Category	Criteria	No	Specification
Security	Secure communication, data transmission and storage	1	The service shall apply best practice **cryptography to data in transit**, …
		2	The service shall apply best practice **cryptography to data at rest**, …
		3	Privacy enhancing technologies such as **Anonymization and Pseudonymization shall be used** according to best practices in order to adequately protect the user's data
	Secure user authentication	4	All passwords used for the service shall be subject to a **state-of-the-art password policy,** …
	Secure service set up, maintenance and update	5	**Guidance for secure installation, configuration, and updates** shall be in place and updated for each release if necessary. Guidance shall be available in a manner that is easy to find and use. …
		6	All software components shall be **updatable in a secure manner**, and verification of security updates shall be in place.
		7	**Updates shall be timely.** Updates addressing critical security vulnerabilities must be available as soon as possible.
		8	**Hard-coded critical security parameters in service software source code** shall not be used.
		9	Any **critical security parameters** used … **shall be unique per service**…
		10	The service provider shall follow **secure management processes** for critical security parameters that relate to the service.
	Vulnerability/breach monitoring/reporting	11	The service-provider shall continually **monitor, identify and rectify security vulnerabilities and/or breaches,** …
		12	**Vulnerabilities and/or personal data breaches shall be communicated** to relevant authorities and impacted data subjects **within 72 hours.**

Data Protection	Privacy policy and user consent	13	The user shall be **informed about the purpose and use of their data** in a permanently and easily accessible privacy policy, in which a Data Protection Officer shall also be identified.
		14	The privacy policy shall provide users with **clear and transparent information about what personal data and cookies are used**, how they are processed and exploited, by whom (including third parties and advertisers), for what purposes, ...
		15	**User consent shall be expressly collected** and obtained separately from the terms and conditions of use of the services. The user must be able to easily withdraw their consent at any time. Parental control shall be enforced if applicable.
	Data collection, storage, exploitation	16	The service provider undertakes to **fully implement data minimization** for all processing activities covered and obtained through a legal basis. ...
		17	**Unless the user expressly consents** to a personalized use, collected usage and/or telemetry **data shall be anonymized**...
	Data retention, access, rectification	18	The service provider shall **minimize the retention of personal data** for service delivery ...
		19	If the personal **data are no longer required** for the service and related storage purposes, they **shall be deleted.** ...
		20	The service provider shall ensure that the **user can access their data** and can exercise their rights ...

Reliability	Reliable service updates	21	The **software version** of the service shall be clearly recognizable.
		22	The service provider shall publish, in an accessible way that is clear and transparent to the user, the **defined support period** and the need for that support period.
	Resilience to service outage	23	**Disaster recovery, business continuity and data backup and restore policies and procedures shall be in place** and regularly tested to ensure ongoing availability of data.
	Functional reliability	24	The service shall provide its users with an extensive, easy-to-understand, easy-to-access **description of its functionalities,** and shall operate in strict accordance with this description.
		25	If relevant, the service shall provision for a secure, precise and **efficient billing and payment system** which employs two-factor authentication and adheres to local and regional norms.
		26	If relevant, the service shall provision for a **delivery system** which fulfils state-of-the-art conditions of the associated specific activity domain.
	Accountability	27	The service shall provide its users with a clear, easy-to-access and easy-to-print service and service **provider identification**.
		28	The service shall **document its compliance with all applicable laws and regulation**...

		29	**User inquiries and complaints shall be treated in a timely fashion**, and relevant alternative dispute resolution mechanisms must be in place to facilitate these processes.
Fair User Interaction	Non-discriminating access	30	The system shall provide a **non-discriminating access to all its potential users**.
	Fair user interfaces	31	**Service interfaces shall be designed so as not to deceive, nor to manipulate the users, and**, .. ("dark patterns") such as Interface Interference (Preselection, Obstruction), Aesthetic Manipulation (Toying with emotions, False Hierarchy), Disguised ads (Trick questions, Sneaking), Forced Actions (Social Pyramid, Gamification, Privacy "Zuckering")...
		32	The service **shall not be designed to exclusively cause user addiction and** shall clearly inform the users about potential addiction risks during its set up.
		33	Services **specifically targeting young children shall provide a parental control** functionality.
	Fair use of AI-based algorithms	34	**There shall be clear information to the user when interacting with AI-based algorithms** and, especially, with automated decision-making algorithms. ...
		35	If **AI-based algorithms** and, especially, automated decision-making algorithms, are used, **the service shall provision for specific mechanisms to assess their robustness, resilience and accuracy, as well as the risks associated with their exploitation**, and shall provide the user with the **possibility to request that a representative of the service provider, reviews and validates the outputs produced by the algorithm.**