GDPR-ის მოთხოვნების გათვალისწინება პროგრამირებაში

MINISTRY OF JUSTICE OF GEORGIA
DATA EXCHANGE AGENCY

დიმიტრი გუგუნავა

OWASP Tbilisi Chapter 1st Meeting

2019.05.15

პირველი ნაწილი

კონტექსტი

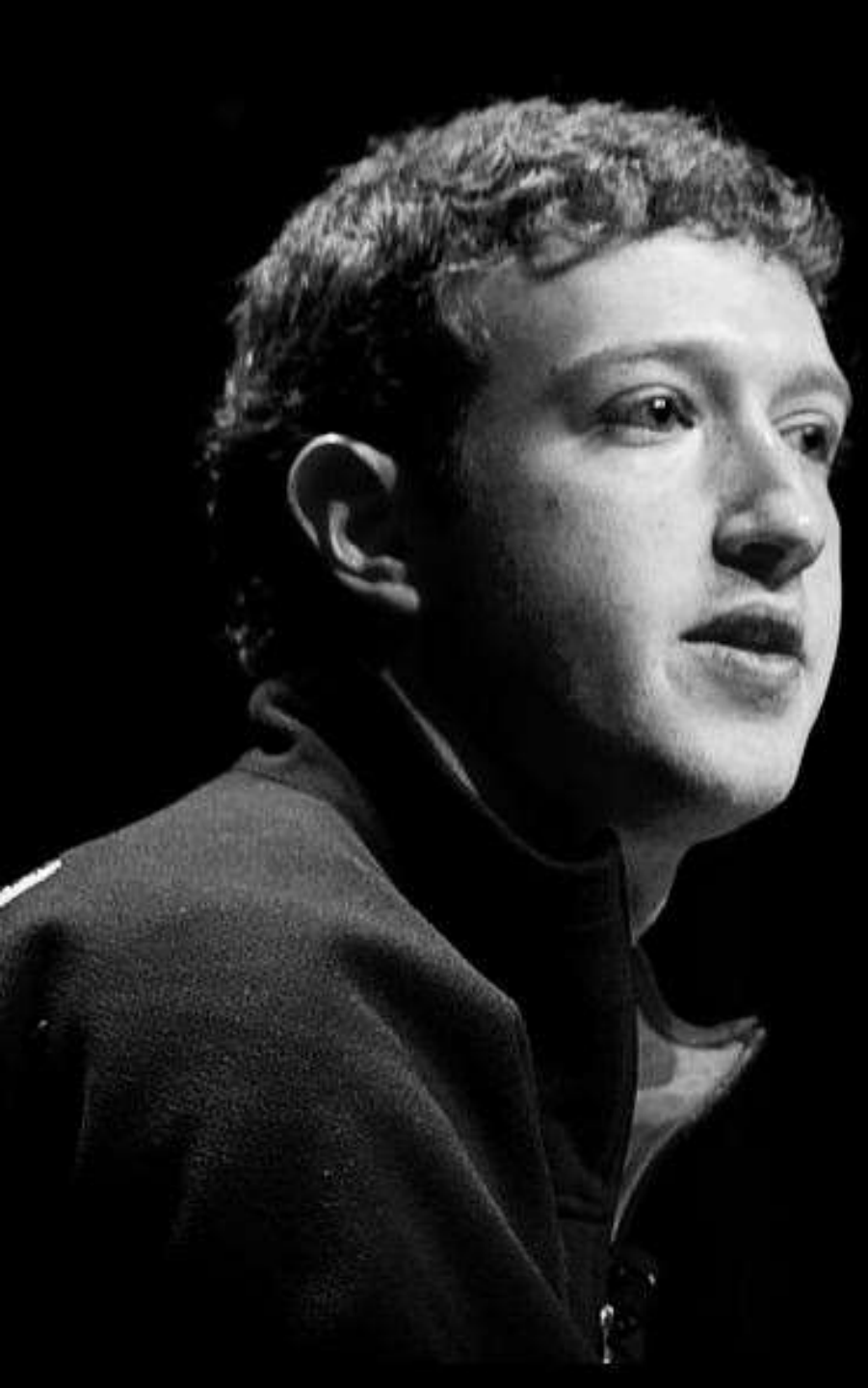
“A child born today will grow up with no conception of privacy at all. They'll never know what it means to have a private moment to themselves an unrecorded, unanalysed thought. And that's a problem because privacy matters, privacy is what allows us to determine who we are and who we want to be.”

Edward Snowden

„ბავშვს, რომელიც დღეს იბადება არ ექნება პრივატულობის განცდა. ისინი ვერასდროს გაიგებენ რას ნიშნავს იცოდე რაღაც მხოლოდ შენ, ისე რომ ეს ინფორმაცია არ იყოს სადმე ჩაწერილი და არ იყოს გაანალიზებული, დამუშავებული.
ეს კი პრობლემაა, რადგან პრივატულობა მნიშვნელოვანია - ის განსაზღვრავს თუ ვინ ვართ და ვინ გვინდა ვიყოთ.“

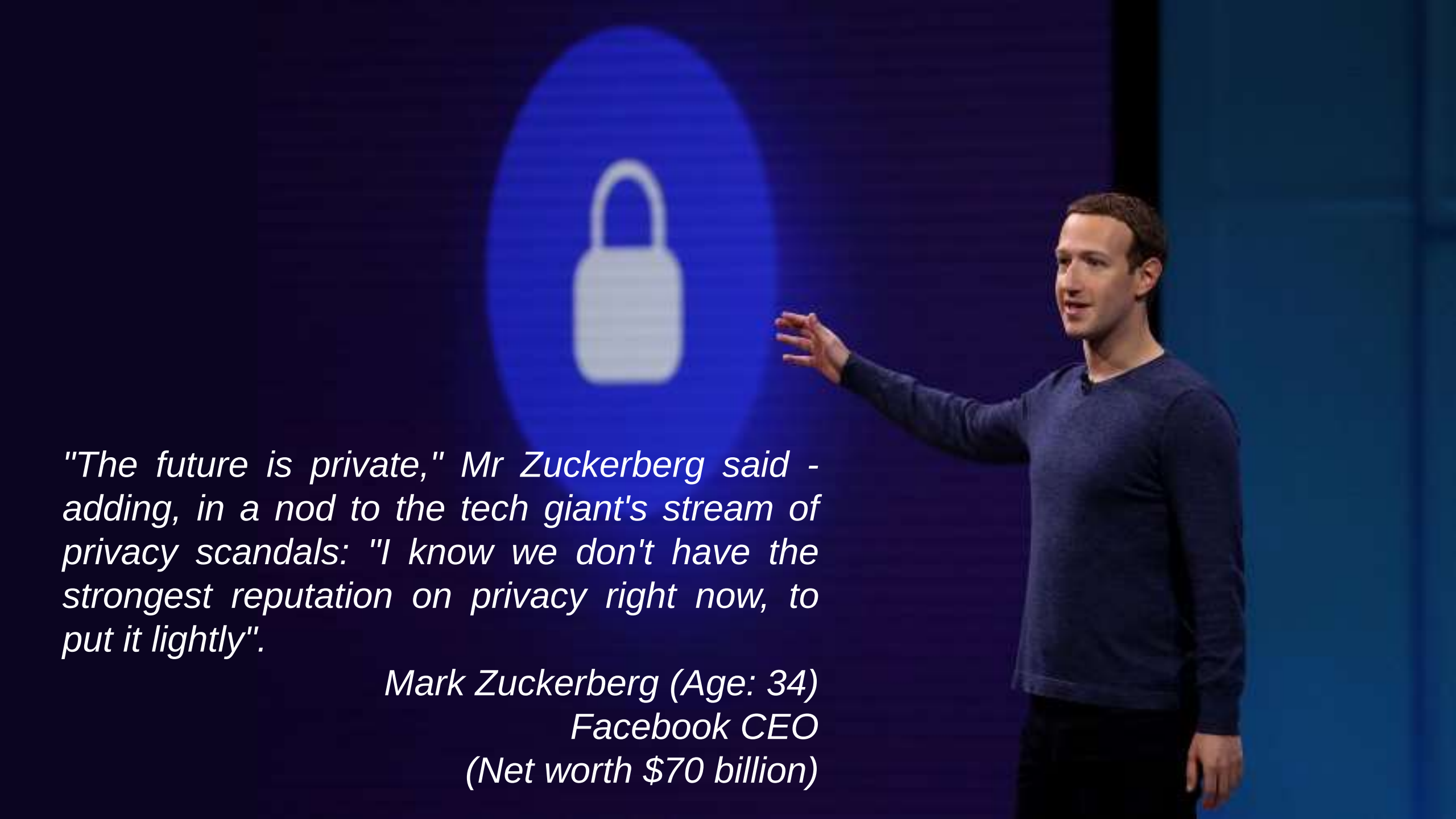
ედვარდ სნოუდენი

"The Alternative Christmas Message 2013". TV Short, www.imdb.com. December 25, 2013.



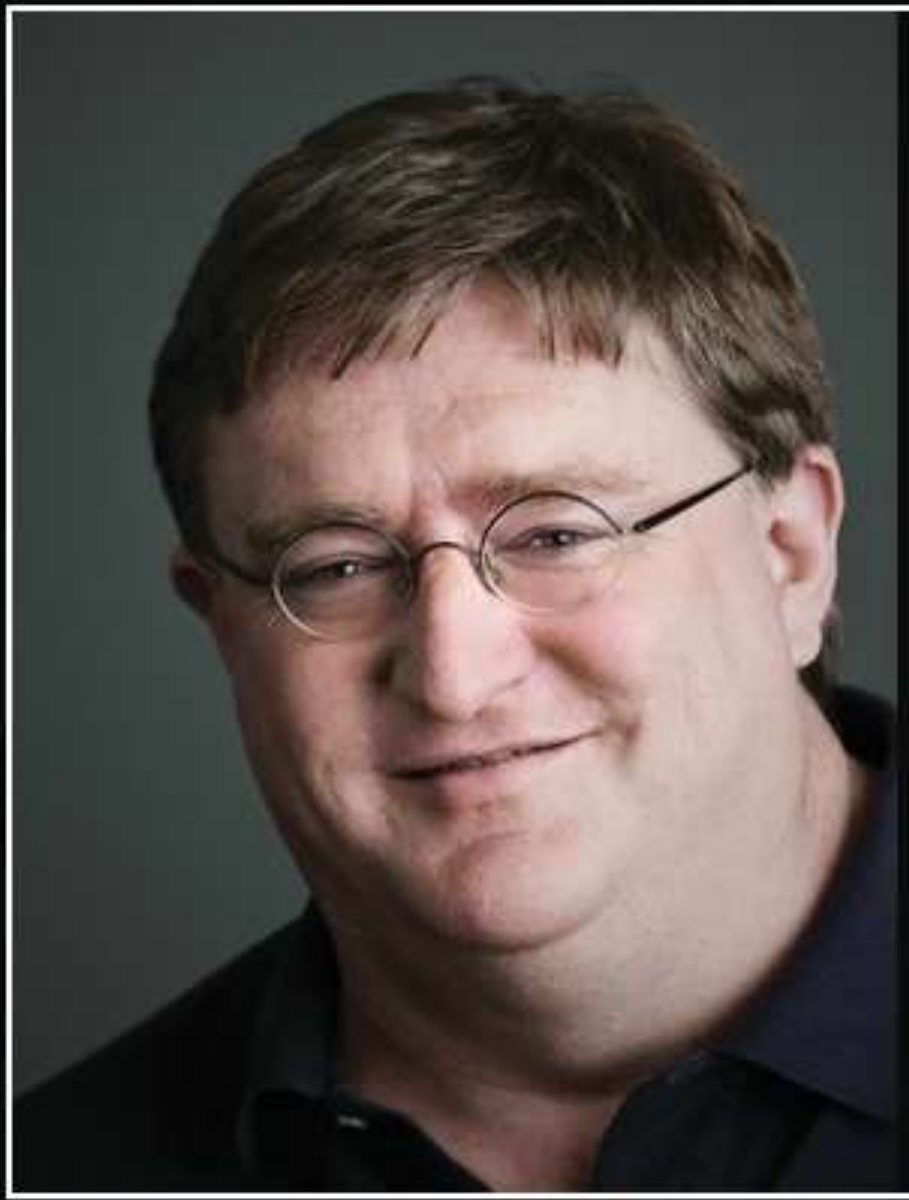
“Privacy is no longer a social norm. People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time.“

Mark Zuckerberg (Age: 26)
Facebook CEO
(Net worth $4 billion)



"The future is private," Mr Zuckerberg said - adding, in a nod to the tech giant's stream of privacy scandals: "I know we don't have the strongest reputation on privacy right now, to put it lightly".

Mark Zuckerberg (Age: 34)
Facebook CEO
(Net worth $70 billion)



The programmers of tomorrow are the wizards of the future. You're going to look like you have magic powers compared to everybody else.

— Gabe Newell —

მეორე ნაწილი

ახალი წესრიგი

მნიშვნელოვანი ფაქტები / თარიღები

2005/2013 – 108-ე კონვენციის რატიფიკაცია

2011 – კანონის მიღება

2013 – ინსპექტორის არჩევა

2014 – საკანონმდებლო ცვლილებები (მანდატის გაფართოება)

2019 - სახელმწიფო ინსპექტორის სამსახური

General Data Protection Regulation

Specify how consumer data should be used and protected

Adopted by the European Parliament in Apr 2016

Enforceable throughout the EU in May 2018

General Data Protection Regulation

Specify how consumer data should be used and protected

Applies to everyone involved in processing data about individuals in the context of selling goods and services to citizens in the EU, regardless of whether the organisation is located within the EU.

General Data Protection Regulation (GDPR)

Consent

Must be confirmed by a statement or other clear affirmative action. You cannot assume consent or even use pre-checked website boxes

Individual rights

Significantly expands the rights of individuals and what information they must be provided with regarding processing activities

Data Protection Officer

Might be obligatory. Requires expert knowledge of data protection law. Could be an employee or via a service contact

Penalties

Could be up to 4% of annual global turnover, or €20m, whichever is greater. You might be fined even if there is no actual loss of data

Privacy from start to finish

Privacy considerations must be built-in everywhere and only data strictly required for stipulated purpose can be used

Data portability

Individuals now have the right to move, copy or transfer personal data—even to a competitor

Wider scope

Covers your business, plus those who process data for you—even outside the EU

Mandatory breach reporting

Data controllers must tell local supervisory authorities, such as the ICO in the UK, within 72 hours of becoming aware. In serious breaches individuals must be informed

ტერმინები

- პერსონალური მონაცემი
- მონაცემთა დამმუშავებელი
- მონაცემთა დამუშავებაზე უფლებამოსილი პირი
- მონაცემთა სუბიექტი
- მონაცემთა დამუშავება

7 ძირითადი პრინციპი

1. კანონიერება, სამართლიანობა და გამჭვირვალობა
2. მიზნების შეზღუდვა
3. მონაცემთა მინიმიზაცია
4. სიზუსტე
5. შენახვის შეზღუდვა
6. მთლიანობა და კონფიდენციალობა (უსაფრთხოება)
7. ანგარიშვალდებულება

უფლებები

1. მონაცემებთან წვდომის უფლება (მ. 15)
2. მონაცემთა გასწორების მოთხოვნის უფლება (მ. 16)
3. მონაცემთა წაშლის უფლება („დავიწყების უფლება“) (მ. 17)
4. მონაცემთა დაბლოკვა (მ. 18)
5. მონაცემთა პორტირების უფლება (მ. 20)
6. დამუშავების შეწყვეტის მოთხოვნის უფლება (მ. 21)
7. გადაწყვეტილების ავტომატიზებული მიღება და „პროფილირება“ (მ. 22)

განსათვალისწინებელი საკითხები

- *“Forget me” (მ.17)*
- *Notify 3rd parties for erasure (მ. 19)*
- *Restrict processing (მ. 18)*
- *Export data (მ. 20)*
- *Allow users to edit their profile (მ. 16)*
- *Consent checkboxes (or yes/no options) (მ. 7)*
- *Re-request consent*
- *“See all my data” (მ. 15)*
- *Age checks (მ. 8)*
- *Keeping data for no longer than necessary (მ. 5)*
- *Cookies (recital 30)*

Requirements

- Consent
- Breach Notification
- Right to Access
- Right to be forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers

In obtaining consent for data use, companies cannot use indecipherable terms and conditions filled with legalese. It must be as easy to withdraw consent as it is to give it.

Requirements

- Consent
- Breach Notification
- Right to Access
- Right to be forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers

In the event of a data breach, data processors have to notify their controllers and customers of any risk within 72 hours.

Notify risk within 72 hours when there is data breach

Requirements

- Consent
- Breach Notification
- Right to Access
- Right to be forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers

Data subjects have the right to obtain confirmation from data controller of whether their personal data are being processed. Data controller should provide an electronic copy of personal data for free to data subjects.

Confirmation of personal data use

Free electronic copy of data

Requirements

- Consent
- Breach Notification
- Right to Access
- Right to be forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers

When data is no longer relevant to its original purpose, data subjects can have the data controller to erase their personal data and cease its dissemination.

Requirements

- Consent
- Breach Notification
- Right to Access
- Right to be forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers

Allows individuals to obtain and reuse their personal data for their own purposes by transferring it across different IT environments

Requirements

- Consent
- Breach Notification
- Right to Access
- Right to be forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers

Calls for inclusion of data protection from the onset of designing systems, implementing appropriate technical and infrastructural measures.

Requirements

- Consent
- Breach Notification
- Right to Access
- Right to be forgotten
- Data Portability
- Privacy by Design
- Data Protection Officers

Public authority

Large scale organisation
> 250 employees

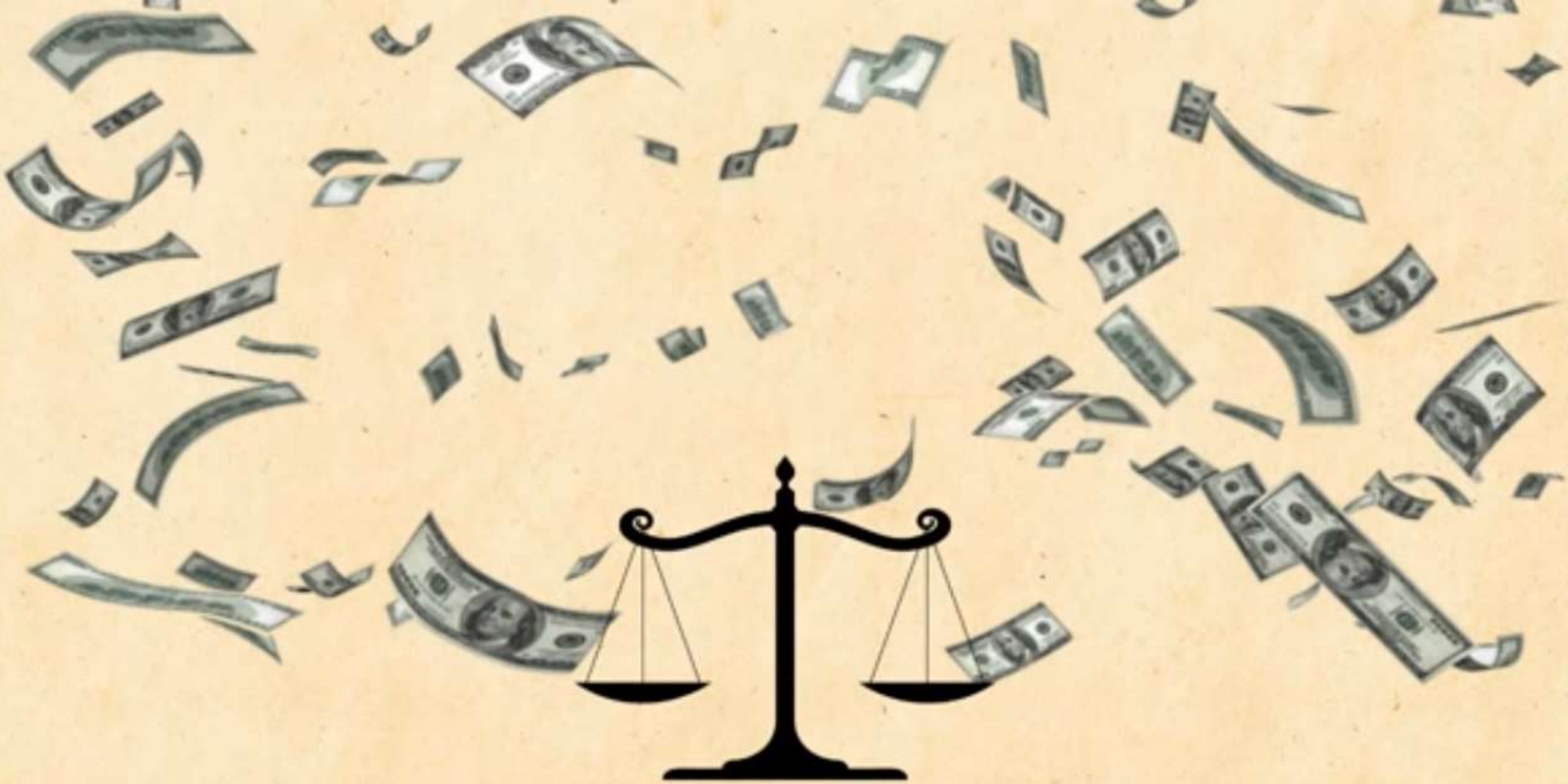
Professionally qualified officers must be appointed in public authorities, or organizations that engage in large scale (>250 employees) systematic monitoring or processing of sensitive personal data

სარგებელი?

- დახვეწილი პროცესები
- მომხმარებლებთან ურთიერთობის გამარტივებული პროცესი - ნაკლები განცხადება
- ნდობა - კონკურენტული უპირატესობა

მესამე ნაწილი

პასუხისმგებლობა



Fined up to €20 Million or 4% of global turnover

Impact of GDPR on business

Restriction on commercial data use

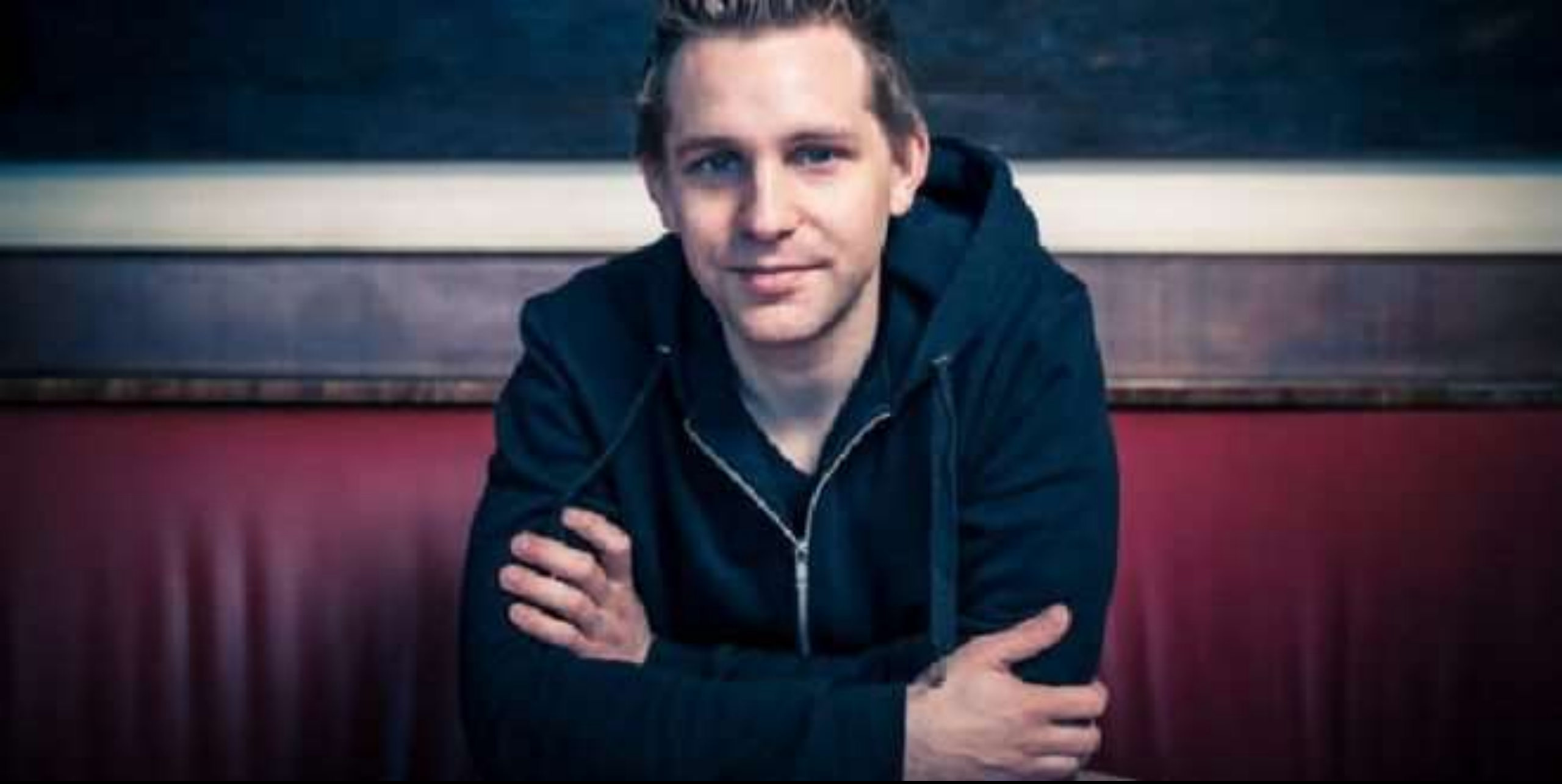
Compliance Spending

Inspire trust and confidence

Safeguard consumer data security rights

GDPR FOR APP DEVELOPERS: THE CHECKLIST

1. Review Data Mapping
2. Rewrite Your Privacy Policy
3. Ensure Data Collection and Storage Systems Are Secure
4. Update Internal and External Notices for GDPR Compliance



მაქს შრემსი (Max Schrems) - ავსტრიელი იურისტი, სამოქალაქო აქტივისტი.

პერსონალურ მონაცემთა დაცვის
ინსპექტორის აპარატი

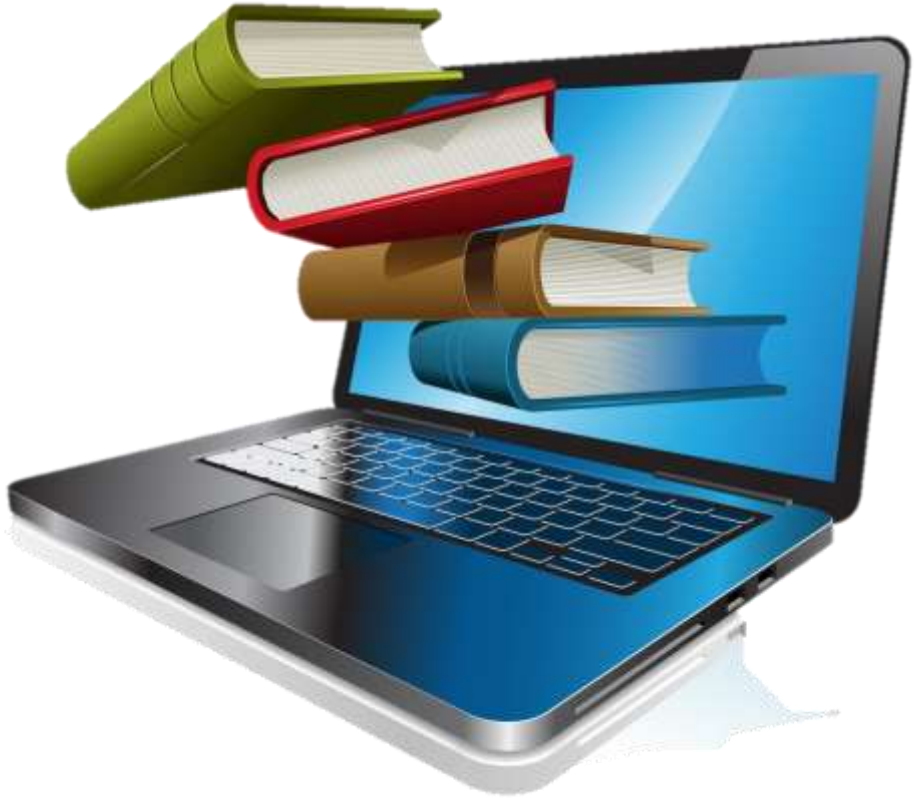
01.07.2013 - 08.05.2019

სახელმწიფო ინსპექტორის სამსახური

08.05.2019 - ?

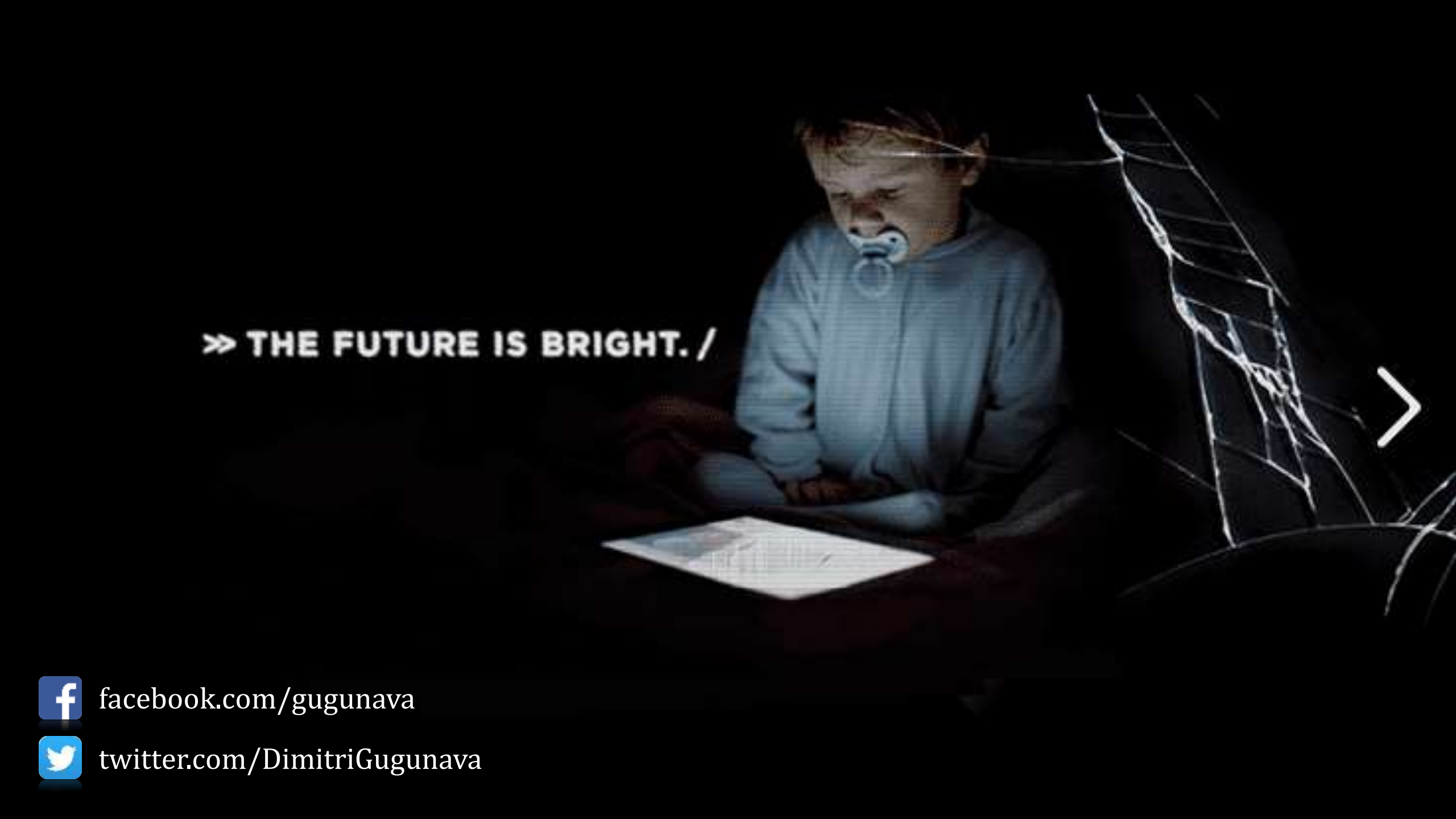
Office of the Personal Data Protection Inspector

გზამკვლევები და რეკომენდაციები



www.pdp.ge

www.personaldata.ge



facebook.com/gugunava

twitter.com/DimitriGugunava