Security Analysis of GDPR Subject Access Request Procedures

Coline Boniface, Imane Fouad, **Nataliia Bielova**,
Cédric Lauradoux, and Cristiana Santos
nataliia.bielova@inria.fr

PUT 2019

Security Analysis of Subject Access Request Procedures

How to authenticate data subjects safely when they request for their data

Coline Boniface[2], Imane Fouad[1], Nataliia Bielova[1], Cédric Lauradoux[2], and Cristiana Santos[3]

[1] Univ. Grenoble Alpes, Inria, France
{cedric.lauradoux,coline.boniface}@inria.fr
[2] Université Côte d'Azur, Inria, France
{nataliia.bielova,imane.fouad}@inria.fr
[3] School of Law, University Toulouse 1 Capitole, SIRIUS Chair
cristiana.santos@ut-capitole.fr

Abstract. With the GDPR in force in the EU since May 2018, companies and administrations need to be vigilant about the personal data they process. The new regulation defines rights for data subjects and obligations for data controllers but it is unclear how subjects and controllers interact concretely. This paper tries to answer two critical questions: is it safe for a data subject to exercise the right of access of her own data? When does a data controller have enough information to authenticate a data subject? To answer these questions, we have analyzed recommendations of Data Protection Authorities and authentication practices implemented in popular websites and third-party tracking services. We observed that some data controllers use unsafe or doubtful procedures to authenticate data subjects. The most common flaw is the use of authentication based on a copy of the subject's national identity card transmitted over an insecure channel. We define how a data controller should react to a subject's request to determine the appropriate procedures to identify the subject and her data. We provide compliance guidelines on data access response procedures.

Keywords: GDPR, data protection, privacy, right of access, identity verification, subject access request (SAR)

I wanted to get a copy of my personal data

What should I do?

I should exercise my rights on my data

- Right to privacy > Data Protection > Rights on our data

  - **Personal data (Art. 4 GDPR):**
    - ✓ Identified of identifiable individual
    - ✓ Factors of identification: number or physical, physiological, mental, economic cultural or social identity
  - **Rights (Chapter 3 GDPR):**
    - Right of access, Right to be informed, right of rectification, right of erasure, right to restriction of processing, right of data portability, right to object, Automated individual decision-making

What I did with Netflix

- Get a copy of my personal data :
- I exercise my right of access

privacy@netflix.com

NETFLIX

- **Visit your account page**

OR

- **Scan of an official issued ID document**

What should I do?

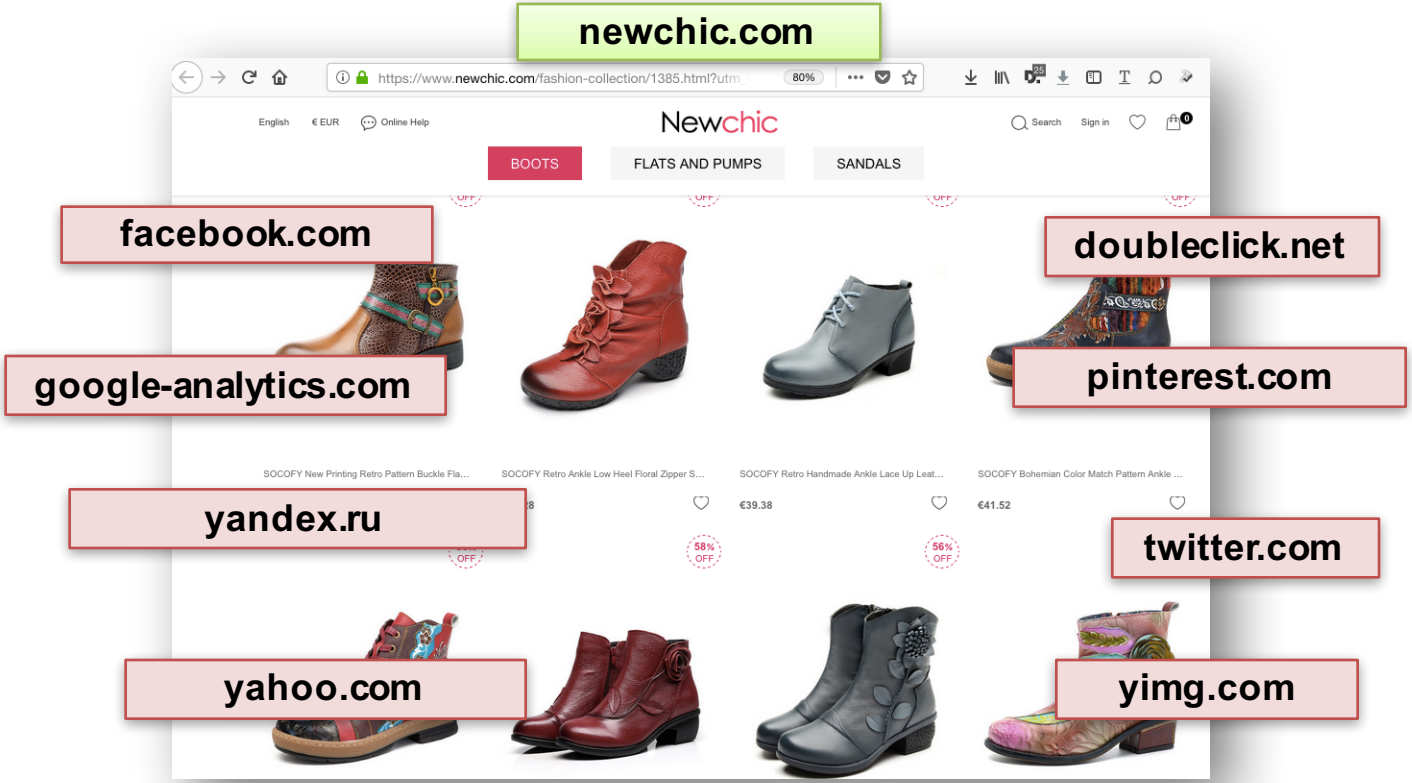
Concrete risks

Data subject	Data controller
• ***How do I exercise my right of access?*** • ***How do I prove my identity to the controller?***	• ***Is the request legitimate?*** • ***What is necessary to identify the subject's data?***
Risks: **•Impersonation (data breach)** ○ "Take the data whoever you are" **•Abusive identity check (privacy invasion)** ○ Nataliia, I need to know your blood type to authenticate you.	Risks: **•Incorrect disclosure (data breach)** ○ You are Nataliia, here is Coline's data. **•Impossibility of authentication (denial of access)** ○ I cannot prove you own the data

What we did in our paper

- DPA recommandations
- How to exercise SAR on popular websites?
- **How to exercise SAR on third-party trackers?**

Third-party tracking



How third parties let me exercise my rights?

Is it clear how to exercise my access rights?	Is there a clear way to exercise our right? DPO contact info?
Authentication of data subject	Is it enough to provide cookies/mobile ID used for tracking or they require a national ID card?
Simplicity	Is there a direct access to my data on a platform or should I send an email?

Third-party tracker	Authentication					Simplicity	
	Online identifier		Other data			Direct access	email
	Cookies	Mobile ID	Name and surname	Email	ID card		
Google domains	∅	∅	∅	∅	∅	∅	∅
facebook.com	∅	∅	∅	∅	∅	∅	∅
adnxs.com	✔	✔	×	×	×	✔	×
casalemedia.com	∅	∅	∅	∅	∅	∅	∅
openx.com	∅	∅	∅	∅	∅	∅	∅
pubmatic.com	✔	✔	✔	✔	✔[1]	×	✔
smartadserver.com	✔	×	×	✔	×	×	✔

[1]pubmatic.com also asks for a witness to sign a form and provide his ID card as well!

Exercising SAR on 30 popular third party trackers

- We identified 25 companies that own top 30 third-party tracking domains

Impossible even to start exercising SAR	4
Not able to get information on how to exercise SAR before we give the data	2
Deny access to third-party data	7
Use third-party cookies as online identifier	12
Require copy of an ID card	4
Direct access without any additional info	**2**

How to fix it?

- **Industrial cookies are bad for you**
  - Cookies are only made by companies
  - Privacy unfriendly by purpose
  - Privacy unfriendly by design
- **Homemade cookies are much better**
  - Cookies chosen by the user
  - Cookies embedding proof of ownership
  - **Have a look on our paper to taste it!**

Security Analysis of Subject Access Request Procedures.
Coline Boniface, Imane Fouad, Nataliia Bielova, Cédric Lauradoux, and Cristiana Santos.
Annual Privacy Forum (APF 2019).