A ChatGPT adatbiztonságával és GDPR-megfelelőségével kapcsolatos kockázatok részletes ismertetése jogszabályi hivatkozásokkal

## 1. A ChatGPT, mint felhőalapú szolgáltatás jellege

A ChatGPT egy mesterséges intelligencia alapú, felhőalapú szolgáltatás, amelyet az OpenAI nyújt, és amelynek infrastruktúráját elsősorban a Microsoft Azure biztosítja. A szolgáltatás használata során semmilyen szoftver vagy AI-modell nem kerül telepítésre a felhasználó helyi eszközére; minden adatfeldolgozás a szolgáltató saját infrastruktúráján történik.

Jogszabályi hivatkozás:

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR) 4. cikk (7) pont – az adatkezelő és adatfeldolgozó fogalma.

## 2. Az adatok továbbítása és titkosítása

A ChatGPT és a felhasználó közötti kommunikáció titkosított csatornán (TLS/SSL) zajlik, amely biztosítja az adatok védelmét a továbbítás során.

Jogszabályi hivatkozás:

- GDPR 32. cikk – Az adatkezelés biztonsága: az adatkezelőnek és az adatfeldolgozónak megfelelő technikai és szervezési intézkedéseket kell alkalmaznia, ideértve az adatok titkosítását is.

## 3. A szerverek biztonsága és az adatokhoz való hozzáférés

A szolgáltató (OpenAI/Microsoft Azure) rendszerei megfelelnek a nemzetközi biztonsági előírásoknak (GDPR, ISO 27001, SOC 2). Az adatkezelés, valamint az adatokhoz való hozzáférés szigorúan szabályozott és naplózott.

Jogszabályi hivatkozás:

- GDPR 5. cikk (1) f) pont – Adatintegritás és bizalmas jelleg

- GDPR 25. cikk – Beépített és alapértelmezett adatvédelem

- GDPR 32. cikk – Az adatkezelés biztonsága

## 4. Az AI-modell működése és adatkezelése

A mesterséges intelligencia modell nem őriz meg egyedi párbeszédeket a munkamenet lezárása után. Az ideiglenes adatmegőrzést a szolgáltató adatkezelési szabályzata szabályozza, üzleti és vállalati csomagok esetén az adatmegőrzés letiltható.

Jogszabályi hivatkozás:

- GDPR 5. cikk (1) c) pont – Adatminimalizálás elve

- GDPR 25. cikk – Beépített és alapértelmezett adatvédelem

## 5. Adatvédelem és GDPR szempontok

Az adatkezelő szervezet felelőssége, hogy csak megfelelő adatokat adjon át a szolgáltatásnak, valamint hogy megkösse a szükséges adatfeldolgozói szerződéseket (DPA).

Jogszabályi hivatkozás:

- GDPR 28. cikk – Az adatfeldolgozó igénybevétele

- GDPR 44–50. cikk – Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása

## 6. Kiberbiztonság és „feltörési” kockázatok

A ChatGPT szolgáltatás nem jelent nagyobb adatbiztonsági kockázatot, mint más, tanúsított vállalati felhőszolgáltatások, mivel a szolgáltató a legszigorúbb biztonsági előírásokat követi.

Jogszabályi hivatkozás:

- GDPR 32. cikk – Az adatkezelés biztonsága

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Info tv.) 7. §, 42–45. §

## 7. Összefoglalás

A fentiek alapján megállapítható, hogy a ChatGPT és hasonló felhőalapú AI-szolgáltatások:

- Megfelelnek a GDPR adatbiztonsági elvárásainak;

- A kommunikáció és adattárolás titkosított, biztonságos;

- Az adatkezelő szervezeteknek szükséges szabályozni az átadott adatokat, illetve megkötni a szükséges szerződéseket.

Megfelelő szervezeti irányelvek és technikai intézkedések alkalmazása esetén a ChatGPT használata nem jelent új vagy rendkívüli adatvédelmi kockázatot a szokásos vállalati felhőalapú alkalmazásokhoz képest.