eighty20 Risk Systems

e20 Safety Portal

General Data Protection Regulations Policy and Terms – April 2018

Eighty20 Risk Systems Ltd. Registered in England No. 8384880. VAT No. 157361502

Suite2, 1 Bridgewater Road
Walkden
Manchester
M28 3JE
office@eighty20risk.com

Section 1. Policy and Clarification

GDPR Statement

At Eighty20, we've long seen consistency, certainty, and compliance around privacy and data protection as a win-win for businesses and consumers alike. With the General Data Protection Regulations (GDPR) coming into effect on May 25 2018, Eighty20 is ready to tackle the GDPR challenge/topic and expects limited impact of the new regulation, if any, on our clients' and partners' ability to work with Eighty20.

The GDPR aims to modernise the EU legal system regarding data, strengthen individuals' rights, and improve the clarity and coherence of the EU rules.

We know that our clients have a lot of questions around the implications of the GDPR legislation, especially when it comes to the different types of data collection.

The GDPR establishes a clear distinction between sensitive personal data and non-sensitive personal data. Since Eighty20 only collects non-sensitive personal data in the form of client entered forms and processes, we are very familiar with those distinctions. Here is how all this data is categorized by the GDPR and the common questions that businesses need to know about when it comes to data management:

Firstly, what is "Personal Data" as defined by the GDPR?

Personal data is anything that contains:

- Directly identifying information such as a person's name, surname, phone numbers, etc.
- Generic data or non-directly identifying information, which does not allow the direct identification of users but allows the singling out of individual behaviours (for instance to serve the right advertisement to the right user at the right moment). This is not an area we are in any way active in, nor will be seeking to do so at any time in the future.

The GDPR establishes a clear distinction between directly identifying information and pseudonymous data. The GDPR encourages the use of pseudonymous information and expressly provides that "the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations". Eighty20 does not directly collect any personal data, rather our clients do so as part of the usage of the platform.

What is "sensitive data" as defined by GDPR?

Sensitive data is any data that reveals:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership

- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health or a natural person's sex life and/or sexual orientation

By nature, the data that Eighty20's clients collect does not qualify as sensitive data as defined by the GDPR. On our side, Eighty20 does not collect any such data (we do not target adverts or services to client-side end users based on use of our system or its data). We would also actively discourage clients from holding any sensitive data on our system at any time.

What type of personal, non-sensitive data does Eighty20 collect?

When working with Eighty20, our clients need only access to pseudonymous data. This generic data includes:

- Work based only email addresses
- Any other technical identifiers that allow Eighty20 to single out group and trend risk behaviour without directly identifying the individuals – e.g. accident trends or action management status

Legitimate Interest and Unambiguous Consent

We do not collect any data intended for marketing purposes now or in the future. We do not currently see any direct requirement for consent from our side of the process. We would actively encourage our clients (controllers…see DPA below) to communicate such a requirement to their own employees / end users however. We will however, to ensure compliance and to be especially diligent, every user of the system will be asked for explicit consent to use the system for its intended purposes. This will include existing users of the system to ensure completeness in approach.

Our strong privacy-by-design practices provide a solid foundation to immediately address all GDPR requirements. While our clients and partners are responsible for providing comprehensive information to their users, our services involve a shared responsibility across our network. Eighty20's long-standing expertise in data protection and user privacy prove that, with proper information and control tools, we can effectively prepare our clients and partners to tackle this GDPR challenge.

Section 2. Data Processing Agreement

Data Processing Agreement (DPA)

The following DPA is entered into between Eighty20 and the Customer and is incorporated into and governed by the terms of the client agreement signed at the time of commencement. This clarifies the various roles and expectations in the agreement and details who is responsible for what.

1. Definitions

Any capitalised term not defined in this DPA shall have the meaning given to it in the Customer Terms.

"Customer Terms"	means the agreement between us and the Customer for the provision of the Services;
"Controller"	means the Customer;
"Data Subject"	shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (as amended from time to time, or replaced by subsequent legislation);
"DPA"	means this data processing agreement
"Personal Data"	shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (as amended from time to time, or replaced by subsequent legislation);
"Processor"	means us;
"Security Documentation"	means the security documents made available by the Processor to the Controller; contained in section 3 of this document
"Standard Contractual Clauses"	means the EU model clauses for Personal Data transfer from controllers to processors c2010-593 - Decision 2010/87EU;
"Sub-Processor"	means any person or entity engaged by us (including a Subsidiary) to process Personal Data in the provision of the Services to the Customer.

2. Purpose

The Processor has agreed to provide the Services to the Controller in accordance with the terms of the Customer Terms. In providing the Services, the Processor shall process Customer Data on behalf of the Controller. Customer Data may include Personal Data. The Processor will process and protect such Personal Data in accordance with the terms of this DPA.

3. Scope

In providing the Services to the Controller pursuant to the terms of the Customer Terms, the Processor shall process Personal Data only to the extent necessary to provide the Services in accordance with both the terms of the Customer Terms and the Controller's instructions documented in the Customer Terms and this DPA.

4. Processor Obligations

The Processor may collect, process or use Personal Data only within the scope of this DPA.

The Processor confirms that it shall process Personal Data on behalf of the Controller and shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not process the Personal Data except on instructions from the Controller.

The Processor shall promptly inform the Controller, if in the Processor's opinion, any of the instructions regarding the processing of Personal Data provided by the Controller, breach any applicable data protection laws.

The Processor shall ensure that all employees, agents, officers and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of the Personal Data and are contractually bound to keep the Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by the terms of this DPA.

The Processor shall implement appropriate technical and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

The technical and organisational measures detailed in the Security Documentation shall be at all times adhered to as a minimum-security standard. The Controller accepts and agrees that the technical and organisational measures are subject to development and review and that the Processor may use alternative suitable measures to those detailed in the attachments to this DPA provided that such updates and modifications do not result in the degradation of the overall security of the Services.

Where Personal Data relating to an EU Data Subject is transferred outside of the EEA it shall be processed only by entities which: (i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) have entered into Standard Contractual Clauses with the Processor; or (iii) have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

Taking into account the nature of the processing and the information available to the Processor, the Processor shall assist the Controller by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights and the Controller's compliance with the Controller's data protection obligations in respect of the processing of Personal Data.

5. Controller Obligations

The Controller represents and warrants that it shall comply with the terms of the Customer Terms, this DPA and all applicable data protection laws.

The Controller represents and warrants that it has obtained any and all necessary permissions and authorisations necessary to permit the Processor, its Subsidiaries and Sub-Processors, to execute their rights or perform their obligations under this DPA.

The Controller is responsible for compliance with all applicable data protection legislation, including requirements with regards to the transfer of Personal Data under this DPA and the Customer Terms.

The Controller has their own obligations to implement their own appropriate technical and organisational procedures to protect Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

The Controller shall take steps to ensure that any natural person acting under the authority of the Controller who has access to Personal Data does not process the Personal Data except on instructions from the Controller.

The Controller may require correction, deletion, blocking and/or making available the Personal Data during or after termination of the Agreement. The Processor will process the request to the extent it is lawful and will reasonably fulfil such request in accordance with its standard operational procedures to the extent possible.

The Controller acknowledges and agrees that some instructions from the Controller, including destruction or return of data from the Processor, may result in additional fees. In such case, the Processor will notify the Controller of such fees in advance unless otherwise agreed.

6. Sub-Processors

The Controller acknowledges and agrees that: (i) Subsidiaries and partners of the Processor may be used as Sub-processors; and (ii) the Processor and its Subsidiaries and partners respectively may engage Sub-processors in connection with the provision of the Services.

All Sub-processors who process Personal Data in the provision of the Services to the Controller shall comply with the obligations of the Processor similar to those set out in this DPA.

Where Sub-processors are located outside of the EEA, the Processor confirms that such Sub-processors: (i) are located in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) have entered into Standard Contractual Clauses with the Processor; or (iii) have other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield or Binding Corporate Rules.

If the Controller objects to a new or replacement Sub-processor the Controller may terminate the Customer Terms with respect to those Services which cannot be provided by the Processor without the use of the new or replacement Sub-processor. The Processor will refund the Controller any prepaid fees covering the remainder of the Term of the Customer Terms following the effective date of termination with respect to such terminated Services.

7. Liability

The limitations on liability set out in the Customer Terms apply to all claims made pursuant to any breach of the terms of this DPA.

The parties agree that the Processor shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of the DPA, subject to any limitations on liability set out in the terms of the Customer Terms.

The parties agree that the Controller shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Subsidiaries as if such acts, omissions or negligence had been committed by the Controller itself.

The Controller shall not be entitled to recover more than once in respect of the same claim.

8. Audit

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.

Any audit conducted under this DPA shall consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of the Controller, the Controller may at its own expense conduct a more extensive audit which will be: (i) limited in scope to matters specific to the Controller and agreed in advance with the Processor; (ii) carried out during UK business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iii) conducted in a way which does not interfere with the Processor's day-to-day business. The Processor may charge a fee (based on its reasonable time and costs) for assisting with any audit. The Processor will provide the Controller with further details of any applicable fee, and the basis of its calculation, in advance of any such audit.

This clause shall not modify or limit the rights of audit of the Controller, instead it is intended to clarify the procedures in respect of any audit undertaken pursuant thereto.

9. Data Deletion

The Controller will enable the Processor to delete Personal Data using the functionality provided by the Service. For certain deletions, a recovery feature is offered by the Processor to enable recovery from accidental deletions for up to 30 days. This may be overridden by the Processor. After any recovery period, the Controller will permanently delete the Personal Data from the live systems.

On termination, the Controller has the option to request the return or deletion of Personal Data. This request must be made within 14 days of termination. The Processor will make the data available for download by the Controller in a machine-readable format. Thereafter the Processor will permanently delete the Personal Data from the live systems in any event.

Following permanent deletion from the live systems, partial data reside on the Processor's archival systems for a period of up to 35 days. If requested by the Controller, the Processor may be able to assist with recovery of partial data from these archives during this period. A fee will be charged for this service.

10. Notification of Data Breach

The Processor shall notify the Controller without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to any Personal Data ("Data Breach").

The Processor will take all commercially reasonable measures to secure the Personal Data, to limit the effects of any Data Breach and to assist the Controller in meeting the Controller's obligations under applicable law.

The Processor's notification of, or response to, a Data Breach under this Section 10 will not be construed as an acknowledgement by the Processor of any fault or liability with respect to the Data Breach.

The Processor will not assess the content of the Controller's data in order to identify information subject to any specific Controller data breach. Controller is solely responsible for complying with data breach notification laws applicable to the Controller and fulfilling any third party notification obligations related to any Data Breaches.

11. Compliance, Cooperation and Response

In the event that the Processor receives a request from a Data Subject in relation to Personal Data, the Processor will refer the Data Subject to the Controller unless otherwise prohibited by law. The Controller shall reimburse the Processor for all costs incurred resulting from providing reasonable assistance in dealing with a Data Subject request or assisting the Controller in complying with its duties. In the event that the Processor is legally required to respond to the Data Subject, the Controller will fully cooperate with the Processor as applicable.

The Processor will notify the Controller promptly of any request or complaint regarding the processing of Personal Data, which adversely impacts the Controller, unless such notification is not permitted under applicable law or a relevant court order.

The Processor may make copies of and/or retain Personal Data in order to comply with it's legal or regulatory requirement including, but not limited to, retention requirements.

The parties acknowledge that it is the duty of the Controller to notify the Processor within a reasonable time, of any changes to applicable data protection laws, codes or regulations which may affect the contractual duties of the Processor. The Processor shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the parties agree that amendments are required, but the Processor is unable to accommodate the necessary changes, the Controller may terminate the part or parts of the Services which give rise to the non-compliance. To the extent that other parts of the Services provided are not affected by such changes, the provision of those Services shall remain unaffected.

The Controller and the Processor and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA.

The parties agree that the Processor will be entitled to charge the Controller additional fees to reimburse the Processor for its staff time, costs and expenses in assisting the Controller, when the Controller requests the Processor to provide assistance pursuant to this DPA. In such cases, the Processor will notify the Controller of its fees for providing assistance, in advance.

12. Term and Termination

The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

13. General

This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

This DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

Section 3. Data Security

Security & Infrastructure

The most important commitment we have is to the security of your data.

This commitment touches every part of our infrastructure, our product, and our corporate policies, and addresses:

1. **Encryption**
2. **Backups**
3. **Redundancy**
4. **Infrastructure**
5. **Policies**
6. **E20 Features**

1.0 Encryption

As example, if you encrypted this sentence it may look like this:

8WAtp8nUEOrzSu67t9tGITEzIdgr6huIpXqofo0rv2w9y3DzSu67A=

Any encrypted data must be decrypted in order to be read. By encrypting your data we're ensuring that only authorised parties (that's you!) can read it.

- Encryption in transit - We encrypt all data as it moves between our servers and your web browser. Our API is fully encrypted so every request to view or update your records automatically encrypts that data behind the scenes.
- Encryption at rest - We encrypt all data that's stored on our servers. This includes both the records stored in our databases and search indexes as well as any files and images you've uploaded to your E20 database.
- Bank-level Encryption - We use both SHA-256 and AES-265 encryption, the strongest encryption available. This is the same level of encryption that banks use.

2.0 Backups

We store multiple copies of every change ever made to your database in multiple locations.

Whether you accidentally delete a single record, or your team delete the entire database again when you weren't looking -- we'll be able to find a backup and restore it.

Restoring from a backup may incur additional fees from our side.

- Active Backups - All recent versions of your records are stored in active databases that can be found and retrieved almost instantly. The number of changes stored in active backups are based on the subscription plan.

- Archives - Older versions of your records are stored in longer term archives. Restoring from these archives can take much longer but they serve as a great long-term backup.

- Encrypted & Redundant - Both our active back-up and archives use the same redundancy and encryption as your database. This means even your backups will be completely secure and reliable.

- Manual Backups – E20 includes export features so you can back up your data at any time. This will give you a CSV file of the data within the object you're exporting. We may need to carry out this export on your behalf. There would not be any fee involved for this service unless such an export involves moving to a different service provider who expects our assistance in using the data.

3.0 Redundancy

A system with high redundancy means that there's no single point of failure. If any one component goes down, a redundant component can step right in with no noticeable difference.

Multiple Databases - We mitigate database failures by storing your data in multiple databases, so if one database goes down the other databases can pick up the slack.

Each change made to your database immediately propagates to these redundant versions.

Multiple Locations - We mitigate location failure by storing the extra databases in different geographic locations.

4.0 Infrastructure

We use Amazon Web Services to power everything that Eighty20 has to offer. 1/3 of all Internet users visit a site hosted by Amazon Web Services each day. As an Eighty20 customer you inherit all the best practices of AWS policies, architecture, and operational processes.

Amazon Web Services is considered the industry leader in cloud services and is trusted by organizations like DOW Jones, Pfizer, and the CDC. Amazon's secure data centres enable the redundancy and scaling that equates to a secure and reliable service for your E20 database.

- Compliance - AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals.

- Amazon has achieved compliance with the strictest compliance programs.

- DDoS Mitigation - AWS provides a robust platform that is not only pre-built to mitigate some attacks, but it also allows us to react quickly to spread out impact if there is an attack.

- We've also added safeguards to underlying servers as an additional level of protection.

- Built in Redundancy – E20 uses AWS features like Auto-Scaling and Elastic Load Balancing to ensure that our production systems remain online and traffic is always routed to healthy instances.

- We continuously replicate your data and have it ready to bring online if any primary nodes fail.

- Geographic Distribution - Amazon operates data centres all over the world, adding redundancy and scaling to your data and backups.

- SOC 3 and ISO 27001 Certified – E20 is automatically certified for many stringent security standards by using AWS as its infrastructure.

- Firewalls - We use firewalls to protect every virtual server, database, and load balancer to ensure that only authorized traffic is accessing those resources.

5.0 Policies

Security doesn't stop with infrastructure. Without the right polices around privacy and access your data can still be susceptible to human error or compromise.

The same amount of attention to infrastructure and technology needs to be allocated to the people and policies responsible for running that technology.

We've carefully implemented security policies around your data's privacy and about how the Eighty20 team can access that data.

5.1 Privacy Policies

This entire document details our approach to GDPR compliance. This particular section specifically details our general approach to privacy whilst using E20.

- Privacy - We maintain a privacy policy that outlines our commitment to respecting your privacy and the privacy of the information in your account.

- Cookies and Traffic Data: Cookies are small text files that are stored on your computer when you visit a website. They are not harmful and do not identify you personally. Cookies are transferred from our products or services and stored on your computer's hard drive. We use cookies to help us provide you with a personalised service and also to help make our products and services a better experience for you. We use the following types of cookies within our products and services:

    1. Strictly necessary
       These are cookies which are needed for our products or services to function properly. For example, these cookies allow you to use your log in details to access our product so that we can identify you from the log in details you use.

2. Functionality
   These cookies allow our products and services to remember choices you make (such as your user name) and provide enhanced, more personal features. They may also be used to provide services you have asked for. The information these cookies collect may be anonymised and they cannot track your browsing activity on other websites.

3. Session Cookies
   These are temporary cookies which are deleted when you close your browser or leave your session in the product or service. We use session cookies in our product or service to identify and track users. Our session cookies may also contain your customer account number, company name and email address. We may also use session cookies and similar technologies in our products or services from time to time where this enables us to offer you certain features of the product or service or where it may help us to improve the product or service.

4. Persistent Cookies
   Persistent cookies enable our product or service to "remember" who you are and to remember your preferences (i.e. your cookies preferences). Persistent cookies will stay on your computer or device after you close your browser or leave your session in the product or service.

5. How to disable cookies or change your cookie preferences
   You may be able to configure your browser to restrict cookies or block all cookies if you wish, however if you disable cookies you may find this affects your ability to use certain parts of our products or services.

- Ultimately, the data in your account is not accessible to anyone, unless you make it accessible.

- Data Ownership - you are the sole owner of your data (see above definitions relating to Data Controller) and completely responsible for it.

- Eighty20 have no ownership of your data and can make no claims on it as long as you are following the terms of agreement.

- You simply are licensing the usage of the E20 software platform (which you do not have any ownership claims to).

5.2 Access Policies

- VPN Access - All access by Eighty20 employees (Processors) to customer data (Controllers) is governed by a secure virtual private network. This access is monitored and can be revoked at any time, so even a stolen laptop presents no privacy risks.

- Access Logging - Every access request to your data by Controllers employees is logged and time-stamped. We can confirm exact access by the Eighty20 team to any data in the unlikely case that this log is needed.

5.3 Team Policies

- NDA and Confidentiality - Each Eighty20 employee signs non-disclosure and confidentiality agreements that provide legal backing for our obligation to keep your data private and confidential.

- Training - Each Eighty20 employee undergoes training and instruction on data access and privacy and how to securely handle customer requests for account or billing access.

- Support Access - The Eighty20 team will sometimes need to access your data for support services. We only do this at your request and when necessary to resolve the issue to your satisfaction.

6.0 E20 Features

- Password Protection - Password protect your apps with encrypted password technology, so that only authenticated users can access it. You can configure multiple registration options for adding new users.

- Roles & Permissions - Assign roles for your users and define exactly which permissions each role has.

- Each page in your interface can be authorised for specific roles.

- Record Level Security – E20 is Designed so that each logged-in user can only access the records that are connected to them.

- Password Encryption - All user passwords are double encrypted and hashed with a salt, which prevents dictionary attacks and adds an extra layer of security.

- Version Tracking – E20 stores every change to every record, whether that happened through your app, directly in the builder, or through the API.

- Secure Files - Option to store files behind your logins so only authenticated users can view and download those files.

- IP Blocking - Optionally restrict access to your app to specific IP addresses or IP blocks.

- Data Encryption - All data displayed in your app and updated back to the database is encrypted and secured with SSL.

Websites (portals) hosting E20 from Eighty20.

If you have a website portal from Eighty20 to host your application, it will be built on the Squarespace Platform. Squarespace is an HTTP2 CMS ensuring state of the art performance and multithreaded concurrent loading of webpages that render with unprecedented speed. All Eighty20 supplied portal websites have TLS (SSL) enabled and are now delivered faster through the HTTP/2 protocol.

With HTTP/2, Squarespace and Eighty20 are continuing to push the web forward. HTTP/2 is already supported by the most current releases of Chrome, Edge, Internet Explorer, Safari, and Firefox. TLS needs to be enabled on Squarespace websites to utilize HTTP/2 as there aren't any browsers that currently support HTTP/2 over an unencrypted connection.