GDPR FACT SHEET

What is the GDPR?

The General Data Protection Regulation ("GDPR") is a new set of laws that will apply to all processing of personal data in the European Union ("EU"). All businesses and non-profits that monitor, process, or store any information "concerning an identified or identifiable natural person" in the EU will need to apply basic standards regarding customer consent, customer access to personal data, breach notification, and security and confidentiality, among other requirements. The GDPR takes effect on **May 25, 2018.**

Who does the GDPR apply to?

The GDPR generally applies to:

1. Data processors and controllers established in the EU, regardless of where data processing occurs,
2. Data processors and controllers that offer goods or services to subjects in the EU, irrespective of whether a payment is required, or
3. Data processors and controllers that monitor the behavior of data subjects in the EU. *This can include monitoring the IP addresses or other web identifiers of EU subjects.*

Definitions:

The "Data Controller" determines the purposes and means of processing personal data.

The "Data Processor" processes personal data on behalf of a controller.

What are the biggest compliance risks?

The GDPR provides for **administrative fines of up to 4% of global revenue or €20 million**, whichever is greater. In addition to these sanctions, national data protection authorities can conduct audits of data processing activities and even halt all processing of personal data on a temporary or indefinite basis. Furthermore, the GDPR provides a private right of action for EU data subjects before both the courts and administrative authorities.

Where should I focus my compliance efforts?

Customer complaints to a regulatory authority or the courts pose the greatest risks to a business under the GDPR. These complaints will likely result from a data breach, failures to

comply with subject access rights, and failure to provide adequate customer-facing privacy notices.

GDPR Starter Checklist:

The checklist below is **not** a comprehensive overview of all GDPR requirements, but addresses some of the most customer-facing and high-risk issues to businesses and non-profits:

- ☑ **Internal Audit of Subject Access Rights:** The GDPR generally requires controllers to respond within 30 days of a data subject's request for information about his/her data, correction of data, erasure of data, restriction of processing, objection to processing, and in certain cases, portability of data. Is your business prepared to handle the operational requirements of these subject access rights?

- ☑ **Update Privacy Notices:** The GDPR has specific requirements concerning the content and readability of privacy notices.

"The GDPR has a 72-hour breach notification requirement"

- ☑ **Update Incident Response Plan:** The GDPR has a 72-hour breach notification requirement to data protection authorities, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

- ☑ **Update Internal Privacy and Information Security Policy:** All controllers and processors must implement appropriate technical and organizational measures to protect personal data.

- ☑ **Document Lawful Bases for Processing Data:** Processing of any personal data is unlawful, unless it fits within specific enumerated exceptions, such as consent, contract performance, and other exceptions.

- ☑ **Data Protection Officer:** Identify whether your organization requires a data protection officer under the GDPR.

Metaverse Law is a sole proprietorship formed by Lily Li (SBN 281922). Ms. Li is licensed to practice law in California. This fact sheet is for advertising and educational purposes only and does not constitute legal advice.