GDPR COMPLIANCE:MEL DEVELOPERS KIT

A Presentation by Sumaiyah A. Omar:

Lawyer& Mediator at Lawyers Hub Kenya,

Presented at the Tamarid Tree Hotel on the 4th December 2019

 @lawyershubkenya

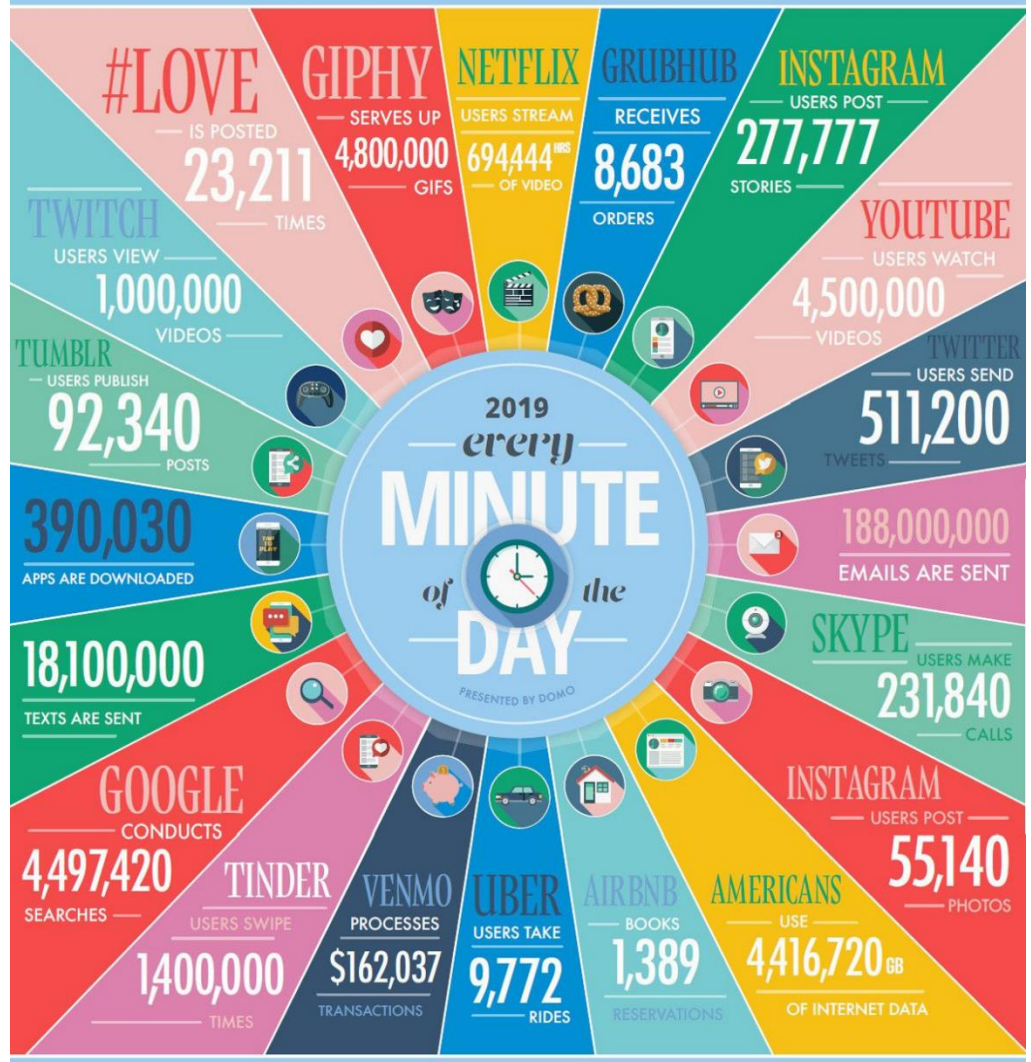
 info@lawyershub.ke

 Lawyers Hub Kenya

DATA NEVER SLEEPS 7.0

How much data is generated *every minute?*

There's no way around it: big data just keeps getting bigger. The numbers are staggering, and they're not slowing down. By 2020, there will be 40x more bytes of data than there are stars in the observable universe. In our 7th edition of Data Never Sleeps, we bring you the latest stats on how much data is being created in every digital minute.



SOURCES: STATISTA, INTERNET LIVE STATS, EXPANDED RAMBLINGS, NATIONAL ASSOCIATION OF CITY TRANSPORTATION OFFICIALS, WIRED

GDPR:

- The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA).
- Is the GDPR a law for the world?
- GDPR was adopted on 14 April 2016, enforceable from 25 May 2018.
- GDPR is a regulation, not a directive, it is directly binding and applicable, but does provide flexibility for certain aspects of the regulation by individual member states.

LAWYERS HUB
Tech for Justice


We are very attached
to our personal data
#ThisIsTheEU


WOCAS
DUE TO THE NEW PRIVACY RESTRICTIONS, SANTA WAS NO LONGER ABLE TO IDENTIFY WHO HAD BEEN NAUGHTY AND WHO HAD BEEN NICE.

Key Terminology

1. Data subject- Person whose personal data is processed
2. Personal Data- Any data about an identifiable/ identified person (Compare with Kenya DPA)
3. Data Processing- Any operation on personal data (Manual and Automated)
4. Controller- Entity that requests and uses the data
5. Data Processor- Any entity that processes data on behalf of a controller (i.e. Cloud Service)

LAWYERS HUB
Tech for Justice

Principles of Data Protection

LAWYERS HUB
Tech for Justice

Processing Personal Data

- User Consent
- Performance of a Contract
- Legitimate Interest of the controller, including Direct Marketing
- Vital need/ Public Interest.
- If required by law
- Any combination.

LAWYERS HUB
Tech for Justice

Rights Under GDPR

planio

LAWYERS HUB
Tech for Justice

Accountability

1. Adopting and implementing data protection policies;

2. Putting written contracts in place with organization's that process personal data on your behalf;

3. Implementing appropriate security measures;

4. Recording and, where necessary, reporting personal data breaches (72 hours)

Compliance Check List

- ☐ We have a lawful basis to carry out profiling and/or automated decision-making and document this in our data protection policy.
- ☐ We send individuals a link to our privacy statement when we have obtained their personal data indirectly.
- ☐ We explain how people can access details of the information we used to create their profile.
- ☐ We tell people who provide us with their personal data how they can object to profiling, including profiling for marketing purposes.
- ☐ The minimum amount of data needed and have a clear retention policy for the profiles we create.
- ☐ We have procedures for customers to access the personal data input into the profiles so they can review and edit for any accuracy issues.
- ☐ We have additional checks in place for our profiling/automated decision-making systems to protect any vulnerable groups (including children).
- ☐ We only collect

LAWYERS HUB
Tech for Justice

As a best practice.

- ☐ We carry out a DPIA to consider and address the risks before we start any new automated decision-making or profiling.

- ☐ We tell our customers about the profiling and automated decision-making we carry out, what information we use to create the profiles and where we get this information from.

- ☐ We use anonymised data in our profiling activities

LAWYERS HUB
Tech for Justice

Success Tips for MEL

1. Organize your data (For individuals/ Government scrutiny)
2. Safely secure data (Anti-virus, encryption, remote access)
3. Data Minimization
4. Internal Privacy Policies, compliant with local laws (the 5 ws)
5. Create Data supplying mechanism, when requested
6. Create Data Deletion / Editing Mechanism
7. Create Express consent (Positively opt-in) and Make it easy to Opt out.
8. Layer Opt in form (more information, relatable)
9. Train all staff on GDPR/Local Privacy Laws.
10. Consult/ get a DPO
11. Buy data from 3rd Parties that are GDPR Compliant.

LAWYERS HUB
Tech for Justice

Don'ts

1. Do not use data for purposes that the user has not agreed to (Request Consent for new purposes)
2. Do not collect unnecessary data on registration fields
3. Do not assume 3rd Parties are compliant
4. Do not assume having ISO Indicates Compliance
5. Do not dump personal data on Public servers.

LAWYERS HUB
Tech for Justice

GDPR Fines and Penalties.

The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

1. Controllers and processors (Articles 8, 11, 25-39, 42, and 43) — Organizations that collect and control data (controllers) and those that are contracted to process data (processors) must adhere to rules governing data protection, lawful basis for processing, and more. As an organization, these are the articles you need to read and adhere to.

2. Certification bodies (Articles 42 and 43) — Accredited bodies charged with certifying organizations must execute their evaluations and assessments without bias and via a transparent process.

3. Monitoring bodies (Article 41) — Bodies that have been designated to have the appropriate level of expertise must demonstrate independence and follow established procedure in handling complaints or reported infringements in an impartial and transparent manner.

LAWYERS HUB
Tech for Justice

GDPR Fines and Penalties.

These types of infringements could result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

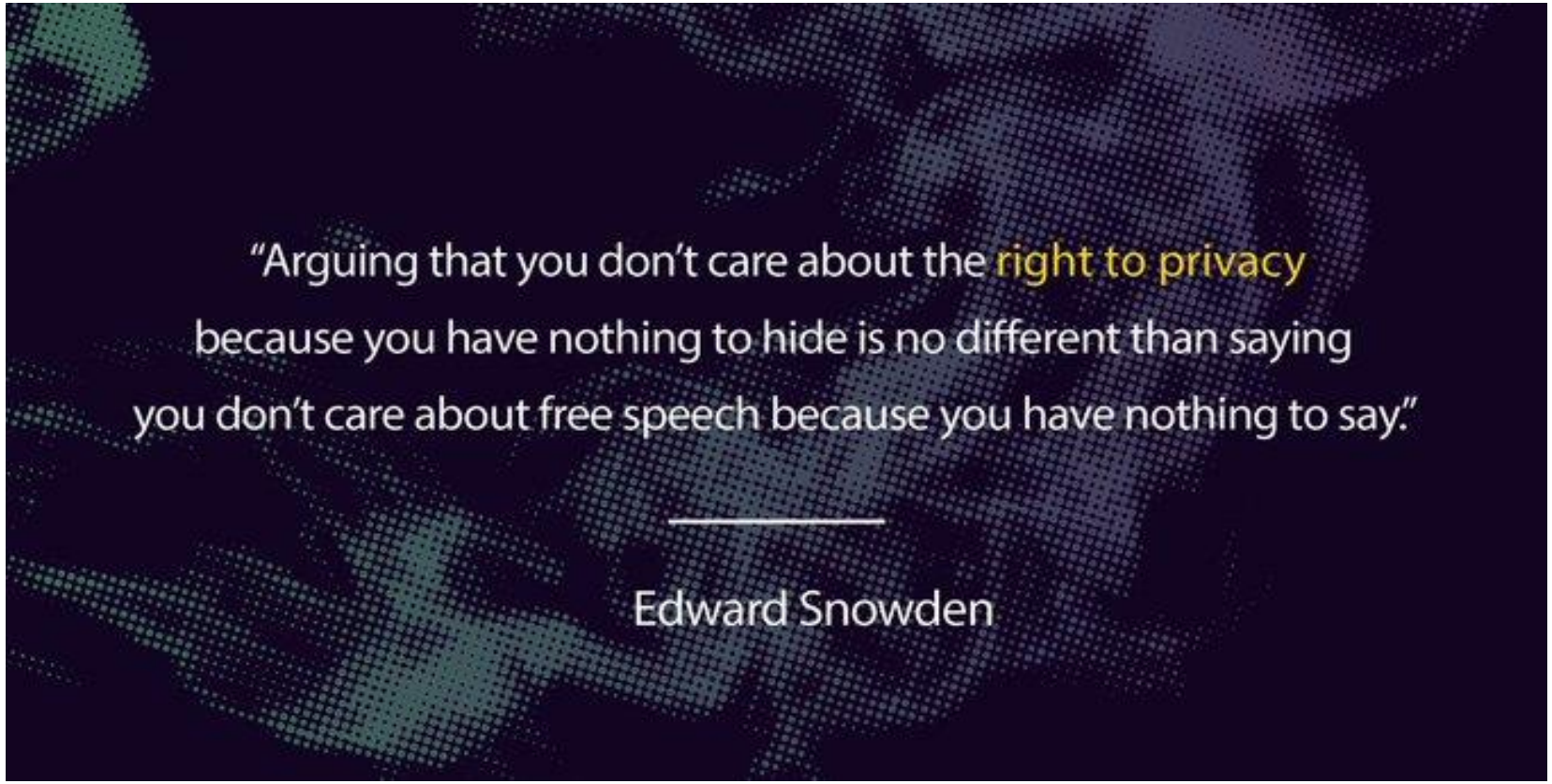
1. The basic principles for processing (Articles 5, 6 and 9) —In addition, certain types of personal data, including racial origin, political opinions, religious beliefs, trade union membership, sexual orientation, and health or biometric data are prohibited except under specific circumstances.

2. The conditions for consent (Article 7) — When an organization's data processing is justified based on the person's consent, that organization needs to have the documentation to prove it.

3. The data subjects' rights (Articles 12-22) — Individuals have a right to know what data an organization is collecting and what they are doing with it. The transfer of data to an international organization or a recipient in a third country (Articles 44-49) — Before an organization transfers any personal data to a third country or international organization, the European Commission must decide that that country or organization ensures an adequate level of protection. The transfers themselves must be safeguarded.

LAWYERS HUB
Tech for Justice

Conclusion



LAWYERS HUB
Tech for Justice