WHITE PAPER

Q2 Data Protection and Privacy

Data privacy laws have recently been enhanced to allow additional and more stringent data protection for individuals. As a result, companies are now subject to new requirements, which raise the bar above current privacy practices. The purpose of this white paper is to illustrate the measures implemented by Q2 Software, Inc. ("Q2") which are designed to maintain compliance with the EU General Data Protection Regulation ("GDPR") and the California Consumer Protection Act ("CCPA") among other applicable privacy laws (collectively referred to as the "Privacy Regulations").

With GDPR now in effect and CCPA effective as of January 1, 2020, Q2 understands the importance of complying with the Privacy Regulations in every phase of product development and Q2's day-to-day operations. Q2 prides itself on being proactive about data privacy and ensuring the strong implementation of verified privacy and security practices to provide its customers with the transparency they deserve.

Q2 is fully aware of the many changes GDPR and CCPA may bring for all organizations and that is why it is critical to ensure all collection and processing of personal data by Q2 is compliant with the various Privacy Regulations.

Overview of the GDPR

GDPR is an EU regulation that establishes a legal framework to protect the personal data of EU residents. It applies to all organizations doing business with individuals in the EU. Organizations that are established in the EU, as well as organizations that process the personal data of EU residents (even if not based in the EU), are required to comply with GDPR.

GDPR aims to bring privacy/data protection laws across Europe in accordance with the drastic technological changes over the past twenty years. GDPR introduces new obligations and liabilities on organizations that handle personal data. GDPR also sets forth a number of rights for Data Subjects.

Overview of CCPA

Due to the evolution and significance of how companies apply their data privacy practices, a new sense of urgency has been created as to how each company approaches data privacy in the U.S. California is one of several states to lead the way on consumer privacy and security protections, including the passing of CCPA. CCPA's objective is to guarantee strong protection for the personal data of individuals and applies to businesses that collect, use, or share consumer data, regardless of how the information was obtained.

Q2 Controls and Internal Practices

Q2 takes comprehensive measures to protect its infrastructure, network, and applications. Q2 also requires mandatory training of all employees in security and privacy practices to ensure that a culture and expectation of privacy is at the forefront of all Q2 practices.

- **Training**
  An integral part of protecting personal data requires building and growing a culture of security and privacy awareness. Q2 employees and contractors are required to agree to security policies prior to obtaining system access. Employees also take part in mandatory security and data privacy training, each year.
- **Encryption**
  Q2 adheres to a strict set of data encryption standards and will ensure these standards are followed by all employees and contractors working on behalf of Q2.
- **International Data Transfers**
  Q2 provides strong contractual guarantees around the privacy of its services and relies on EU Model Contract Clauses to cover international transfers of personal data.
- **Data Protection Officer**
  Q2 has retained a Data Protection Officer (DPO) who is responsible for data protection activities and implementation measures within Q2.

Third Parties Working for Q2

On occasion, Q2 utilizes third parties to perform services on its behalf in relation to the Q2 services which often allows such third parties to have access to personal information. These third parties will only be granted access to personal data, to perform tasks on Q2's behalf and in compliance with our Privacy Policy and privacy protocols. Q2 will remain responsible for their handling of all personal information on its behalf. Every such third party goes through an internal review process, which includes security, compliance, and legal reviews to evaluate their ability to meet Q2's data protection commitments and requirements.

Documentation

The Privacy Regulations contain explicit provisions about documenting processing activities. Q2 must maintain records on several things such as processing purposes, data sharing and retention. Q2 may be required to make the records available to the relevant regulatory authorities on request.

Q2 Documentation Protocols

- Where Q2 is a controller for personal data, Q2 maintains documentation in a manner consistent with the Privacy Regulations.
- Where Q2 is processor for personal data, Q2 maintains documentation in a manner consistent with the Privacy Regulations.
- Q2 conducts regular reviews of the personal data processed and updates documentation accordingly.

Data Protection by Design

In accordance with the Privacy Regulations, Q2 has a general obligation to implement technical and organizational measures designed to show that Q2 has considered and integrated data protection into its processing activities. In order to address this measure and accurately assess any potential exposure of personal data, Q2 carries out a Data Protection Impact Assessment ("DPIA") when using new technologies and the processing is likely to result in a high risk to the data rights of individuals.

Lawful Basis for Processing

Under the Privacy Regulations, there are a number of available lawful bases for processing personal data. Q2 has documented the relevant lawful foundations for processing personal data and the purposes of that processing in its relevant data maps.

Under the Privacy Regulations, the lawful bases for processing are as listed below. At least one of these must apply whenever Q2 processes personal data:

(a) **Consent:** Q2 has been given clear consent to process personal data for a specific purpose.

(b) **Contract:** the processing is necessary for Q2 to perform its obligations under an applicable contract.

(c) **Legal obligation:** the processing is necessary for Q2 to comply with applicable law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary to perform a task in the public interest.

(f) **Legitimate interests:** the processing is necessary for a legitimate interest, as defined in the Privacy Regulations.

Security

The Privacy Regulations require personal data to be processed in a manner that ensures its security. This includes protection of personal data against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Q2 has defined and implemented an Information Security Program designed to maintain effective and proportionate security.

Security Incidents

It is the policy of Q2, regardless of the criticality of the incident, to respond in accordance with a planned and coordinated process in order to identify, protect, detect, respond, and recover from security incidents. In the event of a security incident:

a). A notifiable breach has to be reported by the Data Protection Officer (DPO) to the relevant supervisory authority within 72 hours of Q2 becoming aware of it. The notification must contain the nature of the personal data breach including where possible;

- the categories and approximate number of individuals concerned;
- the categories and approximate number of personal data records concerned;
- the name and contact details of the DPO or other contact point for more information;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken or proposed to be taken to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

b). Where a breach is likely to result in a high risk to the rights and freedoms of individuals, Q2 will notify those concerned directly.

Third Party Agreements

The Privacy Regulations require diligence and clarity when entering into third party relationships where Q2 may share personal data with such third party. Whether Q2 is a processor or controller, there are mandatory requirements relating to the contracts that are in place. When working with third parties, Q2's practices, are as follows:

- Whenever Q2 acts as a controller a written contract must be in place with a third party acting under the agreement as a processor.
- Whenever Q2 acts as a processor, Q2 must only act on the documented instructions of the controller (as specified in a valid written contract).

Compliance

In conjunction with its DPO, Q2 has developed a compliance monitoring plan for Q2's privacy practices and adherence to the Privacy Regulations.

Data Subject Rights

The Privacy Regulations provide certain individual rights to any person whose personal data is being collected, held or processed ("Data Subject"). Individual rights of Data Subjects include, but are not limited to:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object

Data Subject Action Requests

A Data Subject Action Request ("DSAR") is a written or verbal request made by the Data Subject regarding their personal information and/or how their personal information is being processed. In the event the institution receives a DSAR, they may need to contact Q2 for its part in their compliance with the Privacy Regulations. To notify Q2 of a DSAR, please email: **privacy@q2ebanking.com**

Conclusion and Next Steps

Q2 is dedicated to meeting the highest standards for data privacy on a global scale and we will continue to make data privacy a priority. Q2 is closely watching the developments in the data privacy landscape to understand the latest considerations and concerns so we may implement appropriate safeguards for our customers.

Disclaimer

This white paper is provided for informational purposes only and should not be construed as legal or compliance advice. As with most regulations and laws, interpretations of how to apply GDPR, CCPA, and other privacy laws and regulations may vary, especially when the regulations and laws are relatively new, as is the case with GDPR and CCPA. Q2's observation of the Privacy Regulations is based on its current understanding of the Privacy Regulations and their applicability in practice. Over time, as the application and interpretations become clearer, Q2's position on the application of the Privacy Regulations may change. Please note that although GDPR and CCPA provide many rights to the Data Subject, not all may be relevant to Q2 or Q2's products.