GDPR: When the Right to Access Personal Data Becomes a Threat

Luca Bufalieri, Massimo La Morgia, Alessandro Mei, Julinda Stefa

Speaker

Massimo La Morgia

lamorgia@di.uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

The General Data Protection Regulation

Inbox **Squarespace is ready for the GDPR** - Stores GDPR goes into effect on May 25th /> The General Data Protection Regulation, or GDPR,

Inbox **We've Updated Our Privacy Policy** - Regulation (GDPR) coming into effec May 25th 2018. GDPR creates a single set of rules to modern

Inbox **We've updated our Privacy Policy** - UK (GDPR). What is GDPR?

Inbox **Update Your Newsletter Preferences** - ("GDPR") is coming into effect, and you've probably already gotten a few emails about this from ot

Inbox **Updates to Spotify Privacy Policy** - the ("GDPR") We have always strived to provide you with clear and simple information about the perso

Inbox **Updates to our Privacy Statement** - Regulation (GDPR) the new European Union privacy laws, SEEK has made relevant changes to our

Inbox **We've updated our Privacy and Cookie Policy. Here's what you need to know...** - Regulation (GDPR) law takes effect. In a nutshell, it give

Inbox **Act now or lose all this good stuff** - View online http://view.i.tpexpress.co.uk/?qs=

Inbox **An update on our Privacy Policy** - Regulation (GDPR), which comes into effect on the 25th May 2018. At Papa John's, we are committed

Inbox **You're not alone...** - a-gdpr-intervention] A GDPR intervention [https://www.lawscot.org.uk/news-and-events/news/a-gdpr-intervention

Inbox **You're in control** - Your partial postcode: 9AP Royal Bank of Scotland If you are reading this message, either your email

Inbox **Improvements to our Privacy Policy and Privacy Controls** - Regulation (GDPR) takes effect across the European Union. Designed to harr

Inbox **Notice of Terms of Service and Policy Updates** - Regulation (GDPR), which goes into effect on May 25, 2018. We've posted these update

Inbox **Survey of EU/devolved powers, CPD events and more** - under-gdpr] GDPR: What's new for controllers and processors? [https://www.la

Inbox **Mr Callery, data privacy law is changing** - Mr Callery, data privacy law is changing

GDPR

Data Protection Officer (DPO)

Compliance

25 May 2018

Data Breaches

Personal Data

Which is the actual deployment of the GDPR?

How they identify the requester?

How they transmit the personal data?

Do they transmit all the data?

The top 500 sites on the web

334 Web sites

Global By Country By Category

Adult	7.5%	Health	1.8%	Science	3.9%
Arts	5.1%	Kids and Teens	2.8%	Shopping	15.6%
Business	7.8%	News	7.2%	Society	6%
Computers	9.6%	Recreation	12,9%	Sports	5.4%
Games	8.4%	Reference	5.7%		

Chapter 1

Performing the Data Subject Access Request

Privacy Policy Compliance

The controller shall provide the data subject the following information:

- The contact details of the DPO
- The existence of the right to request data

Everything OK!

No user rights (53)
Or
No Contact point (3)

NO GDPR (6)
Or
PP not working (3)

Request methology

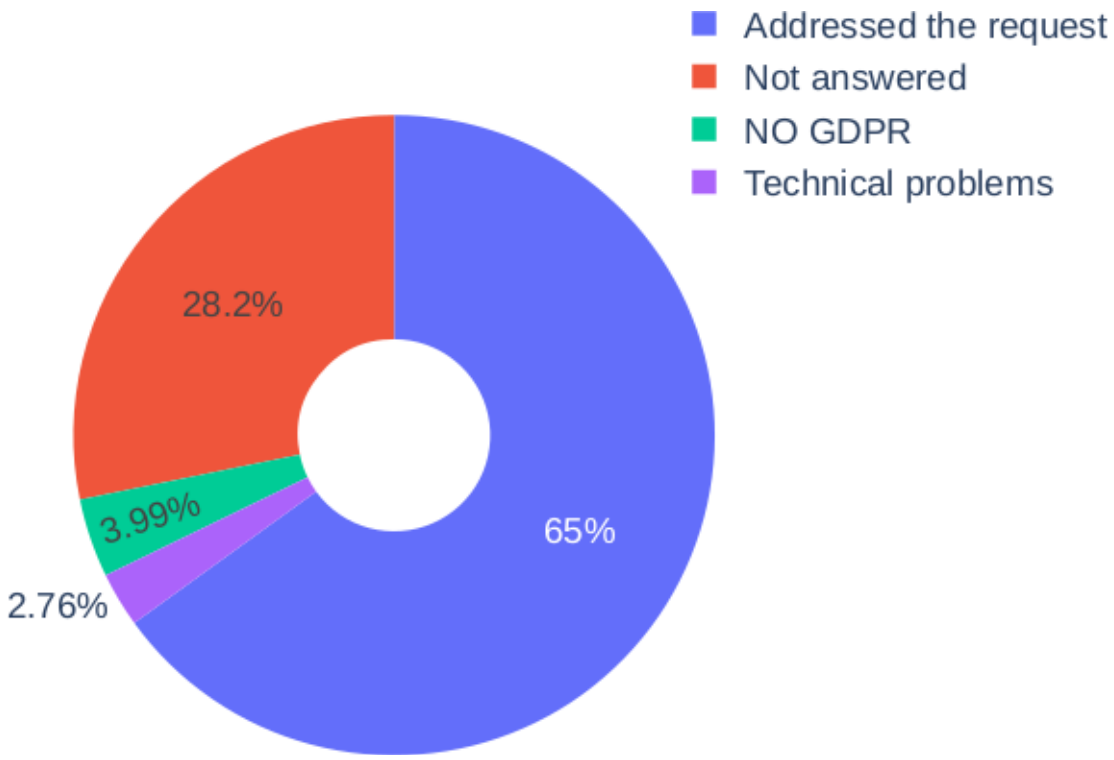
- Email (66%)
- Compile Form and send it via email (3.3%)
- Online Form (28.9%)
- Phone call or standard mail (1.81%)

User Identification

- Identity document (33)
- Knowledgeable Questions (19)
- Cookie (3)
- Sworn declaration (3)
- Email confirmation (21)
- Phone call (3)

- Trust the email address of the requester (51)

Response Obtained



	GDPR Rights	NO GDPR Rights
Addressed the request	195	17
Did not answer	69	23
Refused	0	13
Total	264	53

Response time

Article 12

The controller shall provide information within one month of receipt of the request. That period may be extended by two further months where necessary.

Average response time: 16.4 days

17.54% answered the same day

89.15% answered in time

Data Format

No standard response format

- Email body
- PDF
- Standard mail
- Json

- txt
- HTML
- Docx
- XML

Data Format

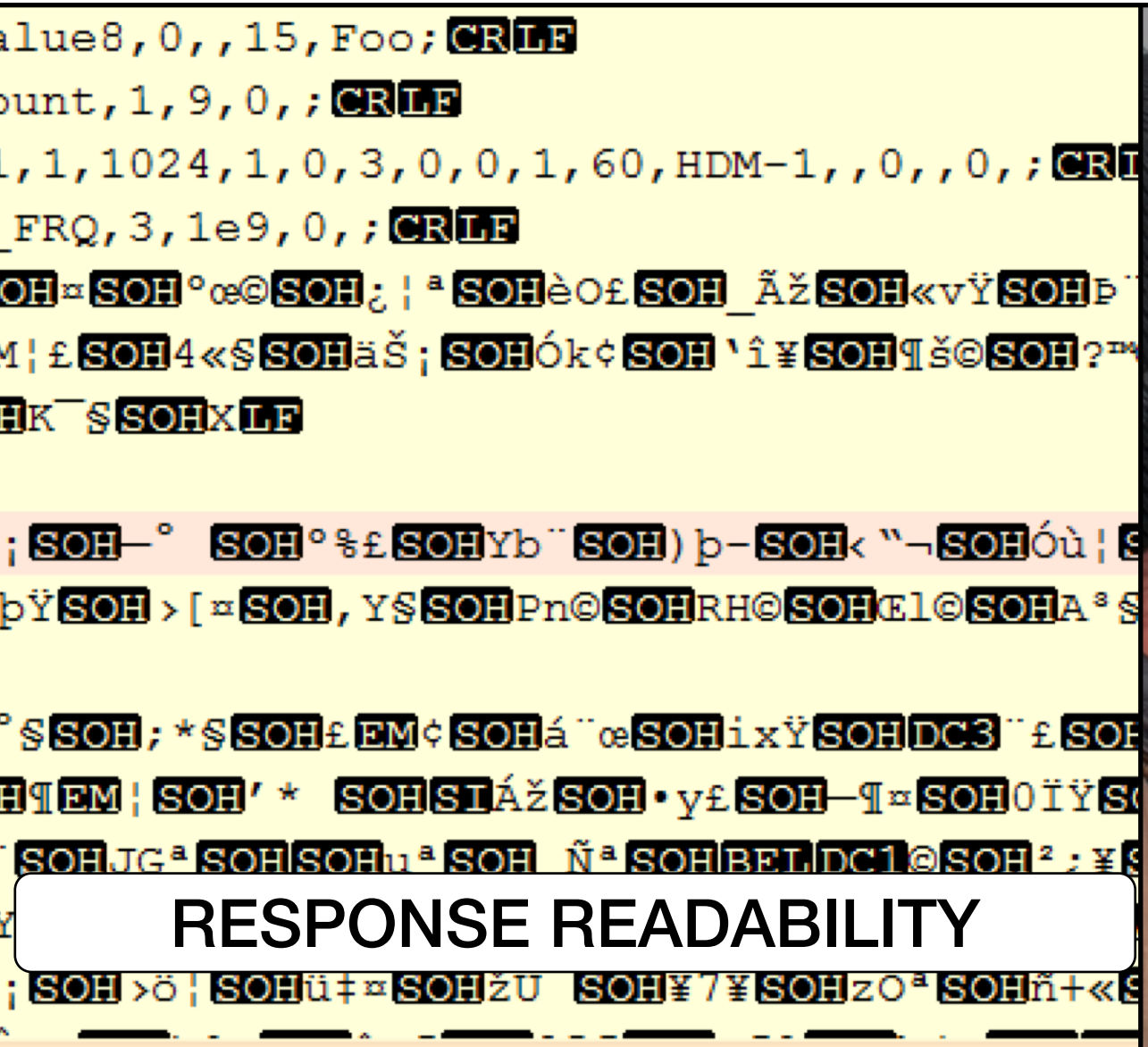
Article 20

The data subject shall have the right to access to the personal data **in a structured, commonly used and machine-readable format.**

52.7%

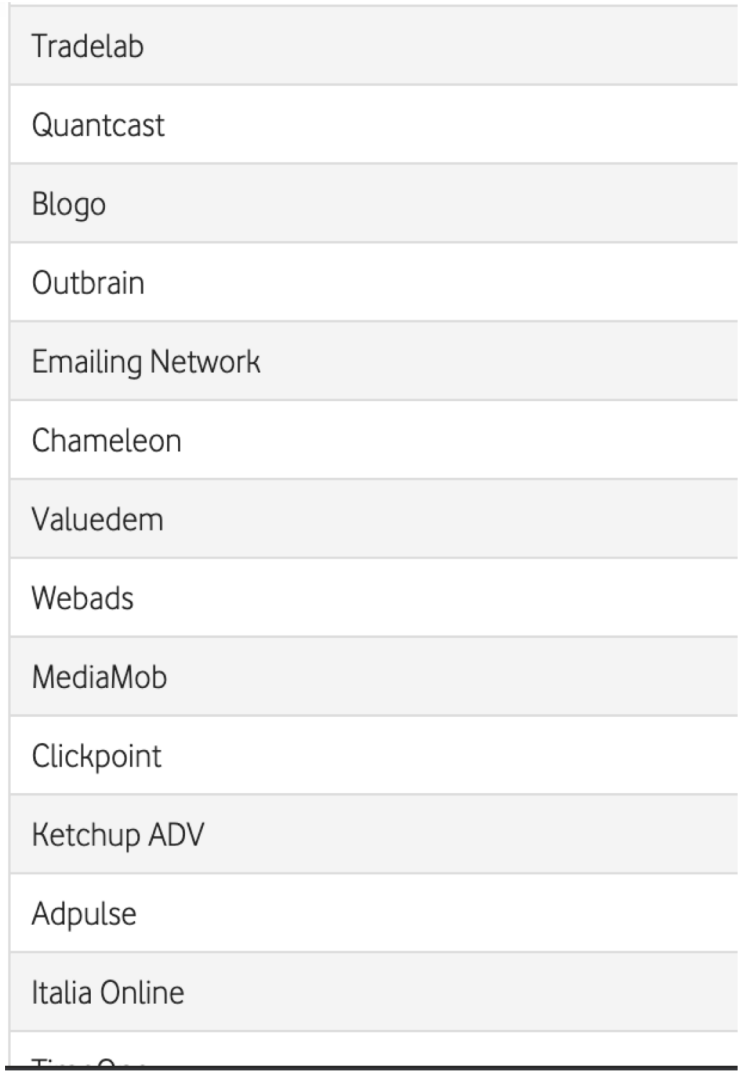
Probably the same way to handle the data access and data portability requests

Information *(not)* achieved



Information *(not)* achieved

- Google Analytics
- Turn
- Prime Real Time
- Google Adwords
- Yahoo
- Doubleclick
- ClickPoint
- Criteo
- Zanox
- Facebook
- Amazon
- Microsoft
- Adform
- Rocketfuel
- Turbo Adv
- AppNexus
- HiMedia
- Adgo!
- Webperformance



Only 6 data controllers provide data about 3rd party trackers.

On average private news media use more than 30 third-party services

Chapter 2

Privacy concerns & experiments

Sharing data

2

No TLS!

Sniffing or man in the middle attacks

Sharing data

82

TLS

+

Plain file

Compromised server Or Incorrect recipient

Sharing data

20

TLS

+

Encrypted data

Password send on the same email

Sharing data

TLS

+

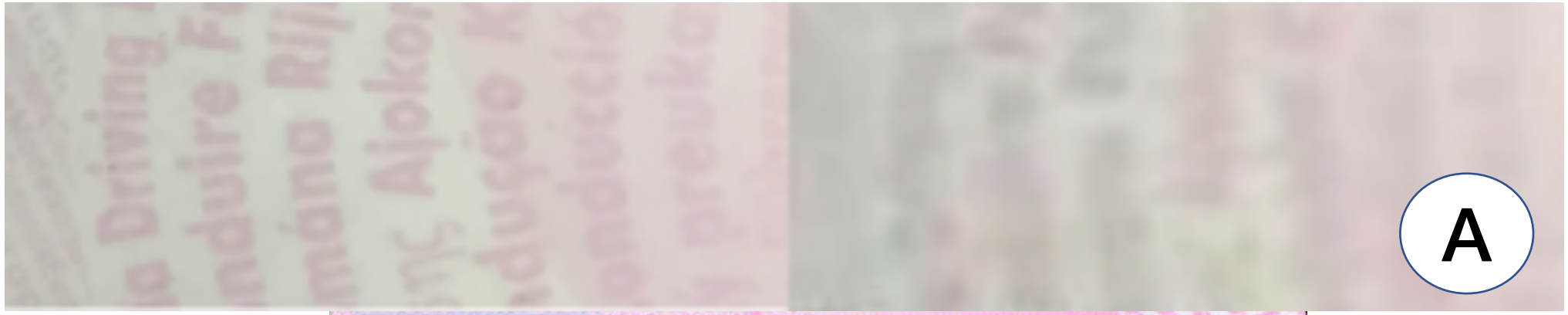
Encrypted data

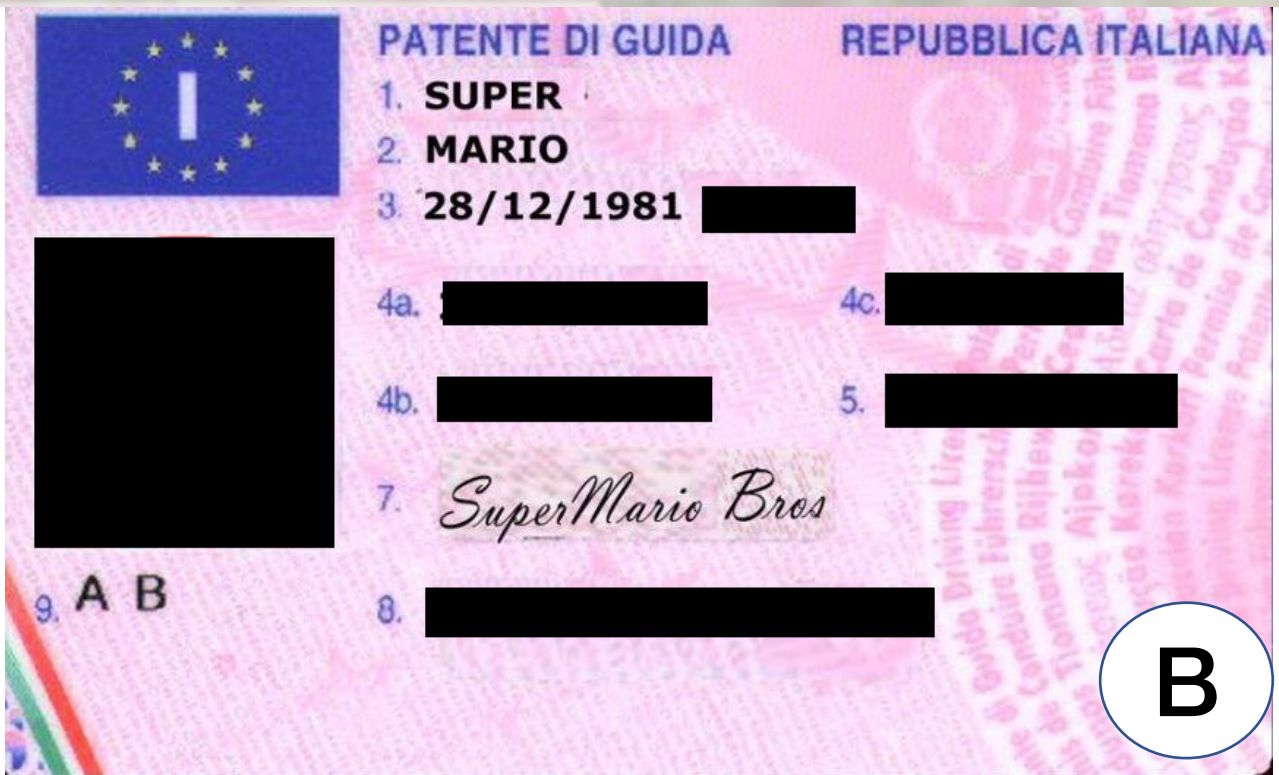
+

Different channel

Same pattern to create the password

Tampering the Identity card





Tampering the Identity card

21 out of 25 accepted the Pixelized + obfuscated document

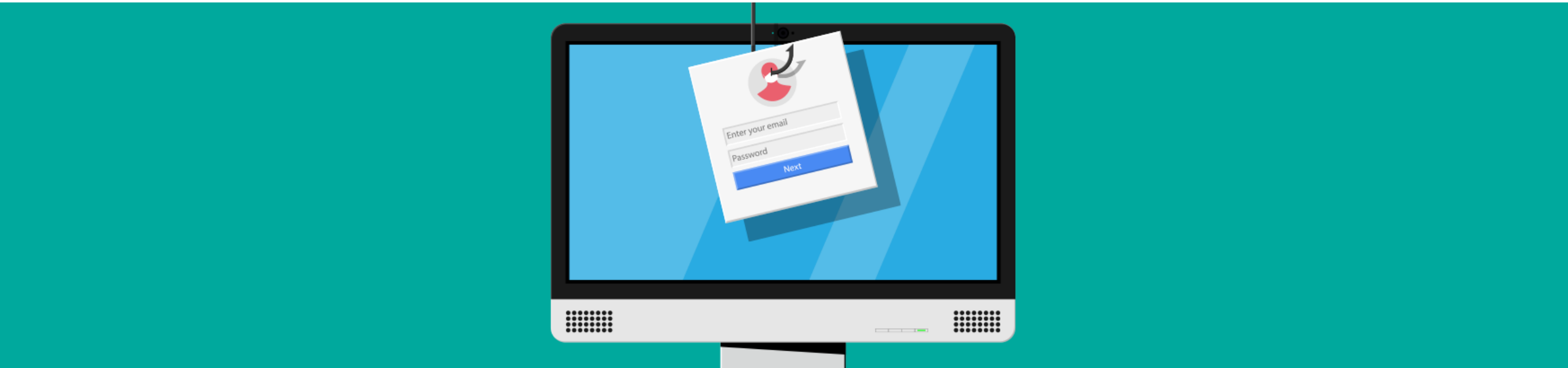
The remaining 4 accepted the pixelized one

Email as authentication

51 data controllers based the user identification on the email address

johndoe@provider.com

johnndoe@provider.com



Email as authentication

19 out of 51 sent us the data

1 data controller **deleted** the account

Data escalation

Starting from few initial information, attackers can build up a chain of request and jeopardize the privacy of the user.

The end

Thank you for your attention!