to an end. Click here to learn more about your rights under GDPR, including data rectification, erasure, processing and lodging a complaint. By signing up or logging in and/or continuing to use our website you are accepting our privacy & security policy and our terms of service. This statement discloses the privacy practices for Promotions Interactive Ltd, our website, and how we safeguard user data.

Controller: Promotions Interactive Ltd is the controller and responsible for your personal data (collectively referred to as "PIL", "we", "us" or "our" in this privacy policy).

If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact the Data Privacy Team using the details set out below.

Contact details: If you have any questions about this privacy policy or our privacy practices, please contact us in the following ways:

Registered data controller number ZA720375
Full name of legal entity: Promotions Interactive Ltd
Email address: dataprivacy@promotionsinteractive.com
Postal address: Hersham Place Technology Park, Molesey Road,
Walton-on-Thames, KT12 4RZ, United Kingdom

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Personal information: We intend to give you as much control as possible over your personal information. In general, you can visit Promotions Interactive on the Web without telling us who you are or revealing any information about yourself. There are times, however, when we may need information from you, such as your name and address. It is our intent to let you know before we collect personal information from you on the Internet. We also make use of cookies, this helps our website remember some details about you, they're commonly used to make it easier for you online.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

• Identity Data includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.

• Contact Data includes billing address, delivery address, email address and telephone numbers.

• Financial Data includes bank account and payment card details.

• Transaction Data includes details about payments to and from you and other details of products and services sold and purchased by supplier members to our operator members.

• Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.

• Profile Data includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.

• Usage Data includes information about how you use our website, products and services.

• Marketing and Communications Data includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share Aggregated Data such as statistical or demographic data for

any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

Our policy is not to work on projects requiring the capture of special category, sensitive personally identifiable information, such as; health, race religion, sexual orientation, criminal records and trade union membership. This website is not intended for children and we do not knowingly collect data relating to children.

If you choose to give us personal information via the Internet that we or our business partners may need to correspond with you, process an interaction or provide you with a subscription, for example it is our intent to let you know how we will use such information. If you tell us that you do not wish to have this information used as a basis for further contact with you, we will respect your wishes. We do keep track of the domains from which people visit us. We analyse this data for trends and statistics, and then we discard it.

Information security and quality: We intend to protect the quality and integrity of your personally identifiable information. We have implemented appropriate technical and managerial procedures to maintain information that is accurate, current, and complete. Data centres we use are ISO27001 certified. We will make a sincere effort to respond to your requests to correct personal information inaccuracies in a timely manner. We are a fully registered user under the Data Protection Act.

Business relationships: The Promotions Interactive site contains links to other Web sites. Promotions Interactive is not responsible for the privacy practices or the content of such Websites.

Cookies: There are various technologies, including one called "cookies", which can be used to provide you with tailored information from a Web site. A cookie is an element of data that a Web site can send to your browser, which may then store it on your system. Some Promotions Interactive pages use cookies or other technologies so that we can better serve you when you return to our site. You can set your browser to notify you when you receive a

cookie, giving you the chance to decide whether to accept it. For more information, please e-mail: dataprivacy@promotionsinteractive.com.

Promotions Interactive is also supporting the development of some technologies that will let you manage and control the release of your personal information wherever you go on the Internet.

Questions regarding this statement should be directed to dataprivacy@promotionsinteractive.com.

Control Statements

1. Protective Monitoring
Data centre perimeter security exceeds ISO27001 standards; including 24 hour security guards, CCTV, 2-factor entry access controls. Within the network, Secarma threat monitoring, web application firewalls and DDoSX, combined with real-person expert monitoring identify and secure against threats in real-time 24/7. Logs are generated, stored and monitored according to Log Management and Forensic Readiness.

2. Anti-malware
All user clients (Mac and Windows) and LINUX servers on the network run endpoint protection. Automated routines check for latest updates and deploy automatically on timed schedules. Where signatures are released to address a critical threat, the updates can be deployed at short notice and outside of normal schedules.

3. Vulnerability scanning
Vulnerability scans are performed monthly or on request by the Network Security team using a dedicated Secarma security service running up-to-date plugins via a business subscription. Scan results are distributed to operational teams for remediation according to criticality, based on the Common Vulnerability Scoring System (CVSS). The Technical Director will oversee the remediation of Critical and High vulnerabilities.

4. Threat monitoring
Built to meet high compliance standards, Threat Monitoring detects all activity across your solution, including servers, VMs and applications, providing you with an overview of any threats and vulnerabilities that put your business at risk. Secarma security engineers take actions to tackle threats 24/7.

5. Software versions

Where possible the Company will run the latest stable version of software, and no older than the previous version provided that it remains supported, in order to maintain stability, supportability and security. Where compatibility issues prevent running the latest version, we will prioritise upgrading or replacing the component causing the compatibility issue, and the residual risk will be documented and kept under review. Where legacy systems have to be tolerated, reference should be made to guidance on securing obsolete systems.

6. Server patching

All servers are included in a rolling patch schedule managed by UKFast. As a leading UK data centre operator, UKFast Plc operate top tier, ISO27001 accredited environments, with clients including government, banks and other enterprises. Where patches are released to address a critical vulnerability, they can be deployed at short notice and outside of normal schedules.

7. Application patching

Applications should have all critical or security patches applied, application owners decide on a case by case basis whether to implement functional patches, low risk patches are implemented automatically.

8. Firmware patching

Where possible the Company will run the latest stable version of firmware, and no older than the previous version provided that it is supported, in order to maintain stability, supportability and security. Where compatibility issues prevent running the latest version, the Company will prioritise upgrading or replacing the component causing the compatibility issue.

9. Encryption

As standard we encrypt your data in transit using secure TLS cryptographic protocols and SSL certificates. PII data is also encrypted at rest.

10. Security policies

We maintain and regularly review and updates our information security policies, at least on an annual basis. Employees must acknowledge policies on an annual basis and undergo additional data information and security awareness training.

Compliance

Failure to comply with this procedure could result in action in line with the Company's Disciplinary Procedure or Capability Procedure.

Compliance checks will be undertaken by the Company's Information Governance functions. The results of compliance checks, their risk assessment and their remediation will be managed by the Information Security Board.