Data Protection Officer & Data Protection Leads Course
Advisory 21
2026

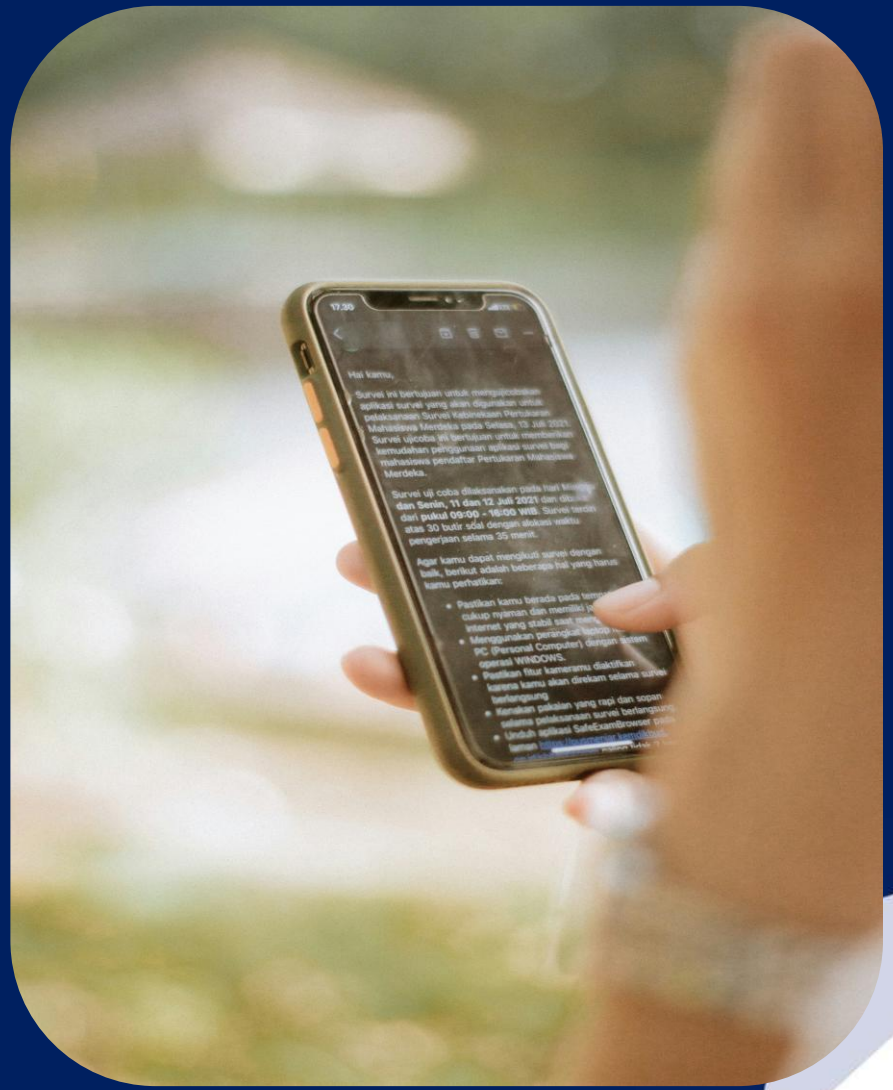
Dr Erika Criscione - email: erika.criscione@gvzh.mt
Dr Hayley Ann Pisani - email: hayley.pisani@gvzh.mt
https://gvzh.mt/
Date: 29th October 2026

GDPR Background

General Data Protection Regulation

Privacy as a Fundamental Right	• Article 8 of the EU Charter of Fundamental Rights and Article 16 of the Treaty on the Functioning of the European Union, both state that everyone has the right to the protection of their personal data.
GDPR's Objectives	• Harmonise fragmented EU data protection laws • Protect the rights and freedom of individuals in the digital age • Reduce barriers to business by facilitating the free movement of data within the EU single market.
GDPR foundations	• Principles-Based Regulation • Principle of Accountability • Extra-territorial scope

Ever wondered if your phone knows too much about you?



PERSONAL DATA = MONEY

What is Personal Data?

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly in particular by reference to an identifier such as a **name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**

Directly, if you are able to identify a specific individual solely through the data you're processing.

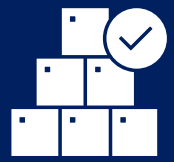
Indirectly, if different sets of data from different sources, when combined, could identify a specific person. (Example: car registration number national insurance number; passport number; or a combination of significant criteria e.g. age, occupation, place of residence).

Examples of Personal Data

Data Subjects Rights
General Rules

Data Subject Rights

Right to erasure
(Right to forgotten)



Rights related to automated decision-making and profiling

Right to object

Right to be informed

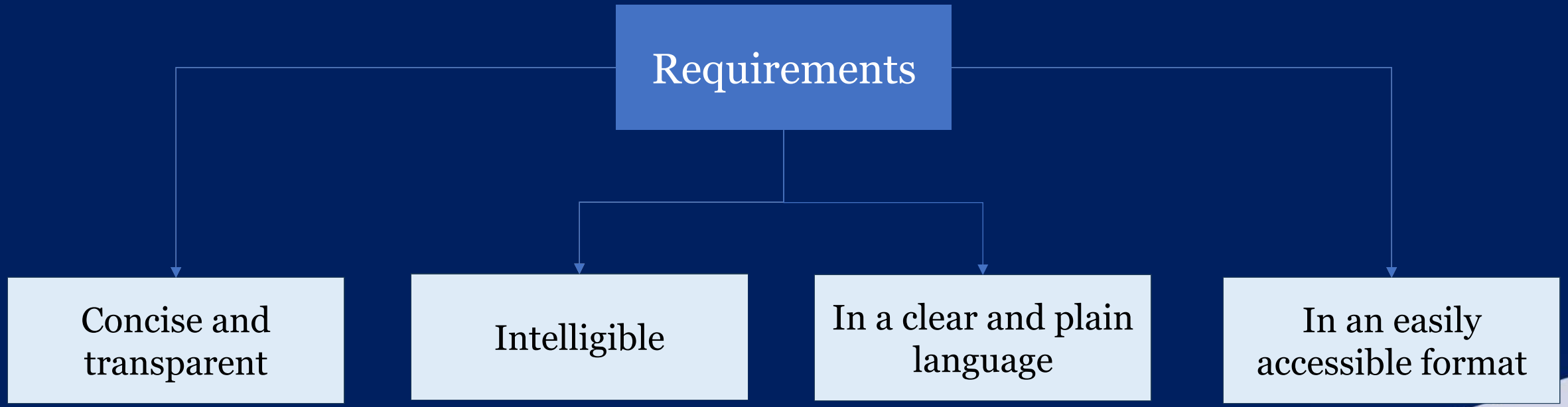
Right of Rectification

Right of access

Right of restriction of processing

Right to data portability

How Should Information be Provided to Data Subjects?



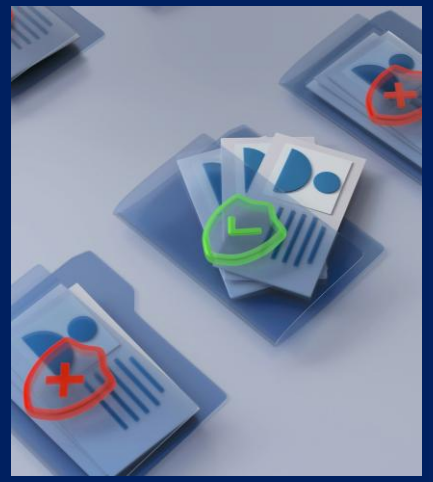
Manifestly Unfounded or Excessive Requests

Manifestly Unfounded

- No real intention of DS to exercise their rights
- When DS target a particular employee
- When request is Malicious
- Request makes unproven accusations

Excessive

- When repeating a previous request and reasonable interval has not elapsed
- Overlaps with other requests having the same content



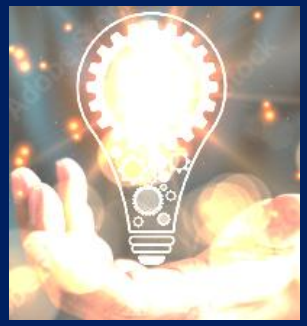
Manifestly Unfounded or Excessive Requests

Controller Responsibility	Controller Options
Demonstrate that a request is manifestly unfounded or excessiv	Request as reasonable fee to deal with the request Refuse to act on the request

1. Reasonable fees should be based on administrative costs.
2. The data subject should be promptly informed on any fees to be charged.

When Can a DSR Request Be Refused?

- When it is deemed to be manifestly unfounded or excessive character of a request
- A third party fails to present sufficient proof of authority to make the request on the data subject's behalf.
- The data subjects cannot be identified unless it provides additional information which the data subject refuses to provide(*clearly inform data subjects that the one-month time frame to respond to a data subject request does not start until we receive a fully completed request and proof of identity*).
- National law provides a basis for denying the request.
- The data controller does not hold any personal data related to the data subject request.



<u>Actions to take in case of refusal:</u>

Inform the data subject of the refusal without delay and at the latest within one month of receipt of the request.
Include in your response:

- the reason of the refusal
- the right to lodge a complaint with a supervisory authority,
- the possibility to seek a judicial remedy.

Timing

The 1 calendar month time limit starts from when the controller receives the request from the data subject through one of its official channels.
Extension of the time limit can be extended by a further 2 months taking into account the complexity of the request.

EXCEPTION

Whenever the controller needs to clarify any issues with the data subject, there might be the need to suspend the one-month time limit

EXTENTION

The deadline of one month to respond can be extended by a maximum of a further two months taking into account **the complexity and the number of the requests,** provided that the data subject has been informed about the REASONS for such delay WITHIN ONE (1) MONTH of the receipt of the request.

Record Keeping

A data controller is required to keep record of all data subject rights requests.

It is suggested to retain:

1. Copies of correspondence – i.e., between data controller and data subject and any other 3rd parties.
2. Evidence that actions have been taken to confirm the identity of the data subject.
3. Record of the decisions taken together with underlying analysis done.
4. Copies of information sent to data subject.

Summary Of Key General Rules on DSR

- Provide the information to DS in a concise, transparent and intelligible manner.
- Communicate with a clear and plain language and in an easily accessible format.
- Provide the most appropriate and user-friendly communication/channels, to enable the data subject to make an effective request.
- If manifestly unfounded or excessive, you can refuse to respond or request a reasonable fee to deal with the request.
- In case of refusal inform the data subject of the refusal without delay and at the latest within one month of receipt of the request.
- Comply with 30-days timeframe to respond
- Keep records of Data Subject requests.

Right to be Informed
Art. 13 & 14 GDPR

How is Information Provided to Individuals?

Information on the processing of data is provided through the privacy notice.

When personal data is obtained directly from the data subject, the specified information must be provided by the controller **at the time the data is obtained**.

Further process of personal data requires **a new notice** covering the new processing

Information to be provided are listed under art 13 & 14 GDPR

Information To Be Included In The Privacy Notice (art 13 & 14) CHECKLIST

- Name and contact details of organization
- Name and contact details of GDPR representative
- Contact details of data protection officer
- Purposes of the processing
- Lawful basis for the processing
- Legitimate interests for the processing
- Categories of personal data
- Recipients or categories of recipients of the personal data
- Details of transfers to third countries or international organisations
- On request, SCCs will be provided to Data Subjects
- Retention periods for personal data
- Rights available to individuals
- Right to withdraw consent
- Right to lodge a complaint with a supervisory authority
- Consequences of failure to provide data
- Details of automated decision-making

Uber fined €10 Million For Lack Of Transparency About Driver Data

Background:

The investigation began after over 170 complaints from French drivers were forwarded by France's data protection authority to the Netherlands DPA, as Uber's European headquarters is in the Netherlands. The main concern of the drivers which filed the complaints was related to access to their personal data.

Findings:

- The Dutch authority criticized Uber's digital form for submitting data access requests, stating it was **not easily accessible, overly complicated, and failed to direct users to the actual request form.**
- The authority found Uber in violation of **Article 12(2) of the GDPR**, which requires controllers to facilitate data subject rights and prohibits refusal to act on such requests.
- The authority also found that the information provided to drivers was **unclear and not in simple language**, noting it was in English rather than French, making it difficult for drivers to understand

AP fined Uber €10 Million For Lack Of Transparency About Driver Data

Issues with the **privacy policy**:

- The privacy policy failed to specify a **retention period**, stating only that data would be kept "as long as necessary" without detailing the criteria. The authority stressed that clear criteria would help data subjects understand how long their personal data is retained.
- The policy did not specify the **non-EEA countries** to which personal data was transferred or the security measures implemented for such transfers.
- The policy failed to mention the **right to data portability**, as the term "receiving data" was deemed ambiguous and could refer to the right of access instead, violating Article 13(2)(b) of the GDPR.

Conclusion:

- The Dutch data protection authority fined Uber Technologies and Uber B.V. **€10 million** for GDPR violations.

Right of Access Art. 15 GDPR

Have You ever Received This Type of Requests?

Please, kindly send me my HR file

Can I have a copy of the notes from my last appraisal?

What information do you hold about me?

What information do you hold about me and for how long are you storing it?

Can I have a copy of the emails sent by my manager to HR, regarding my verbal warning?

Submission Of a DSAR

- No specific requirements
- Can be made **verbally or in writing** (regardless of the DSAR form provided to the Data Subject), including via social media.
- Can be made **to anyone within the company**
- Data subject **does not need** to provide **the reasons** for making the request

Identification & Authentication

Controllers must be able to:

- Identify the data subject
- Authenticate the request (confirm the person's identity)

This ensures secure data processing and prevents unauthorized access.

Identification & Authentication

ONLY if necessary and proportionate to the processing carried out, the ID document of the data subject shall be requested in order to verify him/her.

Identification & Authentication

DOS

- ✓ Let users log in to their account
- ✓ Use email/SMS verification links
- ✓ Ask non-intrusive security questions
- ✓ Only request ID if there's a high risk (e.g. health data)
- ✓ If ID is used, redact unnecessary info (photo, eye color, etc.)
- ✓ Delete ID copy immediately after use

DON'TS

- Don't ask for ID if the person is already authenticated
- Don't request notarised documents without legal basis
- Don't keep ID copies without clear justification

Case Study

- The controller, a retail company, is corresponding with customers asking for their past order details.
- The request came from the same email address which was used by the customer to create their account for online shopping.

CONSIDERATIONS ON THE CASE

The request came from the same email address which was used by the customer to create their account for online shopping, therefore there would be no apparent reasonable doubt about the Data Subject's identity.

However, the Controller is justified in requesting further identification, only if there was a reason to establish the identity (for example, the fact that the account had been recently locked due to A HACKING EVENT)

What is the information to be provided to DS?

- Whether personal data concerning DS is being processed
- The purposes of the processing
- The categories of personal data concerned
- Recipients
- The envisaged period for which the personal data will be stored, or, the criteria
- Information on the data subject's rights
- Right to lodge a complaint with a supervisory authority
- Any source from which the data was collected from (if not collected from the data subject)
- the existence of automated decision-making, including profiling
- appropriate safeguards in case of 3rd country transfers

© GVZH 2025 | THIS DOCUMENT IS CONFIDENTIAL AND ITS CIRCULATION, USE AND/OR REPRODUCTION IN WHOLE OR IN PART ARE RESTRICTED

IDPC decision

-The complainant alleged that the controller failed to handle his request to access all his personal data pursuant to the requirements of the GDPR.

The Commissioner decided that:

- the controller failed to inform the complainant about the limitation of right to access invoked pursuant to article 15(4) of the GDPR, and therefore, the reply lacked the **necessary elements of transparency** and fairness as required by the principles set forth in article 5(1)(a) of the GDPR; and

- the reply of the controller failed to include information in relation to the processing activity as set forth in article 15(1)(a) to (h) of the GDPR, save for the information that the personal data of the complainant were not disclosed to third parties;

- the controller was not justified to limit the right of access pertaining to the complainant in terms of article 15(4) of the Regulation and therefore, the non-disclosure of this personal data led to an infringement of article 15(3) of the GDPR. A reprimand and an order to comply with the right of access.

How To Provide The Information

- The controller shall provide a copy of the personal data undergoing processing.
- For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.
- Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Possible Limitations of Right of Access – Other Parties' Data

Art. 15 requires to consider "**ANY POSSIBLE ADVERSE EFFECT ON THE RIGHTS AND FREEDOMS OF OTHERS**".

In reviewing a request by data subject which could potentially affect other third parties, the rights and information of third parties must always be protected. This means that before the Controller can respond to a DSAR, it should initially consider:

- whether the request requires the **disclosure of information** which contains and identifies a **third-party individual;** and
- whether the **third-party individual has consented** to the disclosure.

How do You Remove Third Parties Data?

Hard copy documents

- ✓ Print out the document or, if it is a paper record, make a photocopy
- ✓ Using a black marker, blank out the information which is not needed
- ✓ Make a photocopy of the blacked-out version and provide it to the data subject.

Soft copy documents

- ✓ Using the highlighter tool, highlight the information which is not needed
- ✓ Save the blacked-out version as a separate copy

Failing to Provide the Complainant with Copy of Personal Data

Background:

- The DPC (Irish SA) investigated a complaint which concerned a data subject's request to Ryanair for access to their personal data. While Ryanair provided some of the requested data, it failed to include a recording of a call made by the complainant, which had been deleted in line with company policy due to a delay in processing the request.

Failing to Provide the Complainant with Copy of Personal Data

Key Findings:

- Ryanair failed to provide the complainant with all personal data undergoing processing at the time of the request, specifically the call recording.
- Ryanair did not inform the complainant about the actions taken in response to their subject access request within the one-month statutory timeframe.
- Ryanair's deletion of the requested call recording, due to its data retention policy, further hindered compliance.

Outcome:

- A reprimand was issued to Ryanair for these violations. The case highlights the importance of timely and comprehensive responses to subject access requests and the need to align data retention policies to ensure that personal data is not deleted if there are any ongoing data subject rights requests.

Steps to Follow and Questions to Ask When Receiving a DSAR

- ☑ *Acknowledge receipt of the request.*
- ☑ *Does the request concern personal data?*
- ☑ *Does the request relate to the requesting person?*
- ☑ Identity check, in case of doubts
- ☑ *Clearly understand the scope of the request*
- ☑ *Is the request manifestly unfounded or excessive?*
- ☑ *Provide a response within the timeline*

Actions To Be Taken To Prepare for DSAR

1. *Prepare a DSAR internal procedure with step-by-step actions for staff*

2. Create and follow a clear ID verification protocol (e.g. require copies of ID documents, utility bills, or use secure authentication systems)

3. *Draft a template acknowledgement letter/mail to be sent upon receival of the request and other template reflecting other possible scenarios (request of additional information, refusal to respond as the request is excessive, request for payment of X amount in case of request for additional copies, etc…)*

Actions To Be Taken To Prepare for DSAR

4. Know where data is stored across clouds, database, archives, third parties' platforms etc.. (Data Mapping exercise) (Register of Processing Activities - ROPA)

5. Assign roles (typically Data Protection Officer or Legal/Compliance department) to assess the DSAR scope

6. *Establish retention periods for personal data you store*

7. *Provide training to staff about DSAR, including how to recognize a DSAR, rules on verification and authentication, what information to provide and timeline to respond.*

8. *Use Tools/Technologies with "DSAR friendly" approach*

9. Consider privacy tech tools for faster data retrieval and redaction.

Right to Rectification
Art. 16 GDPR

Individuals have the right to have personal data rectified

Data subjects have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed.

The right to rectification is closely linked to the accuracy principle. Even if the data was accurate at the time of collection, this right obligates a reassessment of accuracy..

When a request for rectification is received, reasonable steps should be taken to verify the accuracy of the data and rectify it if necessary. Consider the arguments and evidence provided by the data subject.

Right of Erasure
Art. 17 GDPR

Individuals Have The Right To Have Personal Data Erased

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b)the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Individuals Have The Right To Have Personal Data Erased

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take ***reasonable steps****, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.*

Ex. Companies may need to inform search engines to remove certain information (ex cached data) that has been erased from the companies' website.

Individuals Have The Right To Have Personal Data Erased

The Right to Be Forgotten WILL NOT APPLY if the retention/processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health;

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

(e) for the establishment, exercise or defence of legal claims.

(f) To comply with a legal obligation

Right to Restrict Processing
Art. 18 GDPR

www.21Academy.education

Individuals have the right to limit the process of data

- Individuals can exercise the right to restrict processing when they have concerns about the content of the information held or how their data has been processed.

- In most cases, the restriction on an individual's personal data **will not be indefinite, but rather for a designated period**.

- The duration of the restriction will depend on the circumstances and the organization's obligations

Individuals have the right to limit the process of data

When does the right to restrict processing apply?

The individual **contests the accuracy of their personal data**, and you are verifying its accuracy.

The data has been unlawfully processed, and the individual opposes erasure, requesting restriction instead.

The controller no longer needs the personal data, but the individual requires its retention for establishing, exercising, or defending a legal claim.

The individual has objected to the processing under article 21(1), and you are assessing whether your legitimate grounds override their objections.

Individuals have the right to limit the process of data

How do you enable the restriction of personal data

- ❑ Temporarily moving the data to another processing system
- ❑ Making the data unavailable to users
- ❑ Use technical measures in automated filing systems to prevent further processing or changes whilst the restriction is in place.
- ❑ Clearly indicate on your system that the processing of this data has been restricted.

Individuals have the right to limit the process of data

When data cannot be restricted

1. Consent is obtained from the individual.
2. It is for the establishment, exercise, or defence of legal claims.
3. It is for the protection of the rights of another person (natural or legal).
4. It is for reasons of important public interest.

Before lifting the restriction, inform the individual of your decision and about the reasons for refusing to act on their rights.

Right to Data Portability
Art. 20 GDPR

www.21Academy.education

Individuals have the right to portability

The data subject has a right to portability, including:

- to receive a copy of the personal data from the data controller in a structured, commonly used and machine-readable format ex. CSV,XML and JSON formats.

- to transmit it to another controller, including directly from one controller to another, where technically feasible.

The Company has a responsibility to securely transmit the data and ensure it reaches the correct destination.

Inform individuals about potential risks associated with storing the received data in systems with lower security than your own and encourage them to take precautions to protect the information.

Individuals have the right to portability

When does the right to Data Portability apply?

- To personal data which is processed by automated means
- To personal data which the data subject has provided to the controller
- Where the processing is based on the data subject's consent or for the performance of a contract

The right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The right must not adversely affect the rights and freedoms of others.

Failure To Comply With A Data Subject's Portability Request

Background:

A user of an email service requested their data in a structured, commonly used, and machine-readable format, as per Article 20 GDPR. The controller denied the request, claiming that users could export emails one by one in '.eml format' and arguing that it was uncertain whether Article 20 GDPR applied to emails. At the time, the controller had an automated import/export tool, but it was only available to paying customers as part of a beta test. Free-plan users had to rely on manual email exports.

Key Findings:

- The DPA found that manual, one-by-one email exports violated Article 20 GDPR as it was overly burdensome and impractical for users with many emails.
- Restricting the automated export tool to paying customers breached Article 12(5) GDPR by making data portability effectively chargeable.
- The controller delayed compliance, only providing free users access to the tool after the investigation began.

- **Outcome:**
- the DPA fined the controller approximately €55,700 for its GDPR violations. The Finnish DPA issued a reprimand to the controller for violating Articles 20(1) and 12(5) GDPR. It emphasized that organizations must facilitate data portability in a user-friendly and free manner for all data subjects

Right to Object
Art. 21 GDPR

Right to Object

A data subject can object to certain types of processing:

- for direct marketing purposes (no exemptions or grounds to refuse)
- for processing based on legitimate interests or performance of a task in the public interest or exercise of official authority
- for certain scientific or historical research purposes or statistical purposes

Controller must notify individuals of this right at an early stage - clearly and separately from other information

Where processing is carried out online, the data subject must be able to exercise this right by automated means (to object online)

Controller must comply unless:

- can show compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or
- the processing is necessary for the exercise or defence of a legal claim.

Failure to comply with a data subject’s right to object request

Background:

The Romanian DPA fined the controller because it continued sending commercial emails to a data subject despite the data subject's objection and use of the unsubscribe option. The concerned controller was an optician and merchant for glasses, sunglasses as well as contact lenses. As part of its business, the controller sent out commercial messages through its newsletter service. The concerned data subject was one of the newsletter's recipients.

Key Findings:

The data subject exercised their right to object under Article 21 GDPR by unsubscribing from the newsletter, however, the controller ignored the objection and continued sending unsolicited emails, violating Article 21(3) GDPR, which specifically prohibits processing for direct marketing purposes after an objection.

Outcome: The DPA imposed a fine and ordered corrective measures on the controller to ensure compliance with data subject rights.

Automated Decision Making
Art. 22 GDPR

Automated-Decision Making

A data subject has the right not to be subject to:

- ❑ a decision based solely on automated decision-making (including profiling)
- ❑ which produces a legal effect or a similarly significant effect on him or her

Unless the automated decision is:

- ➢ necessary for entering into or performing a contract between the data subject and the data controller
- ➢ based on the explicit consent of the data subject
- ➢ authorised by EU or Member State law

Controller must ensure safeguards for data subject are in place (at minimum, obtain human intervention, express point of view, contest the decision).

Warning for possible automated individual decision-making

Background:

- The Finnish DPA issued a warning to a healthcare provider for potential violations of Article 22 GDPR. A healthcare provider requested prior consultation with the DPA regarding its new Health Benefit Analysis Tool. To assess the legality of the planned processing of personal data the DPA decided to handle the case not as a prior consultation but as a supervision.
- The tool was designed to identify patients with health risks using algorithms but raised concerns about automated decision-making. Patients flagged by the system were reviewed by healthcare professionals, but those not flagged were excluded from healthcare services without further assessment.

Key Findings:

- The envisioned processing would have violated Article 22 GDPR, which prohibits automated decision-making with significant effects. The processing would significantly affect data subjects because they would be deprived of the opportunity to receive a healthcare service.
- **Outcome:** The DPA issued a warning under, emphasizing the need for the controller to ensure compliance with Article 22 GDPR when using automated systems.

Restrictions
Art. 23 GDPR

Restrictions

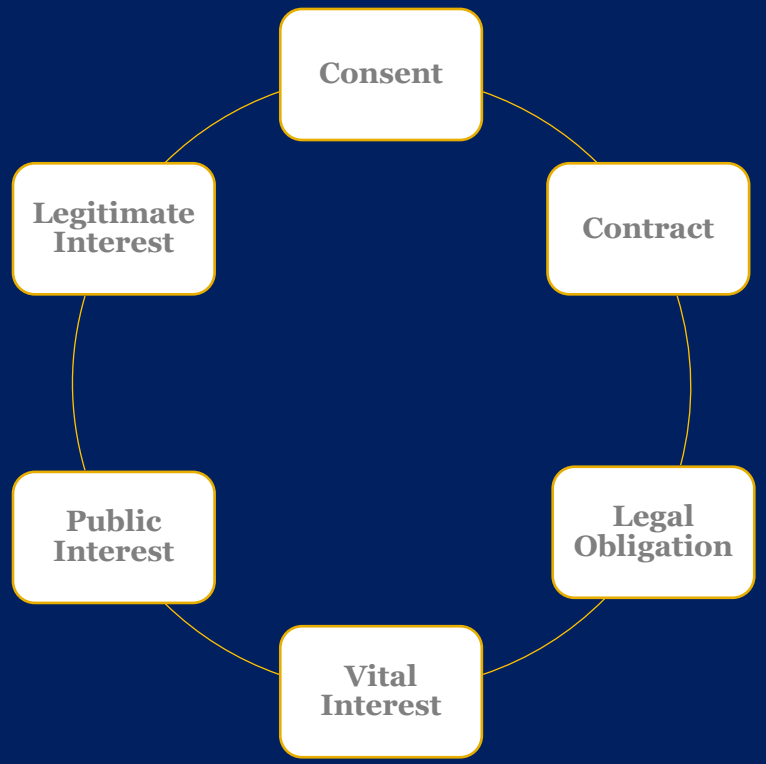
- national security
- defence
- public security
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security
- other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security
- the protection of judicial independence and judicial proceedings
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g)
- the protection of the data subject or the rights and freedoms of others
- the enforcement of civil law claims

Break time

Understanding Consent Under GDPR

Legal Bases for Processing Personal Data (At. 6 GDPR)

Under the GDPR, personal data must be processed lawfully, fairly and transparently. Article 6 sets out 6 lawful bases for processing personal data, at least one must apply for the processing to be lawful:



6 conditions

When assessing which legal basis applies, consider:

- the type of personal data being processed
- the purpose of processing
- the relationship between the controller and the data subject

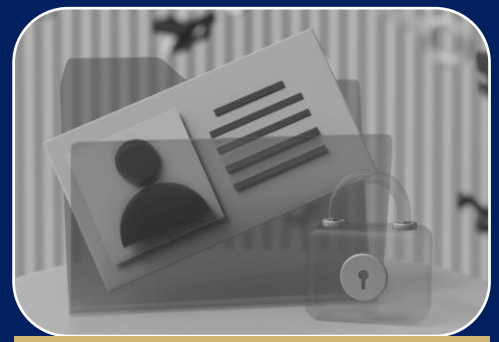
if the processing involves special categories of personal data, an additional lawful basis under Article 9 GDPR is required.

Consent – Art 4(11) GDPR

Must be **freely given**: no pre-ticked boxes or passive behaviour

Must be **specific** to the processing purpose

Must be **informed** with clear and complete information



Must be **unambiguous** and clearly express intent

1	2	3	4
Freely given	**Specific**	**Informed**	**Unambiguous**
No pre-ticked boxes or passive behaviour	Tied to the processing purpose	Clear and complete information	Clearly express intent

All four together = valid consent

Consent: Freely Given

- Must be a genuine choice, not forced
- No coercion or pressure (especially in power-imbalanced relations)
- No “tied consent” - service access cannot depend on unrelated processing.
- Consent must be revocable without detriment
- Example: Employer cannot make staff consent to workplace monitoring
- Legal Reference: GDPR Art. 7(4), Recital 43

EDPB Guidelines: Example

A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services.

Can consent be said to be freely given?

No. If the customer's refuses to provide consent and this leads to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee – **consent is not freely given.**

Yes. If the customer's refusal to consent does not lead to any such **detrimental effect** on him/her (i.e. if there is a real choice/exercise of free will) - **consent is not freely given.**

Freely Given – Bundling Consent

- Consent must not be a condition for accessing services (unless strictly necessary)
- Separate contractual terms from consent requests
- Avoid pre-ticked boxes or “all-or-nothing” options
- Bundled consent presumed invalid (Art. 7(4), Recital 43)

Irish DPC fines Meta €390M over targeted ads

- **Facts / Context**
  - Complaints filed by privacy group NOYB, led by Max Schrems.
  - Meta embedded personalised advertising in its Terms of Service, forcing users to accept targeted ads to access Facebook and Instagram
  - Meta's argument: personalised ads were necessary for the performance of a contract under Article 6(1)(b) GDPR.

- **Issue:** Can personalised advertising be considered contractually necessary under Article 6(1)(b) OR does it require freely given consent under Article 6(1)(a)?

- **Ruling**
  - Irish DPC: initially accepted contractual necessity but noted transparency issues.
  - Other EU DPA's disagreed – case referred to EDPB under the consistency mechanism.
  - EDPB decision: contractual necessity invalid because: 1) ads are not essential to providing the core service, 2) users were not properly informed and 3) users lacked real choice (refusal meant losing access)

Freely Given – Granularity

- Services often involve multiple processing purposes
- Individuals must be able to consent separately for each purpose
- Blanket or bundled consent is not valid
- Separate consents required when different purposes exist
- Consent options should be clear, granular and unambiguous
- Legal Reference: Art. 7(4), Recitals 32 & 43

Example: Users should be able to agree to receive newsletters but decline marketing profiling.

Orange România SA v. ANSPDCP (CJEU, Case C-61/19)

Facts / Context

Orange România's mobile contracts used pre-ticked boxes and required customers to provide handwritten refusals to opt out of storing ID copies.

Issue

Did these practices amount to valid consent under the GDPR, or did they undermine the principle of "freely given" consent?

Ruling

The CJEU held that:

- Bundled consent and misleading contract terms invalidated consent
- Pre-ticked boxes and additional opt-out steps undermined freedom of choice
- Valid consent must be unambiguous, specific, informed, and free from coercion

Orange România was fined and ordered to delete all stored ID copies.

Consent: Specific

- Consent must be purpose-bound and clearly defined
- Separate consent required for distinct activities
- Blanket or vague consent (e.g., “for marketing”) is invalid
- Use individual opt-in boxes for each purpose (e.g., newsletters, analytics, profiling)
- Beware of function creep – widening purposes after initial consent

Real Case Scenario

A retailer asks for one consent to:

1. Send marketing emails
2. Share details with group companies

Issue:

This consent is not granular, as there are no separate consents

for these two distinct purposes.

Therefore, the consent will not be valid under the GDPR.

Correct Approach:

A specific consent should be collected for:

- Marketing emails
- Sharing details with each identified commercial partner

Such consent will only be valid if:

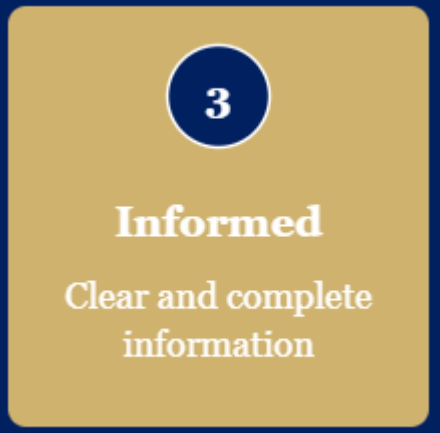
- The identity of each partner is disclosed at the time of collection, and
- The data is used only for the same purpose.

Consent: Informed

For consent to be valid, individuals must clearly understand what they agree to.

Key information required:

- Identity of the controller
- Purpose(s) of processing
- Categories of data collected
- Right to withdraw at any time
- Info on international transfers or automated decision-making (if relevant)



EDPB Guidelines (05/2020): all joint controllers or other organisations relying on consent must be named.

CNIL (France) v. Google, 27th March 2020

- **Facts / Context**
  - CNIL fined Google €50 million for breaches in ad personalization consent.
  - Essential info (purposes, retention, data categories) was scattered across multiple documents, making it hard for users to understand.
- **Issue**
  - Consent for ad personalization was pre-selected (opt-out) instead of opt-in.
  - Users were not provided with clear, concise, or easily accessible information, undermining the requirements of specific, informed, and unambiguous consent.
- **Ruling**
  - CNIL held that Google failed GDPR's transparency obligations and consent standards under Articles 5, 6 and 7 GDPR.
  - Consent was invalid, as users had not given a genuine, informed and active choice.
  - Google was fined 50 million Euro – at the time this was the largest GDPR fine ever issued.

How to Provide Privacy Information

Drafting effective information

- Map data flows (information audit / data mapping)
- Use clear and plain language appropriate for your audience
- Review and update privacy notices regularly

Making it meaningful

- **Layered notices**: key points upfront, details info accessible
- **Icons**: visual cues for specific processing activities
- **Dashboards**: user-friendly tools for managing preferences
- **Timely delivery**: provide privacy info at the point of data collection

Consent: Unambiguous

- Consent must involve a clear and affirmative action.
- Valid examples: ticking a box, clicking “I agree”, adjusting settings.
- Invalid examples: silence, inactivity, or pre-ticked boxes.
- Written or electronic records of consent recommended for accountability.

© GVZH 2025 | THIS DOCUMENT IS CONFIDENTIAL AND ITS CIRCULATION, USE AND/OR REPRODUCTION IN WHOLE OR IN PART ARE RESTRICTED

Planet49 GmbH (CJEU, Case C-673/17)

Facts/Context:

- Planet49 ran an online lottery requiring user registration.
- Registration included pre-ticked checkboxes for cookie consent.

Issue:

- Do pre-ticked boxes constitute valid consent under the GDPR and the ePrivacy Directive?

Ruling:

- Pre-ticked boxes are **not valid consent**.
- Consent requires an **active and affirmative choice** (e.g., ticking a box).
- Silence, inactivity, or default settings cannot amount to consent.
- Controllers must provide **clear and comprehensive information** on the purpose of cookies, their duration and whether third-parties can access the data.

Additional Requirements for Consent

- Demonstrate Consent:

  Where processing is based on consent, the controller must be able to demonstrate that the data subject has consented to processing of their personal data.

- Retain proof of consent

  Proof of consent must be kept for as long as the processing activity continues, and thereafter only as long as legally required or necessary for the establishment, exercise or defence of legal claims.

Withdrawal of Consent

Key Rule (Article 7(3) GDPR)

- The data subject has the right to withdraw consent at any time.
- Withdrawal does not affect the lawfulness of processing carried out before consent was withdrawn.
- Data subjects must be informed of this right before giving consent.
- It must be as easy to withdraw as to give consent.

Practical Requirements:

- When consent is given electronically (e.g., one click, swipe or keystroke), withdrawal must be just as simple.
- Withdrawal must be possible through the same interface used to give consent (e.g., website, app, email system)
- Requiring users to switch platforms or submit manual requests creates undue effort and may breach GDPR transparency.
- **No Detriment to the User**

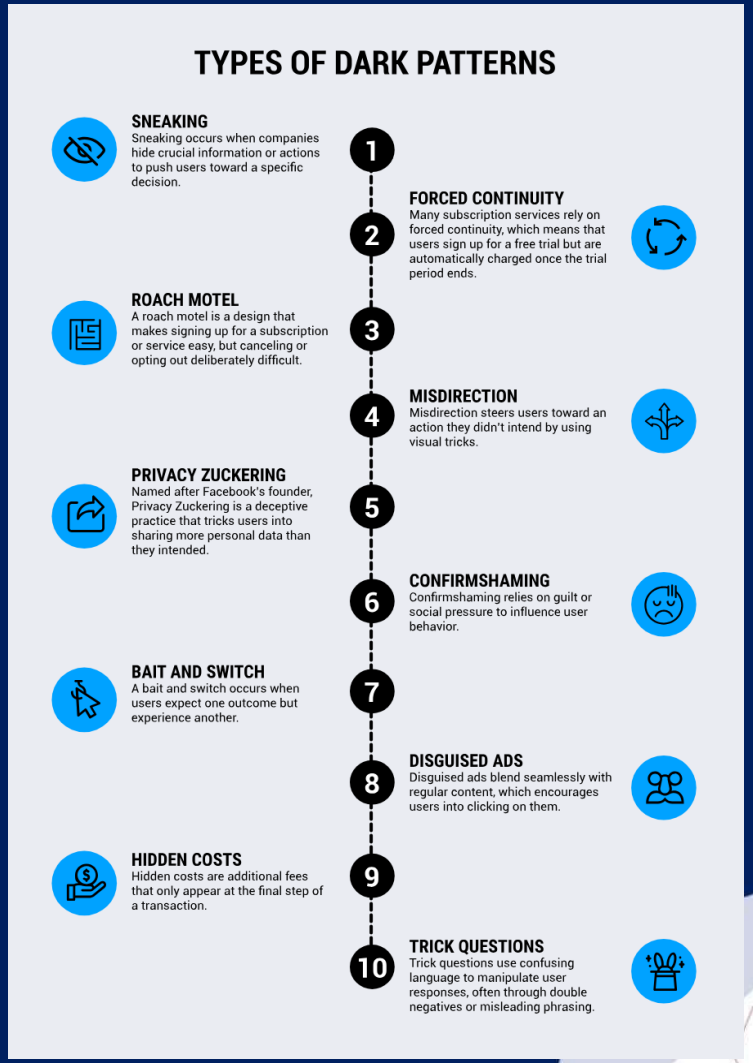
Withdrawal of Consent – Organisational and Technical Measures

- ☑ When consent is withdrawn, the controller must stop all processing that relies solely on that consent.
- ☑ Systems and records should update promptly to reflect withdrawal.
- ☑ Processing completed before withdrawal remains lawful, but any further use is prohibited.
- ☑ Inform all processors and partners relying on the same consent to ensure they also cease processing.
- ☑ Maintain audit trails showing how and when consent was withdrawn and processing was stopped.
- ☑ Provide a simple mechanism for withdrawal — e.g. same interface, unsubscribe button, account settings, or email option.

Are Dark Patterns Undermining GDPR Consent?

- Dark patterns are deceptive interface designs that manipulate or nudge users into actions they might not freely choose, like hiding “Reject” buttons, using bright colours for “Accept all” or using guilt-tripping language.

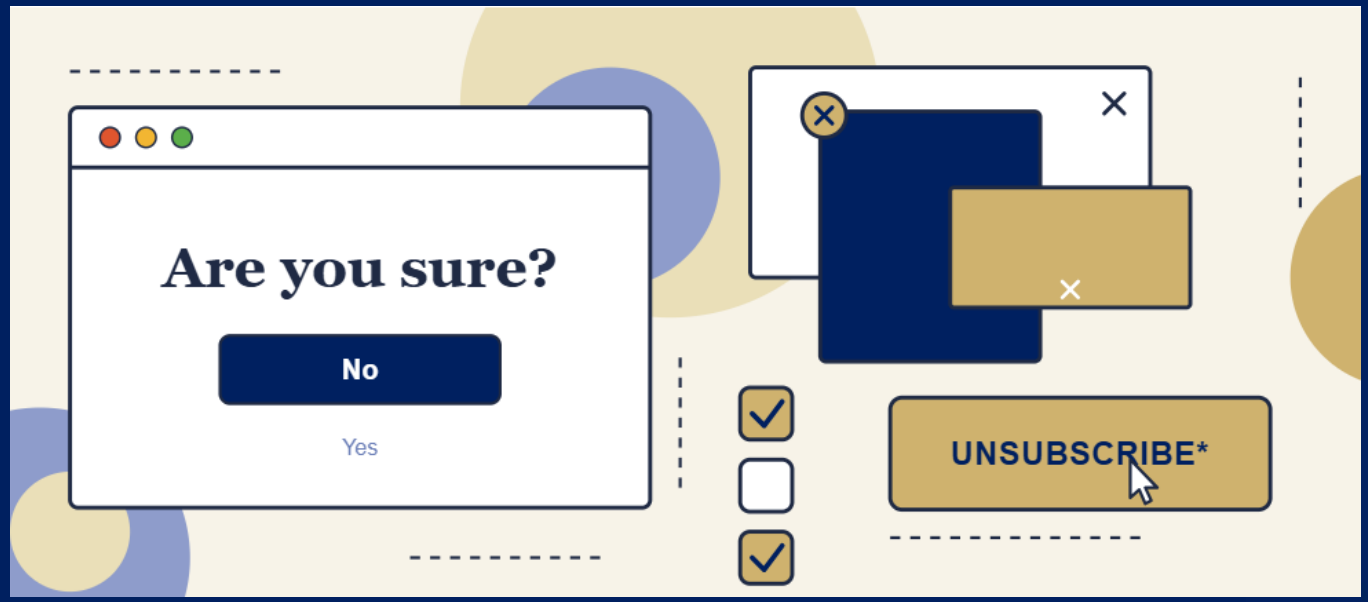
- GDPR requires consent to be freely given, informed, and unambiguous. Dark patterns undermine these principles by pressuring or misleading users into providing consent that is not truly voluntary.



Are Dark Patterns Undermining GDPR Consent?

We set cookies to help us learn how you use our site and serve you more relevant ads. To exercise your choices around cookies, click "Accept", "Reject All", or "Manage Preferences".

ACCEPT ALL | REJECT ALL | MANAGE PREFERENCES

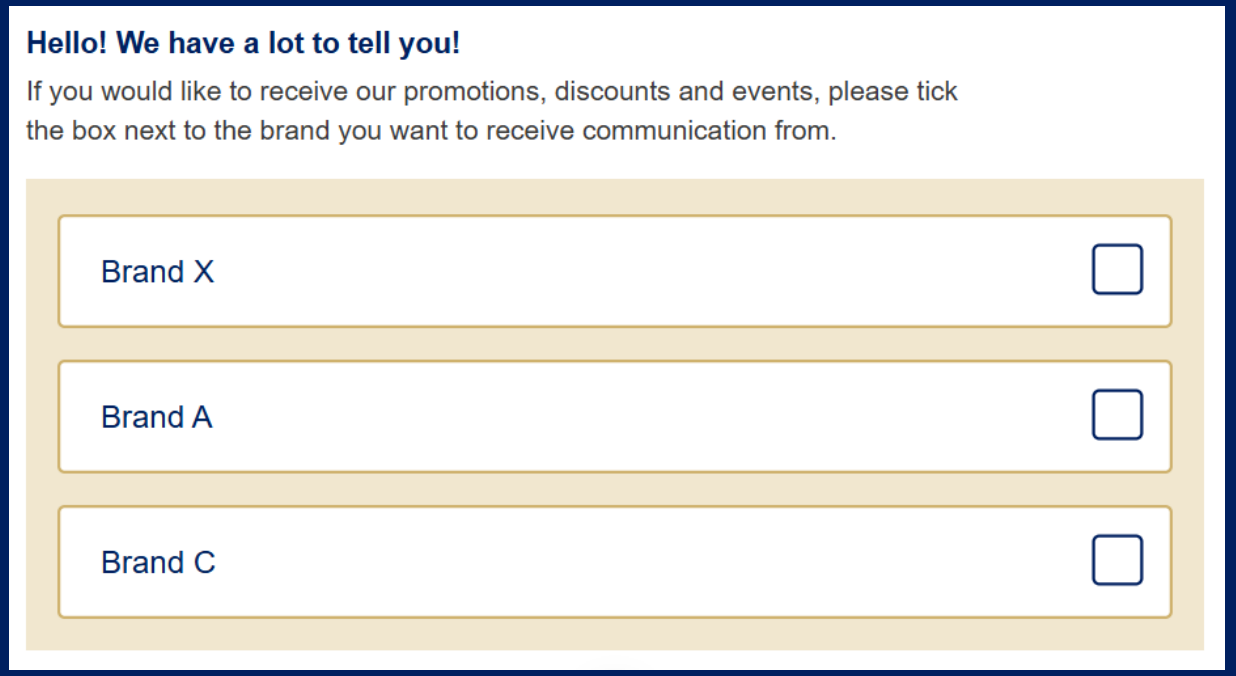


Do’s and Don’ts on Consent

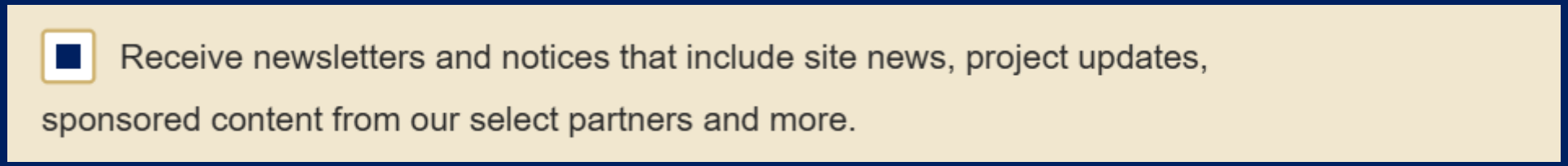
DO'S

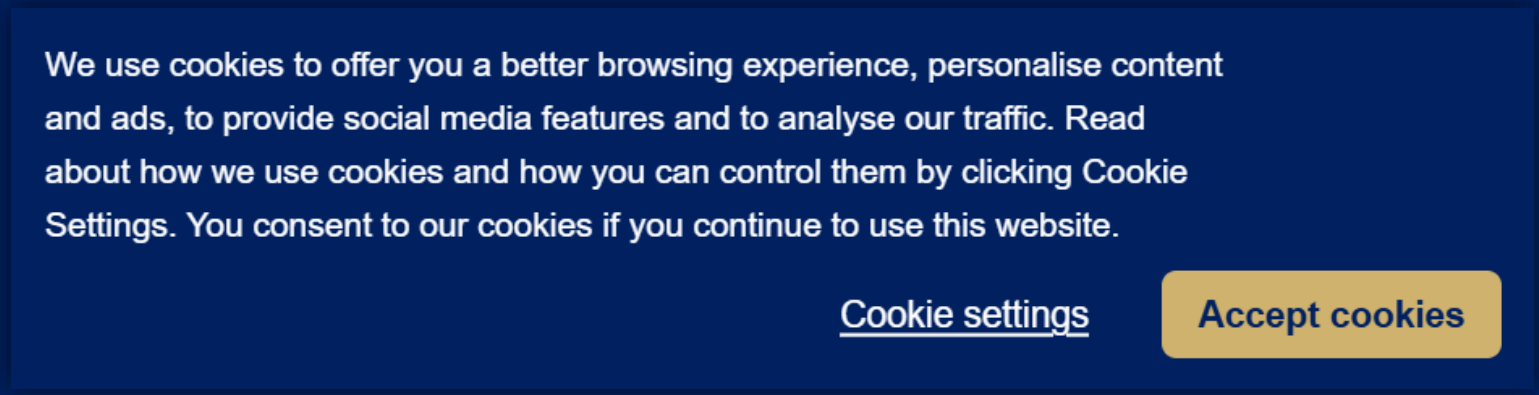
The data controller of the website (company X) intends to share the data with other brands companies for the purpose of direct marketing.

Is the below compliant with the requirement for a valid consent?



DON'TS

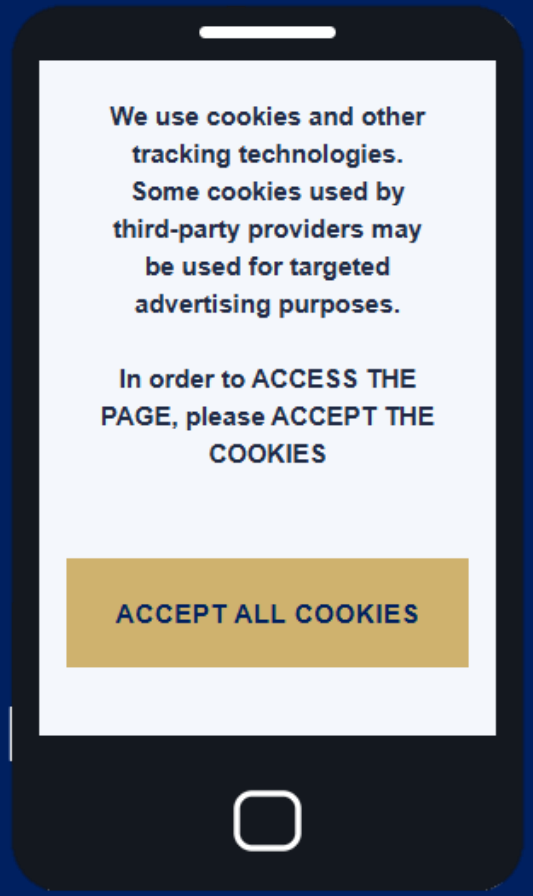




WHY is this not compliant?:
The user is automatically opted in to have their data collected for providing direct marketing;
There is no information on the selected partners that will have access to your data;
If continue to use the website you automatically accept (consent no freely given).
Dark pattern

DON'TS

*Other Examples of **DON'Ts***



The user has no choice other than to ACCEPT. The access to the service is subject to the data subject consent, and this makes such consent not "freely given".

The practice used to obtain consent by means of a user's action, such as scrolling or swiping through a webpage, does not constitute a "clear and affirmative" act in terms of the requirements of article 7 of the GDPR

BY SCROLLING AND VISITING THIS WEBSITE
YOU EXPRESSLY AGREE TO THE USE OF COOKIES
FOR IMPROVING YOUR USER EXPERIENCE.

FOR MORE INFORMATION, YOU MAY READ OUR COOKIE POLICY

Use of Consent and Other Legal Basis

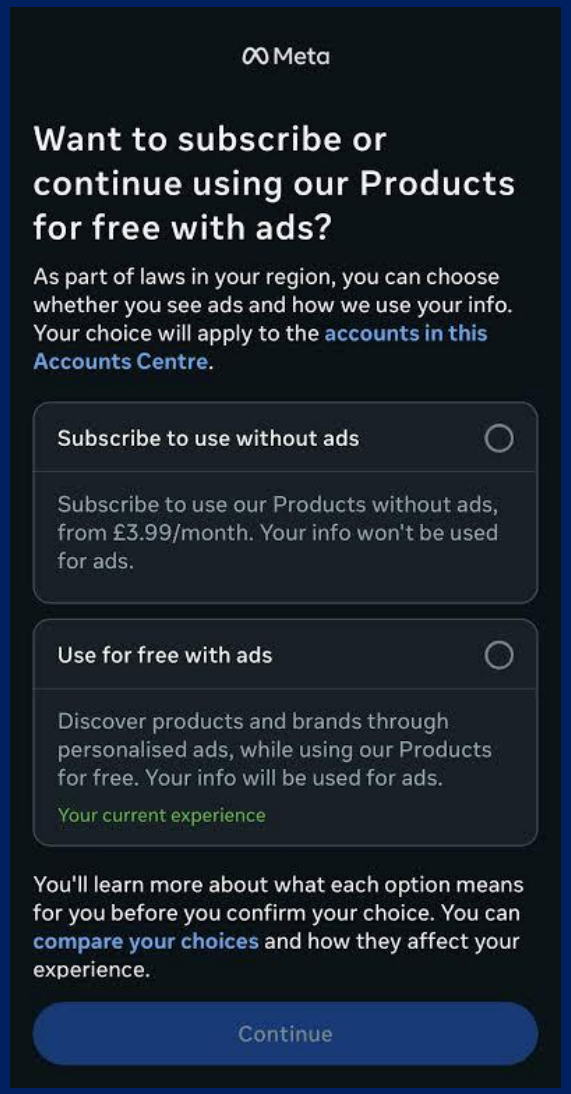
When consent is required?

- ✓ Tracking users' browsing habits for targeted ads
- ✓ Processing of sensitive data (special categories)
- ✓ Bundled processing beyond core service
- ✓ High imbalance situations (e.g., employer-employee)
- ✓ Non-essential cookies & online tracking (ePrivacy Directive)

When Other Lawful Bases Apply

- ➢ Contractual necessity: to perform or prepare a contract (e.g. delivering an order, managing an account).
- ➢ Legal obligation: required by law (e.g. tax reporting, AML/KYC checks).
- ➢ Vital interests: protecting life or safety (e.g. emergency medical disclosure).
- ➢ Public task: carried out in the public interest or under official authority (e.g. census, law enforcement).
- ➢ Legitimate interests: controller's justified interests that do not override the individual's rights (e.g. fraud prevention, IT security, analytics).

New Meta Model: Pay or Consent (introduced November 2023)



- Introduced across the EU/EEA in November 2023.
- Users now face two clear options:
  - Use for free = consent to personalised ads and tracking
  - Pay 9.99 Euro per month = ad-free experience, no tracking.
- Meta says this provides genuine consent under GDPR Article 6(1)(a).
- Regulators question whether this consent is truly freely given.

Background: Meta's Original Legal Basis

- Meta relied on Article 6(1)(b) GDPR – performance of a contract.
- Claimed personalised ads were part of the service users signed up for.
- No separate consent requested for behavioural advertising.
- Challenged by regulators and privacy groups (e.g., NOYB).

CJEU Judgement (C-252/21)

- 4th July 2023: CJEU – Meta Platforms vs Bundeskartellamt (C-252/21)
- Personalised advertising not objectively necessary for providing the service.
- Meta cannot rely on Article 6(1)(b).
- Data use for ads now requires user consent under Article 6(1)(a).
- Meta forced to find a new legal basis

Meta's Transition to Consent (Late 2023)

- After the CJEU ruling, Meta switched to Article 6(1)(a) = User Consent.
- November 2023: rolled out Pay or Consent across EU/EEA
  - Use for free = agree to personalised ads
  - Pay 9.99 Euro per month (12.99 Euro mobile) = ad-free, no tracking.
- Meta claimed this satisfied GDPR choice requirements.
- Regulators question if consent was truly freely given.

EDPB Opinion 08/2024: ‘Consent or Pay’ Models (17 Apr 2024)

- Large platforms with dominant market power = high compliance risk
- Why “Consent-or-Pay” fails:
  - Must offer equivalent free alternative (e.g., contextual ads)
  - No detriment – price must not coerce consent
  - Assess power balance – gatekeeper platforms = suspect consent
- GDPR Consent Criteria
  - Consent separated by purpose – no bundled opt-ins
  - Purposes must be clear, specific, unambiguous
  - Provide full information, no manipulative UI patterns

EDPB Opinion 08/2024: 'Consent or Pay' Models (17 Apr 2024)

- **Appropriateness**:
  - Fees must reflect service value, not treat privacy as a commodity.
  - Cannot act as a "sales price" for personal data.

- **Fairness & non-coercion**:
  - Fees must not be so high that users feel forced to consent.
  - Free/no-ad option must still provide comparable functionality.
  - Declining consent cannot lock users out or reduce service quality.

© GVZH 2025 | THIS DOCUMENT IS CONFIDENTIAL AND ITS CIRCULATION, USE AND/OR REPRODUCTION IN WHOLE OR IN PART ARE RESTRICTED

Meta Platforms Ireland Ltd v. EDPB (General Court, Case T-319/24) & Ongoing Developments

- June 2024: Meta challenged the EDPB Opinion 08/2024 before the General Court.
- April 2025: Court dismissed the case – Opinion is non-binding guidance.
- Meta's claim for damages rejected.
- Opinion remains influential for GDPR enforcement.
- Parallel DMA action: Commission investigating whether Meta's model forces consent.
- Debate continues: Can privacy ever be a paid upgrade?

Action points - Consent

- *Make consent concise and easy to understand*
- Separate it from other terms and conditions
- Don’t use pre-ticked boxes or other default settings
- Give options to consent to different purposes and types of processing
- Keep records to evidence consent
- Make it easy to withdraw
- Inform data subjects that all processing of personal data will cease once consent is withdrawn, however withdrawal does not affect the lawfulness of Processing based on consent before its withdrawal
- Provide information where the privacy notice can be found
- Review and refresh the consent forms if anything changes
- Regularly Audit Consent Practices

ANY QUESTIONS?

Dr Erika Criscione - email: erika.criscione@gvzh.mt

Dr Hayley Ann Pisani - email: hayley.pisani@gvzh.mt

https://gvzh.mt/