Group.RISKS		Risk ID	Asset	Threat	Vulnerability	Mitigation Measures	Comments	CRA Annex I Part I, a) - m)
RISK-G1: Communication interception - MITM [SCM, CRY]	**1**	RT1	**Scheduling function**	Bluetooth communication interception (MITM)	Unencrypted communication		data is not transferred in plain text and is not easily readable. As a result, we have not considered it necessary to encrypt the data during transmission.	(b), (e): secure by default, confidentiality
		RM4	**Bluetooth communication channel**	MITM over Bluetooth	Lack of secure pairing		data is not transferred in plain text and is not easily readable. As a result, we have not considered it necessary to encrypt the data during transmission.	(e), (f), (j): confidentiality, integrity, limit attack surfaces
		RM5	**User data handled by the app**	Data interception in transmission	Absence of TLS Lack of cert validation	Use of TLS for https	The user's email is sent the first time the app is used after installation, it is stored on a secure server	(e), (f): confidentiality, integrity
		RM7	**Cloud server and API endpoints**	Data interception in transmission	Absence of TLS Lack of cert validation	Use of TLS for https		(e), (f): confidentiality, integrity
		RC1	**User Form Data** (Name, Email, etc.)	Data interception during submission	No TLS, invalid certificates	**OpenSSL**: Enforce TLS 1.3		(e), (f): confidentiality, integrity
RISK-G2: Unauthorized access [AUM, ACM, GEC]	**2**	RT2	**On/Off control**	Unauthorized access	Weak/No pairing keys	PIN control in App	We consider that in the intended environment, a PIN will not be necessary in most cases, and to ensure user comfort and ease of use, we have not enabled it by default.	(b),(d), (j): secure by default, protection from unauthorised access, limit attack surfaces
		RT8	**Configuration app**	Social engineering	Lack of app access control	Option to limit Time switch access control with PIN	We consider that mobile phones has its own access control	(d), (j): protection from unauthorised access, limit attack surfaces

		RM3	**Bluetooth communication channel**	Unauthorized Bluetooth access	Lack of authentication and secure pairing	PIN control in App	data is not transferred in plain text and is not easily readable. As a result, we have not considered it necessary to encrypt the data during transmission.	(d), (j): protection from unauthorised access, limit attack surfaces
		RM8	**Cloud server and API endpoints**	Unauthorized API access	Insecure API design Inadequate input validation		We have not considered it necessary to further enhance authentication security, as we consider the risk to be low.	(d), (j): protection from unauthorised access, limit attack surfaces
		RC5	**Email verification process**	Spoofing of verification emails	Improper SPF/DKIM/DMARC setup	Use **SPF, DKIM, DMARC** with SMTP provider		d), (e), (f): confindentiality, integrity, protection from unauthorised access
		RC3	**API endpoints (form submission, verification)**	Unauthorized access attempts	Weak authentication, lack of filtering	**iptables, APF, ModSecurity, Fail2ban:** filter traffic and block brute force		(d), (j), (k): protection from unauthorised access, limit attack surfaces, reduce impact of incidents
		RC9	**Cloud Server**	Rootkit or malware persistence	Lack of detection tools	**LMD, rkhunter:** periodic scans		(d), (k): protection from unauthorised access, reduce impact of incidents
RISK-G3: Unauthorized data access from storage [SSM, GEC]	**3**	RM6	**User data handled by the app**	Unauthorized data access from storage	Unencrypted local data storage	PIN control in App	It has been determined that the stored data is not sensitive personal data	(c), (e), (f): protection from unauthorised access, confidentiality, integrity
		RC2	**User Form Data** (Name, Email, etc.)	Unauthorized access to stored data	Misconfigured DB, weak permissions	**RBAC, DB hardening, encryption at rest**		(d), (e), (f): confindentiality, integrity, protection from unauthorised access
RISK-G4: Brute force attack [ACM, GEC]	**4**	RT3	**PIN configuration code**	Brute force attack	Weak PIN length	App lockout after 6 attempts	PIN is limited to 6 access attempts; if exceeded, access is blocked and it must be unlocked using a Master PIN.	(d), (j), (k): protection from unauthorised access, limit attack surfaces, reduce impact of incidents

		RT4	**Master PIN code**	Social engineering	Spoofed call to the factory	No static Master PIN code	To obtain this Master PIN, the user must call the manufacturer, who will provide a code generated at that moment, which is valid only for that day.	(d), (j): protection from unauthorised access, limit attack surfaces
RISK-G5: Malicious firmware installation **[SUM, UNM, GEC]**	**5**	RT5	**Device firmware**	Malicious firmware installation	No integrity validation	FW update with encryption, firmware signature validation and secure keys if applied	With the mitigation measures adopted, the risk of the device is low; therefore, we have not considered it necessary for it to require security updates upon installation	(a), (c) (e), (f), (h): available without known exploitable vulnerabilities, updates,confidentiality, integrity, availability of essential functions
		RM10	**Firmware/Software Update Mechanism of the App**	Malicious firmware/software update	Lack of update signing and verification	The app can be updated through the stores (Google Play/App Store). Use only official stores, secure developer accounts (double authentication + build certificate)	It is a third party component, In this case, we have included security updates, since it is a device with much broader connectivity and an internet connection. It also lets us add new features over time.	(a), (c), (f), (h): without known exploitable vulnerabilities, updates,integrity, availability of essential functions
RISK-G6: Credential theft/misuse [SSM, CCK]	**6**	RT7	**Pairing data**	Key sniffing	Plaintext key storage	secure storage if applied	Not applied because of low risk	(e), (f): confidentiality, integrity
		RM9	**Authentication credentials**	Credential theft/misuse	Unencrypted storage Outdated libraries	Flutter_secure_storage (or a native equivalent) is currently being used.		(a), (c), (e), (f): without known exploitable vulnerabilities, updates,confidentiality, integrity
		RC7	**Database storing user form data**	Data loss or corruption	No backups, no redundancy	Implement **regular backups, test recovery**		(h), (i), (k):availability of essential functions, minimise negative impact, , reduce impact of incidents
RISK-G7: Compromise via outdated software [SUM, UNM. GEC]	**7**	RM2	**Mobile application code & configurations**	Known flutter libraries threats	Outdated libraries	Flutter libraries updated with identified critical vulnerabilities		(a), (c), (e), (f): without known exploitable vulnerabilities, updates,confidentiality, integrity

		RC8	**Cloud Server**	Compromise via outdated software	Unpatched services	Regular OS and service updates, kernel hardening		(a), (c): available without known exploitable vulnerabilities, updates
RISK-G8: Lack of incident detection [NMM, MON]	**8**	RM11	**Logging & Monitoring**	Lack of detection	No logging implemented	Local logs on the server		(l): recording and monitoring relevant internal activity
		RC11	**Logging and Monitoring**	Lack of incident detection	No log analysis or monitoring	**rsyslog, Logwatch:** enable log collection and daily analysis		(l): monitoring relevant internal activity
RISK-G9: Tracking and targeting [GEC]	**9**	RT6	**BLE network identifiers (name, UUID, MAC)**	Tracking and targeting	Publicly visible identifiers		We consider them non-critical identifiers.	(e): confidentiality
RISK-G10: Reverse engineering of app [SSM, GEC]	**10**	RM1	**Mobile application code & configurations**	Reverse engineering of app	Insufficient app hardening	The Flutter app is compiled (Dart AOT). App is converted to native machine code before it runs	This makes the app faster and harder to reverse-engineer than if it were running interpreted code.	(a), (e), (f): without known exploitable vulnerabilities, confidentiality, integrity
RISK-G11: Excess data collection [DLM, DTM]	**11**	RM12	**Data management**	excess data collection	No minimization controls		Only strictly necessary data is processed	(g): data minimisation
		RC12	**Decommissioning user data**	Residual data post-deletion	No secure deletion policy	Implement secure wipe procedures		(m); possibility to users to remove all data
RISK-G12: Denial of Service [NMM]	**12**	RC4	**API endpoints (form submission, verification)**	Denial of Service	No rate limiting, no WAF	**ModSecurity (WAF), Fail2ban, iptables:** mitigate DoS		(h), (i), (j): availability of essential functions, minimise negative impact, limit attack surfaces
		RC6	**Email verification process**	User does not receive email	Delivery issues	Monitor delivery, retry logic		(d), (e), (f): confindentiality, integrity, protection from unauthorised access
		RC10	**Cloud Server**	Spam from server	Uncontrolled mail flow	**SpamAssassin, SMTP rate limiting**		(l): monitoring relevant internal activity