The draft Recommendations define an “online user account” as a personal online space that is accessible through an authentication mechanism relying on a unique identifier and a password or equivalent. At the same time, the document explicitly excludes from this definition personal spaces that are only accessible via temporary access tokens and do not require a password.

This distinction forms a central pillar of the guidance, yet it is difficult to reconcile with current technical practice. Many online services already rely on so-called “passwordless” authentication patterns in which users gain access to their personal space by receiving a temporary token, typically via email. These tokens can be requested repeatedly and grant access to the same aggregated personal space each time. Functionally, this provides persistent, self-service access to personal data across sessions, even though no password is stored. In practice, this is widely understood and marketed as a login to a personal account, despite falling outside the document’s formal definition.

At the same time, the Recommendations treat persistence as something that is increased through the creation of an account. However, in transactional contexts such as e-commerce, persistence already exists independently of any account mechanism. Orders must be stored for legal, contractual, and operational reasons. They are typically linked to a stable identifier, most often an email address, in order to provide delivery updates, enable customer support, handle returns, and resolve disputes. As a result, the personal data associated with a purchase is already persistent and retrievable over time.

Against this background, the incremental effect of creating an account is limited. In technical terms, the main additional element introduced by an account, as defined in the draft, is the storage of a password or equivalent credential. Yet, as the prevalence of temporary-token authentication demonstrates, the absence of a stored password does not meaningfully change the persistence, accessibility, or linkability of personal data. The same personal space, the same historical data, and the same self-service access can be offered without crossing the formal threshold of an “account” under the Recommendations.

This raises questions about the objective pursued by the guidance. It is unclear which specific privacy risk is mitigated by discouraging mandatory accounts as defined, when equivalent data persistence and access patterns remain possible — and in many cases already exist — without them. The guidance appears to regulate the form of authentication rather than the substance of data processing.

As a result, the practical effect of the Recommendations risks being a shift toward alternative authentication mechanisms that preserve the same underlying data

practices, rather than a reduction in data collection, retention, or reuse. In that sense, the guidance seems primarily to address a user-experience concern — the perceived burden of creating an account — rather than delivering a clear improvement in privacy outcomes as understood through the GDPR's principles of data minimisation, purpose limitation, or storage limitation.

From a technical and practical perspective, it would therefore be helpful for the EDPB to clarify which concrete privacy harms it considers to be uniquely caused by accounts as defined in the draft, and how the proposed distinction meaningfully reduces those harms compared to functionally equivalent, passwordless designs.