Data Protection:
What you should know about it?

Presentation by
Dima Samaro
MENA Policy Researcher, Access Now

Emna Sayadi
MENA Advocacy Lead, Access Now

Topics to be covered:

1- The definition of data protection

2- Main principles of data protection

3- Examples of data protection

4- The concept of GDPR

5- Challenges of data protection law in Tunisia

What is data protection?

It refers to the practices, safeguards, and binding rules put in place to protect your personal information and ensure that you remain in control of it.

In short, you should be able to decide whether or not you **want to share** some information, **who** has access to it, for **how long,** and for **what reason**, and to be able to **modify** some of this information, and more.

In the EU, these rules are defined under the General Data Protection Regulation (GDPR)

What is personal Data?

Any information relating to you (identified or identifiable natural person) whether it relates to your private, professional, or public life, such as

- Name
- Identification number
- Location data
- Online identifier (IP address)
- Factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category data:

Also called 'Sensitive Personal Data' which is subject to **greater controls around processing**; it refers to data regarding:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs, or trade union membership,
- genetic data,
- biometric data (for the purpose of identifying a natural person),
- data concerning health or
- data concerning a natural person's sex life or sexual orientation.

Personal Data

- Work History
- HR file
- CV
- Application Form
- Education
- Swipe access
- Disciplinaries
- Grievances
- Email
- Diary
- Checks
- Performance
- ANPR
- References
- ID details

- Internet
- Netflix choices
- You tube
- Fridge
- Smart devices
- Behaviour
- Cookies
- Tracking
- Contacts
- Communications
- Location Data
- Social Media
- CCTV
- IP addresses
- Email

- License plate
- ANPR
- Cameras
- Black box
- Flight Details
- Hotels
- Destinations
- Tours
- Rail travel
- Shopping

- Credit worthiness
- Taxes
- Bank details
- Savings
- Mortgage
- Loans
- Credit card
- Debit cards
- Store cards
- Loyalty cards
- CCJ
- Bankruptcy

- Date of birth
- Political opinions
- Religious Beliefs
- Biometric Data
- Your audio
- Your photograph
- Your video
- TU membership
- Contact Details
- Sexual Orientation
- Social Services
- Criminal convictions
- Passport
- Ethnicity
- Opinions
- Health
- Name
- Visa

- Dental
- Eyesight
- Chiropractor
- Therapy
- Welfare
- Disability
- DNA
- Blood Type
- Fitness
- Drug tests
- Family Heath History
- Prescriptions
- Dietary
- Care Data
- Mental

Main principles of data protection:

1. **Purpose limitation** - All data should be collected and used only for purposes that were declared by the company, a government body, or an organisation.

2. **Retention** - Personal data should be stored only during the period necessary for purposes processing.

3. **Data minimisation** - You have no right to collect more data than you need to process.

4. **Integrity and confidentiality** - Personal data must be kept securely.

5. **Accuracy** - Personal data must be accurate, kept up to date, and Inaccurate personal data should be corrected or deleted.

6. **Lawfulness, fairness and transparency** - Personal data must be processed lawfully, fairly and in a transparent manner.

Examples of data protection:

- **Grocery stores or supermarkets:**

  Have you ever received an sms (sales, advertisement, etc..) right after leaving the store? Or after a couple of days?

  Whenever you leave your number, name, e-mail or any personal data, your personal data will not be protected anymore, and the store might use for its interest!

- **Social Media platforms:** Facebook, Twitter, Linkedin, Google Instagram and others

  - It doesn’t really matter if you use social media platform occasionally.
  - The collecting and giving away of personal data starts when you sign up for these social network, it continues as users add third-party apps such as games, educational apps etc…

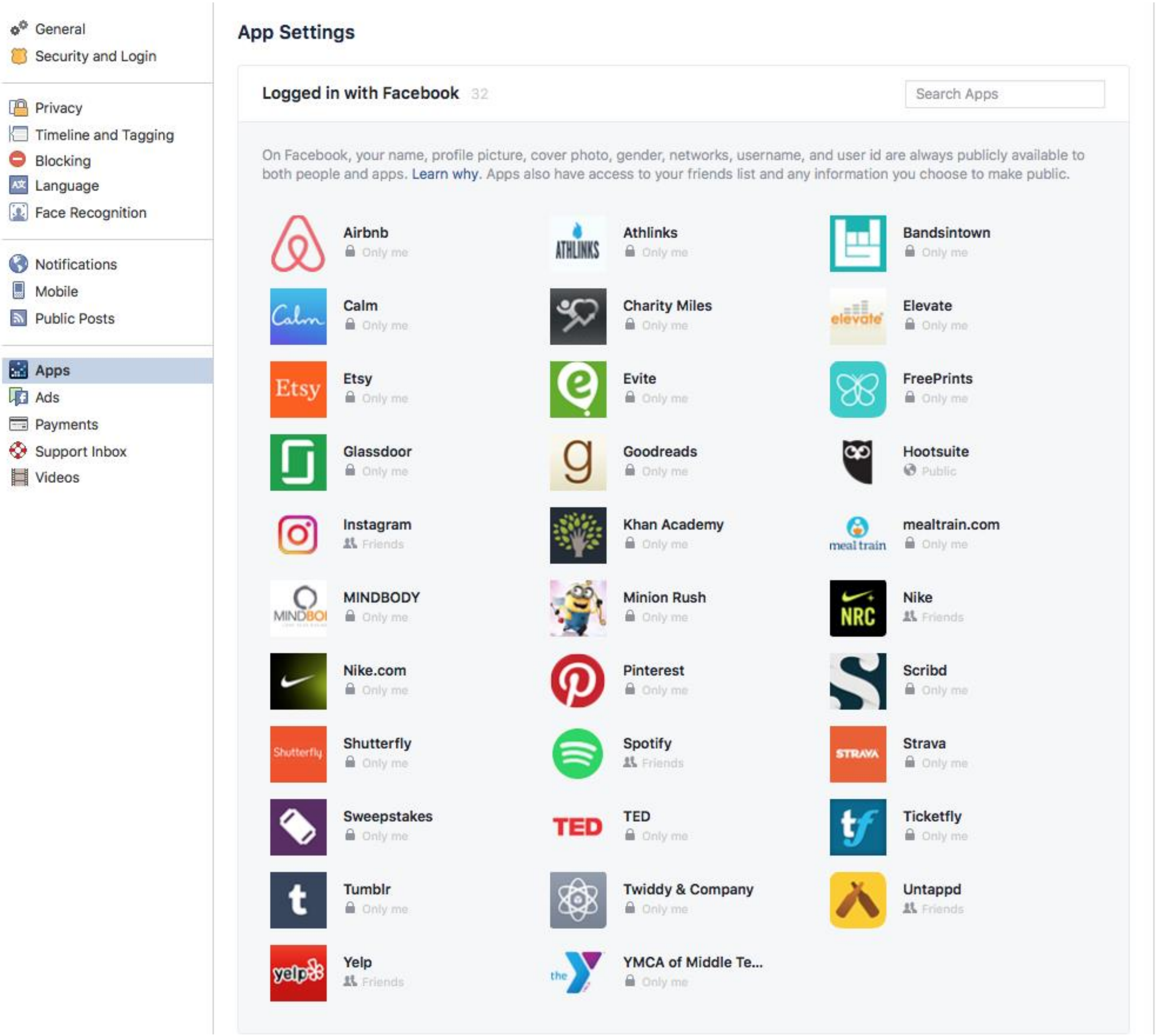
➢ In **Facebook**, for example, **the stored data** are:

- Every ad users click on
- Any additional personal information added to the profile including: schools, maiden name, hometown ,employment, etc..
- Every IP address that the user used when logging into the Facebook account
- Every friend in the network, including friends that have been deleted
- All of the user’s activity—ever.

➢ **What does the third-party app do with my data?**

- The app **sells** the data to someone else. Ex: Cambridge Analytica (the data firm that worked for Trump’s campaign)
- Or they sell it **illegally** on dark web for few dollars!

Applications connected to Facebook



General
Security and Login

Privacy
Timeline and Tagging
Blocking
Language
Face Recognition

Notifications
Mobile
Public Posts

Apps
Ads
Payments
Support Inbox
Videos

App Settings

Logged in with Facebook 32

Search Apps

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available to both people and apps. Learn why. Apps also have access to your friends list and any information you choose to make public.

Airbnb Only me	Athlinks Only me	Bandsintown Only me
Calm Only me	Charity Miles Only me	Elevate Only me
Etsy Only me	Evite Only me	FreePrints Only me
Glassdoor Only me	Goodreads Only me	Hootsuite Public
Instagram Friends	Khan Academy Only me	mealtrain.com Only me
MINDBODY Only me	Minion Rush Only me	Nike Friends
Nike.com Only me	Pinterest Only me	Scribd Only me
Shutterfly Only me	Spotify Friends	Strava Only me
Sweepstakes Only me	TED Only me	Ticketfly Only me
Tumblr Only me	Twiddy & Company Only me	Untappd Friends
Yelp Friends	YMCA of Middle Te... Only me	

- In 2016, **3 billion** **Yahoo** accounts were hacked in one of the biggest breaches of all time. (Oath.com)

- In 2016, **Uber** reported that hackers stole the information of over **57 million** riders and drivers. (Uber)

- At least **87 million** records breached on **Facebook** (though likely many more) users to find out if their personal data was breached (abc news)

➢ How can I protect myself?

1. Get rid of all those third-party apps
2. Turn off location data
3. Be more in control of your privacy (Nobody really knows where your information goes once you click, “Like,”)

What is GDPR?

General Data Protection Regulation (GDPR) is a new set of rules designed to give EU citizens more control over their personal data. On 25 May, 2018 GDPR came into force in all 28 Member States of the EU.

- It aims to simplify the regulatory environment for business, so both citizens and businesses fully benefit from the digital economy.

- It applies to:

  - Any organisation operating within the EU, as well as any organisations outside of the EU which offer goods or services to customers or businesses in the EU.

  - Citizens of the European Union or to individuals located in the EU, no matter where they are from.

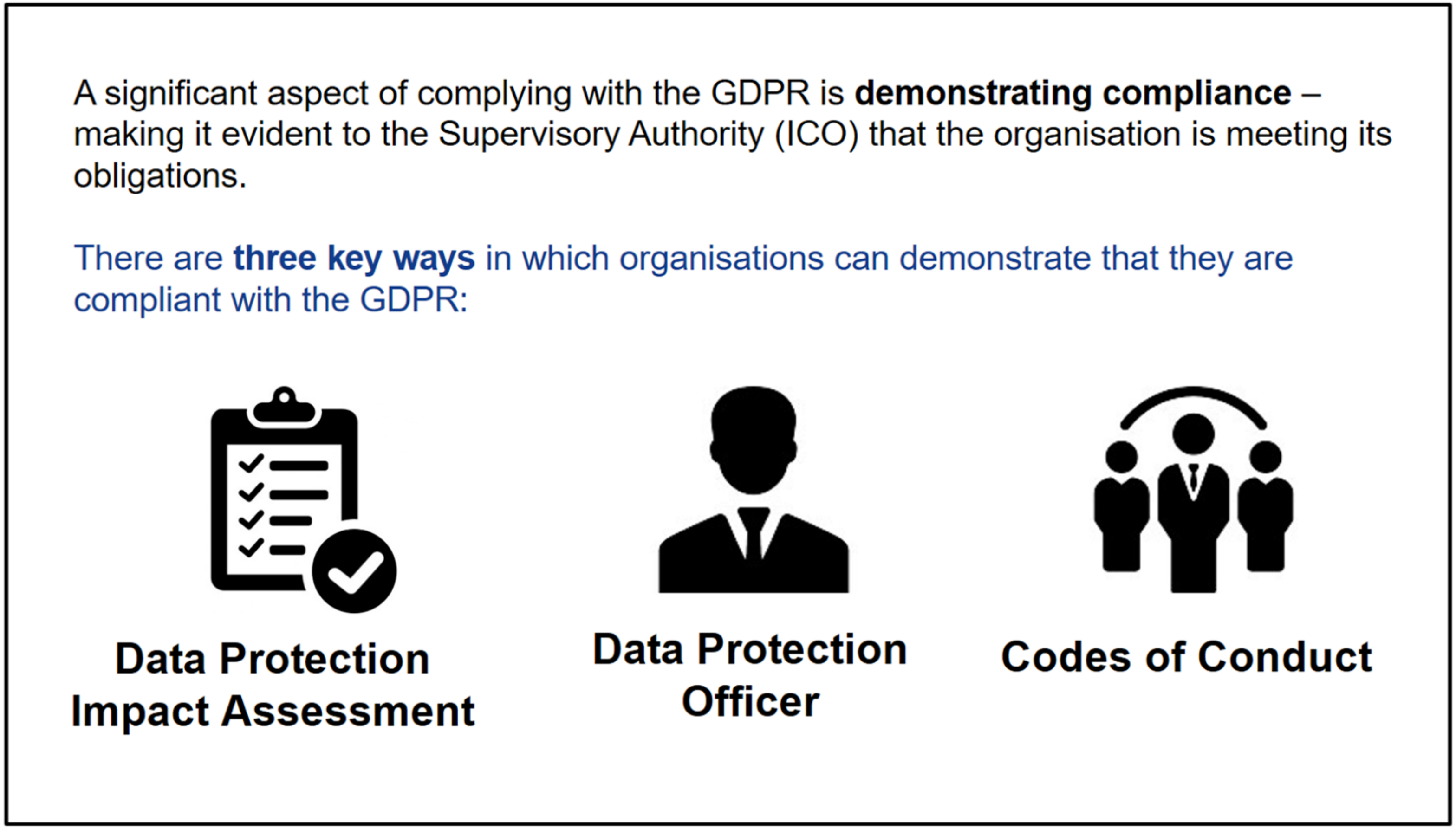
  - Private companies such as Facebook, Microsoft, Dropbox, Amazon, or Spotify and government bodies.

- Not only will organisations have to ensure that personal data is gathered legally and under strict conditions, but those who collect and manage it will be obliged to protect it from misuse and exploitation - or face penalties for not doing so.

- GDPR is also set to bring a clarified 'right to be forgotten' process**,** which provides additional rights and freedoms to people who no longer want their personal data processed to have it deleted, providing there's no grounds for retaining it.

Data Protection Officer?

Mission of DPO:
Safeguard the privacy rights of all individuals with regard to the processing of their personal data.



A significant aspect of complying with the GDPR is **demonstrating compliance** – making it evident to the Supervisory Authority (ICO) that the organisation is meeting its obligations.

There are **three key ways** in which organisations can demonstrate that they are compliant with the GDPR:

Data Protection Impact Assessment

Data Protection Officer

Codes of Conduct

Tunisia and data protection law

- On March 1, 2018, the Tunisian Council of Ministers approved data protection law, in Tunisia.

- The draft law violates the principles of transparency and access to information guaranteed by the Tunisian Constitution (Chapter 32); the definition of personal data did not distinguish between private and public life.

- A conflict and ongoing argument between the two authorities that work under the Data Protection Law; Access to information authority – (access to public info and data) and Data protection authority – (protecting personal data of individuals).

- The access to information authority was not consulted in editing the draft law, which violates Article 38 of Act No. 22 of 2016 on access to information.

- Civil society was not consulted in the drafting Data Protection Law, and their role was limited to submitting written reports.

Thank You :)

For more info on Access Now please visit:

www.accessnow.org

accessnow