Data security

Talk by: Mohamed Maamoun

What's the GDPR?

General Data Protection Regulation.

A legally enforced EU regulation that governs how organizations and companies use and maintain the integrity of personal data

It concerns:

- Users,
- Controller: Person who determines the purposes of the processing of personal data
- Processor: Person who processes personal data on behalf of the controller.

It applies to any company that deals with european citizens.

It obligates companies to obtain their users' consent to process their data.

How did the GDPR affect companies?

GDPR is very influential. For example:

- Google was fined 50m because there was an option that was checked by default.
- Mariott was fined 123m because there was data preach and they didn't tell the government.

What is a PII?

Personally identifiable information. Which is a piece of information that identifies a person like phone number, email, age, address.

GDPR mainly focuses on PII.

Examples: Guide to Identifying Personally Identifiable Information (PII)

How to protect PII?

Through several techniques like

- Anonymization through generalization. For example: Age can be range, it doesn’t have to be the real value.

- Suppressing PII data that you don’t have to keep. Even if you think that you may use it in the future. For example
    - If you have an employee's salary you don’t have to keep the employee’s email in the same dataset.
    - Remove persons image after extracting info from it like sex, age, etc..

- Substitution/Noise addition. For example,
    - Substitute the name with X.
    - Add numbers to the age (simple example).

Why delete data i have i may use in the future?

To save the data you must encrypt it. And save it in a secure place, for example not on your personal computer or printed on a paper.

Security is against usability so people hate it.

You have to take the client's consent to keep the data.

Data has insurance to pay people whose data is leaked.

GDPR limits the time you keep the data.

When can you keep data for future use safely?

If you applied generalization/anonymization you can keep the data since you don’t know whose info is that you have.

But for example if got sheet X and sheet Y each is generalized but adding the two will give me information about the client.

What should the “records of processing activity” document contain?

It contains the purpose of processing operation, a description of categories of data subjects & categories of personal data.

One of the obligations of the GDPR is to maintain records of processing activity.

In digital analytics, how long should data be kept?

To be defined according to the type of processing.

Ref: For how long can data be kept and is it necessary to update it?

Why apply GDPR?

- Minimize the risk.
- Follow the regulators.
- Protect users/customers data.
- Avoid Penalties.
- When you deal with someone who says that he applies the GDPR you will trust him.
- ISO 27001 is the standard ISO for the cloud.

Are there any regulations locally?

قانون حماية أمن المعلومات الجديد

What are some more examples of PII?

Examples of PII include, but are not limited to:

- Name: full name, maiden name, mother’s maiden name, or alias.
- Personal identification numbers: SSN, passport number, driver’s license number, financial account number, or credit card number.
- Personal address information: street address, or email address.
- Personal telephone numbers.
- Personal characteristics: photographic images (particularly of face or other identifying characteristics), fingerprints, or handwriting.
- Biometric data: retina scans, voice signatures, or facial geometry.
- Information identifying personally owned property.
- Asset information: Internet Protocol (IP) or Media Access Control (MAC) addresses that consistently link to a particular person.

The following examples on their own do not constitute PII as more than one person could share these traits.

However, when linked or linkable to one of the above examples, the following could be used to identify a specific person:

- Date of birth
- Place of birth
- Business telephone number
- Business mailing or email address
- Race
- Religion
- Geographical indicators
- Employment information
- Medical information
- Education information
- Financial information