**Megbízhatóság**:

* Az alkalmazásnak pontos és megbízható információkat kell nyújtania a felhasználóknak a hulladékgyűjtők elérhetőségéről, helyszínéről és telítettségi szintjéről.
* Az alkalmazásnak biztonságos és stabil módon kell működnie, minimalizálva a rendszer leállásának vagy meghibásodásának kockázatát.
* Az alkalmazásnak védelmi intézkedéseket kell alkalmaznia az adatok biztonsága érdekében, például az adatvédelmi törvényeknek való megfelelés, az adatok titkosítása és az adatok védelme az illetéktelen hozzáférés ellen.
* Az alkalmazásnak az egyes elvárásoknak megfelelően kell működnie, például az adatok frissítése és az elérhetőség biztosítása.
* Az alkalmazásnak rendelkeznie kell olyan mechanizmusokkal, amelyek lehetővé teszik a meghibásodások vagy hibák azonosítását és javítását, például naplózások készítése, amelyek segítenek a fejlesztőknek a problémák megértésében és javításában.
* Az alkalmazásnak a felhasználók személyes adatainak védelme érdekében biztosítania kell a megfelelő engedélyeket és jogosultságokat.
* Az alkalmazásnak időnként frissítéseket kell biztosítania, amelyek javítják a meglévő hibákat és hozzáadnak új funkciókat, hogy javítsák a használhatóságot és a megbízhatóságot a felhasználók számára.
* A felhasználók hozzájárulása nélkül nem szabad engedélyezni az adatgyűjtést és -felhasználást.
* Az alkalmazásnak a felhasználók számára elérhetővé kell tennie az ügyfélszolgálatot és a támogatást, hogy segítsék őket az esetleges problémák megoldásában és a kérdések megválaszolásában.
* Az alkalmazásnak követnie kell az iparági szabványokat és ajánlásokat, például a mobilalkalmazások tervezésével és fejlesztésével kapcsolatos legjobb gyakorlatokat, hogy biztosítsa a magas minőséget és a felhasználói elégedettséget.

**Megbízhatóságra vonatkozó kérdések:**

Milyen platformon működik az alkalmazás?

* Az alkalmazásnak lehetőleg multiplatformnak kell lennie, azaz elérhető kell lennie különböző operációs rendszereken és eszközökön, például mobiltelefonokon, tableteken és asztali számítógépeken. Az alkalmazásnak a legnépszerűbb operációs rendszerekre (pl.: IOS, Android, Windows) kell készülnie, és kompatibilisnek kell lennie a különböző böngészőkkel (pl.: Chrome, Edge, Firefox stb.).

Felhasználókra milyen szabályok vonatkoznak?

* Az alkalmazás használata során a felhasználóknak be kell tartaniuk az alkalmazás felhasználási feltételeit és az adatvédelmi szabályzatot.\* (pl.: Tilos hamis információt bejelenteniük, ezzel károsítva a többi felhasználót, illetve az üzemeltetőt. Továbbá a felhasználó köteles jelenteni, ha valamilyen hibát észlel az alkalmazásban, és tilos azt kihasználnia.)   
  *\*(Az alkalmazásnak egyértelműen és világosan kell tájékoztatnia a felhasználókat az adatvédelmi politikáról és az általa gyűjtött adatokról, valamint azok felhasználásáról. Az alkalmazásnak lehetőséget kell biztosítania a felhasználóknak adataik törlésére, ha már nem kívánnak tovább használni az alkalmazást.)*

Milyen védelmet alkalmaz az alkalmazás az adatok biztonsága érdekében?

* Az alkalmazásnak védelmi intézkedéseket kell alkalmaznia az adatok biztonsága érdekében. Ez magában foglalhatja az adatvédelmi törvényeknek való megfelelést, az adatok titkosítását, az illetéktelen hozzáférés elleni védelmet, valamint az adatok mentését és helyreállítását vészhelyzet esetén. Továbbá aki böngészőből próbálja meg elérni az oldalt, annak el kell fogadnia a megfelelő sütiket is.

Hogyan kezelik a meghibásodást?

* Az alkalmazásnak olyan mechanizmusokkal kell rendelkeznie, amelyek lehetővé teszik a meghibásodások vagy hibák azonosítását és javítását. Az alkalmazásban használt kódoknak és szoftvereknek folyamatosan frissülniük kell a hibajavítások érdekében. Az alkalmazásnak rendelkeznie kell egy felhasználói támogatási rendszerrel, amely lehetővé teszi a felhasználók számára, hogy jelentsék az esetleges hibákat vagy problémákat, és a fejlesztőknek a lehető leghamarabb kell megválaszolniuk és megoldani ezeket.

Hogyan előznék meg?

* Az adatbiztonság érdekében az alkalmazás fejlesztésekor a tervezési fázisban ki kell dolgozni egy olyan adatvédelmi stratégiát, amelynek része a biztonsági követelmények megállapítása, az adatvédelmi szabályok betartása és a megfelelő védelmi intézkedések kidolgozása. Az alkalmazásban a felhasználói adatokat is védeni kell, például a jelszavakat biztonságos módon kell tárolni, és az alkalmazásnak lehetőséget kell biztosítania a felhasználóknak a jelszó módosítására.