Cycle tracking apps: A combined medical and data privacy scoring

Yasmin TEHRANCHIAN[a], Veronika STROTBAUM[b,c] and Monika POBIRUCHIN[a, b]
[a] *GECKO Institute, Heilbronn University of Applied Sciences, Heilbronn, Germany*
[b] *Consumer Health Informatics SIG, GMDS e. V., Cologne, Germany*
[c] *Maybe Veronika's affiliation, Germany*

Table Developed scoring system for the data privacy, data protection domain. Source is either DIGAV (D) or the App Check project (ACP).

#	Subject	Requirements	Source
Data Privacy			
1	General Data Protection Regulation (GDPR) as the applicable law	The processing of personal data by DiGA and their manufacturers is subject to Regulation (EU) 2016/679 and possibly other data protection regulations?	D
2	Consent	Is a voluntary and informed consent of the user obtained before the processing of personal data that is related to an identifiable natural person?	D
3		Is the consent given through an active action of the user?	D
4		Is the user informed about the right to withdraw their consent before giving their consent?	D,ACP
5	Appropriation	Is the processing of personal data carried out only for the purposes specified in § 4 (2) clause 1 or on the basis of other legal data processing authorizations under § 4 (2) clause 3?	D,ACP
6	Data minimisation and reasonableness	Are the personal data to be processed by the app purpose-appropriate and minimized to the extent possible?	D,ACP
7	Information requirements	Is the privacy policy easily and quickly accessible (within and outside the app)?	D,ACP
8		Does the privacy policy contain a complete imprint?	D,ACP
9		Does the privacy policy contain the name of the data protection officer?	D,ACP

10		Is the user informed of their right to data portability under Article 20 of Regulation (EU) 2016/679 before their user account is deleted?	D,ACP
11	Data disclosure to third parties	Are no personal data disclosed to third parties (except for the immediate fulfillment of the purposes)?	D,ACP
12	Processing in foreign countries	Is the processing of health data as well as personal data carried out exclusively in the country, EU member states, contracting states of the Agreement on the European Economic Area or Switzerland?	D
Data Security			
13	Authentication	Is there a way to protect the app with some form of authentication (e.g. code or password)?	D
14		If a password is used for security, are there secure password guidelines (e.g. minimum password length)?	D
15		When resetting the password (accessing health data), does the app require authentication of the person's authenticity?	D
16		Is there an option for two-factor authentication?	D
According §§ 5 and 6			
17	Interoperability	Is there a possibility to export the user's personal data and exercise the right to data portability?	D,ACP
18		Can the user easily and quickly export the data processed in the app? (subjectively)	D,ACP
19	Consumer protection	Does the app provide the user with all relevant information from the app description before they enter into obligations with the manufacturer or a third party?	D
20		Is the app free of advertising (advertising in this case refers to ads seen directly in the DiGA)?	D
21		Is the app free of trackers?	
22		Are the usage conditions of the app designed to be consumer-friendly? ➔ Does the DiGA not contain opaque offers such as automatically renewing subscriptions or limited-time special offers?	D
23		Is there a free German-language support available?	D,ACP
24		Is it easy to delete the account as well as the associated data? (subjectively)	D,ACP

25	Usability and accessibility	Is the app easy and intuitive to use? (subjectively)	D,ACP
26		Is the app written in a language that is understandable for the target audience? (subjectively)	ACP
27		Does the app offer a tutorial for use?	ACP
28	Patient safety	Does the app inform the user about the risks?	D,ACP
29		Are the transmitted data checked for plausibility?	D,ACP
30		In case of critical measurement values or analysis results, is consultation with a doctor or other healthcare provider recommended?	D,ACP