Criteria Catalogue for the Digital Trust Label

Final Version

Version 1 - November 2021

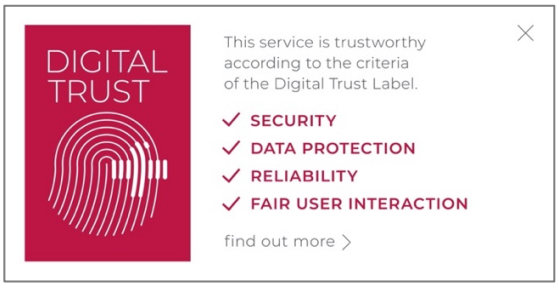
Swiss Digital Initiative

c/o Campus Biotech

Chemin des Mines 9

1202 Geneva

Switzerland



The Label Expert Committee

Coordinated by EPFL Centre for Digital Trust (C4DT, Imad Aad and Martin Rajman)

LEC President: Stéphanie Borg Psaila, Digital Policy Director, DiploFoundation

- Prof. Yaniv Benhamou, Faculty of Law, University of Geneva, Attorney-at-Law
- Prof. Dr. Abraham Bernstein, Department of Informatics, Director Digital Society Initiative, University of Zurich
- Nikki Böhler, Managing Director, OpenData.ch
- Francesca Bosco, Senior Advisor, Cyber Capacity and Foresight, CyberPeace Institute
- Christophe Hauert, Lecturer University of Lausanne, Co-Founder Cybersafe Label
- Prof. Dr. Jean-Pierre Hubaux, Full Professor Laboratory for Data Security, EPFL
- Carla Hustedt, Senior Project Manager, Bertelsmann Foundation (until the end of 2020)
- Dr. Patrick Schaller, Senior Scientist, System Security Group, ETH
- Florian Schütz, Federal Cyber Security Delegate
- Jean-Christophe Schwaab, Fédération Romande des Consommateurs
- Martin Steiger, Attorney, and Entrepreneur for Law in the Digital Space

SWISS DIGITAL INITIATIVE

Category	Criteria	No	Specification	ISO	GDPR
Security	Secure communication, data transmission and storage	1	The service shall apply best practice cryptography to data in transit, ensuring that the cryptography is reviewed and evaluated, delivers the required functions for all transmitted data and is appropriate to the properties of the technology, risk, and usage. All data in transit over open communication lines such as the internet must be encrypted.	X	X
		2	The service shall apply best practice cryptography to data at rest, ensuring that the cryptography is reviewed and evaluated, delivers the required functions for all sensitive and applicable data at rest and is appropriate to the properties of the technology, risk, and usage.	X	X
		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.	X	X
	Secure user authentication	4	All passwords used for the service shall be subject to a state-of-the-art password policy, which includes requirements applicable to the service and ensures that no hard-coded passwords are used, best practice authentication is in place and ensures that brute-force attacks on authentication mechanisms are not feasible.		
	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 access and understand. Any major changes shall lead to a communication to the users in an easy-to-understand format.		
		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.	X	
		8	Hard-coded critical security parameters in service software source code shall not be used.		
		9	Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated service software shall be unique per service and		

			shall implement security measures to protect the integrity and confidentiality of critical security parameters.		
		10	The service provider shall follow secure management processes for critical security parameters that relate to the service.	X	X
	Vulnerability/ breach monitoring/ reporting	11	The service provider shall continually monitor, identify, and rectify security vulnerabilities and/or breaches, and shall provide a public point of contact as part of a vulnerability disclosure policy so that security researchers and others are able to report issues.		X
		12	Critical security vulnerabilities shall be communicated to relevant authorities within 72 hours if not corrected, and the impacted users shall be timely and adequately informed. Personal data breaches shall be communicated to relevant authorities and impacted data subjects within 72 hours.		X
Data Protection	User consent	13	The user shall be informed about the purpose of the processing and the legal basis for processing of their personal data in clear and plain language. Where there is more than one purpose/legal basis, they need to be listed separately in a way that the user is able to easily distinguish between one purpose/legal basis and another.		X
		14	Where user consent is sought for the processing of personal data, such consent shall be expressly collected from the user for each of the purposes and legal basis listed by the service provider and obtained separately from the terms and conditions of use of the services.		X
		15	Where initial user consent is sought for the processing of personal data, the user shall be provided with the option of either opting in, or opting out, expressed through a valid and affirmative action. If checkboxes are used, they shall not pre-ticked. The user shall also be given the possibility of requesting additional information.		X
		16	The user shall be provided with a separate, easy, and accessible way of withdrawing consent.		X

	Data retention and data processing	17	The user shall be informed of the definite time period for which the personal data will be stored. If that is not possible, the user shall be informed of the criteria and reasons used to determine the indefinite period, and a regular timeframe for which a review will be undertaken.		X
		18	In cases in which the service provider anonymises personal data, upon a request by the user, such service provider shall provide a detailed explanation of how personal data is being anonymised, and the safety measures used to prevent de-anonymisation. The service provider shall also update the user on the anonymisation status of any personal data held by the provider at the time of the request.		X
		19	Once the data retention period lapses, the service provider shall either anonymise or delete the personal data. In case of indefinite data retention periods where regular reviews are to be undertaken (criteria 17), the user shall be informed of the outcomes of the review within 30 days.		X
		20	The service provider shall ensure that the user can access their data. Any requests for access need to be acceded to within 30 days. Together with a copy of the personal data, a user is to be provided with names of third parties with whom such personal data has been shared, together with the legal basis under which such data is being held.		X
Reliability	Reliable service updates	21	The software version of the service shall be easy to access and understand.	X	
		22	The service provider shall publish, in a way that is easy to access and understand for the user, the defined support period and the need for that support period.	X	
	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 the service and associated data.	X	X
	Functional reliability	24	The service shall provide its users with an extensive, easy-to-access, easy-to-understand 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 fulfills state-of-the-art conditions of the associated specific activity domain.		
	Accountability	27	The service shall provide its users with an easy-to-access, easy-to-understand, and easy-to-print service and service provider identification.		X
		28	The service shall document its compliance with all applicable laws and regulation and assign a contact representative for easy-to-access and easy-to-understand information about legislation that the service is subject to.		X
		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.		X
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, in particular, shall exclude clearly manipulative techniques ("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). In addition, the use of mildly manipulative techniques shall be clearly announced to the users and proportionate to the objectives of the service.		
		32	The service shall not be designed to exclusively cause user addiction and shall provide the users with an easy-to-access, easy-to-understand information about potential addiction risks during its set up.		
		33	Service providers whose services are illegal to users under the age of 18 shall take proportional steps to verify users' age and prevent under-18s from accessing those services.		

	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. The service provider shall also indicate which user-related data is processed by the algorithms and its relationship to the objectives of the service, in addition to informing why an AI is used for the service. Any risks inherent to the algorithms must be clearly and concisely described to the user.		
		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.		