Exercise 1: Privacy and Data Protection

Question 1: Valid Consent

Service Selected: WhatsApp

Analysis of Consent Mechanism

WhatsApp's consent mechanism shows **mixed compliance** with GDPR requirements:

Areas of Compliance:

Art 7(1) GDPR - Demonstrability of Consent: WhatsApp maintains records of user consent through acceptance of Terms of Service and Privacy Policy during account registration. Users must explicitly accept these documents before using the service, which allows WhatsApp to demonstrate that consent was given.

Art 6(1)(a) GDPR - Specific Purpose: WhatsApp clearly states processing purposes in its Privacy Policy, including service provision, security, and business operations. The purposes are defined with reasonable specificity.

Art 7(3) GDPR - Right to Withdraw: WhatsApp provides mechanisms to withdraw consent, including account deletion options accessible through Settings → Account → Delete My Account. Users can also manage certain data sharing preferences through the app settings.

Areas of Concern:

Art 7(4) GDPR - Freely Given Consent: A significant GDPR compliance issue arises with WhatsApp's data sharing with other Meta companies (Facebook, Instagram). The consent appears **not freely given** because:

- Users cannot use WhatsApp without accepting data sharing with Meta for certain purposes
- The service is conditional on consent to processing that may not be strictly necessary for the core messaging service
- This violates the principle that consent must be "freely given" - users should be able to refuse specific processing while still accessing the service

Art 7(2) GDPR - Clear and Distinguishable: WhatsApp's 2021 privacy policy update was criticized for being lengthy and complex. While the policy attempts to use plain language, the sheer volume of information and the integration with broader Meta data practices makes it challenging for average users to provide truly "informed" consent as required by Art 4(11) GDPR.

Art 7(3) GDPR - Easy Withdrawal: While account deletion is possible, withdrawing consent to specific data processing purposes while maintaining service access is difficult or impossible, which contradicts the requirement that withdrawal should be as easy as giving consent.

Conclusion

WhatsApp's consent mechanism **partially complies** with GDPR but has significant shortcomings, particularly regarding the "freely given" requirement of Art 7(4) GDPR and the bundling of consent for various processing purposes. The European Data Protection Board and several EU regulators have raised concerns about Meta's consent practices, suggesting that consent may not be the appropriate legal basis for all of WhatsApp's data processing activities.

Question 2: Right to Access Personal Data

Relevant GDPR Articles

Art 15(1) GDPR - Right of Access: Data subjects have the right to obtain confirmation of whether personal data is being processed and, if so, access to that data and information about the processing.

Art 15(3) GDPR - Copy of Data: The controller must provide a copy of personal data undergoing processing, with the first copy free of charge.

Art 12(3) GDPR - Response Timeframe: Controllers must respond to access requests without undue delay and at the latest within one month.

WhatsApp's Access Request Mechanism

How to Exercise the Right:

WhatsApp provides the following mechanism to exercise the right of access:

1. **In-App Request Process:**
   - Navigate to Settings → Account → Request Account Info
   - Click "Request Report"
   - WhatsApp generates a downloadable report (usually within 3 days)
   - User receives an in-app notification when the report is ready
   - Report remains available for download for approximately 30 days
2. **Data Included in the Report:**
   - Account information (phone number, profile photo, about/status)
   - Groups information (groups you're part of, group settings)
   - Contact list synchronized with WhatsApp
   - Block list
   - Settings and preferences
   - Message logs metadata (not message content due to end-to-end encryption)
3. **Alternative Method:**
   - Users can contact WhatsApp's Data Protection Officer via email
   - Submit written requests through Meta's privacy help center

Compliance Assessment:

Strengths:

- **Art 15(3) compliance:** WhatsApp provides a straightforward in-app mechanism that allows users to request their data without technical expertise

- **Art 12(3) compliance:** Reports are typically generated within 3 days, well within the one-month legal requirement
- **No cost:** The first copy is provided free of charge as required
- **Electronic format:** Data is provided in downloadable format (HTML/JSON) as preferred for electronic requests under Art 15(3)

Weaknesses:

- **Incomplete information:** The report may not include all information required by Art 15(1), such as:
  - Detailed information about recipients of data (Art 15(1)(c))
  - Specific retention periods for different data categories (Art 15(1)(d))
  - Clear information about data transfers to third countries (Art 15(1)(f))
- **Limited transparency on automated decision-making:** While WhatsApp doesn't heavily rely on automated decision-making visible to users, the information provided about algorithmic processing (if any) may not fully satisfy Art 15(1)(h) requirements
- **Message content limitation:** Due to end-to-end encryption, actual message content is not included in the report. While this is technically justified, it limits the completeness of the data access

Practical Effectiveness

In practice, WhatsApp's access mechanism represents **reasonably good compliance** with Art 15 GDPR. The in-app request feature is user-friendly and efficient, making it easier for data subjects to exercise their rights compared to many other services that require email requests or complex web forms.

However, the **completeness and clarity** of information provided could be improved to fully satisfy Art 15(1)'s comprehensive requirements, particularly regarding data sharing with Meta companies and detailed retention policies.

Question 3: Anonymisation vs Pseudonymisation

Legal Definitions

Pseudonymisation (Art 4(5) GDPR): "The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

Anonymisation: While not explicitly defined in GDPR, anonymisation refers to the irreversible process of transforming personal data so that it can no longer be attributed to a specific data subject, even with the use of additional information. Recital 26 GDPR clarifies that anonymised data falls outside the scope of GDPR.

Key Differences

Aspect	Pseudonymisation	Anonymisation

Aspect	Pseudonymisation	Anonymisation
Reversibility	Reversible with additional information (key)	Irreversible - cannot be re-identified
GDPR Application	Remains personal data - GDPR applies	Not personal data - GDPR does not apply
Data Subject Rights	All rights apply (Art 15-22)	No rights apply
Legal Basis Required	Yes, under Art 6	No legal basis needed
Security Measure	Considered a safeguard (Art 25, 32)	Risk elimination technique
Re-identification Risk	Possible if key is compromised	Not possible (if properly anonymised)

Practical Examples

Pseudonymisation:

- Replacing names with randomly generated IDs (e.g., User123456)
- Hashing email addresses while maintaining behavioral data
- Medical research databases where patient names are replaced with codes, but researchers can re-link data if needed

Anonymisation:

- Aggregated statistics (e.g., "1,000 users aged 25-34")
- Data that has been generalized to the point where individuals cannot be singled out
- Fully stripped datasets where all identifiers and quasi-identifiers are removed without possibility of reversal

Practical Implications

When to use Pseudonymisation:

- When you need to maintain the ability to re-identify individuals (e.g., to respond to data subject requests)
- For internal analytics while reducing privacy risks
- As a security measure to protect against data breaches (Art 32 GDPR)
- Note: You must still comply with all GDPR requirements including having a lawful basis, honoring data subject rights, and maintaining security

When to use Anonymisation:

- When re-identification is not needed for the processing purpose
- For public data sharing or research publication
- When you want to permanently exit GDPR compliance obligations for a dataset

- Caution: True anonymisation is difficult to achieve - must ensure data cannot be re-identified through combination with other datasets or techniques

Recent Developments

The European Data Protection Board (EDPB) published Guidelines 01/2025 on Pseudonymisation in January 2025, emphasizing that:

- Pseudonymisation is an effective technical safeguard but does not remove data from GDPR scope
- Controllers must assess re-identification risks considering all reasonably available means
- Pseudonymised data still requires appropriate legal basis and security measures