



# NETFLIX

**I wanted to get a copy of my personal data collected  
by Netflix**

**How am I supposed to proceed?**

# THE GENERAL DATA PROTECTION REGULATION (GDPR)

**1973** : SAFARI's project

**1978** : " Loi informatique et libertés" + CNIL

**2004** : Law relevant to protection of people against treatment of personal data

**2016** : Law for a digital republic (Loi Lemaire)

**2018** : General Data Protection Regulation

Article 15: **right of access** by the data subject

## DEFINITION OF PERSONAL DATA

### ARTICLE 4 GDPR

*Any information relating to an **identified or identifiable individual***

*An **identifiable person** is one who can be identified, directly or indirectly, in particular by reference to an **identification number** (e.g. social security number) or one or more **factors** specific to his **physical, physiological, mental, economic, cultural or social identity** (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA ...)*

# ANY RIGHTS ON MY DATA?

1. Right to be informed
2. Right of access
3. Right of rectification
4. Right of erasure
5. Right to restriction of processing
6. Right of data portability
7. Right to object
8. Automated individual decision-making



Right of access



# RIGHT OF ACCESS

## What is it for?

- To know the data an organization processed on you
- To check the accuracy of the data

## Which cases are concerned with?

- To know if you are in a file that harms you
- To know the data in your medical file
- To know what a social network has about you

## How to do it concretely?

- **Identify** the organization to contact
- **Authentication** step
- Identification of the **relevant data** by the data controller



# What I did with Netflix



Get a copy of my personal data

[privacy@netflix.com](mailto:privacy@netflix.com)



- Visit your account page
- Scan of an official government issued ID document



**What should I do?**

# **SOME REFLEXIONS ...**

- **Is the Netflix way correct?**
- **Any recommendations from DPAs?**
- **What are popular websites doing?**
- **What about third parties?**



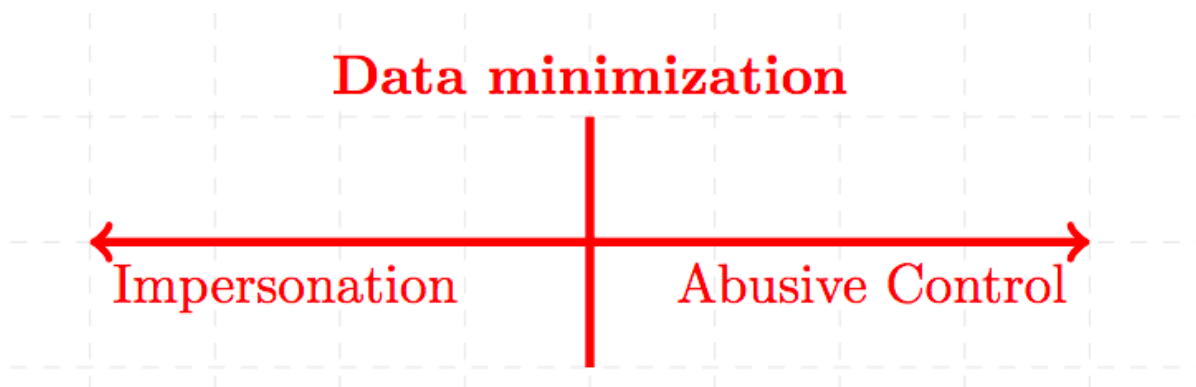
# Is the Netflix way correct?

## Yes on a regular basis

- Article 12.6

*"if reasonable doubts concerning the identity of the natural person making the request ➡ provision of additional information"*

- Prevent risk of **impersonation** (abuse of the access right)



## No on a rational basis

- **Abusive control:** data controller ask unnecessary and irrelevant information
- Abusive control can lead to impersonation

# Any recommendations from DPAs?

**Article 51, 55, 57 GDPR:** *independent public authorities responsible for monitoring the application of the Regulation*

**Indirect access request case:** the DPA acts as a proxy controller

## About the authentication of the data subject?

Country	Recom.	Authentication	Country	Recom.	Authentication
Austria <a href="#">[37]</a>	✓	Customer ID or copy of the national identity card	Italy <a href="#">[69]</a>	✗	Data minimization
Belgium <a href="#">[39]</a>	✓	Copy of the national identity card	Latvia <a href="#">[53]</a>	✓	Data minimization
Bulgaria <a href="#">[45]</a>	✗	Copy of the national identity card	Lithuania	–	–

## 27 European DPAs:

- All explain what are subject's rights
- 17 authorities provide guidelines
- 4 DPAs require a copy of an ID card
- 7 interesting DPAs recommendations

# What are popular websites doing?

- **Top 50 Alexa evaluation criterias**

---

**Authentication of the data subject**



Any extra information required?

**Channel security**



https connections or plaintext email?

**Privacy proxy**



Subject access request managed by another company?

**Simplicity**



Access user-friendly?

**Eligibility**



European citizen/resident?

# Results of my evaluation

	<b>Authentication</b>	<b>Channel security</b>	<b>Privacy proxy</b>	<b>Simplicity</b>	<b>Eligibility</b>
<b>Website</b>	Require a copy of the national identity card?	Use https connection?	Rely on privacy proxy service for subject access right?	Access to data is user-friendly?	Check eligibility as an EU user?
<b>Google</b>	X	✓	X	✓	X
<b>Facebook</b>	X	✓	X	✓	X
<b>Alipay</b>	✓	X	X	X	✓
<b>Amazon</b>	X	✓	X	X	X
<b>Netflix</b>	✓	X	X	✓	✓
<b>Pornhub.com</b>	X	X	✓	✓	X

# What I observed

## Authentication

- Copy of an ID card: Alipay, Netflix

## Channel security

- Use non secure connection: Alipay, Netflix, Pornhub

## Privacy proxy

- Pornhub delegates data subject's request to another company

## Simplicity

- Alipay and Amazon have complicated procedure for data subjects' exercise of their right of access

## Eligibility

- Alipay and Netflix check whether the data subject is an European citizen