This document is a broad overview of the EU General Data Protection Regulation (GDPR) and does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

White Paper: GDPR Key Facts

At CloudFin, we know that many organizations have questions about the GDPR and new obligations under the GDPR and we have outlined a few of the notable provisions of the GDPR below.

What is the GDPR?

The EU General Data Protection Regulation ("**GDPR**") is a new comprehensive data protection law that updates existing EU laws to strengthen the protection of "**personal data**" (any information relating to an identified or identifiable natural person, so called "**data subjects**") in light of rapid technological developments, the increasingly global nature of business and more complex international flows of personal data. It replaces the current patchwork of national data protection laws with a single set of rules, directly enforceable in each EU member state. The GDPR takes effect on May 25, 2018.

Does the GDPR affect my organization?

If you are processing personal data in the context of an organization established in the EU, the GDPR will apply to you, regardless of whether you are processing personal data in the EU or not. "**Processing**" means any operation performed on personal data, such as collection, storage, transfer, dissemination or erasure.

If you are not established in the EU, the GDPR applies to you if you are offering goods or services (whether paid or free) to EU data subjects or monitoring the behavior of EU data subjects within the EU. Monitoring can be anything from putting cookies on a website to tracking the browsing behavior of data subjects to high tech surveillance activities.

Under European data protection law, organizations processing personal data are divided into "**Controllers**", or the entities which control the personal data, and "**Processors**", the entities that process personal data only on the instructions of the Controllers. The GDPR applies to both Controllers and Processors.

How does the GDPR change existing EU data protection laws?

The GDPR changes existing EU data protection laws in several ways:

1. **Expanded definition of "personal data":** The GDPR expands and clarifies the concept of personal data. While the basic concept of personal data largely remains the same, the GDPR makes it clear that location data and online identifiers, such as IP addresses, are considered personal data. The GDPR also expands the concept of sensitive personal data to include genetic data and biometric data.

2. **Expanded and new rights for EU individuals:** The GDPR provides expanded rights for EU data subjects such as: ○ Deletion: This right is sometimes referred to as the "right to be forgotten". The data subject has the right to require that the Controller erase personal data about him/her in certain conditions, including if the personal data is no longer necessary for the original purpose of the processing or if the data subject withdraws consent for the processing. This right has been extended to the online world as a means to require internet service providers to delete out-of-date publicly available information, in particular that information which appears in search results.
○ Restriction: Under the GDPR, a data subject has the right to obtain from a Controller a restriction on the processing of personal data in a number of circumstances, including if the accuracy of the personal data is contested by the data subject for a certain period of time. A restriction on processing means that the organization holding the data is entitled to continue to store it, but cannot process it any further.
○ Portability of personal data: Data subjects also now have the right, in certain circumstances, to receive the personal data that they have provided to a Controller in a structured, commonly used and machine-readable format.
CloudFin's data processing addendum takes into account these expanded and new rights.

3. **Security measures:** The GDPR requires Controllers and Processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented.

4. **Breach notification**: The GDPR requires organizations to report certain personal data breaches to the relevant data protection authority, and in some circumstances, to the affected data subjects. Controllers must notify the relevant data protection authority "without undue delay" (and where feasible, within 72 hours of having become aware of it), unless the breach is not likely to present any risk to the rights and freedoms of the data subjects concerned. If circumstances require it, Controllers may also be required to communicate the data breach to data subjects. Processors, for their part, are required to notify Controllers "without undue delay" after becoming aware of a personal data breach. CloudFin's data processing addendum takes into account this new obligation.

5. **Data Protection Impact Assessments**: Where certain processing is likely to be classified as "high risk" to data subjects, the Controller may be required to carry out a data protection impact assessment identifying the impact of the proposed processing operations on the personal data. CloudFin's data processing addendum takes into account this new obligation.

6. **International transfers**: European data protection law restricts the transfer of personal data outside of the EU unless there are appropriate safeguards in place to protect that data. The GDPR continues to recognize current mechanisms (e.g. EU standard contractual clauses, EU Commission adequacy decisions, etc.) for legally transferring personal data outside of the EU. The GDPR also formally recognizes Binding Corporate Rules ("**BCRs**"), a set of company-specific, group-wide data

protection policies approved by European data protection authorities to facilitate transfers of personal data from the EU to other countries.

7. **Consent:** Consent is subject to additional requirements under the GDPR. The GDPR defines consent as “any freely given, specific, informed and unambiguous indication of a data subject’s wishes through a statement or clear affirmative action”. The concept of consent is used throughout the GDPR as a means to legitimize certain processing activities from a legal perspective.

8. **Transparency:** The GDPR requires that Controllers provide data subjects with information about their processing operations at the time when the personal data are collected. This information includes the identity and contact details of the Controller, the contact details of the data protection officer (if relevant), the purposes and the legal bases for the processing of the personal data, the recipients of the data and a number of other fields to ensure that the personal data is being processed in a fair and transparent manner. In addition, Controllers are required to provide information to data subjects even in circumstances where the personal data has not been obtained directly from the data subject.

9. **Profiling**: The GDPR introduces the concept of “profiling” or any form of automated processing that uses personal data to evaluate personal aspects and in particular to analyze or predict aspects relating to an individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Data subjects must be informed of the existence of profiling and any consequences of the profiling.

10. **Enforcement**: Fines for non-compliance under the GDPR can be substantial. Data protection authorities have a number of enforcement powers under the GDPR, including the ability to fine organizations up to €20 million or 4% of annual global turnover, whichever is higher. These are maximum fines and it remains to be seen how regulators will use their newly-acquired enforcement powers.

11. **‘One Stop Shop’**: Under the GDPR, organizations that are established in more than one EU member state or are processing personal data affecting data subjects in more than one EU country will have greater clarity about their supervising data protection authority. Supervisory authority for the main European establishment of that organization will act as the lead authority. This authority will cooperate with the other supervisory authorities concerned in respect of cross-border data protection issues.