1. Valid Consent

For this question, I chose Spotify as the service to which I have given consent for the processing of my personal data.

According to Spotify's Privacy Policy, users consent to the collection and processing of their personal data (such as name, email address, location, and usage data) when creating an account. Under Art. 6 (1) a) GDPR, processing is lawful if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes."

Furthermore, Art. 7 (1)–(4) specifies that consent must be:

- Freely given, specific, informed, and unambiguous (Art. 4 (11), Art. 7 (2)),
- Capable of being withdrawn as easily as it was given (Art. 7 (3)).

Users can withdraw consent through account settings, which fulfills the transparency and withdrawal conditions.

Since account creation is required to use the service, the consent could arguably not be "freely given" (Art. 7 (4)), because access is conditional on agreeing to the data processing terms. While the consent is informed and revocable, it may not fully satisfy the GDPR's requirement that consent be freely given.

2. Right to Access Your Personal Data

Under Art. 15 GDPR, the data subject has the right of access, meaning they can obtain confirmation as to whether personal data concerning them is being processed and, if so, access to:

- The purposes of the processing (Art. 15 (1) a)),
- The categories of personal data (Art. 15 (1) b)),
- The recipients or categories of recipients (Art. 15 (1) c)),
- The envisaged period for which the data will be stored (Art. 15 (1) d)),
- Information about rights to rectification, erasure, restriction, or objection (Art. 15 (1) e)).

I submitted a data access request to Google, since I use several of their services (Gmail, Drive, Maps). Google provides a dedicated tool called "Google Takeout", accessible via takeout.google.com, which allows users to download a copy of the data associated with their account.

This mechanism clearly supports the right of access in practice, as users can see what categories of data are processed and even download it in a structured format, which aligns with Art. 15 (3) (“The controller shall provide a copy of the personal data undergoing processing.”). Google’s implementation appears to respect Art. 15, even though it is automated rather than personalized.

3. Anonymisation & Pseudonymisation

Anonymisation refers to processing personal data in such a way that the data subject is no longer identifiable. Once data is truly anonymised, it no longer falls under the scope of the GDPR because it cannot be linked back to an individual.

Pseudonymisation, defined in Art. 4 (5) GDPR, means processing personal data so that it can no longer be attributed to a specific data subject without the use of additional information (for example, replacing names with ID numbers).