# General Data Protection Regulation: User consent & Privacy policies

Nataliia Bielova

nataliia.bielova@inria.fr

This presentation contains cookies that will be stored in your memory to give you the best user experience. By attending this presentation, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

# GENERAL DATA PROTECTION REGULATION

# GDPR

## TERRITORIAL SCOPE

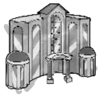
EU Establishments

Non-EU Established Organizations

Offer goods or services or engaging in monitoring within the EU.

## THE PLAYERS

Data Subjects

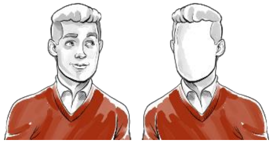


Data Controllers

Data Processors

Supervisory Authorities

## PERSONAL DATA



Identified

Identifiable

## SENSITIVE DATA

Racial or Ethnic Origin

Religious or Philosophical Beliefs

Political Opinions

Trade Union Membership

Sex Life

Health

Genetic Data

Biometric Data

## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

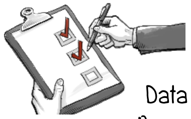
Security

Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

Record of Data Processing Activities

Maintain a documented register of all activities involving processing of EU personal data.

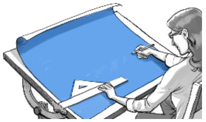


Data Impact Assessment

For high risk situations

Data Protection by Design

built in starting at the beginning of the design process



## LAWFUL PROCESSING

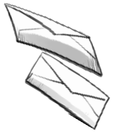
Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests

## CONSENT

Consent must be freely given, specific, informed, and unambiguous.

## DATA BREACH NOTIFICATION



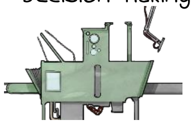
A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

## RIGHTS OF DATA SUBJECTS

Transparency



Automated Decision Making

"Right not to be subject to a decision based solely on automated processing, including profiling."

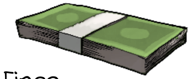
Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

## ENFORCEMENT



Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:

compensation for material and non-material harm.

## INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY 2019

www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

Please ask permission to reuse or distribute

## TERRITORIAL SCOPE

EU Establishments

Non-EU Established Organizations

Offer goods or services or engaging in monitoring within the EU.

## THE PLAYERS

Data Subjects

Data Controllers

Data Processors

Supervisory Authorities

## PERSONAL DATA

Identified

Identifiable

## SENSITIVE DATA

Racial or Ethnic Origin

Religious or Philosophical Beliefs

Political Opinions

Trade Union Membership

Sex Life

Health

Genetic Data

Biometric Data

## LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests

## CONSENT

Consent must be freely given, specific, informed, and unambiguous.

## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security

Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

Record of Data Processing Activities

Maintain a documented register of all activities involving processing of EU personal data.

Data Impact Assessment

For high risk situations

Data Protection by Design

built in starting at the beginning of the design process

## GDPR

## DATA BREACH NOTIFICATION

A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

## RIGHTS OF DATA SUBJECTS

Transparency

Automated Decision Making

"Right not to be subject to a decision based solely on automated processing, including profiling."

Access and Rectification

Right to Erasure

Purpose Specification and Minimization

Right to Data Portability

## ENFORCEMENT

Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.

Effective Judicial Remedies:

compensation for material and non-material harm.

## INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Binding Corporate Rules (BCRs)

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY 2019

www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

Please ask permission to reuse or distribute

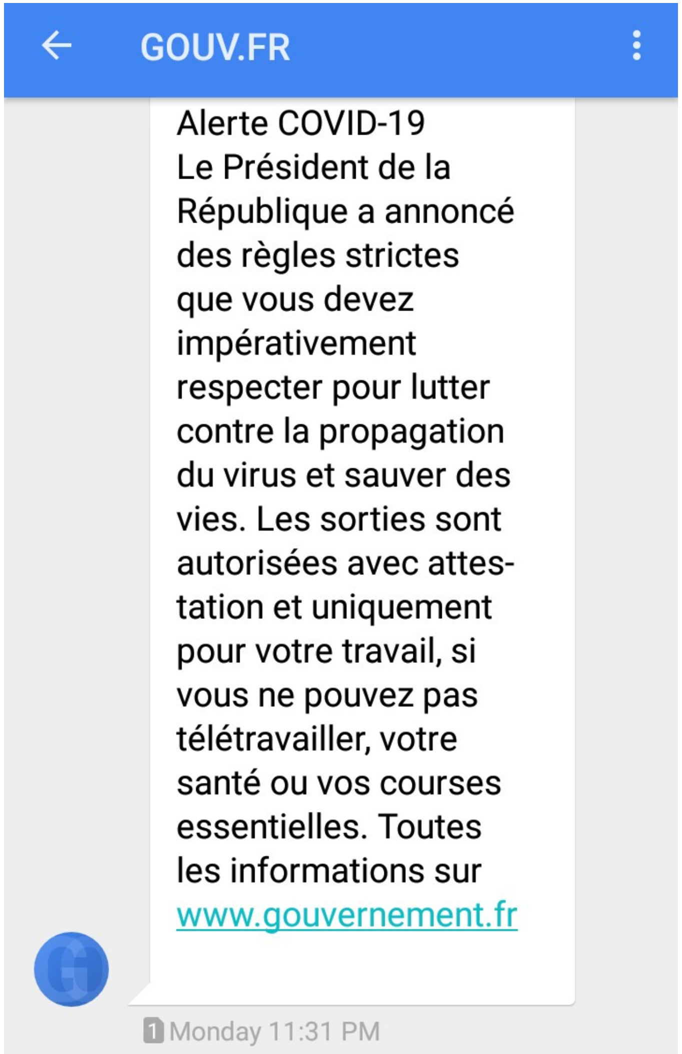
# LAWFUL PROCESSING OF PERSONAL DATA

# Legal bases for processing personal data

1. **Consent**
2. **Contract necessity** for the performance of a contract between the controller and subject
3. **Compliance with a Legal Obligation**
4. **Task in the Public Interest,** official functions or a task in the public interest
5. **Protecting Vital Interests** of the data subject, e.g., to protect someone´s life during medical emergency (life and death)
6. **Legitimate Interest of the data controller** balanced against the rights and freedoms of the individual

https://gdpr-info.eu/art-6-gdpr/ https://gdpr-info.eu/recitals/no-40/

# Which legal basis?



GOUV.FR

Alerte COVID-19
Le Président de la République a annoncé des règles strictes que vous devez impérativement respecter pour lutter contre la propagation du virus et sauver des vies. Les sorties sont autorisées avec attestation et uniquement pour votre travail, si vous ne pouvez pas télétravailler, votre santé ou vos courses essentielles. Toutes les informations sur www.gouvernement.fr

Monday 11:31 PM

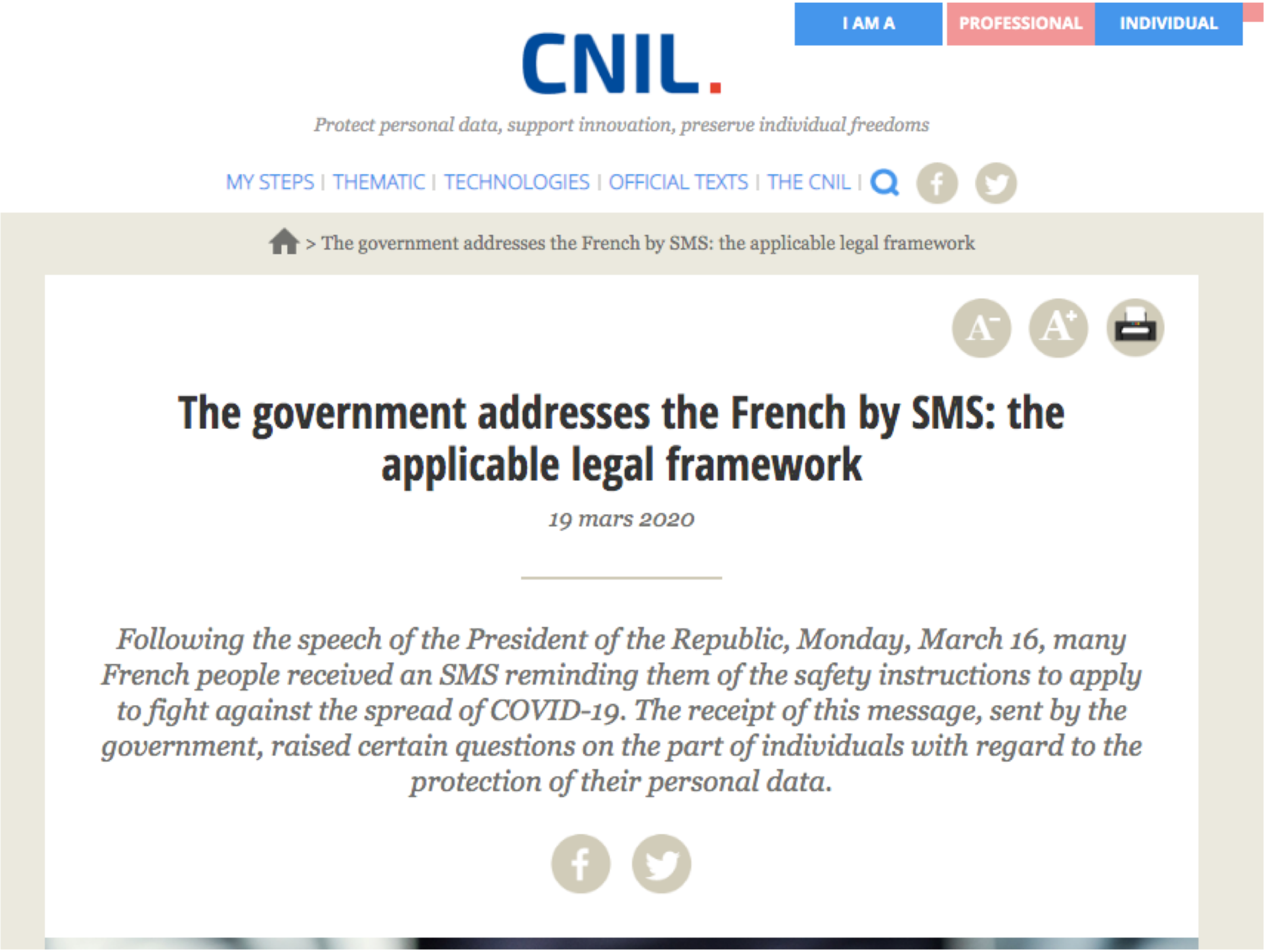
- Does the government has access to all the mobile phone numbers of people in France?
- Does GDPR apply and how is it possible?

SMS I received on Monday, 16 March 2020

# CNIL responded…

- No telephone number transmitted to the government!
- « the government only sent a message to the operators, who were responsible, with their own databases, for routing it to individuals.»

# https://www.cnil.fr/fr/le-gouvernement-sadresse-aux-francais-par-sms-le-cadre-legal-applicable

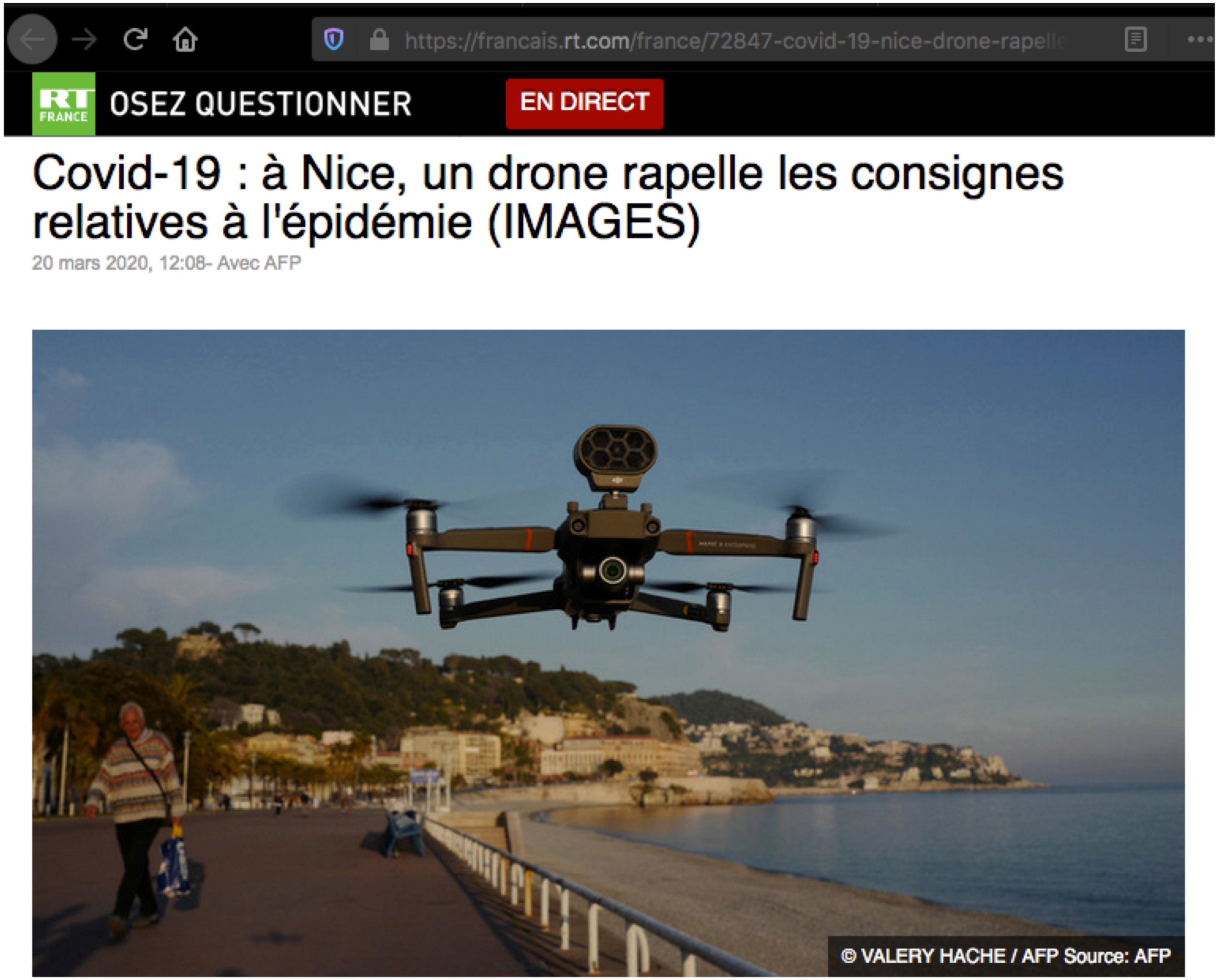

I AM A
PROFESSIONAL
INDIVIDUAL
CNIL.
Protect personal data, support innovation, preserve individual freedoms
MY STEPS | THEMATIC | TECHNOLOGIES | OFFICIAL TEXTS | THE CNIL |
> The government addresses the French by SMS: the applicable legal framework
A⁻ A⁺

## The government addresses the French by SMS: the applicable legal framework

*19 mars 2020*

*Following the speech of the President of the Republic, Monday, March 16, many French people received an SMS reminding them of the safety instructions to apply to fight against the spread of COVID-19. The receipt of this message, sent by the government, raised certain questions on the part of individuals with regard to the protection of their personal data.*

# Which legal basis?


https://francais.rt.com/france/72847-covid-19-nice-drone-rapelle
RT FRANCE
OSEZ QUESTIONNER
EN DIRECT

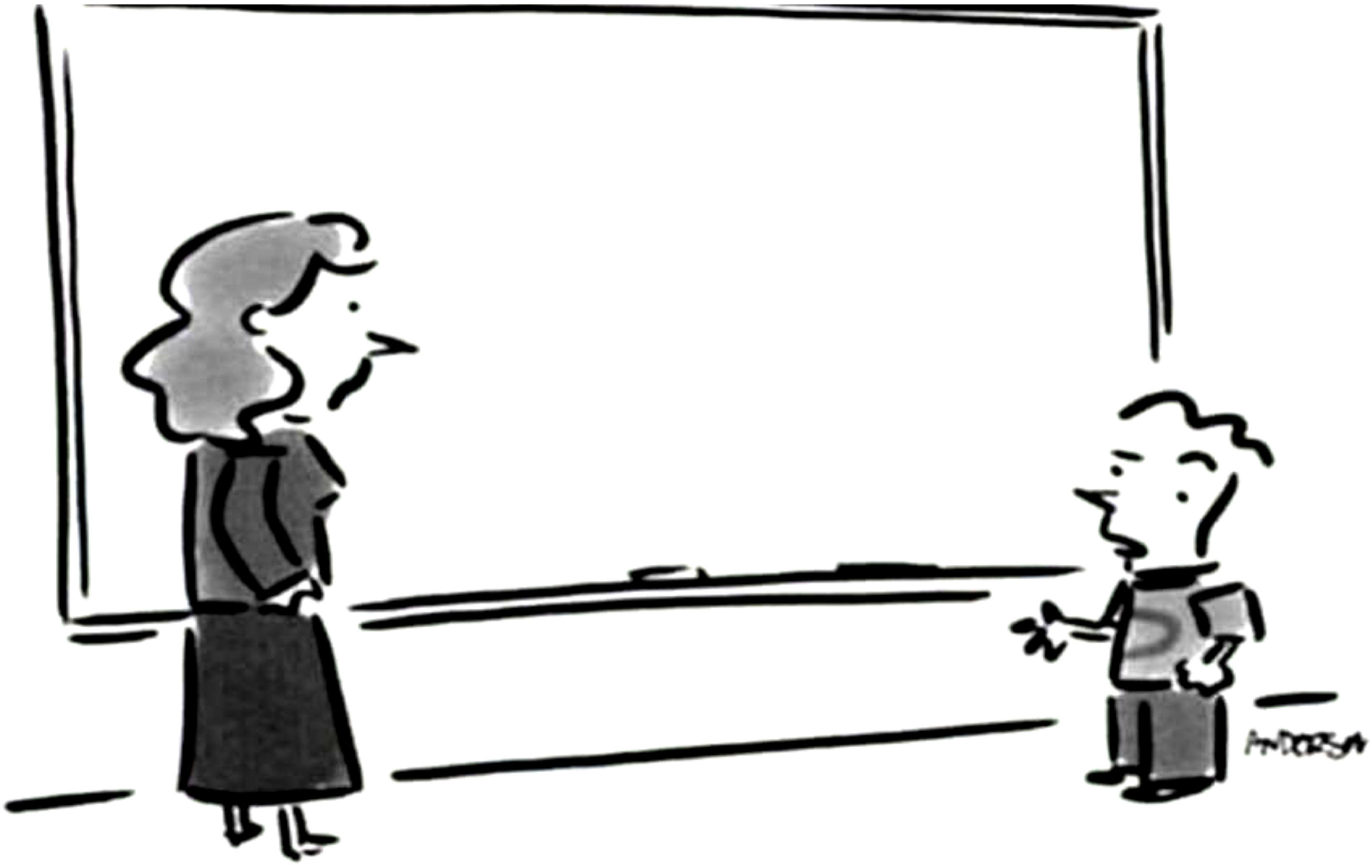
## Covid-19 : à Nice, un drone rapelle les consignes relatives à l'épidémie (IMAGES)

20 mars 2020, 12:08- Avec AFP

© VALERY HACHE / AFP Source: AFP

A Nice, sur la promenade des Anglais, un drone survole la ville et ordonne aux personnes de rentrer chez elles. Nice, le 20 mars 2020.

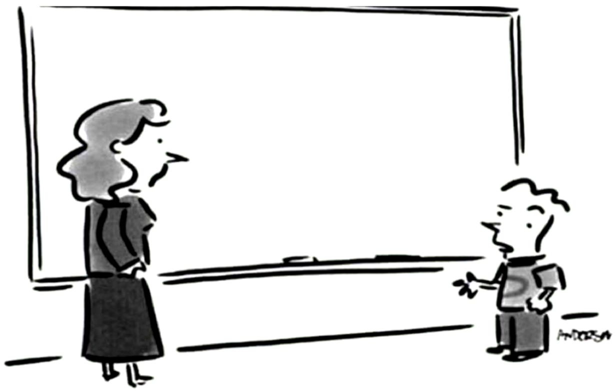
# Consent



"Before I write my name on the board, I'll need to know how you're planning to use that data."

# Consent

- **What?** Mechanism to give data subjects control/**choice** over whether or not personal data concerning them will be processed
- **When?** Given before processing starts
- **How?** No limits on form
- **Elements of valid consent** (Article 4(11) of GDPR)
  1. Free
  2. Specific
  3. Informed
  4. Unambiguous



"Before I write my name on the board, I'll need to know how you're planning to use that data."

https://gdpr-info.eu/art-4-gdpr/

# Freely given Consent

- Not valid when there is no real choice:
  - i. **Imbalance of power**: data subject is compelled, pressured, influenced, fear to consent
  - ii. **Conditionality**: consent asked in the scope of a contract or service
  - iii. **Detriment**: has to endure negative consequences by not consenting

# Free vs Imbalance of Power

- Presumption of **imbalance of power** if controller is **public authority, employer, medical service** (dominant position).
- Data subject fearing adverse consequences, has **no** realistic alternative to accept the processing terms (invalid consent) (GDPR Recital §43)

- Cases:
  - Fear or real risk of detrimental effects as a result of a refusal
  - Risk of deception, intimidation, coercion or significant negative consequences, e.g. substantial extra costs for non consenting
  - Compulsion, pressure or inability to exercise free will

- **Other lawful bases** more appropriate to the activity of public authorities (legal obligation, public interest)

# Example of a free balanced consent

A local municipality is planning road maintenance works. The municipality offers its citizens the opportunity to subscribe to an email list to receive updates on the progress of the works and on expected delays.

The municipality makes clear that there is **no obligation to participate** and asks for consent to use email addresses for this (exclusive) purpose. Citizens that do not consent will not miss out on **any core service** of the municipality or the exercise of any right, so they are able to give or refuse their consent to this use of data freely. All information on the road works will also be available on the municipality's website.

# Free vs Conditionality

- **Tying, bundling, disguising** the consent request as a **condition** for the performance of contract.
- Consent and contract cannot be merged

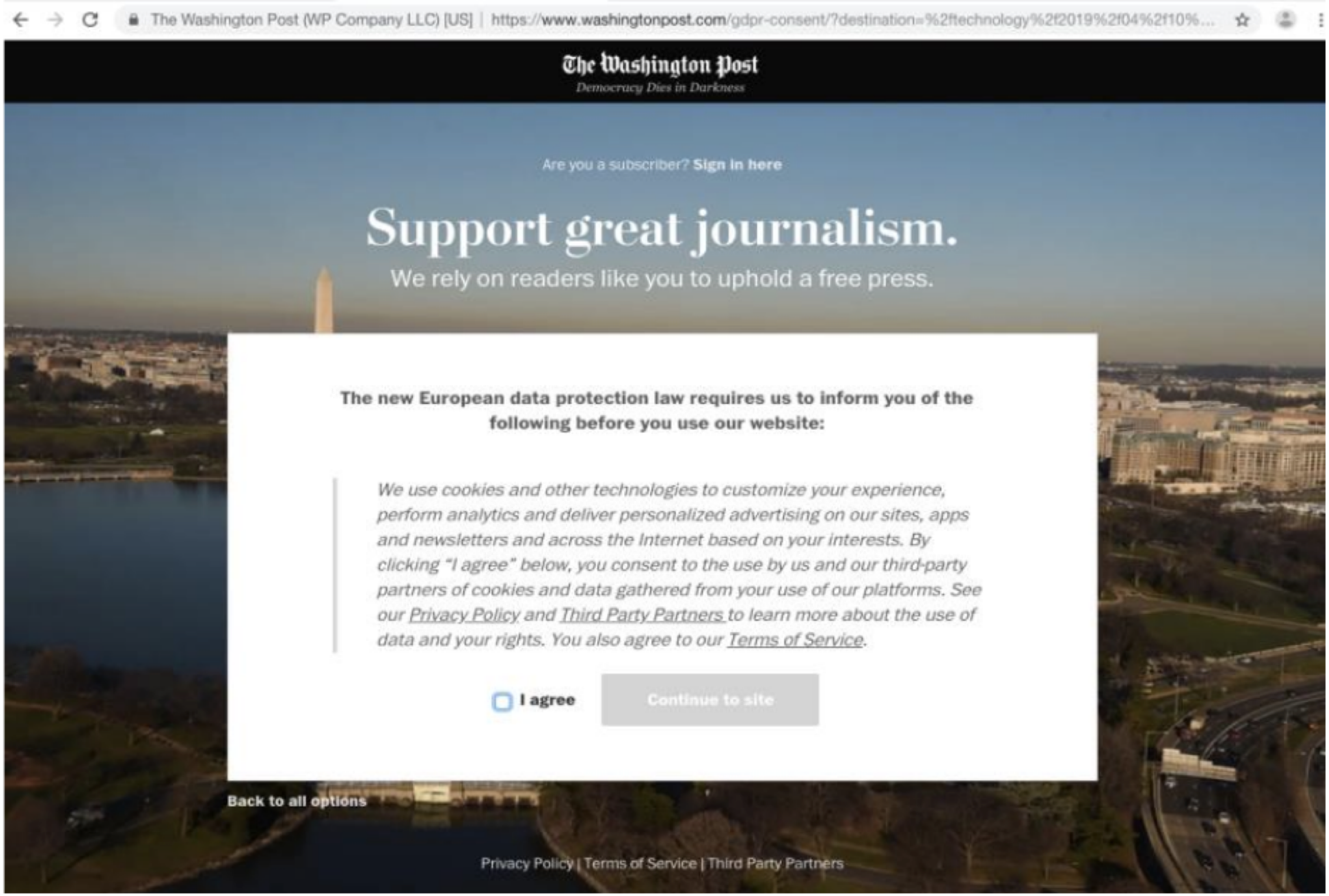
- **Assessment:**
  - Scope/**core** of contract; data necessary for that contract
  - "**Necessity**" to fulfill the contract with each individual data subject**,** e.g., address for goods to be delivered, credit card details for payment
  - Direct/objective **link** between the processing of the data and the purpose of the execution of the contract

GDPR Article 7(4), Recital §43

# Example of Conditionality

Bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. The customer’s refusal to consent implies denial of banking services, closure of the bank account, or an increase of fees.

# Example of Conditionality



The Washington Post (WP Company LLC) [US] | https://www.washingtonpost.com/gdpr-consent/?destination=%2ftechnology%2f2019%2f04%2f10%...
The Washington Post
Democracy Dies in Darkness
Are you a subscriber? Sign in here

Support great journalism.

We rely on readers like you to uphold a free press.

**The new European data protection law requires us to inform you of the following before you use our website:**

> *We use cookies and other technologies to customize your experience, perform analytics and deliver personalized advertising on our sites, apps and newsletters and across the Internet based on your interests. By clicking "I agree" below, you consent to the use by us and our third-party partners of cookies and data gathered from your use of our platforms. See our Privacy Policy and Third Party Partners to learn more about the use of data and your rights. You also agree to our Terms of Service.*

# Free vs Detriment

- Withdraw consent without detriment

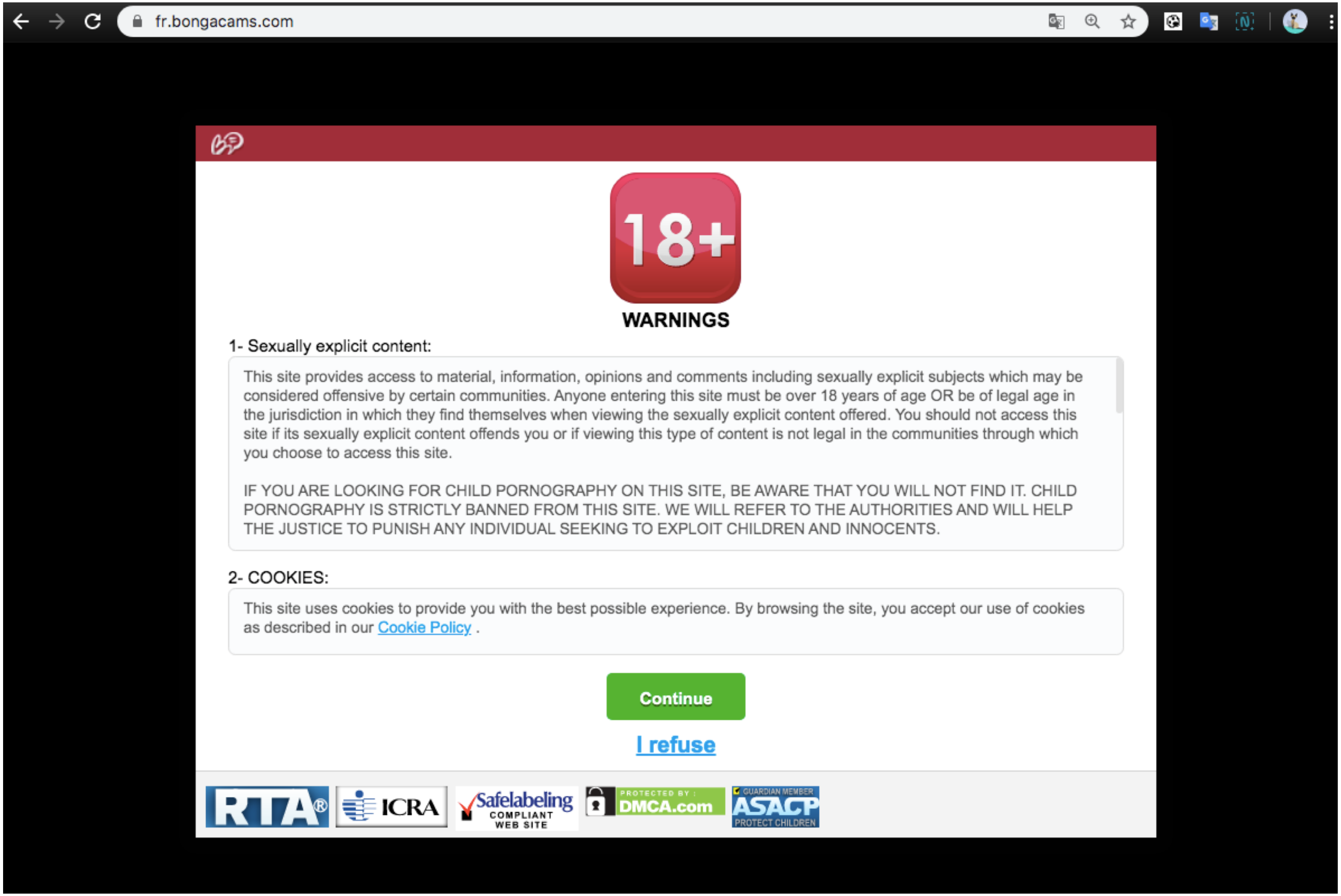
- Detrimental effects can be: leading to **any costs** or **clear disadvantage**:
  - Deception
  - Intimidation
  - Coercion
  - Downgrading of the service
  - Other significant negative consequence

GDPR Recital §42

# Example of non-detrimental effects

Celine subscribes to a fashion retailer’s newsletter with general discounts. The retailer asks for consent to collect more data on shopping preferences to tailor the offers based on shopping history, or a questionnaire that is voluntary to fill out. When she revokes consent, she will receive non-personalized fashion discounts again.

# Example of detrimental effect



**WARNINGS**

1- Sexually explicit content:

This site provides access to material, information, opinions and comments including sexually explicit subjects which may be considered offensive by certain communities. Anyone entering this site must be over 18 years of age OR be of legal age in the jurisdiction in which they find themselves when viewing the sexually explicit content offered. You should not access this site if its sexually explicit content offends you or if viewing this type of content is not legal in the communities through which you choose to access this site.

IF YOU ARE LOOKING FOR CHILD PORNOGRAPHY ON THIS SITE, BE AWARE THAT YOU WILL NOT FIND IT. CHILD PORNOGRAPHY IS STRICTLY BANNED FROM THIS SITE. WE WILL REFER TO THE AUTHORITIES AND WILL HELP THE JUSTICE TO PUNISH ANY INDIVIDUAL SEEKING TO EXPLOIT CHILDREN AND INNOCENTS.

2- COOKIES:

This site uses cookies to provide you with the best possible experience. By browsing the site, you accept our use of cookies as described in our Cookie Policy .

Continue
I refuse
RTA®
ICRA
Safelabeling COMPLIANT WEB SITE
PROTECTED BY : DMCA.com
GUARDIAN MEMBER ASACP PROTECT CHILDREN

# 2. Specific Consent

- **Consent must be specific for each purpose**

- **Criteria:**
  - **Purpose specification:** as a safeguard to avoid "function creep" or widening or blurring of purposes; explain what and why
  - **Granularity in consent requests**: separate opt-in for each purpose
  - **Clear separation of information** on obtaining consent for data processing activities, from information about other matters

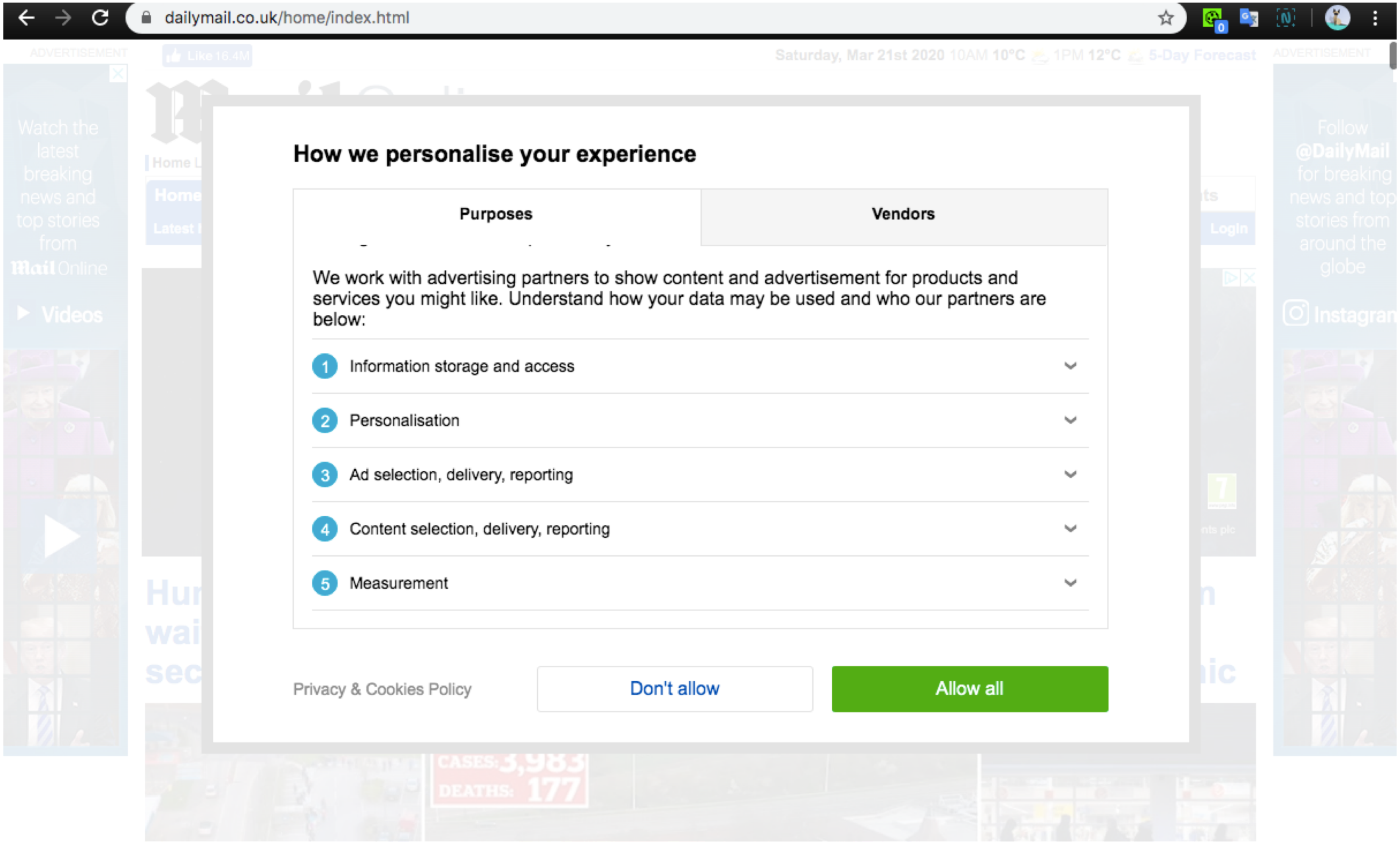
- Examples of non-specific, general purposes:
  - "improving users' experience", "marketing purposes", "IT-security purposes", "future research"

GDPR Article 6(1)(a), Recitals § 43 and § 32, 29WP 03/2013

# Example of Non-Specificity

A cable TV network **collects subscribers’ personal data**, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network **decides to enable third parties to send** (or display) **targeted advertising** on the basis of the subscriber’s viewing habits.

# Example of Non-specific to purpose



**How we personalise your experience**

We work with advertising partners to show content and advertisement for products and services you might like. Understand how your data may be used and who our partners are below:

1. Information storage and access
2. Personalisation
3. Ad selection, delivery, reporting
4. Content selection, delivery, reporting
5. Measurement

# 3. Informed Consent

- **What information must be presented?**
  - Identity of the (joint) controllers (Recital § 42)
  - Purposes of the processing (Recital § 42)
  - Type of data to be collected and shared
  - Existence of the right to withdraw consent (Article 7(3))
  - Info on the use of data for automated decision-making (Article 22 (2)(c))
  - Info on the risks of data transfers (Article 46)

Based on slides of Cristiana Santos

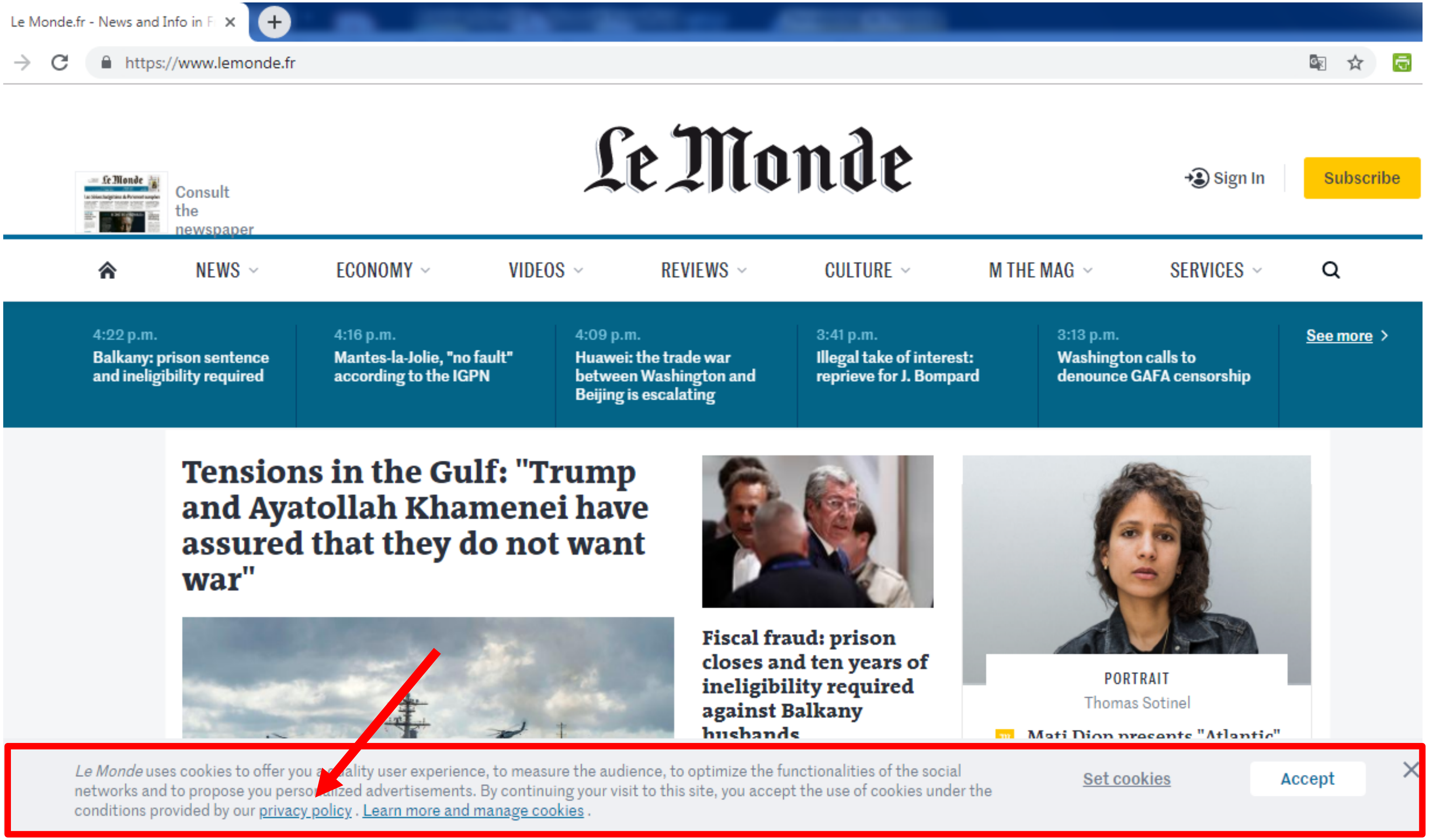
29WP 259 Guidelines on Consent

# 3. Informed Consent

- **How to provide information?**
  - Should be accessible before using the service (e.g., in the first layer of the cookie banner)
  - Intelligible and easy accessible form – not hidden in T&Cs
  - Distinguishable (separate and distinct) from other matters

29WP 259 Guidelines on Consent, GDPR Articla 7(2), Recitals § 32, § 42

# Example of accessible information



4:22 p.m. Balkany: prison sentence and ineligibility required

4:16 p.m. Mantes-la-Jolie, "no fault" according to the IGPN

4:09 p.m. Huawei: the trade war between Washington and Beijing is escalating

3:41 p.m. Illegal take of interest: reprieve for J. Bompard

3:13 p.m. Washington calls to denounce GAFA censorship

Tensions in the Gulf: "Trump and Ayatollah Khamenei have assured that they do not want war"

Fiscal fraud: prison closes and ten years of ineligibility required against Balkany husbands

PORTRAIT

Thomas Sotinel

Mati Diop presents "Atlantic"

*Le Monde* uses cookies to offer you a quality user experience, to measure the audience, to optimize the functionalities of the social networks and to propose you personalized advertisements. By continuing your visit to this site, you accept the use of cookies under the conditions provided by our privacy policy . Learn more and manage cookies .

# 3. Informed Consent

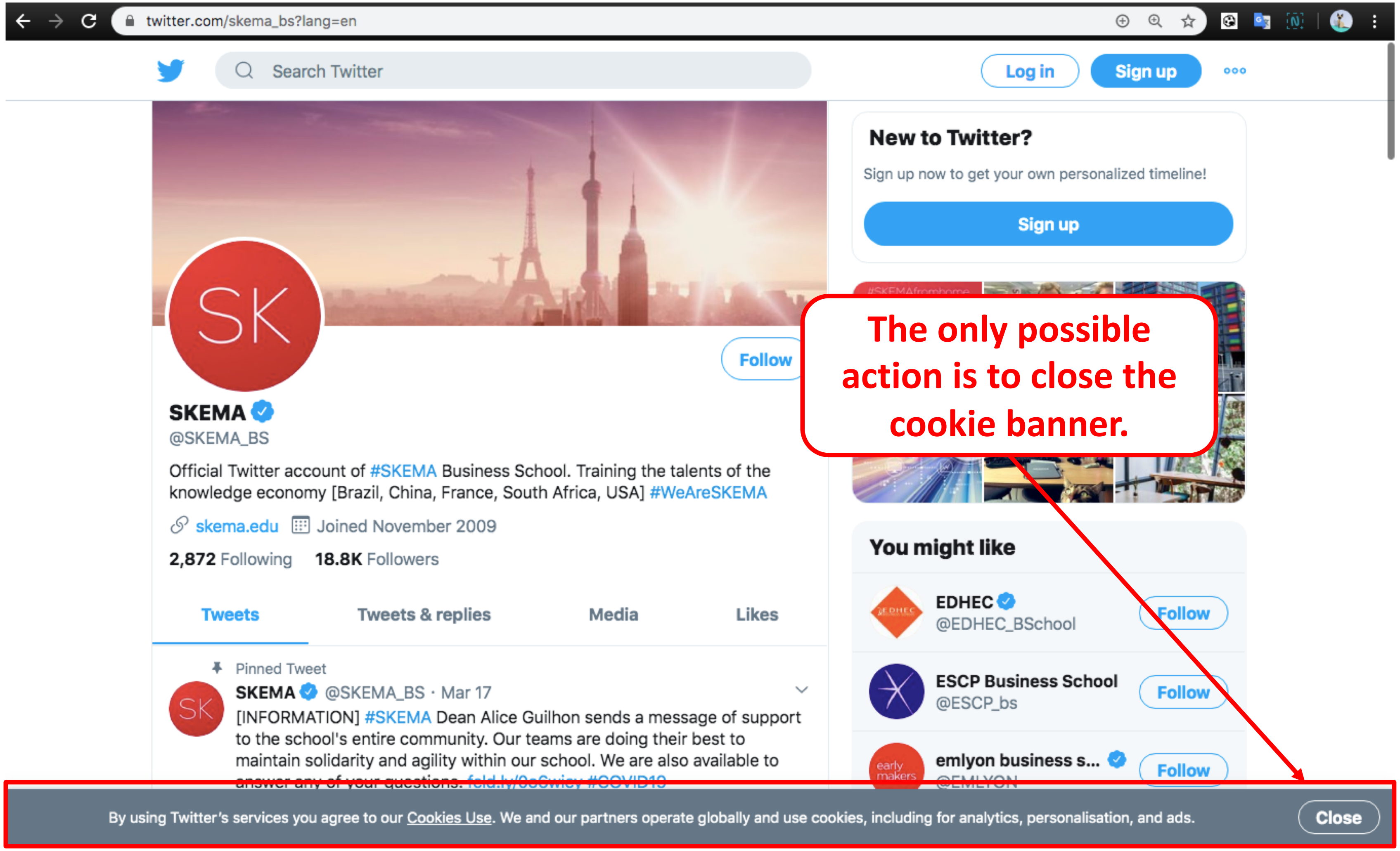
- **Requirements on form/language of information:**
  - Free form/shape, e.g. written or oral statements, or audio or video messages
  - Clear and plain language for lay people – understandable
  - Should not contain unfair terms, Directive 93/13/EC – if in doubt, consumer law defines more requirements

29WP 259 Guidelines on Consent, GDPR Articla 7(2), Recitals § 32, § 42

# 4. Unambiguous Consent

| | **GDPR** 4(11) §3 | **29WP** 259 on Consent |
|---|---|---|
| **Valid**<br>YES PLEASE ☑<br>NO THANKYOU □ | • any oral/written statement, or clear affirmative action<br>•ticking a box when visiting a website<br>•choosing technical settings for information society services | "if you – click a button or link, tick a box, swipe a bar on a screen, waive in front of a smart camera, turn a smartphone around clockwise, – you agree to the use of information X for purpose Y" |
| **Non Valid** | •Inaction, silence, inferred<br>•pre-ticked boxes<br>•condition to other actions | •scrolling down a website<br>• swiping through a website<br>(difficult to distinguish) |

# Example of Ambiguous consent



**New to Twitter?**

Sign up now to get your own personalized timeline!

**SKEMA**
@SKEMA_BS

Official Twitter account of #SKEMA Business School. Training the talents of the knowledge economy [Brazil, China, France, South Africa, USA] #WeAreSKEMA

skema.edu Joined November 2009

2,872 Following 18.8K Followers

Pinned Tweet

**SKEMA** @SKEMA_BS · Mar 17

[INFORMATION] #SKEMA Dean Alice Guilhon sends a message of support to the school's entire community. Our teams are doing their best to maintain solidarity and agility within our school. We are also available to answer any of your questions. fold.ly/0oGwicy #COVID19

**You might like**

| | |
|---|---|
| EDHEC @EDHEC_BSchool | Follow |
| ESCP Business School @ESCP_bs | Follow |
| emlyon business s... @EMLYON | Follow |

By using Twitter's services you agree to our Cookies Use. We and our partners operate globally and use cookies, including for analytics, personalisation, and ads.

The only possible action is to close the cookie banner.

# 4. Unambiguous Consent

- **Ambiguous cookie banner designs:**
  - Allowing only to close a cookie banner
  - Pre-ticked boxes
  - Disappearance of a banner while browsing the website
  - Allowing only to accept cookies without allowing to reject

# Obligation to Proof Consent?

- Controller has to demonstrate consent

- **How to demonstrate**?
  - **Record** of consent statement received: who, what, when, how

    Eg. name, session Id, username, dated doc, documentation of the consent workflow at the time of the session, online timestamp, copy of the info presented, form

- **Expiration date?**
  - No “evolving consent” vs specific
  - Depends on context, scope of original consent, expectations of the data subject, evolution of processing.
  - **Refreshed** consent at appropriate intervals

GDPR Article 7(1), Recital §42

# Withdrawal of Consent

- **When?** Be informed before, at any time
- **How? As easy as to give**, without undue effort
  - mouse-click, swipe, keystroke,
  - log-on account,
  - interface of an IoT device,
  - e-mail
- **Without detriment –** free or without lowering service levels

GDPR Articles 7(3), 17(1)b, Recital §39

# Exercise

- Open history of your browser
- Choose 3 websites from your browsing history
- Open these 3 websites in a private/incognito window
- Is there a consent banner? Does it comply with elements of valid consent?
    1. Free
    2. Specific
    3. Informed
    4. Unambiguous
- Check the slides to validate your analysis
- Write 2 page report with your analysis
- Deadline: 11 December 2020