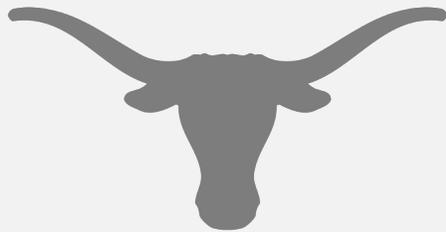


Analyzing GDPR Compliance Through the Lens of Privacy Policy

Jayashree Mohan, Melissa Wasserman,
Vijay Chidambaram



vmware®



TEXAS

The University of Texas at Austin

General Data Protection Regulation (GDPR)

Respect the rights of
data owner

Gathered legally,
for a purpose

**Personal
Data**

Protect it from
misuse/exploitation

Non-compliance can result in hefty **finances and penalties**

2019 : The year of enforcement!

Google (\$55 million)

Jan 2019

Lack of explicit consent
and transparency

Taxa 4x35 (\$180 K)

March 2019

No timely deletion

Haga Hospital(\$550 K)

July 2019

Lax controls over logging
and access

**Mariott
(\$124 million)**

July 2019

Poor data security

**British Airways
(\$230 million)**

July 2019

Poor data security

2019 : The year of enforcement!

Google (\$55 million)

Jan 2019

Lack of explicit consent
and transparency

Taxa 4x35 (\$180 K)

March 2019

No timely deletion

Haga Hospital(\$550 K)

July 2019

Lax controls over logging
and access

Mariott
(\$124 million)

July 2019

Poor data security

British Airways
(\$230 million)

July 2019

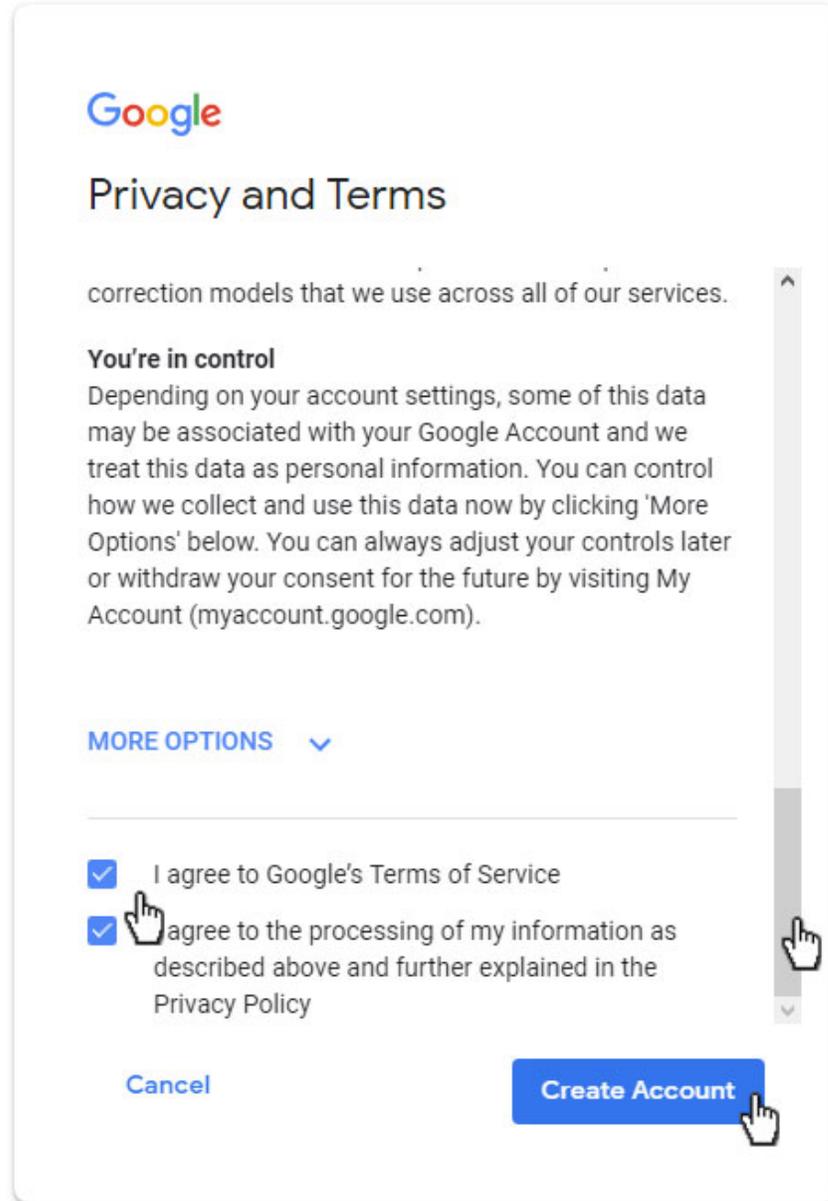
Poor data security

Transparency

Google (\$55 million)

Jan 2019

Lack of explicit consent
and transparency



The screenshot shows the Google 'Privacy and Terms' page during account creation. At the top is the Google logo and the title 'Privacy and Terms'. Below this is a paragraph about 'correction models that we use across all of our services.' followed by a section titled 'You're in control' which explains that data is treated as personal information and can be controlled via 'More Options'. A 'MORE OPTIONS' link with a downward arrow is visible. Below this are two checked checkboxes: 'I agree to Google's Terms of Service' and 'I agree to the processing of my information as described above and further explained in the Privacy Policy'. At the bottom are 'Cancel' and 'Create Account' buttons. A vertical scrollbar on the right side of the content area is visible, with a mouse cursor pointing to it. Another mouse cursor is pointing to the 'Create Account' button.

What GDPR Requirements did Google fail to meet?

“Lack of transparency, inadequate information and lack of valid consent regarding ads personalization”

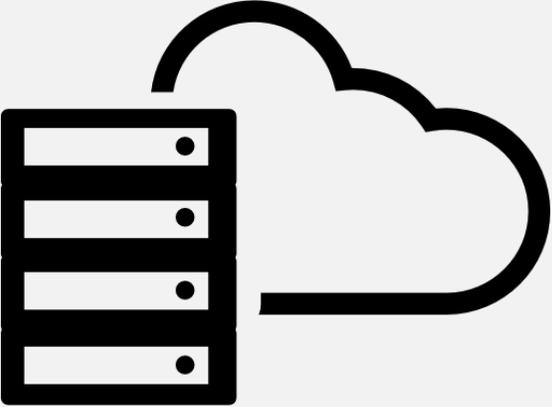
Transparency

GDPR Article 12

The controller shall take appropriate measures to provide any information... relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Clear and Concise Privacy Policy

Privacy Policy



Data Processor/ Controller



Ask consent and establish user rights via privacy policy



Users/ Customers

Privacy Policy



Long



Use jargons



Difficult to comprehend

How can users consent to their personal-data use if they cannot read/understand privacy policies?

Main takeaways

1. What are the key information any GDPR compliant system should provide to its user in a straight-forward way?
2. Identifying GDPR dark patterns : Case study of privacy policy of 10 popular cloud services
3. A systems perspective on solving GDPR dark patterns

Main takeaways

1. **What are the key information any GDPR compliant system should provide to its user in a straight-forward way?**
2. **Identifying GDPR dark patterns : Case study of privacy policy of 10 popular cloud services**
3. **A systems perspective on solving GDPR dark patterns**

Outline

- GDPR-compliant privacy policy
- Case study of privacy policy of 10 cloud services
- GDPR dark patterns
- Future directions

Outline

- **GDPR-compliant privacy policy**
- Case study
- GDPR dark patterns
- Future directions

GDPR Compliant Privacy Policy

1 **WHO** uses the collected data

Processing Entities : The source of data, and the entities with whom data is shared.

GDPR Compliant Privacy Policy

1 **WHO** uses the collected data

2 **WHAT** personally identifiable data is collected

Data categories: Attributes of personally identifiable information collected

GDPR Compliant Privacy Policy

1 **WHO** uses the collected data

2 **WHAT** personally identifiable data is collected

3 **WHY** is the data being collected

Purpose: The legal basis for collection and processing of each data category

GDPR Compliant Privacy Policy

- 1 **WHO** uses the collected data
- 2 **WHAT** personally identifiable data is collected
- 3 **WHY** is the data being collected
- 4 **WHEN** will the collected data expire and be deleted
Retention: The policy or period of retention for each data category

GDPR Compliant Privacy Policy

- 1 **WHO** uses the collected data
- 2 **WHAT** personally identifiable data is collected
- 3 **WHY** is the data being collected
- 4 **WHEN** will the collected data expire and be deleted
- 5 **HOW** can a user exercise control over his/her data
User controls: How can users access/enforce their rights over data

GDPR Compliant Privacy Policy

- 1 **WHO** uses the collected data
- 2 **WHAT** personally identifiable data is collected
- 3 **WHY** is the data being collected
- 4 **WHEN** will the collected data expire and be deleted
- 5 **HOW** can a user exercise control over his/her data
- 6 **DOES** the controller ensure safety of user data
Data Protection: Measures taken to ensure safety and protection of user data

GDPR Compliant Privacy Policy

- 1 **WHO** uses the collected data
- 2 **WHAT** personally identifiable data is collected
- 3 **WHY** is the data being collected
- 4 **WHEN** will the collected data expire and be deleted
- 5 **HOW** can a user exercise control over his/her data
- 6 **DOES** the controller ensure safety of user data
- 7 **DOES** the controller appropriately notify users of changes in policy
Policy updates: Notify users appropriately of changes to privacy policy and ask consent

GDPR Compliant Privacy Policy

- 1 **WHO** uses the collected data
- 2 **WHAT** personally identifiable data is collected
- 3 **WHY** is the data being collected
- 4 **WHEN** will the collected data expire and be deleted
- 5 **HOW** can a user exercise control over his/her data
- 6 **DOES** the controller ensure safety of user data
- 7 **DOES** the controller appropriately notify users of changes in policy

Outline

- GDPR-compliant privacy policy
- **Case study**
- GDPR dark patterns
- Future directions

	Processing	Data	Retention	Purpose	Controls	Protection	Updates
Bloomberg	✗	✓	✗	✓	✗	✗	✗
Onavo	✗	✓	✗	✓	✗	✗	✓
Instagram	✗	✓	✗	✓	✓	✗	✓
Uber	✗	✓	✓	✓	✗	✗	✓
edx	✓	✓	✓	✓	✗	✗	✗
Snapchat	✓	✓	✓	✓	✓	✓	✗
icloud	✗	✓	✓	✓	✓	✓	✓
Whatsapp	✓	✓	✓	✓	✓	✓	✓
Flybe	✓	✓	✓	✓	✓	✓	✓
Metro bank	✓	✓	✓	✓	✓	✓	✓

5.4 6. HOW WE USE YOUR PERSONAL DATA

As part of our processing of your Personal Information, we are required to tell you what we use your Personal Information for and the lawful basis on which we can process your Personal Information:

Process	Purpose	Type of Personal Information	Lawful basis for processing	Details
Adyen Simon 1011 D Amster The Ne	To monitor browsing on our website or use our app	<ul style="list-style-type: none">• Technical Data	<ul style="list-style-type: none">• Legitimate interest• Consent	To improve the functionality and content of our website or our app. For more information please see our Cookie Policy.
Lloyds Cardne Phoeni Christo Basildc Essex SS14 3	To create an account with us	<ul style="list-style-type: none">• Identity Data• Contact Data	<ul style="list-style-type: none">• Legitimate interest	To collect information about our potential customers. We will not send you any electronic marketing unless you have expressly consented to receive it. To improve the speed at which you can purchase flights and services from us.

Outline

- GDPR-compliant privacy policy
- Case study
- **GDPR dark patterns**
- Future directions



GDPR Dark Patterns

Oftentimes we simply click 'I agree'. What are we signing up for ?

- 4 common dark-patterns in cloud service



1. User rights : All or Nothing



One checkbox to access all services



Deactivate account to object to processing any piece of collected info

No fine-grained control over personal data

Uber's Privacy Policy

"Uber may continue to process your information notwithstanding the objection to the extent permitted under GDPR"

edx's Privacy Policy

"Deleting user information does not apply to "historical activity logs or archives unless and until these logs and data naturally age-off"

2. Purpose bundling

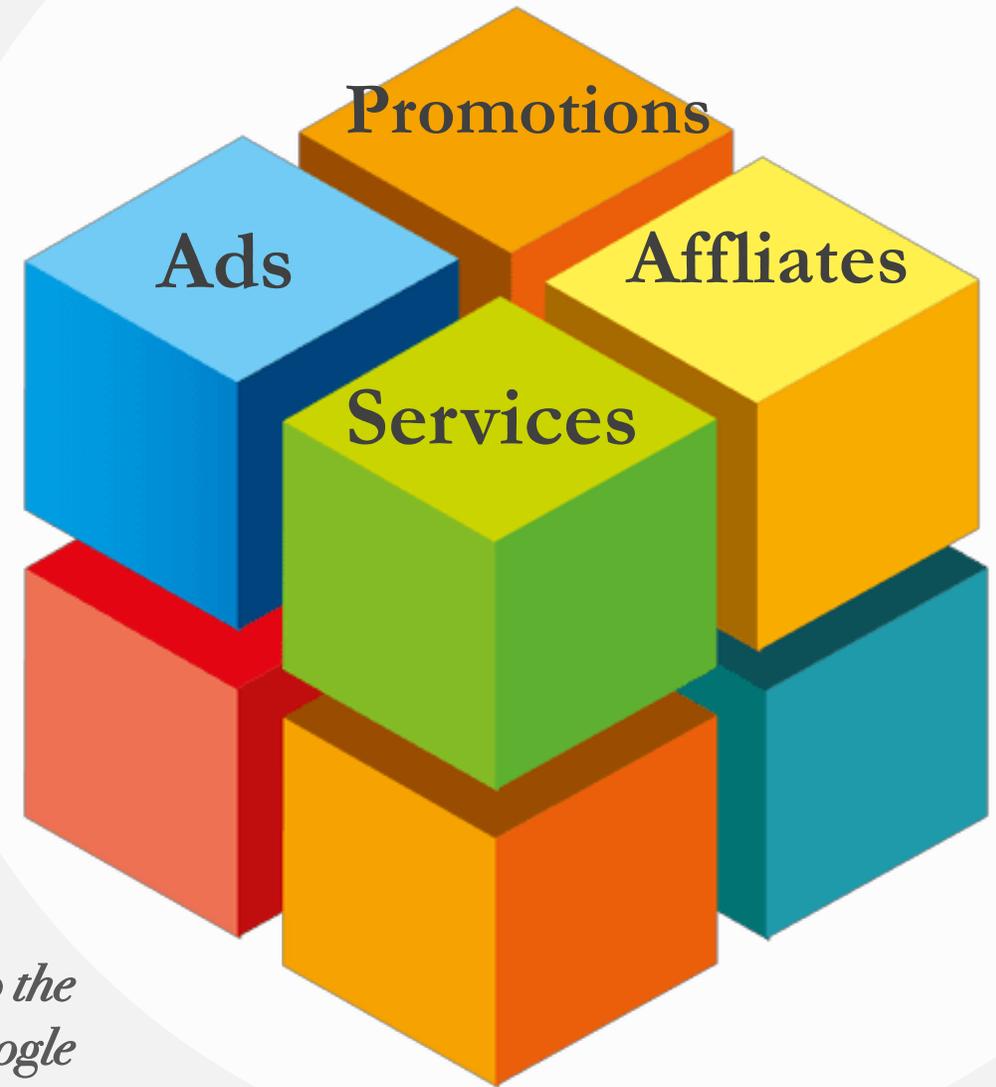
- No option to opt of specific services
- All the processing is bundled into one consent box

Instagram:

*“Our Service Providers will be given access to your information as is **reasonably** necessary to provide the Service under **reasonable** confidentiality terms”*

Google was fined \$55 Million for a similar charge

“Google’s consent flow doesn’t comply with the GDPR according to the CNIL. By default, Google really pushes you to sign in or sign up to a Google account. The company tells you that your experience will be worse if you don’t have a Google account. According to the CNIL, Google should separate the action of creating an account from the action of setting up a device – consent bundling is illegal under the GDPR.”



3. Notifications

- **Notify users of changes in privacy policy by appropriate means**
 - Ask for consent to the modified policy
 - Show users the new additions to privacy policy instead of asking them to accept the new terms by reading the entire policy document

Edx, Bloomberg

"Label the Privacy Policy as "Revised (date)[...]. By accessing the Site after any changes have been made, you accept the modified Privacy Policy and any changes contained therein"



Outline

- GDPR-compliant privacy policy
- Case study
- GDPR dark patterns
- **Future directions**

Is it enough if companies get their privacy policy right?

Are users able to enforce their rights that the privacy policy claims to provide?

Sarah Wipperman @swipp_it · May 22
4/ Recently, I opened up the Pokémon GO app after nearly 3 years to see what was new. They had a new terms of use and privacy policy. So I read it.

Sarah Wipperman @swipp_it · May 22
5/ In their privacy policy (nianticlabs.com/privacy), there is a section for "Your rights and choices":

7. Your rights and choices

You have certain rights in relation to your Personal Data. In order to exercise these rights, please contact us at:

- For Pokémon GO [here](#).
- For Ingress [here](#).
- For Harry Potter: Wizards Unite [here](#).
- For all other Services at privacy@nianticlabs.com.

You can:

- Request access to the Personal Data we hold on you.
- Delete or correct your Personal Data. The easiest way to update your account information is via your in-app settings. You can also submit a customer support request through our support website [here](#) for Pokémon GO, [here](#) for Ingress, or [here](#) for Harry Potter: Wizards

Sarah Wipperman @swipp_it · May 22
6/ So, as per the instructions, I wrote to the Pokémon GO contact form to a) object to them processing my Personal Data, and b) ask them to stop using my Personal Data for marketing and promotional purposes.

Sarah Wipperman @swipp_it · May 22
7/ What I got back was instructions on how to delete my account. Then, when I said I didn't want to delete my account but instead limit use of my data, I got more instructions on how to delete my account.

Note I never mentioned "delete" in any of my emails.





Carl Miller ✓
@carljackmiller

Friends! An investigation we've been working really hard on has been broadcast on [@BBCClick](#) today. I spent a month using GDPR to try to pull all my personal data into one place: 7000 pages in total.



Carl Miller ✓ @carljackmiller · May 25

And I didn't feel welcome in the land of the second business model. Getting my data back was like pulling teeth: broken portals, hard to find privacy policies with both legalistic and vague wording at the same time.

1 2 8



Carl Miller ✓ @carljackmiller · May 25

GDPR is helping us shine a light on the world of personal data, but it is still far from practical to do it. It is a time consuming, frequently frustrating journey to try to understand a world whose entire existence is based on trying to understand us.



 **Katarzyna**
@szymielewicz

Ad auction systems are "obscure by design": there is no way for users to exercise their rights to correct or delete marketing categories (even very sensitive ones). *IAB and IAB Europe to fix this failure*. Today we filed a complaint with the UK, Ireland and Poland regulators.

 **AdGuard**
@AdGuard

Twitter is accused of refusing a request to provide a user with information about their collected personal data, the company said it would require "disproportionate effort". This supposedly goes against #GDPR, an investigation is launched already.

 **Paul Joseph Watson**

SING to hand over data on why it was blocked 6 months later. This is in violation of GDPR. I'm going to drop it? I won't. I won't drop the data.

 **Johnny Ryan** @johnnyryan · Jan 28
Today @jimkillock of @OpenRightsGroup, @mika of @Panoptikon, and I filed new regulators the UK, Poland, and Ireland @ICOnews [brave.com/update-rtb-ad-...](https://www.brave.com/update-rtb-ad-...)
[Show this thread](#)



How do you advise their individual GDPR rights to their processors? It's an incredibly difficult question.

6 Retweets

 **Itkovian** @ltkovian ·
Replying to @Ruben
Are you going to follow?

 **Ruben Verborgh**
Of course. I live for it.

Twitter faces investigation by privacy watchdog over user tracking
Ireland's Data Protection Commission has launched an investigation into Twitter after it refused a request inquiring into its collection of location data from users.
[telegraph.co.uk](https://www.telegraph.co.uk)

APL · Apr 11
I've been unable to...
provide users with...
article 15
violation of our...
provide this...
of others, as set out in...
our Community...
have reported the breach...
triggers disablements...
protocols by potentially...
allow to adjust their behaviour...
ply with the request for this

2 17 19

597 4K 13.2K

Enable users a hassle-free control over their personal data

GDPR-compliant systems

Understand how GDPR affects the design and operation of Internet companies

[Seven GDPR Sins : HotCloud'19]

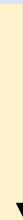


Translate these to the need for infrastructural changes

[Impact of GDPR on Storage Systems: HotStorage'19]

Simple, straight-forward privacy policies

Write clear, concise privacy policies



Tools to parse and identify GDPR compliance and user rights from a privacy policy

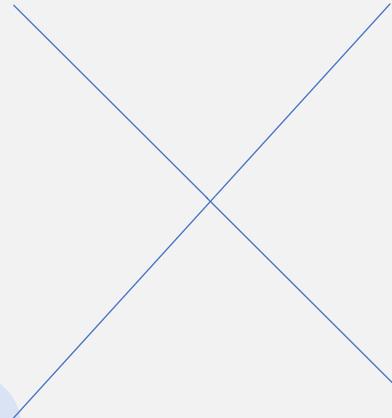
[Polisis: Security'18]

**Security &
Privacy**

Policy

Access Control

Systems





More works on analyzing GDPR from a systems perspective

<https://utsaslab.github.io/research/gdpr/>

Thanks