

Iránymutatások



03/2022. számú iránymutatás
a közösségimédia-platformok interfészein előforduló
meztévesztő tervezési megoldásokról:
hogyan ismerjük fel és kerüljük el őket

2.0. változat

Az elfogadás időpontja: 2023. február 14.

Korábbi változatok

2.0. változat	2023. február 14.	Az iránymutatás nyilvános konzultációt követő elfogadása
1.0. változat	2022. március 14.	Az iránymutatás nyilvános konzultációra történő elfogadása

ÖSSZEFOGLALÓ

Ez az iránymutatás gyakorlati ajánlásokat fogalmaz meg a közösségimédia-szolgáltatók mint a közösségi média adatkezelői, a közösségimédia-platformok tervezői és a felhasználói számára arra vonatkozóan, hogy hogyan értékeljék és kerüljék el az úgynevezett „megtévesztő tervezési megoldásokat” a közösségimédia-interfészekben, amelyek sértik az általános adatvédelmi rendelet követelményeit. E célból az Európai Adatvédelmi Testület azt ajánlja, hogy az adatkezelők alkalmazzanak interdiszciplináris csoportokat, amelyek többek között tervezőkből, adatvédelmi felelősökből és döntéshozókból állnak. Fontos megjegyezni, hogy a megtévesztő tervezési megoldások és bevált gyakorlatok jegyzéke, valamint a használati esetek nem teljes körűek. A közösségimédia-szolgáltatók továbbra is felelősek és elszámoltathatók annak biztosításáért, hogy platformjaik megfeleljenek az általános adatvédelmi rendeletnek.

Megtévesztő tervezési megoldások a közösségimédia-platformok interfészein

Ezen iránymutatás összefüggésében „megtévesztő tervezési megoldásoknak” minősülnek a közösségimédia-platformokon megvalósított olyan interfészek és felhasználói útvonalak (user journey), amelyek úgy próbálják befolyásolni a felhasználókat, hogy azok személyes adataik kezelésével kapcsolatban nem szándékos, akaratlan és potenciálisan káros, gyakran saját legjobb érdekükkel ellentétes és a közösségimédia-platformok érdekeinek javát szolgáló döntéseket hozzanak. A megtévesztő tervezési megoldások célja, hogy befolyásolják a felhasználók magatartását, és akadályozhatják őket abban, hogy hatékonyan megvédjék személyes adataikat és tudatos döntéseket hozzanak. Az adatvédelmi hatóságok felelősek a megtévesztő tervezési megoldások alkalmazásának szankcionálásáért, amennyiben ezek sértik az általános adatvédelmi rendelet követelményeit. Az ezen iránymutatásban tárgyalt megtévesztő tervezési megoldások a következő kategóriákba sorolhatók:

- A **túlterhelés (overloading)** azt jelenti, hogy a felhasználókat a kérések, információk, opciók vagy lehetőségek nagy mennyiségével árasztják el, amivel arra sarkallják őket, hogy még több adatot osszanak meg, vagy akaratlanul lehetővé tegyék a személyes adataik kezelését az érintett elvárásaival ellentétes módon.
Ebbe a kategóriába a következő három típusú megtévesztő tervezési megoldás tartozik: a ***folyamatos noszogatás (continuous prompting)***, az ***adatvédelmi útvesztő (Privacy maze)*** és a ***túl sok választási lehetőség (Too many options)***.
- Az **átugrás (skipping)** azt jelenti, hogy az interfészt vagy a felhasználói útvonalat úgy tervezik meg, hogy a felhasználók elfeledkezzenek az adatvédelmi szempontok mindegyikéről vagy egy részéről, illetve ne is gondoljanak azokra.
Ebbe a kategóriába a következő kettő típusú megtévesztő tervezési megoldás tartozik: a ***megtévesztő biztonság (Deceptive snugness)*** és a ***figyelemelterelés (Look over there)***.
- A **felkavarás (Stirring)** az érzelmeikre való apellálással vagy vizuális ösztönzéssel befolyásolja a felhasználók döntéseit.
Ebbe a kategóriába a következő kettő típusú megtévesztő tervezési megoldás tartozik: az ***érzelmi befolyásolás (Emotional steering)*** és a ***bújtatott közzététel (Hidden in plain sight)***.

- Az **akadályozás (Obstructing)** azt jelenti, hogy a felhasználókat akadályozzák vagy gátolják a tájékozódásban vagy adataik kezelésében azáltal, hogy megnehezítik vagy lehetetlenné teszik a tevékenység végrehajtását.
Ebbe a kategóriába a következő három típusú megtévesztő tervezési megoldás tartozik: a ***zsákutca (Dead end)***, az ***indokolatlanul hosszú folyamatok (Longer than necessary)*** és a ***megtévesztő tevékenység (Misleading action)***.
- Az **összezavarás (Fickle)** azt jelenti, hogy az interfész kialakítása következetlen és nem egyértelmű, ami megnehezíti a felhasználó számára, hogy eligazodjon a különböző adatvédelmi ellenőrzési eszközökön, és megértse az adatkezelés célját.
Ebbe a kategóriába a következő három típusú megtévesztő tervezési megoldás tartozik: a ***hierarchia hiánya (Lacking hierarchy)***, a ***váratlan szövegkörnyezetbe helyezés (Decontextualising)***, a ***következetlen interfész (Inconsistent Interface)*** és a ***nyelvi akadályok (Language Discontinuity)***.
- A **tájékoztatás hiánya (Left in the dark)** azt jelenti, hogy az interfész úgy került kialakításra, hogy elrejtse az információkat vagy az adatvédelmi beállításokat, vagy hogy a felhasználókat bizonytalanságban tartsa az adataik kezelésének módjával és a jogaik gyakorlásával kapcsolatosan.
Ebbe a kategóriába a következő kettő típusú megtévesztő tervezési megoldás tartozik: az ***egymásnak ellentmondó információk (Conflicting information)*** és a ***félreérthető megfogalmazás vagy tájékoztatás (Ambiguous wording or information)***.

Az általános adatvédelmi rendeletnek a megtévesztő tervezési megoldások értékelésére vonatkozó releváns rendelkezései

Ami a közösségimédia-ágazaton belüli online alkalmazások felhasználói felületeinek adatvédelmi megfelelését illeti, az alkalmazandó adatvédelmi elveket az általános adatvédelmi rendelet 5. cikke határozza meg. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában meghatározott tisztességes adatkezelés elve szolgál kiindulópontként annak értékeléséhez, hogy egy interfésztervezési megoldás ténylegesen „megtévesztő tervezési megoldásnak” minősül-e. Az értékelésben szerepet játszó további elvek az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) és c) pontja valamint (2) bekezdése szerinti átláthatóság, adattakarékosság és elszámoltathatóság elve, továbbá egyes esetekben az általános adatvédelmi rendelet 5. cikke (1) bekezdésének b) pontja szerinti célhoz kötöttség elve. Más esetekben a jogi értékelés emellett az általános adatvédelmi rendelet 4. cikkének 11. pontja és 7. cikke szerinti hozzájárulási feltételeken vagy más egyedi kötelezettségeken, például az általános adatvédelmi rendelet 12. cikkén alapul. Nyilvánvaló, hogy az érintettek jogaival összefüggésben az általános adatvédelmi rendelet harmadik fejezetét is figyelembe kell venni. Végezetül az általános adatvédelmi rendelet 25. cikke szerinti beépített és alapértelmezett adatvédelemre vonatkozó követelmények alapvető fontosságú szerepet játszanak, mivel azok alkalmazása egy interfészkiakítás elindítása előtt segítené a közösségimédia-szolgáltatókat a megtévesztő tervezési megoldások elkerülésében.

Példák megtévesztő tervezési megoldásokra egy közösségimédia-fiók életciklusának használati eseteiben

Az általános adatvédelmi rendelet rendelkezései a közösségimédia-platformok működtetésének részeként végzett személyesadat-kezelés teljes folyamatára, azaz a felhasználói fiók teljes életciklusára vonatkoznak. Az Európai Adatvédelmi Testület konkrét példákat hoz a megtévesztő tervezési megoldások típusaira az életcikluson belüli következő különböző használati esetekre: a regisztrációs folyamat; az adatvédelmi nyilatkozattal, a közös adatkezeléssel és az adatvédelmi incidensekre vonatkozó kommunikációval kapcsolatos információhasználati esetek; hozzájárulás és az adatvédelem kezelése; az érintettek jogainak gyakorlása a közösségi média használata során; végül pedig a közösségimédia-fiók bezárása. Az általános adatvédelmi rendelet rendelkezéseivel való kapcsolat kétféleképpen magyarázható: először is, minden egyes használati eset részletesebben kifejti, hogy az általános adatvédelmi rendelet fent említett rendelkezései közül melyek azok, amelyek különösen fontosak az adott esetben. Másodszor, a megtévesztő tervezési megoldásokra vonatkozó példákat körülvevő bekezdések kifejtik, hogy ezek hogyan sértik az általános adatvédelmi rendeletet.

Bevált gyakorlat: ajánlások

A megtévesztő tervezési megoldások példái mellett az iránymutatás az egyes használati esetek végén, valamint ezen iránymutatás II. mellékletében bevált gyakorlatokat is bemutat. Ezek konkrét ajánlásokat tartalmaznak az általános adatvédelmi rendelet hatékony végrehajtását elősegítő felhasználói felületek kialakítására vonatkozóan.

A megtévesztő tervezési megoldások kategóriáinak ellenőrző listája

A megtévesztő tervezési megoldások kategóriáit tartalmazó ellenőrző lista ezen iránymutatás I. mellékletében található. Áttekintést nyújt a fent említett kategóriákról és a megtévesztő tervezési megoldások típusairól, valamint felsorolja a használati esetekben említett megtévesztő tervezési megoldások példáit. Egyes olvasók hasznosnak találhatják, hogy az ellenőrző listát használják kiindulópontként ezen iránymutatás megismeréséhez.

Tartalomjegyzék

1	Hatály	8
2	Alkalmazandó elvek – Mit kell szem előtt tartani?	12
2.1	Elszámoltathatóság	13
2.2	Átláthatóság	13
2.3	Beépített és alapértelmezett adatvédelem	14
3	A közösségimédia-fiók életciklusa: az elvek átültetése a gyakorlatba	16
3.1	Közösségimédia-fiók létrehozása	16
1.	használati eset: Fiók regisztrálása	16
3.2	Tájékozódás a közösségi médiában	29
2a.	használati eset: Többszintű adatvédelmi nyilatkozat	29
2b.	használati eset: Az érintett tájékoztatása a közös adatkezelésről, az általános adatvédelmi rendelet 26. cikkének (2) bekezdése	36
2c.	használati eset: Az érintett tájékoztatása az adatvédelmi incidensről	38
3.3	Védettség a közösségi médiában	41
3a.	használati eset: A hozzájárulás kezelése a közösségimédia-platform használata során	41
3b.	használati eset: Az adatvédelmi beállítások kezelése	49
3.4	Jogérvényesítés a közösségi médiában: Az érintettek jogai	57
4.	használati eset: Hogyan biztosíthatók megfelelő funkciók az érintettek jogainak gyakorlásához?	57
3.5	Viszlát, és minden jót: a közösségimédia-fiók bezárása	66
5.	használati eset: a fiók szüneteltetése / az összes személyes adat törlése	66
4	I. melléklet: A megtévesztő tervezési megoldások kategóriáinak és típusainak jegyzéke	75
4.1	Túlterhelés.....	75
4.1.1	Folyamatos noszogatás.....	75
4.1.2	Adatvédelmi útvesztő.....	76
4.1.3	Túl sok választási lehetőség.....	76
4.2	Átugrás	76
4.2.1	Megtévesztő biztonság.....	76
4.2.2	Figyelemelterelés	77
4.3	Felkavarás.....	77
4.3.1	Érzelmi befolyásolás	77
4.3.2	Bújtatott közzététel	78
4.4	Akadályozás	78
4.4.1	Zsákutca.....	78
4.4.2	Indokolatlanul hosszú folyamatok.....	79

4.4.3	Megtévesztő tevékenységek	79
4.5	Összezavarás.....	79
4.5.1	A hierarchia hiánya	79
4.5.2	Váratlan szövegkörnyezetbe helyezés	80
4.5.3	Következetlen interfész	80
4.5.4	Nyelvi akadályok	80
4.6	Sötétben hagyás	81
4.6.1	Egymásnak ellentmondó információk	81
4.6.2	Félreérthető megfogalmazás vagy tájékoztatás	81
5	II. melléklet: Bevált gyakorlatok.....	83

Az Európai Adatvédelmi Testület,

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének e) pontjára,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére¹,

tekintettel eljárási szabályzatának 12. és 22. cikkére,

ELFOGADTA A KÖVETKEZŐ IRÁNYMUTATÁST

1 HATÁLY

1. Ezen iránymutatás célja, hogy ajánlásokkal és iránymutatással szolgáljon a közösségimédia-platformok felületeinek kialakításához. Ezen iránymutatás alkalmazásában közösségi média alatt olyan online platformokat értünk, amelyek lehetővé teszik olyan felhasználói hálózatok és közösségek kialakulását, amelyek információkat és tartalmakat osztanak meg egymás között². Az iránymutatás használható akár a felhasználói felület tervezési fázisában, hogy eleve elkerülhető legyen a megtévesztő tervezési megoldások³ alkalmazása, akár egy meglévő szolgáltatás esetében az interfész megfelelőségének értékelésére. A közösségimédia-szolgáltatókat mint a közösségi média adatkezelőit célozza, akik a közösségimédia-platformok tervezéséért és működéséért felelősek. E tekintetben az iránymutatás célja, hogy emlékeztessen az általános adatvédelmi rendeletből eredő kötelezettségekre, különös tekintettel a jogszerűség, a tisztességes eljárás, az átláthatóság, a célhoz kötöttség és az adattakarékosság elvére a felhasználói felületek kialakítása, valamint a webes szolgáltatásaik és alkalmazásaik tartalmának megjelenítése során. A fent említett elveket érdemben meg kell valósítani, és technikai szempontból a szoftverek és szolgáltatások – köztük a felhasználói felületek – tervezésére vonatkozó követelményeket jelentenek. Részletes tanulmány készül az általános adatvédelmi rendelet követelményeinek a felhasználói felületekre és a tartalom megjelenítésre történő alkalmazásáról, ami tisztázza, hogy mi tekintendő „megtévesztő tervezési megoldásnak”, azaz a tartalomtervezés és -megjelenítés olyan módjának, amely alapjaiban sérti ezeket a követelményeket, miközben formálisan továbbra is megfelel a követelményeknek. Ez az iránymutatás arra is alkalmas, hogy növelje a felhasználók tudatosságát a jogaikkal, valamint a túl sok adat megosztásából vagy az adataik ellenőrizetlen megosztásából eredő esetleges kockázatokkal kapcsolatban. Az iránymutatás célja továbbá, hogy segítse a felhasználókat a(z) alábbiakban meghatározott) „megtévesztő tervezési

¹ A dokumentumban a „tagállamokra” való hivatkozásokat az „EGT-tagállamokra” való hivatkozásként kell értelmezni.

² A fogalom meghatározás megegyezik az Európai Adatvédelmi Testületnek a közösségi média felhasználóinak megcélzásáról szóló 8/2020. számú iránymutatásának 1. pontjával, részletesebb leírásért lásd az 1. lábjegyzetet; elérhető a következő internetcímen: https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_hu_0.pdf.

³ Ezen iránymutatás 2.0. verziójában az Európai Adatvédelmi Testület a „sötét megoldás” helyett az inkluzívabb és szemléletesebb „megtévesztő tervezési megoldás” kifejezést használja.

megoldások” felismerésében, valamint abban, hogy a magánéletük tudatos védelme érdekében hogyan nézhetnek szembe velük. Az elemzés részeként a közösségimédia-fiókok életciklusát öt felhasználási mód alapján vizsgáltuk: „Közességimédia-fiók létrehozása” (1. sz. használati eset), „Tájékozódás a közösségi médiában” (2. sz. használati eset), „Védettség a közösségi médiában” (3. sz. használati eset), „Jogérvényesítés a közösségi médiában: az érintettek jogai” (4. sz. használati eset), valamint „Viszlát, és minden jót: a közösségimédia-fiók bezárása” (5. sz. használati eset).

2. Ebben az iránymutatásban a „felhasználói felület” kifejezés a közösségi médiaplatformokkal való interakció eszközeinek felel meg. A dokumentum a grafikus felhasználói felületekre összpontosít (pl. a számítógéphez és okostelefonhoz használt interfészekre), de egyes észrevételek vonatkozhatnak hangvezérelt (pl. okos hangszórókhoz használt) vagy gesztusalapú (pl. virtuális valóságban használt) interfészekre is. A „felhasználói útvonalt” kifejezés azoknak a műveleteknek vagy lépéseknek a sorozatát jelenti, amelyeket a felhasználóknak el kell végezniük céljuk elérése érdekében; ezek a közösségi hálózatokon olyan dolgok lehetnek, mint például a hírfolyamuk böngészése, egy poszt megosztása, preferenciáik meghatározása stb. A „felhasználói élmény” kifejezés a felhasználók közösségimédia-plattformokkal kapcsolatos általános tapasztalatát jelenti, amely magában foglalja a felhasználói felülettel való interakció érzékelt hasznosságát, a felület egyszerű használatát és hatékonyságát. A felhasználói felületek kialakítása és a felhasználói élmény tervezése az elmúlt évtizedben folyamatosan fejlődött. Újabban a mindenütt jelenlévő, személyre szabott és úgynevezett zökkenőmentes felhasználói interakciók és élmények terjedtek el: a tökéletes felületnek nagy mértékben személyre szabottnak, könnyen használhatónak és multimodálisnak kell lennie⁴. Bár ezek a tendenciák növelhetik a digitális szolgáltatások egyszerű használatát, felhasználhatók oly módon, hogy főként az általános adatvédelmi rendelet szellemével ellentétes felhasználói magatartást mozdítanak elő⁵. Ez különösen fontos a figyelemgazdasággal összefüggésben, ahol a felhasználói figyelmet árucikknek tekintik. Ezekben az esetekben az általános adatvédelmi rendelet által jogilag megengedett határok túllépésére is mód van, és a felület és a felhasználói élmény ilyen esetekhez vezető kialakítását az alábbiakban „megtévesztő tervezési megoldásokként” mutatjuk be.
3. Ezen iránymutatás összefüggésében „megtévesztő tervezési megoldások” azok a közösségimédia-plattformokon megvalósított felületek és felhasználói útvonaltak, amelyek célja, hogy a felhasználókat személyes adataikkal kapcsolatban olyan nem szándékos, akaratlan, illetve potenciálisan káros döntések meghozatalára ösztönözzék, amelyek gyakran a felhasználók mindenkifelett álló érdekével ellentétesek és a közösségimédia-plattformok érdekeinek javát szolgálják. A megtévesztő tervezési megoldások célja, hogy befolyásolják a felhasználók magatartását, általában kognitív torzításokra támaszkodva, és akadályozhatják a felhasználók azon képességét, hogy „hatékonyan megvédjék személyes adataikat és tudatos döntéseket hozzanak”⁶, például azért, hogy lehetetlenné teszik számukra, hogy „tájékozott és önkéntes hozzájárulást adjanak”⁷. Ezt a kialakítás számos aspektusában

⁴ További részletekért lásd a CNIL 6. sz. IP-jelentését: Shaping Choices in the Digital World (A választások alakítása a digitális világban), 2019, 9. o.;

https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

⁵ Shaping Choices in the Digital World (A választások alakítása a digitális világban), 2019, 10. o.

⁶ Shaping Choices in the Digital World (A választások alakítása a digitális világban), 2019, 27. o.

⁷ Lásd: Norvég Fogyasztói Tanács, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy* (Szándékosan megtévesztve: Hogyan használják a technológiai vállalatok a sötét megoldásokat arra, hogy eltántorítsák minket a magánélethez való jogaink gyakorlásától), 10. o. <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>, valamint CNIL, Shaping Choices in the Digital World, 30. és 31. o.

ki lehet használni, például a felületek színválasztásában és a tartalom elhelyezésében. Ezzel szemben ösztönzőkkel és felhasználóbarát kialakítással támogatható az adatvédelmi előírások megvalósítása.

4. A megtévesztő tervezési megoldások nem feltétlenül csak az adatvédelmi szabályok megsértését eredményezik; megsérthetik például a fogyasztóvédelmi előírásokat is. Az adatvédelmi hatóságok által szankcionálható jogsértések és a nemzeti fogyasztóvédelmi, versenyjogi vagy egyéb hatóságok által szankcionálható jogsértések közötti határok átfedésben lehetnek egymással⁸. Az általános adatvédelmi rendelet értelmében az adatvédelmi hatóságok felelősek a megtévesztő tervezési megoldások alkalmazásának szankcionálásáért, amennyiben azok ténylegesen megsértik az adatvédelmi normákat, és így az általános adatvédelmi rendeletet. Az általános adatvédelmi rendelet követelményeinek megsértését eseti alapon kell értékelni. Ez az iránymutatás csak azokra a megtévesztő tervezési megoldásokra terjed ki, amelyek e szabályozási felhatalmazás hatálya alá tartozhatnak. Ezért a megtévesztő tervezési megoldások példái mellett az iránymutatás olyan bevált gyakorlatokat is bemutat, amelyek felhasználhatók olyan felhasználói felületek kialakítására, amelyek elősegítik az általános adatvédelmi rendelet hatékony végrehajtását. Ezek a bevált gyakorlatok jelenthetik az első lépést ahhoz, hogy a felhasználók szabványosított módon rendelkezhessenek adataik felett és gyakorolhassák jogaikat.
5. Az ezen iránymutatásban tárgyalt megtévesztő tervezési megoldások⁹ a meglévő interfészek interdiszciplináris elemzéséből származnak, és a következő kategóriákba sorolhatók:

Túlterhelés: a felhasználókat a kérések, információk, opciók vagy lehetőségek nagy mennyiségével árasztják el, amivel arra sarkallják őket, hogy még több adatot osszanak meg, vagy akaratlanul lehetővé tegyék a személyes adataik kezelését az érintett elvárásaival ellentétes módon.

Átugrás: az interfész vagy a felhasználói útvonal oly módon történő megtervezése, hogy a felhasználók megfeledkeznek az adatvédelmi szempontokról vagy azok egy részéről, illetve eszükbe se jutnak azok.

Felkavarás: az érzelmeikre való apellálással vagy vizuális ösztönzéssel befolyásolja a felhasználók döntéseit.

Akadályozás: a felhasználókat akadályozzák vagy gátolják a tájékozódásban vagy adataik kezelésben azáltal, hogy megnehezítik vagy lehetetlenné teszik a művelet végrehajtását.

Összezavarás: az interfész kialakítása következtelen és nem egyértelmű, ami megnehezíti a felhasználók számára, hogy eligazodjanak a különböző adatvédelmi beállításokon, és megértsék az adatkezelés célját.

⁸ E tekintetben a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról szóló, 2022. október 19-i (EU) 2022/2065 rendelet (a digitális szolgáltatásokról szóló rendelet) 25. cikkének (2) bekezdése egyértelművé teszi, hogy az online interfészek megtévesztésre vagy manipulálásra alkalmas tervezésére vonatkozó, a rendelet 25. cikkének (1) bekezdésében foglalt tilalom nem alkalmazandó a 2005/29/EK irányelv (az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól szóló irányelv) vagy az általános adatvédelmi rendelet hatálya alá tartozó gyakorlatokra. Az Európai Bizottság közleménye (2021/C 526/01) szintén iránymutatást nyújt az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól szóló irányelv értelmezéséhez és alkalmazásához, beleértve a „sötét mintákra” vonatkozó 4.2.7. szakaszt is.

⁹ A megtévesztő tervezési megoldások kategóriáit és a megtévesztő tervezési megoldások e kategóriákon belüli típusait az iránymutatások szövegében **félkövér dőlt** betűtípus jelöli. A részletes áttekintést a melléklet tartalmazza.

Sötétben hagyás: az interfész úgy került kialakításra, hogy elrejtse az információkat vagy az adatvédelmi beállításokat, vagy hogy a felhasználókat bizonytalanságban tartsa az adataik kezelésének módjával és a jogaik gyakorlásával kapcsolatosan.

6. A megtévesztő tervezési megoldások a felhasználók viselkedésére gyakorolt hatásuk alapján ezekben a kategóriákba történő csoportosítása mellett ezek a megoldások tartalomalapú és interfészalapú megoldásokra is feloszthatók, kimondottan a felhasználói felület vagy a felhasználói útvonal szempontjainak figyelembe vétele érdekében. A tartalomalapú megoldások a tényleges tartalomra, tehát a mondatok és az információk elemek megfogalmazására és kontextusára is vonatkoznak. Emellett azonban léteznek olyan elemek is, amelyek közvetlenül befolyásolják a tényezők megítélését. Ezek az interfészalapú megoldások a tartalom megjelenítésének, az azon keresztül történő navigálásnak vagy a vele való interakciónak a módjaihoz kapcsolódnak.
7. Fontos szem előtt tartani, hogy a megtévesztő tervezési megoldások további aggályokat vetnek fel a közösségi médiaplatformra regisztráló gyermekekre¹⁰, valamint az emberek más kiszolgáltatott csoportjaira, például az idősekre, a látássérültekre, vagy a másoknál digitálisan kevésbé jártas személyekre gyakorolt lehetséges hatásokkal kapcsolatban. Az olyan kiszolgáltatott csoportok, mint az idős felhasználók, gyakran nem csak, hogy kevésbé képesek észrevenni a manipulatív tervezési gyakorlatokat, de azzal is kevésbé vannak tisztában, hogy digitális magatartásuk befolyásolható. Az általános adatvédelmi rendelet további biztosítékokat ír elő abban az esetben, ha az adatkezelés gyermekek személyes adataira vonatkozik, mivel ez utóbbiak kevésbé lehetnek tisztában az adatkezeléshez való jogukat érintő kockázatokkal és következményekkel¹¹. Az (58) preambulumbekzdés világosan kimondja, hogy a kifejezetten gyermekekre vonatkozó adatkezelés vonatkozásában minden információt és kommunikációt olyan világos és közérthető nyelven kell megfogalmazni, amelyet a gyermek könnyen megért. Ezenkívül az általános adatvédelmi rendelet az egyének – különösen a gyermekek – adatainak kezelését kifejezetten azon helyzetek közé sorolja, amikor az egyének jogait és szabadságait érintő – változó valószínűségű és súlyosságú – kockázatok származhatnak a személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek¹².
8. A fentieket szem előtt tartva egyértelmű, hogy a megtévesztő tervezési megoldások nem kizárólag a közösségimédia-platfomokra jellemzőek. Az iránymutatással kapcsolatos nyilvános konzultáció során határozott vélemények hangzottak el erről a kérdéstről. Az interfészek sok más esetben is jelen vannak, amikor a felhasználók adatkezelési tevékenységeken alapuló vagy azokhoz kapcsolódó termékekkel és szolgáltatásokkal lépnek kapcsolatba. Ezek közé tartozhatnak weboldalak és süti bannerek¹³, online boltok, videojátékok, mobilalkalmazások és mikrofizetések stb. Bár előfordulhat, hogy az alábbiakban ismertetett megtévesztő tervezési megoldások nem pontosan ugyanabban a formában fordulnak elő, változataik mégis sérthetik az érintettek vagy a fogyasztók jogait.

¹⁰ Lásd még az (EU) 2022/2065 rendelet (a digitális szolgáltatásokról szóló jogszabály) (81) preambulumbekzdésének negyedik mondatát.

¹¹ Az általános adatvédelmi rendelet (38) preambulumbekzdése.

¹² Az általános adatvédelmi rendelet (75) preambulumbekzdése; lásd még az Európai Adatvédelmi Testületnek a közösségi média felhasználóinak megcélzásáról szóló 8/2020. számú iránymutatásának 16. pontját, https://www.edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_hu_0.pdf.

¹³ A Digitális Jogok Európai Központjától kapott számos panasz miatt az Európai Adatvédelmi Testület munkacsoportja véleménycserét folytatott a süti bannerek több tervezési eleméről. A felügyeleti hatóságok által az alkalmazandó többretegű jogi keret értelmezése során elfogadott közös nevezőt a süti banner munkacsoport által végzett munkáról szóló, 2023. január 17-i jelentés foglalja össze, amely a következő címen érhető el: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

Mindazonáltal ez az iránymutatás kizárólag a közösségimédia-platformok megtévesztő tervezési megoldásaira összpontosít, mivel e platformoknak az emberek és nemzetek mindennapi életére gyakorolt befolyása folyamatosan nő, amit az Európai Adatvédelmi Testület korábbi dokumentumai is egyértelművé tettek.¹⁴

2 ALKALMAZANDÓ ELVEK – MIT KELL SZEM ELŐTT TARTANI?

9. Ami a közösségimédia-ágazaton belüli online alkalmazások felhasználói felületeinek adatvédelmi megfelelését illeti, az alkalmazandó adatvédelmi elveket az általános adatvédelmi rendelet 5. cikke határozza meg. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában meghatározott tisztességes adatkezelés elve kiindulópontként szolgál annak értékeléséhez, hogy a meglévő megoldások megtévesztőnek minősülnek-e. Amint azt az Európai Adatvédelmi Testület már megállapította, a tisztességes eljárás olyan átfogó elv, amely megköveteli, hogy a személyes adatokat ne kezeljék az érintettre nézve hátrányos, hátrányosan megkülönböztető, váratlan vagy félrevezető módon¹⁵. Ha az interfész elégtelen vagy félrevezető információt tartalmaz a felhasználók számára, és megfelel a megtévesztő tervezési megoldások jellemzőinek, akkor tisztességtelen adatkezelésnek minősíthető. A tisztességes eljárás elvének egységességet biztosító szerepe van, és egyetlen megtévesztő tervezési megoldás sem felel meg annak, függetlenül attól, hogy megfelelnek-e más adatvédelmi elveknek.
10. Az adatkezelés tisztességességére vonatkozó ezen alapvető rendelkezés mellett az elszámoltathatóság, az átláthatóság és az általános adatvédelmi rendelet 25. cikkében foglalt, a beépített adatvédelemre vonatkozó kötelezettség elvei a tervezési keret tekintetében is relevánsak, a megtévesztő tervezési megoldások pedig sérthetik ezeket a rendelkezéseket. Lehetséges azonban, hogy a megtévesztő tervezési megoldások jogi értékelése az általános fogalom meghatározások elemein alapulhat, például az általános adatvédelmi rendelet 4. cikkének 11. pontján, a hozzájárulás fogalom meghatározásán vagy más konkrét kötelezettségeken, például az általános adatvédelmi rendelet 12. cikkén. Az általános adatvédelmi rendelet 12. cikke (1) bekezdésének első mondata előírja az adatkezelők számára, hogy hozzanak megfelelő intézkedéseket annak érdekében, hogy az érintettek jogaival kapcsolatos tájékoztatást, valamint minden információt tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtanak. Amint azt az átláthatóság elvéről szóló (39) preambulumbekkezdés harmadik mondata mutatja, ez a követelmény azonban nem korlátozódik az adatvédelmi nyilatkozatokra¹⁶ vagy az érintettek jogaira¹⁷, hanem a személyes adatok kezelésével összefüggő minden információra és kommunikációra vonatkozik. A preambulumbekkezdés ötödik mondata szintén előírja, hogy az érintettet a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról tájékoztatni kell, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat.

¹⁴ Az Európai Adatvédelmi Testület 8/2020. sz. iránymutatása a közösségi média felhasználóinak megcélzásáról, a 2/2019. sz. nyilatkozat a személyes adatok politikai kampányok során történő felhasználásáról

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb-2019-03-13-statement-on-elections_hu.pdf.

¹⁵ Az Európai Adatvédelmi Testület 4/20219. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, a 2020. október 20-án elfogadott 2.0. verzió, 16. o.; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_hu.

¹⁶ Ezzel ezen iránymutatás 3.2. része – a 2a. használati eset foglalkozik.

¹⁷ Ezzel a 4. és 5. használati eset, azaz ezen iránymutatás 3.4. és 3.5. része foglalkozik.

11. Az online alkalmazások felhasználói felületeinek tervezésekor fontos figyelembe venni az általános adatvédelmi rendelet 5. cikke (1) bekezdésének b) pontja szerinti célhoz kötöttség elvét, valamint az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja szerinti adattakarékossági elvet is. Az adatvédelmi megfelelés biztosítása érdekében az adatkezelőknek mindenesetre tanácsos alaposan ellenőrizniük az általános adatvédelmi rendelet szerinti valamennyi adatvédelmi elvnek való megfelelést.

2.1 Elszámoltathatóság

12. Az elszámoltathatóság elvének minden felhasználói felület kialakításban tükröződnie kell.
13. Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése kimondja, hogy az adatkezelő felelős az általános adatvédelmi rendelet 5. cikkének (1) bekezdésében leírt elveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására. Ezért ez az elv szorosan kapcsolódik a fent említett vonatkozó elvekhez. Az elszámoltathatóság olyan elemekkel biztosítható, amelyek bizonyítják, hogy a közösségimédia-szolgáltató megfelel az általános adatvédelmi rendeletnek. A felhasználói felület és a felhasználói útvonal dokumentációs eszközként használható annak bizonyítására, hogy a felhasználók a közösségimédia-platfromon végzett tevékenységeik során elolvasták és figyelembe vették az adatvédelmi információkat, önkéntesen hozzájárulást adtak, könnyen gyakorolták jogaikat stb. A kvalitatív és kvantitatív felhasználói kutatási módszerek, mint például az A/B tesztelés, a szemkövetés vagy a felhasználói interjúk, azok eredményei és elemzése szintén felhasználhatók a megfelelés bizonyításának alátámasztására. Fontos megjegyezni, hogy az ilyen kutatási módszerek gyakran személyes adatok kezelésével is járnak, ezért annak összhangban kell lennie az általános adatvédelmi rendelettel. Ha például a felhasználóknak ki kell pipálniuk egy jelölőnégyzetet, vagy több adatvédelmi lehetőség valamelyikére kell kattintaniuk, a felületekről készült képernyőfotók bemutatják a felhasználók útját az adatvédelmi információkon keresztül, és elmagyarázhatják, hogy a felhasználók hogyan hoznak tájékozott döntést. Az ezen az interfészen végzett felhasználói kutatások eredményei további elemekkel szolgálnának, amelyek részletezik, hogy az interfész miért optimális a tájékoztatási cél eléréséhez.
14. A felhasználói felületek területén ilyen dokumentációs elemek található bizonyos megállapodások nyilvánosságra hozatalakor és mindenekelőtt – például a hozzájárulás megadására vagy az elolvasás megerősítésére vonatkozó – bizonyítékszerzésekor.

2.2 Átláthatóság

15. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában foglalt átláthatósági elv nagymértékben átfedésben van az általános elszámoltathatóság területével. Bár az adatkezelőknek védeniük kell bizonyos érzékeny üzleti információkat harmadik felekkel szemben, az adatkezelésre vonatkozó dokumentáció hozzáférhetővé vagy rögzíthetővé tétele segíthet az elszámoltathatóság biztosításában: Az elolvasás megerősítése kérhető például az olyan szövegek esetében, amelyeket az adatkezelőnek az átláthatóság elvének megfelelően hozzáférhetővé kell tennie. Ez egyúttal minden esetben az átláthatóság biztosítását is szolgálhatja az érintettek felé.
16. Az általános adatvédelmi rendelet 5. cikkében meghatározott valamennyi adatvédelmi elvet az általános adatvédelmi rendelet tovább részletezi. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja előírja, hogy a személyes adatok kezelését az érintett számára átlátható módon kell végezni. Az átláthatóságról szóló iránymutatás meghatározza az általános adatvédelmi rendelet 12. cikkében meghatározott átláthatósági elemeket, azaz azt, hogy az információkat „tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva” kell

rendelkezésre bocsátani¹⁸. Ez az iránymutatás arra vonatkozóan is útmutatást nyújt, hogy miként kell teljesíteni az általános adatvédelmi rendelet 13. és 14. cikke szerinti, a közösségimédia-szolgáltatókra vonatkozó tájékoztatási kötelezettségeket.

17. Emellett az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában foglalt adatvédelmi elvek szövege és a rendeleten belüli egyéb különös jogi rendelkezések számos további részletet tartalmaznak az átláthatóság elvére vonatkozóan, amelyek konkrét jogelvekhez kapcsolódnak, például az általános adatvédelmi rendelet 7. cikkében foglalt, a hozzájárulás megszerzésére vonatkozó különleges átláthatósági követelményekhez.

2.3 Beépített és alapértelmezett adatvédelem

18. Az általános adatvédelmi rendelet 25. cikkének (1) bekezdése előírja, hogy az adatkezelőknek olyan megfelelő technikai és szervezési intézkedéseket kell végrehajtaniuk, amelyek célja az adatvédelmi elvek megvalósítása, míg az általános adatvédelmi rendelet 25. cikkének (2) bekezdése egyértelművé teszi, hogy ilyen intézkedéseket annak biztosítása érdekében is végre kell hajtani, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. A beépített és alapértelmezett adatvédelemről szóló 04/2019. sz. iránymutatással összefüggésben az adatkezelőknek és adatfeldolgozóknak néhány kulcsfontosságú elemet figyelembe kell venniük a beépített adatvédelemnek a közösségimédia-platformok kapcsán történő megvalósítása során. Ezek egyike, hogy a tisztességes eljárás elvét illetően az adatkezeléssel kapcsolatos információkat és lehetőségeket tárgyilagos és semleges módon kell bemutatni, kerülve a megtévesztő vagy manipulatív nyelvezetet vagy megfogalmazást¹⁹. Az iránymutatás meghatározza többek között az alapértelmezett adatvédelem és a beépített adatvédelem elveinek azon elemeit, amelyek még lényegesebbé válnak a megtévesztő tervezési megoldások tekintetében:²⁰

- Autonómia – az érintettek számára a lehető legnagyobb mértékű autonómiát kell biztosítani ahhoz, hogy meghatározzák, hogyan használják fel személyes adataikat, továbbá a felhasználás és kezelés hatóköre és feltételei feletti ellenőrzés tekintetében.
- Interakció – az érintettek számára lehetővé kell tenni, hogy az adatkezelő által kezelt személyes adatokkal kapcsolatban kommunikálhassanak az adatkezelővel, és gyakorolhassák jogaikat vele szemben.
- Elvárások – az adatkezelésnek meg kell felelnie az érintettek észszerű elvárásainak.
- A fogyasztó választása – az adatkezelő nem „tarthatja fogva” tisztességtelen módon a felhasználóit. Amennyiben egy személyes adatok kezelésével járó szolgáltatás védett, a felhasználó a szolgáltatásból nem tud kilépni, ez adott esetben nem tisztességes, ha gátolja az érintetteket a 20. cikk szerinti adathordozhatósághoz való joguk gyakorlásában.
- Kiegyenlített erőviszonyok – a kiegyenlített erőviszonyok fontos célja kell hogy legyen az adatkezelő és az érintett közötti kapcsolatnak. Kerülni kell a kiegyensúlyozatlan

¹⁸ A 29. cikk szerinti munkacsoport az (EU) 2016/679 rendelet szerinti átláthatóságról szóló iránymutatása – az Európai Adatvédelmi Testület által jóváhagyva; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

¹⁹ Az Európai Adatvédelmi Testület 04/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 18. o., 70. pont.

²⁰ Kivonat – a teljes listát lásd a 25. cikk szerinti beépített és alapértelmezett adatvédelemről szóló iránymutatás 70. pontjában.

erőviszonyokat. Ha ez nem lehetséges, azt megfelelő ellenintézkedésekkel kell elismerni és figyelembe venni.

- **Megtévesztés tilalma** – az adatkezeléssel kapcsolatos információkat és lehetőségeket tárgyilagos és semleges módon kell bemutatni, kerülve a megtévesztő vagy manipulatív nyelvezetet vagy megfogalmazást.
- **Őszinteség** – az adatkezelőnek tájékoztatást kell adnia a személyes adatok kezelésének módjáról, és az elmondottaknak megfelelően kell eljárnia, nem vezetheti félre az érintetteket.

19. Az alapértelmezett adatvédelemnek és a beépített adatvédelemnek való megfelelés fontos a megtévesztő tervezési megoldások értékelésekor, mivel ez eleve azok elkerülését eredményezné. A szolgáltatás és a kapcsolódó interfészek összevetése az alapértelmezett és a beépített adatvédelem elveit alkotó – például a fent említett – elemekkel segít még a szolgáltatás elindítása előtt azonosítani a szolgáltatás azon aspektusait, amelyek megtévesztő tervezési megoldást képeznek. Ha például az adatvédelmi tájékoztatást a „megtévesztés tilalma” elv követése nélkül nyújtják, az valószínűleg a **bújtatott közzététel** vagy az **érzelmi befolyásolás** megtévesztő tervezési megoldást jelenti, amelyeket az 1. használati esetről fogunk részletesebben kifejteni.

3 A KÖZÖSSÉGIMÉDIA-FIÓK ÉLETCIKLUSA: AZ ELVEK ÁTÜLTETÉSE A GYAKORLATBA

20. Az általános adatvédelmi rendelet a személyes adatok automatizált módon történő kezelésének teljes folyamatára alkalmazandó²¹. A közösségimédia-platformok működtetésének részeként végzett személyesadat-kezelés esetén ez az általános adatvédelmi rendelet és elveinek a felhasználói fiók teljes életciklusára való alkalmazását eredményeik.

3.1 Közösségimédia-fiók létrehozása

1. használati eset: Fiók regisztrálása

a. A kontextus leírása

21. Egy közösségimédia-platformhoz való hozzáféréshez a felhasználóknak első lépésként regisztrálniuk kell, egy felhasználói fiók létrehozásával. A regisztrációs folyamat részeként a felhasználóknak meg kell adniuk személyes adataikat, például vezeté- és utónevüket, e-mail-címüket, illetve néha telefonszámukat. A felhasználókat tájékoztatni kell személyes adataik kezeléséről, és általában arra kéri őket, hogy erősítsék meg, hogy elolvasták az adatvédelmi nyilatkozatot, és elfogadják a közösségimédia-platform használati feltételeit. Ezeket az információkat világosan és közérthetően kell megfogalmazni, hogy a felhasználók könnyen megérthessék azokat, és tudatosan adhassák hozzájárulásukat.
22. A regisztrációs folyamat e kezdeti szakaszában a felhasználóknak meg kell érteniük, hogy pontosan mire regisztrálnak, vagyis a közösségimédia-platform és a felhasználók közötti megállapodás tárgyát a lehető legvilágosabban és legegyszerűbben kell leírni.
23. Ezért a közösségimédia-szolgáltatóknak figyelembe kell venniük a beépített adatvédelem elvét az érintettek jogainak és szabadságainak hatékony védelme érdekében²².

b. Vonatkozó jogi rendelkezések

24. A közösségimédia-szolgáltatóknak gondoskodniuk kell arról, hogy interfészeik tervezése során megfelelően alkalmazzák az általános adatvédelmi rendelet 5. cikkében foglalt elveket. Bár az átláthatóság az érintettek felé mindig alapvető fontosságú, ez különösen igaz akkor, ha valaki közösségimédia-platformon hoz létre fiókot. Adatkezelői vagy adatfeldolgozói pozíciójuk miatt a közösségimédia-platformoknak hatékonyan és tömören, valamint az egyéb, nem adatvédelemmel kapcsolatos tájékoztatástól egyértelműen megkülönböztetve kell tájékoztatniuk a felhasználókat a regisztráció során²³. Az adatkezelők átláthatósági kötelezettségeinek része, hogy tájékoztassák a felhasználókat jogaikról, amelyek közül az egyik az, hogy hozzájárulásukat bármikor visszavonhatják, ha a hozzájárulás az alkalmazandó jogalap²⁴.

i. A regisztrációs folyamat szakaszában megadott hozzájárulás

25. Amint azt az általános adatvédelmi rendelet 4. cikkének 11. pontja és 7. cikke kimondja, amelyet a (32) preambulumbekzdés pontosít, ha a hozzájárulást választják az adatkezelés jogalapjaként, az „az

²¹ Lásd az általános adatvédelmi rendelet 2. cikkének (1) bekezdését.

²² Lásd a 25. cikk szerinti beépített és alapértelmezett adatvédelemről szóló 04/2019. sz. iránymutatást.

²³ Lásd az átláthatóságról szóló iránymutatás 8. pontját.

²⁴ Átláthatóságról szóló iránymutatás, 30. pont és 39. o.

érintett akaratának önkéntes, konkrét, tájékozott és egyértelmű kinyilvánítása” kell, hogy legyen, „amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez”. A hozzájárulásra vonatkozó valamennyi fenti követelménynek együttesen kell teljesülnie ahhoz, hogy érvényesnek minősüljön.

26. Azon közösségimédia-szolgáltatók számára, amelyek különböző adatkezelési célokból kérik a felhasználók hozzájárulását, az Európai Adatvédelmi Testület hozzájárulásról szóló 05/2020. sz. iránymutatása értékes iránymutatást nyújt a hozzájárulás megszerzéséhez²⁵. A közösségimédia-platformok nem játszhatják ki a feltételeket, például az érintettek azon képességét, hogy önkéntes hozzájárulásukat adják, olyan grafikus kialakítás vagy olyan megfogalmazás révén, amely megakadályozza az érintetteket az említett akarat gyakorlásában. E tekintetben az általános adatvédelmi rendelet 7. cikkének (2) bekezdése kimondja, hogy a hozzájárulás iránti kérelmet más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. A közösségimédia-platformok felhasználói a regisztrációs folyamat során, illetve később az adatvédelmi beállításokon keresztül adhatnak hozzájárulást a hirdetésekhez vagy speciális elemzési típusokhoz. Mindenesetre, amint azt az általános adatvédelmi rendelet (32) preambulumbekzdése hangsúlyozza, a hozzájárulást mindig egyértelmű megerősítő cselekedettel kell megadni, az előre bejelölt négyzetek vagy a felhasználó nem cselekvése ezért nem minősülnek hozzájárulásnak.²⁶
27. Amint azt az Európai Adatvédelmi Testület hozzájárulásról szóló iránymutatása már kiemelte: ahhoz, hogy a hozzájárulás „tájékoztaton alapuló” legyen, a szükséges információk minimális szintjét kell biztosítani a felhasználók számára.²⁷ Ha nem ez a helyzet, a regisztrációs eljárás során megszerzett hozzájárulás nem tekinthető érvényesnek az általános adatvédelmi rendelet értelmében, ami jogellenessé teszi az adatkezelést.
28. A felhasználóktól hozzájárulást kérnek különböző célokhoz (pl. személyes adatok további kezelése). A hozzájárulás nem konkrét, és ezért nem érvényes, ha a felhasználókat nem tájékoztatják egyértelműen arról, hogy mihez járulnak hozzá²⁸. Amint azt az általános adatvédelmi rendelet 7. cikkének (2) bekezdése előírja, a hozzájárulást oly módon kell kérni, hogy az egyértelműen megkülönböztesse azt más információktól, függetlenül attól, hogy az információt hogyan mutatják be az érintettek. Különösen, ha a hozzájárulást elektronikus úton kérik, ez a hozzájárulás nem szerepelhet a szerződési feltételekben²⁹. Figyelembe véve, hogy egyre több felhasználó a közösségimédia-platformokhoz okostelefonjaik interfészén keresztül fér hozzá, hogy regisztráljon a platformra, a közösségimédia-szolgáltatóknak különös figyelmet kell fordítaniuk a hozzájárulás kérésének módjára annak biztosítása érdekében, hogy ez a hozzájárulás megkülönböztethető legyen. A felhasználókat nem szabad túlzott mennyiségű információval szembesíteni, ami arra készteti őket, hogy kihagyják ezen információk elolvasását. Máskülönben, ha a felhasználóknak a fiók létrehozásához „meg kell erősíteniük”, hogy elolvasták a teljes adatvédelmi szabályzatot, és elfogadják a közösségimédia-szolgáltató feltételeit, beleértve az összes adatkezelési műveletet, ez az ott megnevezett különleges feltételekhez való kikényszerített hozzájárulásnak minősülhet. Ha a hozzájárulás megtagadása a szolgáltatás

²⁵ Az Európai Adatvédelmi Testület 05/2020. sz. iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról, 1.1. verzió, elfogadva 2020. május 4-én; https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_hu.pdf.

²⁶ Lásd: az Európai Unió Bíróságának 2019. október 1-jei ítélete, Verbraucherzentrale Bundesverband e.V. kontra Planet 49 GmbH, C-673/17, 62–63. pont.

²⁷ A hozzájárulásról szóló 05/2020. sz. iránymutatás, 64. pont; lásd még alább az ezen iránymutatás 3.3. részében szereplő 3a. használati esetet.

²⁸ Lásd a hozzájárulásról szóló 05/2020. sz. iránymutatás 68. pontját.

²⁹ Az átláthatóságról szóló iránymutatás 8. pontja.

megtagadásához vezet, az nem tekinthető önkéntesnek, részletesnek és konkrétan, amint azt az általános adatvédelmi rendelet előírja. A közösségimédia-szolgáltató szerződési feltételeinek elfogadásával „összekapcsolt” hozzájárulás nem minősül „önkéntesnek”³⁰. Ez igaz akkor is, ha az adatkezelő a szerződés vagy szolgáltatás nyújtását a hozzájárulás iránti kérelemhez „köti”, tehát olyan személyes adatokat kezel, amelyek nem szükségesek a szerződés adatkezelő általi teljesítéséhez.

29. Míg a hozzájárulást a felhasználók pozitív cselekedetével kell kifejezni, a hozzájárulás megadásáig a hozzájárulás hiányát kell alapértelmezett állapotnak tekinteni. A felhasználók általi elutasítás kifejezése ezért nem igényel semmilyen műveletet a részükre, vagy olyan művelettel kell lehetővé tenni, amely ugyanolyan egyszerű, mint a hozzájárulás kifejezése³¹.

ii. A hozzájárulás visszavonása – az általános adatvédelmi rendelet 7. cikkének (3) bekezdése

30. Az általános adatvédelmi rendelet 7. cikke (3) bekezdésének első mondatával összhangban a közösségimédia-platformok felhasználói bármikor visszavonhatják hozzájárulásukat. A hozzájárulás megadása előtt a felhasználókat tájékoztatni kell a hozzájárulás visszavonásához való jogról is, amint azt az általános adatvédelmi rendelet 7. cikke (3) bekezdésének harmadik mondata előírja. Az adatkezelőknek különösen azt kell bizonyítaniuk, hogy a felhasználóknak módjukban áll a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárukra válna. A közösségimédia-platformok azon felhasználói számára, akik egy kattintással – például egy jelölőnégyzet kipipálásával – hozzájárulnak személyes adataik kezeléséhez, ugyanolyan egyszerű módon vissza kell tudniuk vonni hozzájárulásukat³². Ez hangsúlyozza, hogy a hozzájárulásnak visszafordítható döntésnek kell lennie, hogy az érintett bizonyos mértékben továbbra is rendelkezzen az adatai felett³³. Az általános adatvédelmi rendelet 7. cikke (3) bekezdésének negyedik mondata szerint a hozzájárulás egyszerű visszavonása az érvényes hozzájárulás előfeltétele, és annak a szolgáltatási szintek csökkentése nélkül is lehetségesnek kell lennie³⁴. Például nem tekinthető érvényesnek a hozzájárulás az általános adatvédelmi rendelet értelmében, ha a hozzájárulás megszerzése egyetlen egérekattintással, suhintással vagy billentyű leütésével történik, de a visszavonás több lépést tesz szükségessé³⁵, nehezebb elérni vagy több időt vesz igénybe.

c. Megtévesztő tervezési megoldások

31. Az általános adatvédelmi rendelet több rendelkezése a regisztrációs folyamatra vonatkozik. Ezért számos megtévesztő tervezési megoldás fordulhat elő, ha a közösségimédia-szolgáltatók nem hajtják végre megfelelően az általános adatvédelmi rendeletet.

i. Tartalomalapú megoldások

Túlterhelés – Folyamatos noszogató (I. melléklet, az ellenőrző lista 4.1.1. pontja)

³⁰ Lásd az Európai Adatvédelmi Testületnek a közösségi média felhasználóinak megcélzásáról szóló 8/2020. számú iránymutatásának 57. pontját.

³¹ Lásd az általános adatvédelmi rendelet (42) preambulumbekzdésének ötödik mondatát.

³² Lásd az átláthatóságról szóló iránymutatás 113. és azt követő pontjait.

³³ A hozzájárulásról szóló 05/2020. sz. iránymutatás, 10. pont.

³⁴ A hozzájárulásról szóló 05/2020. sz. iránymutatás, 114. pont.

³⁵ Lásd a hozzájárulásról szóló 05/2020. sz. iránymutatás 114. pontját.

32. A **folyamatos noszogatás** megtévesztő tervezési megoldás akkor fordul elő, ha a felhasználókat – azáltal, hogy újra és újra további adatok szolgáltatására vagy az adatkezelés valamely céljához való hozzájárulásra kéri őket – rábírják arra, hogy az adatkezelés céljaihoz szükségesnél több személyes adatot adjanak meg, vagy hogy hozzájáruljanak adataik más célú felhasználásához. Ezek az ismétlődő felszólítások egy vagy több eszközön keresztül is bekövetkezhetnek. A felhasználók végül valószínűleg beadják a derekukat, mivel belefáradnak abba, hogy minden egyes alkalommal, amikor a platformot használják, vissza kell utasítaniuk a kérést.

1. példa:

„A” változat: A regisztrációs folyamat első lépése során a felhasználóknak a regisztrációhoz különböző lehetőségek közül kell választaniuk. Megadhatják e-mail-címüket vagy telefonszámukat. Ha a felhasználók az e-mail-címet választják, a közösségimédia-szolgáltató továbbra is megpróbálja meggyőzni őket arról, hogy adják meg telefonszámukat, kijelentve, hogy azt fiókbiztonság céljából fogják használni, anélkül, hogy alternatívát biztosítana a felhasználók által megadható vagy már megadott adatokra vonatkozóan. Konkrétan, a regisztrációs folyamat során több ablak ugrik fel a telefonszám megadására szolgáló mezővel, valamint a következő magyarázattal: „*Telefonszámodat a fiókbiztonság céljából fogjuk használni*”. Bár a felhasználók bezárhatják az ablakot, végül túlterhelődnek, feladják és megadják telefonszámukat.

„B” változat: Egy másik közösségimédia-szolgáltató minden alkalommal arra kéri a felhasználót, amikor bejelentkezik a fiókjába, hogy adja meg telefonszámát, annak ellenére, hogy a felhasználó korábban megtagadta annak megadását, akár a regisztrációs folyamat során, akár az utolsó bejelentkezéskor.

33. A fenti példa azt a helyzetet szemlélteti, amikor a felhasználókat folyamatosan bizonyos személyes adatok, például telefonszámuk megadására kéri. Míg a példa „A” változatában erre a **folyamatos noszogatásra** a regisztrációs folyamat során kerül sor több alkalommal, a „B” változat azt mutatja, hogy a felhasználók azt követően is találkozhatnak ezzel a megtévesztő tervezési megoldással, hogy már regisztráltak. E megtévesztő tervezési megoldás elkerülése érdekében különösen szem előtt kell tartani az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja szerinti adattakarékosság elveit, valamint – az 1. példa „A” változatában ismertetettekhez hasonló esetekben – az általános adatvédelmi rendelet 5. cikke (1) bekezdésének b) pontja szerinti célhoz kötöttség elvét is. Ezért amikor a közösségimédia-szolgáltatók azt állítják, hogy a telefonszámot „fiókbiztonság céljából” fogják használni, csak az említett biztonsági célokból kezelhetik a telefonszámot, és nem kezelhetik tovább a telefonszámot az eredeti célon túlmutató módon.
34. Az adattakarékosság elvének tiszteletben tartása érdekében a közösségimédia-szolgáltatók nem kérhetnek további adatokat, például telefonszámot, ha a regisztrációs folyamat során a felhasználók által már megadott adatok elegendők. A fiókbiztonság biztosítása céljából például telefonszám nélkül is van lehetőség megerősített hitelesítésre, egyszerűen egy kód elküldésével a felhasználó e-mail-fiókjába, vagy számos más módon.
35. A közösségi hálózatok szolgáltatóinak ezért olyan biztonsági eszközökre kell támaszkodniuk, amelyeket a felhasználóknak könnyebb ismételtel kezdeményezniük. A közösségimédia-szolgáltató például egy további kommunikációs csatornán – például egy korábban a felhasználó által mobiltelefonjára telepített biztonsági alkalmazáson – keresztül azonosító számot küldhet a felhasználónak, amelyhez nincs szükség a felhasználó mobiltelefonszámára. Az e-mail-címen keresztül történő

felhasználóazonosítás szintén kevésbé tolatódó, mint a telefonszámon keresztüli, mivel a felhasználók egyszerűen létrehozhatnak egy új e-mail-címet kifejezetten a regisztrációs folyamathoz, amelyet elsősorban a közösségi oldallal összefüggésben használhatják. Egy telefonszám ugyanakkor nem könnyen helyettesíthető, mivel nagyon valószínűtlen, hogy a felhasználók új SIM-kártyát vásárolnának, vagy új telefonszerződést kötnének kizárólag hitelesítés céljából.

36. Nem szabad elfelejteni, hogy ha az ilyen kérés célja annak bizonyítása, hogy a felhasználók jogszerűen rendelkeznek a közösségi oldalra való belépéshez használt eszközzel, ez a cél többféle módon is elérhető, a telefonszám csak az egyik. Így a telefonszám megadása csak egy releváns, önkéntes alapon választott opciót jelenthet a felhasználók számára. Végezetül a felhasználóknak el kell dönteniük, hogy kívánják-e ezt az eszközt hitelesítési faktorként használni. Különösen az egyszeri ellenőrzéshez nincs szükség a felhasználók telefonszámára, mivel a regisztrációs folyamat során az e-mail cím jelenti a felhasználókkal való rendszeres kapcsolattartási pontot.
37. Az 1. példa „A” változatában bemutatott gyakorlat félrevezetheti a felhasználókat, és arra készítheti őket, hogy akaraton kívül megadják ezeket az információkat, abban a hitben, hogy ez a fiók aktiválásához vagy védelméhez szükséges. A valóságban azonban a felhasználók számára soha nem ajánlottak fel alternatívát (pl. e-mail használata a fiók aktiválásához és biztonsági célokra). Az 1. példa „B” változatában a felhasználókat nem tájékoztatják az adatkezelés céljáról. Ez a változat azonban ennek ellenére is a **folymatos noszogatas** megtévesztő tervezési megoldásnak minősül, mivel a közösségimédia-szolgáltató figyelmen kívül hagyja azt a tényt, hogy a felhasználók korábban megtagadták a telefonszám megadását, és továbbra is annak megadására kéri őket. Ha a felhasználóknak az a benyomásuk, hogy csak akkor kerülhetik el ezt az ismételt kérést, ha megadják az adataikat, akkor valószínűleg engedni fognak.
38. A következő példában a felhasználókat ismételtlen arra szólítják fel, hogy biztosítsanak hozzáférést a közösségimédia-platform számára névjegyeikhez:

2. példa:A közösségimédia-platform információ vagy egy kérdőjel ikon segítségével ösztönzi a felhasználókat az aktuálisan kért „opcionális” cselekvésre. A platform azonban ahelyett, hogy csupán tájékoztatást nyújtana azoknak a felhasználóknak, akik ezektől a gomboktól segítségre számítanak, egy „Let’s do it” (Csináljuk meg) szöveget tartalmazó felugró ablak ismételt megjelenítésével arra buzdítja a felhasználókat, hogy fogadják el a névjegyeik importálását az e-mail-fiókjukból.

39. Ez a **folymatos noszogatas** – különösen a regisztrációs folyamat során – arra ösztönözheti a felhasználókat, hogy végül is engedjenek a platform kérésének, hogy ezáltal végre befejezhessék regisztrációjukat. Ezen megtévesztő tervezési megoldás hatását fokozza, ha motivációs nyelvezettel kombináljuk, mint ebben a példában, ami a sürgősség érzetét kelti.
40. Az alábbiakban az **érzelmi befolyásolás** megtévesztő tervezési megoldás vizsgálatakor részletesebben foglalkozunk a megfogalmazás és a vizuális elemek befolyásoló hatásaival.³⁶

Akadályozás – Megtévesztő tevékenység (I. melléklet, az ellenőrző lista 4.4.3. pontja)

³⁶ Lásd az 1. használati eset 43. és azt követő pontjait, valamint a példák áttekintését a melléklet ellenőrző listájában.

41. Egy másik példa arra a helyzetre, amikor a közösségimédia-szolgáltatók szükségtelenül kérik a felhasználók telefonszámait, a platform alkalmazásának használatát érinti:

3. példa: Ha a felhasználók asztali böngészőn keresztül regisztrálnak egy közösségimédia-platformra, arra kérik őket, hogy használják a platform mobilalkalmazását is. A regisztrációs folyamat látszólag egy újabb lépése során a felhasználókat arra kérik, hogy fedezzék fel az alkalmazást. Amikor az ikonra kattintanak, arra számítva, hogy az egy alkalmazásboltba irányítja őket, ehelyett arra kérik őket, hogy adják meg a telefonszámukat, hogy szöveges üzenetet kapjanak az alkalmazásra mutató hivatkozással.

42. Az, hogy a felhasználók számára azzal indokolják a telefonszám megadásának szükségességét, hogy megkaphassák az alkalmazás letöltéséhez szükséges hivatkozást, több okból is **meztévesztő tevékenységnek** minősül: Először is, a felhasználók többféle módon is használhatnak egy alkalmazást, például QR-kód beszkenelésével, hivatkozás használatával vagy az alkalmazásnak az alkalmazásboltból való letöltésével. Másodszor, ezek az alternatívák azt mutatják, hogy nincs kényszerítő indok arra, hogy a közösségi platform szolgáltatója elkérje a felhasználók telefonszámát. Amikor a felhasználók befejezték a regisztrációs folyamatot, a bejelentkezési adataikkal (azaz általában e-mail címükkel és jelszavukkal) be kell tudniuk jelentkezni, függetlenül attól, hogy milyen eszközt – asztali vagy mobil böngészőt, illetve alkalmazást – használnak. Ezt még inkább hangsúlyozza az a tény, hogy a felhasználók okostelefon helyett telepíthetik az alkalmazást a táblagépekre is, amely nincs telefonszámhoz kötve.

Felkavarás – Érzelmi befolyásolás (1. melléklet, az ellenőrző lista 4.3.1. pontja)

43. Az **érzelmi befolyásolás** meztévesztő tervezési megoldással a szövegeket vagy vizuális elemeket (például stílust, színeket, képeket stb.) oly módon használják, ami az információt a felhasználóknak vagy nagyon pozitív perspektívából közvetíti, amitől a felhasználók jól, biztonságban vagy megjutalmazva érzik magukat, vagy rendkívül negatív perspektívából, ami miatt a felhasználók szoronganak, bűnösnek vagy büntetve érzik magukat. Az, ahogyan az információkat a felhasználók rendelkezésére bocsátják, olyan módon befolyásolja érzelmi állapotukat, amely arra készíti őket, hogy az adatvédelmi érdekeik ellen cselekedjenek. Az ilyen gyakorlatok hatásai még hatékonyabbak lehetnek, ha a platform által gyűjtött adatokon alapulnak. A döntéseknek az egyéneknek nyújtott elfogult információk révén történő befolyásolása általában tisztességtelen gyakorlatnak tekinthető, amely ellentétes az adatkezelés tisztességességének az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában meghatározott elvével. Ez a közösségimédia-platformon belüli teljes felhasználói útvonal során előfordulhat. A regisztrációs folyamat során azonban a befolyásolás különösen erős lehet, tekintettel arra, hogy a felhasználóknak a regisztráció befejezéséhez szükséges lépések mellett túl sok információt kell feldolgozniuk.
44. A fentiek fényében a közösségimédia-platformon való regisztráció szakaszában az **érzelmi befolyásolás** még nagyobb hatást gyakorolhat a gyermekekre, az idősekre és más csoportokra (azaz több személyes adatot adhatnak meg, mivel nem értik az adatkezelési tevékenységeket), tekintettel az érintettek kiszolgáltatott voltára³⁷. Amennyiben a közösségimédia-platformszolgáltatások gyermekeket vagy más kiszolgáltatott érintetteket céloznak, biztosítaniuk kell, hogy a használt nyelv – beleértve annak hangnemtét és stílusát is – megfelelő legyen ahhoz, hogy a kiszolgáltatott helyzetben lévő felhasználók

³⁷ Lásd még a fenti 7. pontot.

az üzenet címzettjeiként könnyen megértsék a nyújtott információkat³⁸. Figyelembe véve a gyermekek, az idősek és más érintettek kiszolgáltatottságát, a megtevesztő tervezési megoldások arra sarkallhatják ezeket a felhasználókat, hogy több információt osszanak meg, mivel a „parancsoló” kifejezések miatt úgy érezhetik, hogy meg kell ezt tenniük, például azért, hogy népszerűnek tűnjenek társaik körében, vagy mert úgy gondolják, hogy az adatok megadása kötelező.

45. Amikor a közösségimédia-platformok felhasználóit arra szólítják fel, hogy gyorsan adják meg adataikat, nincs idejük arra, hogy „feldolgozzák”, és így valóban megértsék a rendelkezésükre bocsátott információkat annak érdekében, hogy tudatos döntést hozzanak. A közösségimédia-platformok motivációs nyelvezete arra ösztönözheti a felhasználókat, hogy a szükségesnél több adatot adjanak meg, ha úgy érzik, hogy amit a közösségimédia-platform javasol, az az, amit a legtöbb felhasználó tenne, ezért ez a folytatás „helyes módja”.

4. példa:A közösségimédia-platform a következő szöveggel kéri a felhasználókat arra, hogy megosszák földrajzi helyzetüket: „Magányos farkas vagy? A megosztás és a másokkal való kapcsolódás hozzájárul ahhoz, hogy a világ jobb helyé váljon! Oszd meg földrajzi helyzetedet! Hagyd, hogy a körülötted lévő helyek és emberek inspiráljanak!”

46. A regisztrációs folyamat során a felhasználók célja a regisztráció befejezése, hogy használhassák a közösségimédia-platformot. Az olyan megtevesztő tervezési megoldások, mint az **érzelmi befolyásolás**, erősebb hatást gyakorolnak ebben az összefüggésben. Ezek a kockázatok a regisztrációs folyamat kezdetéhez képest felerősödnek a közepe vagy vége felé, mivel a felhasználók legtöbbször „sietve” végzik el a szükséges lépéseket, vagy fogékonyabbak a sürgetésre. Ebben az összefüggésben a felhasználók nagyobb valószínűséggel egyeznek bele abba, hogy minden kért adatot megadjanak, anélkül, hogy időt szánának arra, hogy megkérdőjelezzék, meg kell-e ezt tenniük. Ebben az értelemben a közösségimédia-szolgáltató által használt motivációs nyelvezet hatással lehet a felhasználók azonnali döntésére, ahogyan a motivációs nyelvezet a nyomtatékosítás más formáival, például felkiáltójelekkel való kombinációja is, ahogyan az alábbi példában is látható.

5. példa:A közösségimédia-szolgáltató arra ösztönzi a felhasználókat, hogy a ténylegesen szükségesnél több személyes adatot osszanak meg, azáltal, hogy azt kéri tőlük, mutakozzanak be: „Meséj nekünk arról a csodálatos emberről, aki te vagy! Alig várjuk, szóval ne habozz, mutasd meg, ki vagy!”

47. Ezzel a gyakorlattal a közösségimédia-platformok részletesebb profilt kapnak felhasználóikról. Az esettől függően azonban előfordulhat, hogy több személyes adat – például a felhasználók személyiségére vonatkozó – megadása nem feltétlenül szükséges magának a szolgáltatásnak a használatához, és ezért sérti az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja szerinti adattakarékosság elvét. Amint azt az 5. példa szemlélteti, az ilyen technikák nem segítik elő a felhasználók szabad akaratát az adataik közzétevése tekintetében, mivel az alkalmazott előíró nyelv miatt a felhasználók úgy érezhetik, hogy be kell mutatkozniuk, ha már időt fordítottak a regisztrációra, és azt be kívánják fejezni. A regisztráció folyamata során kevésbé valószínű, hogy a felhasználók időt szánnak arra, hogy átgondolják, milyen bemutatkozást írnak, vagy hogy egyáltalán szeretnének-e bemutatkozni. Ez különösen igaz abban az esetben, ha a használt nyelv a sürgősség érzését kelti, vagy felszólításként hangzik. Ha a felhasználók ezt kötelezettségként élik meg, még akkor is, ha az adatszolgáltatás valójában nem kötelező, az hatással lehet „szabad akaratukra”. Ez azt is jelenti, hogy a közösségimédia-platform által szolgáltatott információk nem voltak egyértelműek.

³⁸ Lásd az átláthatóságról szóló iránymutatás 18. pontját.

6. példa:A regisztrációs folyamat azon része, ahol a felhasználóknak képet kell feltölteniük magukról, egy „?” gombot tartalmaz. A gombra kattintva a következő üzenet jelenik meg: „Nem kell előbb fodrászhoz menned. Csak válassz ki egy fényképet, amely bemutatja, milyen is vagy te.”

48. Még ha az is a 6. példában szereplő mondatok célja, hogy motiválják a felhasználókat, és látszólag leegyszerűsítsék számukra a folyamatot (pl. nincs szükség hivatalos képre a regisztráláshoz), az ilyen gyakorlatok hatással lehetnek azon felhasználók végső döntésére, akik eredetileg úgy döntöttek, hogy nem osztanak meg képet fiókjukhoz. A kérdőjelek kérdések esetében használatosak, és ikonként a felhasználók arra számíthatnak, hogy hasznos információkat fognak kapni, amikor rájuk kattintanak. Ha ez az elvárás nem teljesül, és ehelyett a felhasználókat megint csak arra ösztönzik, hogy tegyék meg azt a műveletet, amellyel kapcsolatban bizonytalanok, a felhasználók a fényképük kezelésével kapcsolatos tájékoztatás nélkül megadott hozzájárulása nem érvényes, mivel nem felel meg az általános adatvédelmi rendelet 4. cikkének 11. pontjával összefüggésben értelmezett 7. cikke szerinti „megfelelő tájékoztatáson alapuló” és „önkéntes” hozzájárulás követelményeinek. Az érzelmi tényező tehát erősen befolyásolja a hozzájárulás legitimitását.

Akadályozás – Indokolatlanul hosszú folyamatok (I. melléklet, az ellenőrző lista 4.4.2. pontja)

49. Ha a felhasználók az adatvédelemmel kapcsolatos ellenőrzést próbálnak aktiválni, de a felhasználói útvonal úgy van kialakítva, hogy a felhasználóknak több lépést kell végrehajtaniuk, mint ahány lépés az invazív opciók aktiválásához szükséges, ez az **indokolatlanul hosszú folyamatok elnevezésű** megtévesztő tervezési megoldást jelenti. Ez a megoldás nagy valószínűséggel eltántorítja a felhasználókat az adatvédelmi ellenőrzések aktiválásától. A regisztrációs folyamat során ez egy pop-in vagy pop-up felugró ablak formájában nyilvánulhat meg, amely arra kéri a felhasználókat, hogy erősítsék meg döntésüket, amikor korlátozó lehetőséget választanak (pl. úgy döntenek, hogy profiljukat privátra állítják). Az alábbi példa egy másik olyan esetet szemléltet, amikor egy regisztrációs folyamat **indokolatlanul hosszú**.

7. példa:A regisztrációs folyamat során azoknak a felhasználóknak, akik a „kihagy” gombra kattintva elkerülik bizonyos adatok megadását, felugró ablakot jelenítenek meg, amely megkérdezi, hogy „Biztos vagy benne?”. A döntésük megkérdőjelezésével és ezáltal kétségbe vonásával a közösségimédia-szolgáltató arra ösztönzi a felhasználókat, hogy vizsgálják felül azt, és tegyék közzé az ilyen típusú adatokat, például nemüket, kapcsolati listájukat vagy fényképüket. Ezzel szemben azok a felhasználók, akik úgy döntenek, hogy egyenesen megadják az adatokat, nem látnak olyan üzenetet, amely a választásuk újragondolását kérné tőlük.

Ebben az esetben az, hogy a felhasználókat arra kéri, erősítsék meg, hogy nem kívánnak kitölteni egy adatmezőt, arra készítheti őket, hogy megváltoztassák eredeti döntésüket, és megadják a kért adatokat. Ez különösen igaz azokra a felhasználókra, akik nem ismerik a közösségimédia-platform funkcióit. Az **indokolatlanul hosszú folyamatok** megtévesztő tervezési megoldás célja a felhasználók döntéseinek befolyásolása azáltal, hogy feltartja őket és megkérdőjelezi eredeti döntésüket, emellett szükségtelenül meghosszabbítja a regisztrációs folyamatot, ami sérti az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja szerinti tisztességes eljárás elvét. A példa azt mutatja, hogy a megtévesztő tervezési megoldás arra készítheti a felhasználókat, hogy az eredeti döntésükhöz képest több személyes adatot tegyenek közzé. A személyes adatokat rögtön közzétevő és a személyes adatokat közzé nem tevő felhasználókkal szembeni egyenlőtlen

bánásmódot írja le: Csak az adatok közlését megtagadó személyeket kérik arra, hogy erősítsék meg döntésüket, míg az adatokat közzé tevő felhasználóktól nem kérik ezt. Ez sérti az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja szerinti tisztességes eljárás elvét azon felhasználók tekintetében, akik nem kívánják közzétenni ezeket a személyes adatokat.

ii. Interfészalapú megoldások

Felkavarás – Bújtatott közzététel (I. melléklet, az ellenőrző lista 4.3.2. pontja)

50. Az átláthatóság elvének megfelelően az érintettek számára egyértelmű tájékoztatást kell nyújtani annak érdekében, hogy megérthessék, hogyan kezelik személyes adataikat, és hogyan rendelkezhetnek azok felett. Emellett ennek az információnak könnyen észrevehetőnek kell lennie az érintettek számára. Az adatvédelemmel kapcsolatos információkat, különösen a hivatkozásokat azonban gyakran úgy jelenítik meg, hogy azok könnyen elkerüljék a felhasználók figyelmét. A **bújtatott közzététel** ilyen praktikai olyan vizuális stílust használnak a tájékoztatáshoz vagy az adatvédelmi beállításokhoz, amely a felhasználókat az adatvédelmi szempontból előnyös lehetőségekről a kevésbé szigorú és így invazívabb lehetőségek felé tereli.
51. A kis betűméret vagy egy olyan szín használata, amely nem eléggé kontrasztos ahhoz, hogy megfelelő olvashatóságot biztosítson (pl. fehér háttéren halványszürke színű szöveg) negatív hatással lehet a felhasználókra, mivel a szöveg kevésbé látható, és a felhasználók vagy figyelmen kívül hagyják azt, vagy nehézségekbe ütköznek annak elolvasása során. Ez különösen abban az esetben igaz, ha a kötelező adatvédelmi információk mellett egy vagy több feltűnő elemet helyeznek el. Ezek az interfésztechnikák félrevezetik a felhasználókat, és megnehezítik és időigényesebbé teszik az adatvédelemmel kapcsolatos információk azonosítását, mivel több időre és nagyobb alaposagra van szükség a releváns információk kiszűréséhez.

8. példa:A regisztráció befejezése után a felhasználók már csak úgy férhetnek hozzá az adatvédelmi információkhoz, ha megnyitják a közösségimédia-platform általános menüjét, és átböngészik az almenü azon részét, amely az „*adatvédelmi és adatbeállítások*” hivatkozást tartalmazza. Az oldal meglátogatásakor az adatvédelmi szabályzatra mutató hivatkozás első pillantásra nem látható. A felhasználóknak az oldal egyik sarkában egy apró ikont kell észrevenniük, amely az adatvédelmi szabályzatra mutat, ami azt jelenti, hogy a felhasználók aligha veszik észre, hol vannak az adatvédelemmel kapcsolatos szabályokra vonatkozó információk.

52. Fontos megjegyezni, hogy még ha a közösségimédia-szolgáltatók az általános adatvédelmi rendelet 13. és 14. cikke szerinti összes információt az érintettek rendelkezésére is bocsátják, ezen információk bemutatásának módja továbbra is sértheti az általános adatvédelmi rendelet 12. cikkének (1) bekezdése szerinti átfogó átláthatósági követelményeket. Ha az információ **bújtottan van közzétéve**, és ezért valószínű, hogy a felhasználók nem veszik észre, ez zavarodottsághoz vagy tájékozatlansághoz vezet, és nem tekinthető érthetőnek és könnyen hozzáférhetőnek, ami ellentétes az általános adatvédelmi rendelet 12. cikkének (1) bekezdésével.
53. Bár a fenti példa a megtévesztő tervezési megoldást a regisztrációs folyamat befejezését követően mutatja be, ez a megoldás már a regisztrációs folyamat során is előfordul, amint azt az alábbiakban bemutatott példa mutatja, amely a **bújtatott közzététel** és a **megtévesztő biztonság** megtévesztő tervezési megoldást ötvözi.

Átugrás – Megtévesztő biztonság (1. melléklet, az ellenőrző lista 4.2.1. pontja)

54. A közösségimédia-szolgáltatóknak szem előtt kell tartaniuk az alapértelmezett adatvédelem elvét is. Ha az adatbeállításokat előre kiválasztják, a felhasználókra egy adott adatvédelmi szint vonatkozik, amelyet alapértelmezés szerint a szolgáltató határoz meg, nem pedig a felhasználók. Emellett a felhasználók nem mindig kapnak azonnali lehetőséget arra, hogy a beállításokat szigorúbb, az adatvédelemnek inkább megfelelő beállításokra módosítsák. Az általános adatvédelmi rendeletnek való megfelelés e tekintetben nem jelenti azt, hogy minden lehetőségnek pontosan azonosnak kell lennie. Ha azonban a közösségimédia-szolgáltatók kiemelik az egyik lehetőséget, és így ráirányítják a felhasználók figyelmét arra, a személyes adatok tekintetében ennek kell a legszigorúbbnak lennie, többek között az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja szerinti adattakarékosság elvének való megfelelés érdekében.
55. Ha a leginkább invazív funkciók és opciók vannak alapértelmezés szerint engedélyezve, akkor ez a **megtévesztő biztonság** megoldásnak minősül. Az alapértelmezett hatás miatt, amely arra ösztönzi az egyéneket, hogy megtartsák az előre kijelölt opciót, a felhasználók valószínűleg akkor sem változtatnak ezeken, ha lehetőségük van rá. Ez a gyakorlat gyakran érvényesül a regisztrációs folyamatokban, amint azt az alábbi 9. példa is szemlélteti, mivel hatékony módja az olyan invazív opciók aktiválásának, amelyeket a felhasználók egyébként valószínűleg elutasítanak. Az ilyen megtévesztő tervezési megoldások ellentétesek az általános adatvédelmi rendelet 25. cikkének (2) bekezdése szerinti alapértelmezett adatvédelem elvével, különösen akkor, ha érintik a személyes adatok gyűjtését, az adatkezelés mértékét, az adattárolás időtartamát és az adatokhoz való hozzáférhetőséget³⁹.

³⁹ Lásd még az ír adatvédelmi hatóság Instagramra (Meta Platforms Ireland Limited) vonatkozó végleges határozatának 446. pontját az Európai Adatvédelmi Testület 2022. július 28-i kötelező erejű vitarendezési határozatát követően, https://www.edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_hu.

Sign-up


Just one more step to join your friends!

Your birthdate


Day Month Year

29 12 1996


Share it with
no one



Share it with
my friends



Share it with
everyone



Join the network!

Skip this step and sign up

9. példa: Ebben a példában, amikor a felhasználó megadja születési idejét, felszólítják, hogy válassza ki, kivel osztja meg ezt az információt. Bár kevésbé invazív lehetőségek is elérhetőek, alapértelmezetten a „*megosztás mindenkivel*” opció van kijelölve, ami azt jelenti, hogy mindenki – azaz a regisztrált felhasználók, valamint minden internethasználó – láthatja a felhasználó születési idejét.

56. A 9. példa a **megtévesztő biztonság** megoldást illusztrálja, mivel alapértelmezés szerint nem a legmagasabb szintű adatvédelmet nyújtó opció van kijelölve, és ezáltal aktiválva. Ezen túlmenően a megoldás alapértelmezett hatása arra sarkallja a felhasználókat, hogy megtartsák az előre kijelölt lehetőséget, azaz ne szánjanak időt arra, hogy ebben a szakaszban mérlegeljék a többi lehetőséget, és később se térjenek vissza a beállítás megváltoztatására. Ezen az interfészen a **bújtatott közzététel** megoldást is alkalmazzák. A születési dátum megadása ugyanis nem kötelező, mivel a felhasználók kihagyhatják ezt a regisztrációs lépést a „*Lépés átugrása és regisztrálás*” hivatkozásra kattintva, amely a „*Csatlakozás a hálózathoz!*” gomb alatt található. Az a tény, hogy a születési dátum mező és a megerősítés gomb ilyen feltűnő, alighanem arra készíti a felhasználókat, hogy megadják születési dátumukat, és azt közlétegyék a közösségi hálózaton, mert nem veszik észre azt a lehetőséget, hogy nem kell megosztaniuk ezt az információt. Ez a hatás még jelentősebb lehet, ha a mező mellett animált köröket és gombokat használnának, amelyek erőteljesen vonzzák a felhasználók figyelmét.

57. A beépített és alapértelmezett adatvédelem elvének tiszteletben tartása nem jelenti azt, hogy minden felkínált lehetőségnek pontosan ugyanúgy kell kinéznie. Ha azonban az adatkezelők úgy döntenek, hogy az egyik lehetőséget jobban kiemelik, mint a többit, a kiemelt lehetőségnek kell az adatkezelés tekintetében a legszigorúbbnak lennie.
58. Amellett, hogy a közösségimédia-szolgáltatók arra ösztönzik a felhasználókat, hogy olyan opciót tartsanak meg, amely nem feltétlenül felel meg a preferenciáiknak, előfordulhat, hogy a regisztrációs folyamat befejezését követően nem kérik a felhasználókat arra, hogy ellenőrizzék vagy a preferenciáiknak megfelelően módosítsák adatvédelmi beállításait. Emellett ezen alapértelmezett beállítások megváltoztatásához több lépésre is szükség lehet. Ha a felhasználók semmilyen módon nem kapnak ösztönzést arra, hogy ellenőrizzék vagy módosítsák adatvédelmi beállításait, vagy nem irányítják őket egyértelműen bármely kapcsolódó információhoz, adatvédelmi szintjük saját kezdeményezőkézségüktől függ. Annak érdekében, hogy a felhasználók könnyebben rendelkezessenek adataik felett, úgynevezett adatvédelmi irányítópultok használhatóak, amelyek célja, hogy központosítsák és megkönnyítsék ezt a törekvést.
59. Fontos szem előtt tartani, hogy a beépített és alapértelmezett adatvédelem hiánya a fent említett alapértelmezett hatással együtt káros következményekkel járhat az érintettek számára, beleértve a kiberbiztonságukat is. A más online szolgáltatások által végzett hitelesítési folyamatokhoz használt személyes adatok – például a születési idő – nyilvános megjelenítése megkönnyítheti a bűnözők számára, hogy hozzáférjenek a felhasználók vásárlási, banki és egyéb fiókjaihoz. Egy másik káros következmény a közösségimédia-platfomon való kapcsolattartási lehetőségeket érinti: ha a felhasználóknak küldött kapcsolatfelvételi kérelmek vagy üzenetek alapértelmezett beállítása „bárki”, ez növeli a szexuális visszaélés online előkészületének és a csalásnak a kockázatát, különösen a kiszolgáltatott csoportok esetében.
60. Végezetül, amikor a **megtévesztő kényelmet** a hozzájárulás megszerzésére alkalmazzák, ami egyenértékű a felhasználók alapértelmezés szerinti hozzájárulásának feltételezésével – például előre kipipált jelölőnégyzet használatával vagy a nem cselekvést jóváhagyásnak tekintve – nem teljesülnek az általános adatvédelmi rendelet 4. cikkének 11. pontjában meghatározott hozzájárulási feltételek, és az adatkezelés az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja és 6. cikke (1) bekezdésének a) pontja értelmében jogellenesnek minősül.

Akadályozás – Zsákutca (I. melléklet, az ellenőrző lista 4.4.1. pontja)

61. Fontos kiemelni, hogy a regisztrációs folyamat szakasza meghatározó pillanat a felhasználók számára a tájékozódás szempontjából. Ha keresnek valamilyen információt, és azt nem találják meg, mivel nem áll rendelkezésre átirányító hivatkozás, vagy a hivatkozás nem működik, az a **zsákutca** tervezési megoldásnak minősül, mivel a felhasználók nem tudják elérni a kívánt célt.

10. példa: A regisztrációs folyamat megkezdése után a felhasználók nem kapnak semmilyen hivatkozást az adatvédelmi információkhoz. A felhasználók nem találhatják meg ezeket az információkat, mivel a regisztrációs felületen sehol sem szerepelnek, még a láblécben sem.

62. A gyakorlatban ez a példa azt jelenti, hogy a felhasználók vagy félbehagyják a regisztrációt, és visszatérnek a kezdőlapra, ha az tartalmazza az adatvédelmi nyilatkozatra mutató hivatkozást, vagy befejezik a regisztrációt, bejelentkeznek a közösségimédia-platfomra, és csak ezt követően férnek hozzá az adatvédelemmel kapcsolatos információkhoz. Ez sérti az átláthatóság és az információkhoz

való könnyű hozzáférés elvét, amelyet az érintettek számára az általános adatvédelmi rendelet 12. cikkének (1) bekezdésében előírtak szerint biztosítani kell. Emellett nem felel meg az általános adatvédelmi rendelet 13. cikkének (1) és (2) bekezdésében foglalt követelményeknek sem, mivel a személyes adatok megszerzésének időpontjában nem tájékoztatják az érintettet és az információk nem hozzáférhetők.

63. A **zsáktuca** tervezési megoldás más módon is előfordulhat, ha a felhasználóknak a regisztrációs folyamat során olyan adatvédelmi vonatkozású műveletet vagy lehetőséget biztosítanak, amelyet később, a szolgáltatás használata közben nem találhatnak meg újra.

11. példa: A regisztrációs folyamat során a felhasználók hozzájárulhatnak személyes adataik hirdetési célú kezeléséhez, és tájékoztatják őket arról, hogy döntésüket a regisztrációt követően bármikor megváltoztathatják az adatvédelmi szabályzatra kattintva. Azt követően azonban, hogy a felhasználók befejezték a regisztrációs folyamatot, és felkeresik az adatvédelmi szabályzatot, nem találnak semmilyen lehetőséget vagy támpontot arra vonatkozóan, hogy hogyan vonhatják vissza az adatkezeléshez való hozzájárulásukat.

64. Ebben a konkrét példában a felhasználóknak nincs lehetőségük arra, hogy a regisztrációt követően visszavonják hozzájárulásukat. Ebben az esetben a **zsáktuca** megtévesztő tervezési megoldás sérti az érintetteknek az általános adatvédelmi rendelet 7. cikke (3) bekezdésének első és negyedik mondata szerinti azon jogát, hogy a hozzájárulást bármikor és ugyanolyan könnyen visszavonhassák, mint ahogyan megadták azt.
65. Végezetül, ha a felhasználókat egy olyan hivatkozásra irányítják, amely állítólag az adatvédelemmel kapcsolatos oldalakra, például a beállításokhoz vagy adatvédelmi információkhoz vezet, az is a **zsáktuca** tervezési megoldásra példa, ha a hivatkozás nem működik, és nem állnak rendelkezésre olyan tartalék hivatkozások, amelyek segítenék a felhasználókat abban, hogy megtalálják, amit keresnek. Ily módon a felhasználók nem kereshetik meg a vonatkozó információkat, miközben nem kapnak magyarázatot arra, hogy ez miért történik (pl. technikai problémák). Ilyen esetben ugyanazok a kérdések merülnek fel az átláthatósággal és a tájékoztatáshoz való könnyű hozzáféréssel kapcsolatban, mint amelyeket az 58. pont ismertet.

d. Bevált gyakorlatok

Az általános adatvédelmi rendelet hatékony végrehajtását elősegítő felhasználói felületek kialakítása érdekében az Európai Adatvédelmi Testület a következő bevált gyakorlatok alkalmazását javasolja a regisztrációs folyamat tekintetében:

Hivatkozások: A felhasználók számára adataik és adatvédelmi beállítások kezeléséhez gyakorlati segítséget nyújtó információkra, műveletekre vagy beállításokra mutató hivatkozásoknak mindenhol elérhetőnek kell lenniük, ahol a kapcsolódó információkkal vagy tapasztalatokkal találkoznak (pl. az adatvédelmi szabályzat vonatkozó részeire átirányító hivatkozások).

Elérhetőségek: Az adatvédelmi szabályzatban egyértelműen fel kell tüntetni az adatvédelmi kérések kezelésére szolgáló vállalati kapcsolattartási címet. Ennek egy olyan részen kell szerepelnie, ahol a felhasználók számíthatnak rá, például az adatkezelő személyazonosságára vonatkozó részben, a jogokkal kapcsolatos részben vagy az elérhetőségek részben.

A felügyeleti hatóság elérése: A felügyeleti hatóság konkrét megnevezésének feltüntetése, valamint a hatóság honlapjára vagy a panasz benyújtásához kapcsolódó weboldalra mutató hivatkozás. Ennek az

információnak egy olyan részen kell szerepelnie, ahol a felhasználók számítanak rá, például a jogokkal kapcsolatos részben.

Az adatvédelmi szabályzat áttekintése: Az adatvédelmi szabályzat elején/tetején meg kell jeleníteni egy (összecsukható) tartalomjegyzéket címsorokkal és alcímekkel, amelyek az adatvédelmi nyilatkozat különböző szakaszait mutatják. Az egyes szakaszok nevei egyértelműen a pontos tartalomhoz vezetik a felhasználót, és lehetővé teszik számára, hogy gyorsan beazonosítsa és elérje a keresett részt.

Változásfigyelés és összehasonlítás: Az adatvédelmi nyilatkozat módosítása esetén a korábbi változatok hozzáférhetővé tétele a verzió dátumával együtt, valamint a változások kiemelése.

Koherens megfogalmazás: A weboldal ugyanazokat a kifejezéseket és meghatározásokat használja ugyanazon adatvédelmi kérdések kapcsán. Az adatvédelmi szabályzatban használt kifejezéseknek meg kell egyezniük a platform többi részén használt kifejezésekkel.

Fogalommeghatározások: Ismeretlen vagy technikai szavak vagy szakzsargon használata esetén a közérthető nyelven megfogalmazott fogalommeghatározás segíti a felhasználókat abban, hogy megértsék a rendelkezésükre bocsátott információkat. A fogalommeghatározás közvetlenül a szövegben is megadható, amikor a felhasználók a szó fölé viszik a kurzort, illetve glosszáriumban is közzétehető.

Kontrasztos adatvédelmi elemek: Az adatvédelemmel kapcsolatos elemek vagy intézkedések vizuálisan feltűnővé tétele egy olyan felületen, amely nem közvetlenül a témával foglalkozik. Például, amikor nyilvános üzenetet tesznek közzé a platformon, a földrajzi helymeghatározás társítása feletti rendelkezésnek közvetlenül elérhetőnek és jól láthatónak kell lennie.

Adatvédelem a csatlakozáskor: Közvetlenül a fiók létrehozását követően a közösségimédia-szolgáltató az adatvédelemmel kapcsolatos pontokat épít bele a bemutatási élménybe, hogy a felhasználók zökkenőmentesen felfedezhessék és beállíthassák preferenciáikat. Ez történhet például úgy, hogy első barátjuk hozzáadása vagy első bejegyzésük megosztása után kéri fel őket, hogy határozzák meg adatvédelmi preferenciáikat.

Példák használata: Az adatkezelés célját egyértelműen és pontosan feltüntető kötelező információk mellett példákkal lehet szemléltetni egy konkrét adatkezelést, hogy az a felhasználók számára kézzelfoghatóbbá váljon.

Háttér-információk: A teljes körű adatvédelmi szabályzat mellett a legmegfelelőbb időpontban rövid információmorzsákat lehet biztosítani a felhasználónak, hogy konkrét és folyamatos tájékoztatást kapjon adatainak kezeléséről.

3.2 Tájékozódás a közösségi médiában

2a. használati eset: Többszintű adatvédelmi nyilatkozat

a. A kontextus leírása

66. Amint azt az átláthatóságról szóló iránymutatás már kiemelte, az átláthatóság elve igen szorosan kapcsolódik a személyes adatok tisztességes kezelésének elvéhez⁴⁰. A személyes adatok kezelésére vonatkozó tájékoztatás azonban arra is készíti az adatkezelőket, hogy megvizsgálják saját intézkedéseiket, érthetőbbé teszi az adatkezelést az érintettek számára, és végső soron lehetővé teszi számukra, hogy – különösen jogaik gyakorlása révén – rendelkezzenek adataik felett. Az érintett személyek képességeinek ebből eredő kiegyenlítése tisztességes személyesadat-feldolgozási rendszert

⁴⁰ Az átláthatóságról szóló iránymutatás, 4–5. pont.

eredményez. A több információ azonban nem feltétlenül jelent jobb tájékoztatást. A túl sok irreleváns vagy zavaró információ elhomályosíthatja a fontos tartalmi elemeket, vagy csökkentheti azok megtalálásának valószínűségét. Ezért ezen a területen alapvető fontosságú a tartalom és az érthető megjelenítés közötti megfelelő egyensúly. Ha ez az egyensúly nem valósul meg, megtévesztő tervezési megoldások fordulhatnak elő.

b. Vonatkozó jogi rendelkezések

67. Az imént vázolt kapcsolatok az általános adatvédelmi rendelet 5. cikke alapján válnak egyértelművé. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja már rendszeresen egymás mellett említi az átláthatóságot és a tisztességes eljárást, mivel az egyik összetevő meghatározza a másikat. Azt a tényt, hogy nemcsak a külső, hanem a belső átláthatóságnak is fenn kell állnia, az általános adatvédelmi rendelet 5. cikkének (2) bekezdésében foglalt elszámoltathatósági követelmény is egyértelművé teszi. A belső átláthatóság legfontosabb része az általános adatvédelmi rendelet 30. cikke szerinti, az adatkezelési tevékenységek nyilvántartására vonatkozó követelmény. A külső átláthatóság érdekében a közösségimédia-szolgáltatók – egyéb tájékoztatási eszközök mellett – többszintű adatvédelmi nyilatkozatot biztosíthatnak a felhasználók részére⁴¹. Az érthetőségre és a tisztességes adatkezelésre vonatkozó követelmény az általános adatvédelmi rendelet 12. cikkének (1) bekezdésében foglalt követelményeket is maga után vonja, amely kimondja, hogy az általános adatvédelmi rendelet 13. és 14. cikkében említett valamennyi információt tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell rendelkezésre bocsátani. Következésképpen a tájékoztatás tartalmát akadálymentesen hozzáférhetővé kell tenni. Ha az általános adatvédelmi rendelet 12. cikkében foglalt követelmények nem teljesülnek, akkor az általános adatvédelmi rendelet 13. és 14. cikke tükrében nincs megfelelő információ. Ezért a hatékony ellenőrzés érdekében az adatkezelők és az adatfeldolgozók felelősségre vonhatók, ami a gyakorlatban az általános adatvédelmi rendelet követelményeinek hatékonyságához vezet.

c. Megtévesztő tervezési megoldások

i. Tartalomalapú megoldások

68. Ebben a használati esetben a tartalomalapú megoldások korlátait az általános adatvédelmi rendelet 12. cikkének (1) bekezdése jelenti, amely pontos és érthető formát, valamint világos és közérthető megfogalmazást ír elő a nyújtott információk tekintetében.

Sötétben hagyás – Egymásnak ellentmondó információk (I. melléklet, az ellenőrző lista 4.6.2. pontja)

69. Ennek egyik legnyilvánvalóbb példája, amikor ***egymásnak ellentmondó információkat*** adnak meg, ami a felhasználókat bizonytalanságban hagyja azzal kapcsolatban, hogy mit kellene tenniük és milyen következményekkel járnak cselekedeteik, ezért nem tesznek semmit, vagy megtartják az alapértelmezett beállításokat.
70. Az e területen elkövetett jogsértéseket, például az általános adatvédelmi rendelet 12. cikke (1) bekezdésének megsértését más hatások, például az ***érzelmi befolyásolás*** felerősíthetik. A motivációs szövegek, képek és színek, valamint a vonzó reklám elviekben megengedett. Valószínű azonban, hogy ezek fokozzák a megtévesztő tervezési megoldások hatását, beleértve az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja értelmében vett tisztességtelen adatkezelést is.

⁴¹ Lásd az alábbi 3.2. szakaszban a 2a. használati esetet.

Sharing your information

On our platform you can **share everything and anything!** The more you share, the **more exciting** your **experience** will be! And at any time you can set your preference on the visibility of the information you share on our platform.

For example, you can decide if you want to **share your geolocation** or who will be able to read your posts.

If you **change the publicity of your information** once it is posted online, you will lose visibility and some people might not be able to see it anymore.



12. példa: Ebben a példában az adatmegosztással kapcsolatos információk rendkívül pozitív színben tüntetik fel az adatkezelést, azáltal, hogy kiemeli a lehető legtöbb adat megosztásának előnyeit. A labdával játszó cuki állat fényképét ábrázoló illusztrációval együtt ez az **érzelmi befolyásolás** a biztonság és a kényelem illúzióját keltheti a felhasználóban a platformon történő információmegosztás lehetséges kockázatait tekintetében. Másrészt az adatok nyilvánosságáról való rendelkezésre vonatkozó információk nem egyértelműek. Először azt állítják, hogy a felhasználók bármikor módosíthatják megosztási preferenciáikat. Ezt követően azonban az utolsó mondat azt jelzi, hogy ez nem lehetséges, ha már közzétettek valamit a platformon. Az **egymásnak ellentmondó információk** miatt a felhasználók bizonytalanok abban, hogy hogyan rendelkezhetnek adataik nyilvánosságáról.

Összefoglalás – A hierarchia hiánya (I. melléklet, az ellenőrző lista 4.5.1. pontja)

71. Hasonló hatások léphetnek fel, mint az **egymásnak ellentmondó információk** és az **érzelmi befolyásolás** esetében, ha az információ megjelenítése nem követ egy belső rendszert vagy valamiféle hierarchiát. Az adatvédelemre vonatkozó, **hierarchiát nélkülöző** információk akkor fordulnak elő, ha az információk több helyen is feltűnnek, és többféleképpen kerülnek bemutatásra. A felhasználókat valószínűleg összezavarja ez a redundancia, és nem értik teljesen, hogyan kezelik adataikat, és hogyan rendelkezhetnek azok felett. Ez a felépítés megnehezíti az információk megértését, mivel a teljes kép nem könnyen hozzáférhető. A következő példában ismertetetthez hasonló esetekben ez sérti az általános adatvédelmi rendelet 12. cikkének (1) bekezdése szerinti, az érthetőségre és könnyű hozzáférhetőségre vonatkozó követelményeket.

13. példa: Az érintettek jogaival kapcsolatos információk az adatvédelmi nyilatkozatban találhatóak. Bár az érintettek különböző jogait a „**Választási lehetőségeid**” című szakasz ismerteti, a panasz benyújtásához való jogot és a pontos kapcsolattartási címet csak több, különböző témákkal foglalkozó szakasz és réteg után tüntetik fel. Az adatvédelmi nyilatkozat ezért részben kihagyja az elérhetőségi adatokat azokban a szakaszokban, ahol ez kívánatos és tanácsos lenne.

72. A **hierarchia hiánya** akkor is megjelenhet, ha az adott információ oly módon van strukturálva, ami megnehezíti a felhasználók számára a tájékozódást, amint azt az alábbi példa mutatja.

14. példa: Az adatvédelmi szabályzat nincsen különböző főcímekekkel és tartalommal rendelkező szakaszokra osztva. A szabályzat több mint 70 oldalból áll. A weboldalon azonban nincs navigációs menü oldalt vagy a tetején, amely lehetővé tenné a

felhasználók számára, hogy könnyen hozzáférjenek az általuk keresett szakaszhoz. A 67. oldalon található lábjegyzetben magyarázat található a szolgáltató által megalkotott „létrehozási adatok” kifejezésre.

Sötétben hagyás – Félreérthető megfogalmazás vagy tájékoztatás (I. melléklet, az ellenőrző lista 4.6.3. pontja)

73. Még ha a szóhasználat nem is nyíltan ellentmondásos, a felhasználók tájékoztatása során problémák merülhetnek fel a kétértelmű és homályos kifejezések használatából. Ilyen tájékoztatás mellett a felhasználók valószínűleg bizonytalanok maradnak az adatkezelés módját, illetve azt illetően, hogy miként rendelkezhetnek az adatok felett. Ha feltételezhető, hogy az átlagos felhasználók különleges ismeretek nélkül nem értik a tájékoztatás valódi üzenetét, az általános adatvédelmi rendelet 12. cikkének (1) bekezdésében foglalt feltételek nem teljesülnek. Így aztán a **félreérthető megfogalmazás vagy tájékoztatás** használata ellentétes lehet az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában foglalt tisztességes eljárás elvével, mivel az információk nem tekinthetők átláthatónak, ami lehetetlenné teszi az érintettek számára, hogy megértsék személyes adataik kezelését, illetve hogy jogaikat gyakorolják.

15. példa: Az adatvédelmi nyilatkozat homályos és pontatlan módon írja le az adatkezelés egy részét, mint ebben a mondatban: „Az Ön adatait felhasználhatjuk szolgáltatásaink javítására.” Emellett a személyes adatokhoz való hozzáférés joga az általános adatvédelmi rendelet 15. cikkének (1) bekezdése alapján alkalmazandó az adatkezelésre, de ez oly módon kerül említésre, hogy a felhasználók számára nem egyértelmű, hogy mihez teszi lehetővé számukra a hozzáférést: „Az információk egy részét megtekintheted a fiókodban és a platformon közzétett üzeneteid áttekintésével.”

74. A példában a feltételes mód („felhasználhatjuk”) használata miatt a felhasználók nem biztosak abban, hogy adataikat felhasználják-e az adatkezeléshez vagy sem. A „szolgáltatások” kifejezés valószínűleg túl általános ahhoz, hogy „világosnak” minősüljön. Emellett nem világos, hogy hogyan fogják kezelni az adatokat a szolgáltatások javítása érdekében. Az Európai Adatvédelmi Testület emlékeztet arra, hogy a feltételes mód vagy a homályos megfogalmazás használata nem minősül „világos és közérthető megfogalmazásnak”, amint azt az általános adatvédelmi rendelet 12. cikke (1) bekezdésének első mondata előírja, és csak akkor alkalmazható, ha az adatkezelők bizonyítani tudják, hogy ez nem veszélyezteti a tisztességes adatkezelést⁴².

Összszavarás – Nyelvi akadályok (I. melléklet, az ellenőrző lista 4.5.4. pontja)

75. Amennyiben az online szolgáltatásokat bizonyos tagállamok lakosai számára kínálják és címezték, az adatvédelmi nyilatkozatokat ezeken a nyelveken is fel kell ajánlani⁴³. Ebben az összefüggésben fontos, hogy egy adott nyelv kiválasztása manuálisan is megváltoztatható legyen, és megszakítás nélkül, folyamatosan alkalmazható legyen. Ha ezek a kritériumok nem teljesülnek, az érintettek **nyelvi akadályokkal** szembesülnek, így nem érthetik meg az adatvédelemmel kapcsolatos tájékoztatást. A felhasználók akkor találják magukat szembe ezzel a megtévesztő tervezési megoldással, ha az adatvédelmi információkat nem annak az országnak a hivatalos nyelvein biztosítják számukra, mint

⁴² Lásd az átláthatóságról szóló iránymutatás 12. pontját, beleértve a „Példák a helytelen gyakorlatra” című szövegdobozt, valamint a 13. pontot.

⁴³ Lásd az átláthatóságról szóló iránymutatás 13. pontját és 15. lábjegyzetét.

ahol élnek, miközben a szolgáltatást ezen a nyelven nyújtják. Ha a felhasználók nem ismerik azt a nyelvet, amelyen az adatvédelmi információkat biztosítják, azokat nem fogják tudni könnyen elolvasni, ezért nem lesznek tisztában személyes adataik kezelésének módjával. Fontos megjegyezni, hogy a **nyelvi akadályok** összezavarhatják a felhasználókat, és olyan beállítási környezetet hozhatnak létre, amelynek használatát nem értik. Ez a megtévesztő tervezési megoldás különböző módokon jelenhet meg, amint az ezen iránymutatásban is látható lesz.

16. példa:

„A” változat: A közösségimédia-platform elérhető a felhasználók által választott nyelven, horvátul (vagy spanyolul, annak az országnak a nyelvén, amelyben tartózkodnak), míg az adatvédelemmel kapcsolatos információk vagy azok egy része csak angolul.

„B” változat: Valahányszor a felhasználók felkeresnek bizonyos oldalakat, például a sűgóoldalt, ezek automatikusan átváltanak annak az országnak a nyelvére, amelyben a felhasználók tartózkodnak, még akkor is, ha korábban más nyelvet választottak.

76. Az „A” változat azt az esetet szemlélteti, amikor nem áll rendelkezésre információ az érintett által nyilvánvalóan beszélt nyelven. Ez azt jelenti, hogy nem tudja elolvasni az információkat, és következésképpen nem értheti, hogyan kezelik személyes adatait. A tájékoztatás nem tekinthető érthetőnek az általános adatvédelmi rendelet 12. cikkének (1) bekezdésében előírtak szerint. Az érthető nyelven történő adatvédelmi tájékoztatás hiánya miatt nem tekinthető úgy, hogy az érintettek megkapták az általános adatvédelmi rendelet 13., illetve 14. cikkében előírt információkat.
77. A „B” változat azt az esetet írja le, amikor az adatvédelmi információkat tartalmazó oldalakat a felhasználók egyértelmű nyelvválasztása ellenére alapértelmezés szerint a lakóhelyük szerinti ország nyelvén jelenítik meg. Ez azt jelenti, hogy a felhasználóknak minden alkalommal újra meg kell határozniuk nyelvi preferenciájukat, amikor egy adatvédelmi információs oldalra lépnek. Ez tisztességtelen gyakorlatnak tekinthető az érintettekkel szemben, és hozzájárulhat az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában foglalt tisztességes eljárás elvének megsértéséhez.

ii. Interfészalapú megoldások

78. Egyes esetekben a közösségimédia-szolgáltatók sajátos gyakorlatokat alkalmaznak adatvédelmi beállításaik bemutatására. A regisztrációs folyamat során a felhasználók számára rengeteg információt és különböző adatvédelmi beállítást nyújtanak. Annak biztosítása érdekében, hogy a platform használata során bármikor megtalálhassák ezeket a beállításokat és módosításokat hajthassanak végre, a beállításoknak könnyen hozzáférhetőnek és releváns információkkal társítottaknak kell lenniük, hogy a felhasználók tájékoztatáson alapuló döntést hozhassanak. A „könnyen hozzáférhető” elem azt jelenti, hogy az érintetteknek nem kell keresniük a tájékoztatást. Ami az adatvédelmi szabályzatokat illeti, a 29. cikk szerinti munkacsoport már megállapította, hogy az olyan elhelyezés vagy színsémák, amelyek a szöveget vagy a hivatkozást kevésbé észrevehetővé, vagy nehezen megtalálhatóvá teszik egy weboldalon, nem tekinthetők könnyen hozzáférhetőnek⁴⁴.

⁴⁴ Lásd az átláthatóságról szóló iránymutatás 11. pontját.

Túlterhelés – Adatvédelmi útvesztő (I. melléklet, az ellenőrző lista 4.1.2. pontja)

79. Az átláthatóságról szóló iránymutatás szerint az adatvédelmi nyilatkozatnak könnyen hozzáférhetőnek, azaz a weboldalon egyetlen kattintással elérhetőnek kell lennie⁴⁵. A többszintű megközelítés módszerének alkalmazása segíthet érthetően bemutatni az adatvédelmi tájékoztatót az általános adatvédelmi rendelet 12. cikkének (1) bekezdése értelmében⁴⁶. Ez azonban nem eredményezheti azt, hogy szükségtelenül megnehezíti a fontos funkciók vagy jogok gyakorlását egy számtalan rétegből álló, összetett adatvédelmi szabályzat biztosítása révén, amely megtévesztő tervezési megoldást (**adatvédelmi útvesztő**) eredményezne. Ez a megoldás annak felel meg, hogy egy információ vagy adatvédelmi beállítás különösen nehezen megtalálható, mivel a felhasználóknak számos oldalon kell átnavigálniuk anélkül, hogy átfogó és kimerítő áttekintést kapnának. Ez valószínűsíthetően azt eredményezi, hogy a felhasználók nem veszik észre a vonatkozó információkat/beállításokat, vagy felhagynak a kereséssel. A többszintű elrendezés célja, hogy elősegítse az olvashatóságot és tájékoztatást nyújtson az érintetti jogok gyakorlásáról, nem pedig az, hogy megnehezítse azt. Alapvető fontosságú annak biztosítása, hogy a felhasználók könnyen követhessék a magyarázatokat.
80. E tekintetben a felhasználók számára legjobb megközelítés nem a mindenki által egységesen alkalmazható megközelítés, és számos kritériumtól függ, például a platform felhasználóinak típusától vagy az alkalmazás általános kialakításától. Amennyiben lehetséges, felhasználók közreműködésével el kell végezni a megvalósított többszintű megközelítés tesztelését, hogy visszajelzést kapjunk a megközelítés hatékonyságának felmérése érdekében. Emiatt nem lehet konkrétan meghatározni a maximálisan megengedett információs rétegek számát. Ezért mindig eseti alapon kell eldönteni, hogy túl sok réteget használnak-e, és nem fordulnak-e elő megtévesztő tervezési megoldások. Minél nagyobb ez a szám, annál inkább feltételezhető, hogy az el fogja tántorítani vagy meg fogja téveszteni a felhasználókat. A rétegek nagy száma csak olyan különleges egyedi esetekben megfelelő, amikor az összetett információkat nem könnyű teljeskörűen biztosítani. Ugyanakkor a többszintű megközelítéssel nem szabad visszaélni, mélyebb rétegekbe rejtve az információkat vagy szükségtelen rétegek hozzáadásával.
81. Ezt azonban másként kell értékelni, amikor a felhasználók jogainak gyakorlásáról van szó. Az általános adatvédelmi rendelet előírja, hogy e jogok gyakorlását mindig biztosítani kell. Ez a keret határozza meg a kapcsolódó funkciókra és a jogok gyakorlására vonatkozó információk bemutatását. Ha a felhasználók élni kívánnak jogaikkal, a lépések számának a lehető legalacsonyabbnak kell lennie. Ennek eredményeként a felhasználóknak a lehető legközvetlenebb módon el kell tudniuk jutni ahhoz a funkcióhoz, amely lehetővé teszi számukra jogaik gyakorlását. A legtöbb esetben az, hogy a felhasználóknak nagyszámú információs rétegen kell átnavigálniuk magukat, mielőtt a funkciók segítségével ténylegesen gyakorolhatják jogaikat, visszatartja őket e jogok gyakorlásától. Ha ez számos lépést vesz igénybe, a közösségimédia-szolgáltatónak képesnek kell lennie annak bizonyítására, hogy ez milyen előnyökkel jár a felhasználók mint az általános adatvédelmi rendelet szerinti érintettek számára. Az érintettek jogainak az adatvédelmi nyilatkozatban az általános adatvédelmi rendelet 13. cikke (2) bekezdésének b), c) és d) pontjában előírtak szerinti ismertetése mellett a jogok gyakorlásának e tájékoztatótól függetlenül is hozzáférhetőnek kell lennie. Például lehetővé kell tenni a felhasználók számára, hogy a platform menüjén keresztül is gyakorolhassák az érintetti jogokat.

⁴⁵ Lásd az átláthatóságról szóló iránymutatás 11. pontjában szereplő példát.

⁴⁶ A digitális környezetben alkalmazott többszintű megközelítésre vonatkozó részleteket lásd az átláthatóságról szóló iránymutatás 35–37. pontjában.

17. példa: A közösségimédia-szolgáltató a platformján elérhetővé tesz egy „*hasznos tanácsok*” elnevezésű dokumentumot, amely az érintettek jogainak gyakorlásáról is tartalmaz fontos információkat. Az adatvédelmi szabályzat azonban nem tartalmaz erre a dokumentumra mutató hivatkozást vagy más utalást. Ehelyett megemlíti, hogy további részletek a weboldal „Kérdések és válaszok” részében található. A felhasználók, akik az adatvédelmi irányelvekben várnak tájékoztatást a jogaikról, nem találják meg ezeket a magyarázatokat, ezért tovább kell böngészniük, és át kell nézniük a „Kérdések és válaszok” részt.

82. Ez a példa egyértelműen az **adatvédelmi útvesztő** megoldás jegyeit viseli magán, amely az általános adatvédelmi rendelet 12. cikkének (2) bekezdésével ellentétben megnehezíti az érintettek jogaira, és különösen azok gyakorlásának módjára vonatkozó további információkhoz való hozzáférést. Ezenkívül, ha az adatvédelmi szabályzat hiányos, az sérti az általános adatvédelmi rendelet 13. cikke (2) bekezdésének b), c) és d) pontját, illetve 14. cikke (2) bekezdésének c), d) és e) pontját is. Míg a részletesebb információk vagy a jogok gyakorlásának közvetlen eszközei egyetlen kattintással elérhetőek lehetnének arról a helytől, ahol azokat az adatvédelmi szabályzat megemlíti, a példában szereplő felhasználóknak a „Kérdések és válaszok” részre kell navigálniuk és át kell nézniük azt, hogy megtalálják a „*hasznos tanácsokat*” tartalmazó dokumentumot.
83. Fontos megjegyezni, hogy még a túl sok réteg⁴⁷ által okozott hatásoknál is erősebb hatások fordulhatnak elő, ha a felhasználók nemcsak több eszközt, hanem több, ugyanazon közösségimédia-platform által biztosított alkalmazást, például speciális üzenetküldő alkalmazásokat is használnak. Az ilyen típusú másodlagos alkalmazást használó felhasználóknak nagyobb akadályokkal és erőfeszítésekkel kell szembenézniük, ha a böngészős verziót vagy az elsődleges alkalmazást kell felkeresniük az adatvédelmi vonatkozású információk megszerzése érdekében. Egy ilyen – nemcsak eszköz-, hanem alkalmazásközi – helyzetben a releváns információknak mindig közvetlenül elérhetőnek kell lenniük, függetlenül attól, hogy a felhasználók hogyan használják a platformot.

Akadályozás – Zsákutca (I. melléklet, az ellenőrző lista 4.4.1. pontja)

84. A jogi követelmények megsértése akkor is bekövetkezhet, ha az általános adatvédelmi rendeletben előírt adatvédelmi információkat további műveletek – például hivatkozásra vagy gombra kattintva – révén teszik elérhetővé. Különösen a hatástalan funkciókhoz vezető, rosszul címzett hivatkozások vagy az interfészek nem következetes kialakítása nem minősíthető tisztességesnek az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja értelmében, mivel ezek megtevesztik a felhasználókat, amikor megpróbálnak bizonyos információkat elérni vagy megpróbálják megadni adatvédelmi preferenciáikat. Ezért minden esetben el kell kerülni az olyan **zsákutcákat**, amelyek esetében a felhasználók a jogaik gyakorlásához szükséges funkciók nélkül maradnak, és amelyek közvetlenül sértik az általános adatvédelmi rendelet 12. cikkének (2) bekezdését, amely kimondja, hogy az adatkezelőnek elő kell segítenie a jogok gyakorlását.

18. példa: Egy közösségimédia-szolgáltató adatvédelmi szabályzatában számos hiperhivatkozást kínál olyan oldalakra, amelyek további információkat tartalmaznak bizonyos témákról. Az adatvédelmi szabályzatnak azonban több olyan része is van, amely csak általános kijelentéseket tartalmaz arra vonatkozóan, hogy további információkhoz lehet hozzáférni, anélkül, hogy megmondaná, hol és hogyan.

⁴⁷ Lásd a fenti 81. és 82. pontot.

85. Az adatvédelmi szabályzatot általában olyan dokumentumnak tekintik, amely az általános adatvédelmi rendelet 12., 13. és 14. cikkében meghatározott kötelezettségekkel összhangban központosítja az adatvédelmi kérdésekre vonatkozó valamennyi információt. Ezért biztosítani kell a közösségimédia-platform valamennyi érintett helyére történő átirányítást, hogy a felhasználók rendelkezhessenek adataik felett vagy gyakorolhassák jogait. A fenti 18. példában ez csak részben valósul meg, mivel egyes elemek esetében szerepelnek további információkra mutató hivatkozások, mások esetében azonban nem. Ezeknél a **zsákutca** tervezési megoldás az általános adatvédelmi rendelet 12. cikke (1) bekezdésének megsértését eredményezheti azáltal, hogy egyes adatvédelmi információkat nehezen hozzáférhetővé tesz, vagy az általános adatvédelmi rendelet 12. cikkének (2) bekezdésének megsértését, azáltal, hogy nem segíti elő a jogok gyakorlását.

d. **Bevált gyakorlatok**

Ragadós navigáció: Egy adatvédelemmel kapcsolatos oldal megtekintése során a tartalomjegyzék folyamatosan megjeleníthető a képernyőn, lehetővé téve a felhasználók számára, hogy mindig be tudják tájolni magukat az oldalon, és gyorsan navigálhassanak a tartalomban a horgonyhivatkozásoknak (anchor links) köszönhetően.

Vissza az oldal tetejére: Az oldal alján vagy az ablak alján ragadós elemként el lehet helyezni egy „vissza az oldal tetejére” gombot, hogy megkönnyítse a felhasználók számára az oldalon való navigációt.

Hivatkozások: A fogalom meghatározást lásd az 1. használati esetről (22. o.). *(pl. az adatvédelmi nyilatkozatban minden egyes adatvédelmi információhoz olyan hivatkozásokat kell beszúrni, amelyek közvetlenül a közösségimédia-platform kapcsolódó adatvédelmi oldalaira irányítanak).*

Elérhetőségek: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

A felügyeleti hatóság elérése: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

Az adatvédelmi szabályzat áttekintése: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

Változásfigyelés és összehasonlítás: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

Koherens megfogalmazás: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

Fogalom meghatározások: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

Példák használata: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

2b. használati eset: Az érintett tájékoztatása a közös adatkezelésről, az általános adatvédelmi rendelet 26. cikkének (2) bekezdése

a. **A kontextus és a vonatkozó jogi rendelkezések leírása**

86. Az általános adatvédelmi rendelet 26. cikke (2) bekezdésének második mondata további átláthatósági rendelkezéseket ír elő a közös adatkezelés sajátos esetében⁴⁸. Ezek biztosítják, hogy a közös

⁴⁸ A közös adatkezelés meghatározását lásd: az általános adatvédelmi rendelet 26. cikke (1) bekezdésének első mondatával összefüggésben értelmezett 4. cikkének 7. bekezdése, valamint az Európai Adatvédelmi Testület 2021. július 7-én elfogadott, az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról szóló 07/2020. sz. iránymutatása, 2.1. verzió, 46–49. pont, elérhető a következő internetcímen:

https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf.

adatkezelési megállapodás lényege az érintettek rendelkezésére álljon⁴⁹. Az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról szóló 07/2020. sz. iránymutatásában az Európai Adatvédelmi Testület azt ajánlja, hogy a lényeg legalább az általános adatvédelmi rendelet 13. és 14. cikkében említett információk valamennyi olyan elemét foglalja magában, amelyeknek már hozzáférhetőnek kell lenniük az érintett számára, és a megállapodásnak ezen elemek mindegyikére vonatkozóan meg kell határozni, hogy melyik közös adatkezelő felelős az ezen elemeknek való megfelelés biztosításáért⁵⁰. A megállapodás lényegének részeként a kapcsolattartót is meg kell adni, amennyiben kijelöltek ilyet. A közös adatkezelők feladata eldönteni, hogy mi a leghatékonyabb módja annak, hogy a megállapodás lényegét az érintettek rendelkezésére bocsássák⁵¹.

b) Megtévészto tervezési megoldások

19. példa: Ami a megtévészto tervezési megoldásokat illeti, e konstellációban az adatkezelők számára kihívást jelent, hogy ezeket az információkat oly módon integrálják az online rendszerbe, hogy könnyen észlelhetők legyenek, és ne veszítsék el egyértelműségüket és érthetőségüket, annak ellenére, hogy az általános adatvédelmi rendelet 12. cikke (1) bekezdésének első mondata nem hivatkozik közvetlenül az általános adatvédelmi rendelet 26. cikke (2) bekezdésének második mondatára. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja és (2) bekezdése szerinti tisztességes eljárás, átláthatóság és elszámoltathatóság adatvédelmi elvei miatt azonban hasonló követelmények vonatkoznak a közös adatkezelés esetére is. Ha a közös adatkezelők adatvédelmi nyilatkozatban tájékoztatnak a megállapodás lényegéről, ezt is világos és átlátható módon kell megtenniük. Ezért az adatkezelés már nem tekinthető tisztességesnek, ha a kezeléssel kapcsolatos információk nehezen érthetők meg, mert nem biztosítottak hivatkozásokat hozzájuk, vagy az információk több információs terület között oszlanak meg. Az **adatvédelmi útvesztő**⁵² elnevezésű megtévészto tervezési megoldás még zavaróbb lehet, mint amikor egy adatvédelmi nyilatkozatban fordul elő, mivel a felhasználók arra számíthatnak, hogy az általános adatvédelmi rendelet 26. cikke (2) bekezdésének második mondata szerinti információkat egyben kapják meg. Egy közösségimédia-szolgáltató az adatvédelmi szabályzatban mindig „*létrehozási adatokra*” hivatkozik, és nem használja a személyes adat kifejezést. A többszintű adatvédelmi nyilatkozat csak a 90. oldalon tartalmazza azt a magyarázatot, miszerint „*a létrehozási adatok magukban foglalhatják a felhasználók személyes adatait*”. Az érintettek rendelkezésére bocsátott közös adatkezelési megállapodás lényege szintén használja a „*létrehozási adatok*” kifejezést, magyarázat nélkül. A másik közös adatkezelő (B) a személyes adatok fogalmát saját adatvédelmi szabályzatában határozza meg. Az adatvédelmi szabályzatnak a közösségimédia-szolgáltatóval való közös adatkezelésről szóló részében azonban „B” csak a közösségimédia-szolgáltató által biztosított megállapodásra mutató hivatkozást adja meg, egyéb magyarázat nélkül.

⁴⁹ Lásd az Európai Adatvédelmi Testületnek az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról szóló 07/2020. sz. iránymutatásának 179. pontját.

⁵⁰ Lásd az Európai Adatvédelmi Testületnek az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról szóló 07/2020. sz. iránymutatásának 180. pontját, a következő mondat esetében is.

⁵¹ Lásd az Európai Adatvédelmi Testületnek az adatkezelő és az adatfeldolgozó GDPR szerinti fogalmáról szóló 07/2020. sz. iránymutatásának 181. pontját.

⁵² Lásd fent a 2a. használati esetet, az ezen iránymutatásban szereplő 17. példában.

87. Az általános adatvédelmi rendelet 26. cikke (2) bekezdésének második mondata szerinti magyarázatokat nehezebb megérteni, ha azok nem koherensek. Ez az inkoherenciahatás felerősödik, ha a közösségimédia-platformok olyan, saját maguk által létrehozott terminológiát használnak, amelyet a felhasználók általában nem társítanak a személyes adatok kezeléséhez, amint azt a fenti 19. példa mutatja. A példában mindkét közös adatkezelő megsérti az általános adatvédelmi rendelet 26. cikke (2) bekezdésének második mondatát, valamint az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontját, mivel a közös adatkezelésről szolgáltatott információk nem egyértelműek, és ezért nem átláthatóak az érintettek számára.

2c. használati eset: Az érintett tájékoztatása az adatvédelmi incidensről

a. A kontextus és a vonatkozó jogi rendelkezések leírása

88. Az adatvédelmi incidens azonosításához és kezeléséhez az adatkezelőnek képesnek kell lennie arra, hogy felismerje azt⁵³. Az általános adatvédelmi rendelet 4. cikkének 12. bekezdése értelmében „adatvédelmi incidens” „a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi”. Ami a közösségimédia-adatkezelőket illeti, adatvédelmi incidensek többféleképpen is bekövetkezhetnek. Például, ha egy támadó hozzáfér a személyes adatokhoz és a felhasználók csevegési üzeneteihez. Vagy ha programozási hiba miatt egy alkalmazás a felhasználók által megadott engedélyek hatókörén kívül is hozzáférhet a személyes adatokhoz. Egy másik példa, ha a felhasználók a „legjobb barátaimmal való megosztás” beállítás keretében képeket osztanak meg, de képeiket az emberek szélesebb köre számára is elérhetővé teszik. Végül, ha például egy programhiba lehetővé teszi egy valós idejű videomegosztáson alapuló közösségimédia-platform számára, hogy a tartalom streamelését továbbra is megossa annak ellenére, hogy a felhasználó korábban megnyomta a felvételt leállító gombot.
89. Adatvédelmi incidens esetén az adatkezelőnek minden esetben értesítenie kell az általános adatvédelmi rendelet 33. cikke szerinti illetékes felügyeleti hatóságot, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jelent kockázatot a természetes személyek jogaira és szabadságaira nézve. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek az általános adatvédelmi rendelet 34. cikkének (1) és (2) bekezdésével összhangban általában tájékoztatnia kell az érintetteket az incidensről. Ebben az esetben az adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintetteket. Ennek a tájékoztatásnak világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, mivel az általános adatvédelmi rendelet 12. cikke is alkalmazandó. Ezen túlmenően ezen tájékoztatásnak legalább a következő információkat és intézkedéseket kell tartalmazniuk (lásd az általános adatvédelmi rendelet 33. cikke (3) bekezdésének b)–d) pontja, az általános adatvédelmi rendelet 34. cikkének (2) bekezdésével együtt értelmezve):
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei,
 - az adatvédelmi incidensből eredő, valószínűsíthető következmények ismertetése, valamint

⁵³ Lásd még az Európai Adatvédelmi Testület 2021. december 14-én elfogadott, az adatvédelmi incidensek bejelentésével kapcsolatos példákra szóló 01/2021. sz. iránymutatását, 2.0. verzió, 4. pont, elérhető a következő internetcímen:

https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_hu.pdf.

- az adatkezelő által az incidens orvoslására tett vagy tervezett intézkedések ismertetése, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is⁵⁴.

90. Az ilyen, adatvédelmi incidensekről szóló, az általános adatvédelmi rendelet 34. cikke szerinti tájékoztatás szintén magában foglalhat megtévesztő tervezési megoldásokat. Ilyen például, ha az érintett adatkezelő minden szükséges információt megad az érintetteknek ahhoz, hogy tájékoztassa őket az adatvédelmi incidens kiterjedéséről, de emellett általános és irreleváns információkat, valamint a következményeket és az adatkezelő által hozott vagy javasolt óvintézkedéseket is közli velük. Ez a részben irreleváns információ félrevezető lehet, és előfordulhat, hogy a jogsértés által érintett felhasználók nem értik meg teljes mértékben a jogsértés következményeit, vagy alábecsülik a (potenciális) hatásokat.

b) Megtévesztő tervezési megoldások

91. Hogy felvázoljunk néhány negatív példát, az adatvédelmi incidensekről szóló értesítésekkel kapcsolatos, az általános adatvédelmi rendelet 12. cikkével összefüggésben értelmezett 34. cikkét sértő jogellenes gyakorlatok az alábbiak szerint fordulhatnak elő:

i. Tartalomalapú megoldások

Sötétben hagyás – Egymásnak ellentmondó információk (I. melléklet, az ellenőrző lista 4.6.2. pontja)

20. példa:

- Az adatkezelő csak egy harmadik fél intézkedéseire hivatkozik, miszerint az adatvédelmi incidenst harmadik fél (pl. egy adatfeldolgozó) okozta, és ezért nem történt adatvédelmi incidens. Az adatkezelő kihangsúlyoz néhány olyan bevált gyakorlatot is, amelyeknek semmi közük az aktuális incidenshez.
- Az adatkezelő az adatvédelmi incidens súlyosságáról saját maga vagy az adatfeldolgozó vonatkozásában, nem pedig az érintett vonatkozásában nyilatkozik.

Sötétben hagyás – Félreérthető megfogalmazás vagy tájékoztatás (I. melléklet, az ellenőrző lista 4.6.3. pontja)

92. Ami az érintettek incidenssel kapcsolatos tájékoztatásának nyelvezetét illeti, alapvető fontosságú, hogy az adatkezelők szem előtt tartsák: a legtöbb címzett nincs hozzászokva az adatvédelemhez kapcsolódó sajtóságos, esetleg technikai vagy jogi jellegű nyelvezethez.

21. példa: Egy közösségimédia-platfomon előforduló adatvédelmi incidens révén számos egészségügyi adatsor vált véletlenül hozzáférhetővé illetéktelen felhasználók számára. A közösségimédia-szolgáltató csak arról tájékoztatja a felhasználókat, hogy „*a személyes adatok különleges kategóriái*” véletlenül nyilvánosságra hozták.

93. Ez **félreérthető megfogalmazást** jelent, mivel az átlagfelhasználók nem értik a „*személyes adatok különleges kategóriái*” kifejezést, és ezért nem tudják, hogy egészségügyi adataik szivárogtak ki. Ez

⁵⁴ A 29. cikk szerinti munkacsoport adatvédelmi incidensek bejelentéséről szóló iránymutatása – az Európai Adatvédelmi Testület által jóváhagyva, 20. pont; <https://ec.europa.eu/newsroom/article29/items/612052/en>.
Elfogadott

annak tudható be, hogy a „különleges” kifejezés a hétköznapi nyelvben nagyon eltérő jelentéssel bír, mint az általános adatvédelmi rendelethez kapcsolódó szűk nyelvhasználatban. Az átlagos felhasználók nem tudják, hogy az általános adatvédelmi rendelet 9. cikkének (1) bekezdése szerint a „személyes adatok különleges kategóriái” közé a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok tartoznak. Így a „személyes adatok különleges kategóriái” megnevezés megtévesztő tervezési megoldásnak minősül ebben a forgatókönyvben, mivel félrevezeti a felhasználókat, hiszen nem kísérik további magyarázatok. Ez arra a helyzetre példa, amikor az adatkezelő megpróbálja tájékoztatni az érintetteket az incidensről, de nem tesz teljes mértékben eleget az általános adatvédelmi rendelet 34. cikke szerinti, az adatvédelmi incidensről történő tájékoztatásra vonatkozó kötelezettségének, mivel az átlagos olvasó alábecsüli az incidens súlyosságát. A példában szereplő rövid tájékoztatás emellett nem érthető, amint azt az általános adatvédelmi rendelet 12. cikke (1) bekezdésének első mondatával összefüggésben értelmezett 34. cikke előírja.

94. Egy másik példa a **félreérthető megfogalmazásra** a következő:

22. példa: Az adatkezelő csak homályos részleteket közöl az érintett személyes adatok kategóriáinak meghatározásakor, pl. az adatkezelő a felhasználók által benyújtott dokumentumokra hivatkozik anélkül, hogy meghatározná, hogy ezek a dokumentumok a személyes adatok mely kategóriáit tartalmazzák, és mennyire voltak érzékenyek.

95. Fontos megjegyezni, hogy ez a megtévesztő tervezési megoldás az adatvédelmi incidensről szóló értesítés valamennyi részében előfordulhat. Míg a fent említett két példa az érintett adatkategóriák nem egyértelmű megfogalmazására vonatkozik, a következő példa azt mutatja, hogy az érintettek kategóriája lehet hasonlóképpen nem egyértelmű:

23. példa: Az incidens bejelentésekor az adatkezelő nem határozza meg pontosan az érintett személyek kategóriáját, pl. az adatkezelő csak azt említi, hogy az érintettek diákok voltak, de arról nem szól, hogy az érintettek kiskorúak vagy kiszolgáltatott érintettek csoportjai voltak-e.

96. Végezetül, az incidens súlyosságát is alábecsülhetik, ha az alábbi példához hasonlóan **félreérthető tájékoztatást** adnak:

24. példa: Az adatkezelő – amikor értesíti a felügyeleti hatóságot és az érintettet az incidensről – úgy nyilatkozik, hogy a személyes adatokat más forrásokból nyilvánosságra hozták. Az érintett ezért úgy véli, hogy nem történt adatvédelmi incidens.

ii. Interfészalapú megoldások

97. Az adatvédelmi incidens bejelentésének negatív példái – az általános adatvédelmi rendeletnek az általános adatvédelmi rendelet 12. cikkével összefüggésben értelmezett 34. cikkével ellentétben – lehetnek interfészalapú megtévesztő tervezési megoldások is, amint azt az alábbiak mutatják:

Átugrás – Figyelemelterelés (I. melléklet, az ellenőrző lista 4.2.2. pontja)

25. példa:

• Az adatkezelő olyan szövegeken keresztül számol be az incidensről, amelyek rengeteg nem releváns információt tartalmaznak, és kihagyják a lényeges részleteket.

• A hozzáférési hitelesítő adatokat és más típusú adatokat érintő biztonsági incidensek esetén az adatkezelő úgy nyilatkozik, hogy az adatok titkosítottak vagy hasheltek, miközben ez csak a jelszavak esetében igaz.

98. Ebben az esetben, még ha a vonatkozó részletek szerepelnek is a jelentésben, az érintettek figyelme valószínűleg elterelődik azokról a nem releváns információk okozta túlterhelés miatt.

c) Bevált gyakorlatok

Értesítések: Az értesítések felhasználhatók arra, hogy felhívják a felhasználók figyelmét a személyes adatok kezelésével kapcsolatos szempontokra, változásokra vagy kockázatokra (*pl. adatvédelmi incidens esetén*). Ezek az értesítések többféle módon is megvalósíthatók, például bejövő üzenetek, felugró ablakok, a weboldal tetején elhelyezett rögzített szalaghirdetések stb. révén.

A következmények magyarázata: Ha a felhasználók egy adatvédelmi ellenőrzést kívánnak be- vagy kikapcsolni, vagy hozzájárulásukat akarják adni vagy vissza kívánják vonni azt, semleges módon kell tájékoztatni őket az ilyen intézkedések következményeiről.

Hivatkozások: A fogalom meghatározást lásd az 1. használati esetről (22. o.) (*pl. hivatkozás biztosítása a felhasználók számára a jelszó visszaállításához*).

Koherens megfogalmazás: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

Fogalom meghatározások: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

Példák használata: A fogalom meghatározást lásd az 1. használati esetről (22. o.).

3.3 Védettség a közösségi médiában

3a. használati eset: A hozzájárulás kezelése a közösségimédia-platform használata során

a. A kontextus és a vonatkozó jogi rendelkezések leírása

99. A közösségimédia-platformok felhasználóinak az adatkezelési tevékenységek különböző szakaszaiban – például a személyre szabott hirdetések fogadása előtt – hozzájárulásukat kell adniuk. Amint azt az Európai Adatvédelmi Testületnek a közösségi média felhasználóinak megcélzásáról szóló iránymutatása is kifejtette, a hozzájárulás csak akkor lehet megfelelő jogalap, ha az érintett ellenőrzési és tényleges választási lehetőséget kap⁵⁵. Ezenkívül az általános adatvédelmi rendelet 4. cikkének 11. pontja szerint a hozzájárulásnak konkrétan, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie⁵⁶. Fontos hangsúlyozni, hogy az általános adatvédelmi rendelet szerinti érvényes hozzájárulásra vonatkozó követelmények nem jelentenek további kötelezettséget, hanem a felhasználók személyes adatai jogszerű kezelésének előfeltételei. Ezenkívül az online marketing vagy az online nyomkövetési módszerek esetében a 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) alkalmazandó. Az elektronikus hírközlési adatvédelmi irányelv szerinti érvényes

⁵⁵ Lásd az Európai Adatvédelmi Testületnek a közösségi média felhasználóinak megcélzásáról szóló 08/2020. számú iránymutatásának 51. pontját.

⁵⁶ Lásd még a fenti 25–29. pontot.

hozzájárulás előfeltételei azonban megegyeznek az általános adatvédelmi rendelet hozzájárulásra vonatkozó rendelkezéseivel⁵⁷.

100. Tekintettel az általános adatvédelmi rendelet 5. cikkének (2) bekezdésében meghatározott elszámoltathatóság elvére, valamint arra, hogy az adatkezelőnek képesnek kell lennie annak bizonyítására, hogy az érintettek hozzájárultak személyes adataiknak az általános adatvédelmi rendelet 7. cikkének (1) bekezdése szerinti kezeléséhez, alapvető fontosságú, hogy a közösségimédia-szolgáltató bizonyítani tudja, hogy megfelelően gyűjtötte a felhasználók hozzájárulását. Ezt a feltételt nehéz lehet bizonyítani, pl. ha a felhasználóknak a süti (cookie-k) elfogadásával kell megadniuk hozzájárulásukat. Ezenkívül előfordulhat, hogy az érintettek nem mindig tudják, hogy hozzájárulásukat adják, miközben gyorsan rákattintanak egy kiemelt gombra vagy az előre kijelölt opciókra. Mindazonáltal, amint azt az általános adatvédelmi rendelet 7. cikkének (1) bekezdése hangsúlyozza, a felhasználók önkéntes hozzájárulásának bizonyítási terhe az adatkezelőre hárul.

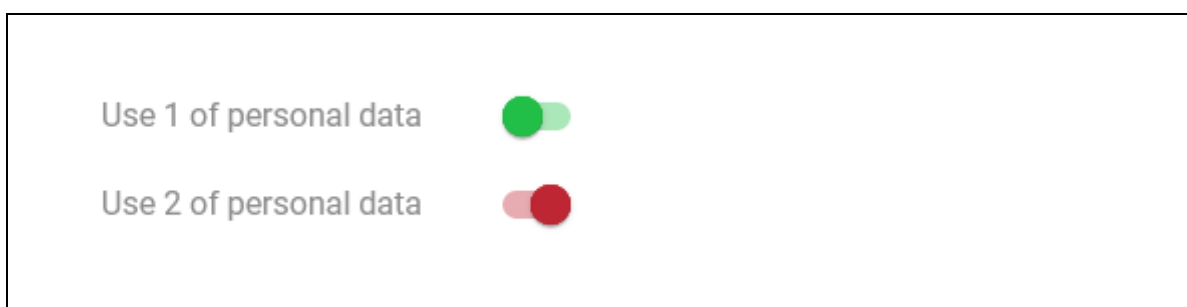
b. Megtévesztő tervezési megoldások

i. Tartalomalapú megoldások

101. A korábban már kifejtett tartalomalapú megoldásokon kívül, amelyek a hozzájárulási kérelemmel kapcsolatos információkra vonatkozhatnak⁵⁸, a hozzájárulással kapcsolatban két további tartalomalapú megtévesztő tervezési megoldás fordulhat elő.

Egymásnak ellentmondó információk – Sötétben hagyás (1. melléklet, az ellenőrző lista 4.6.2. pontja)

26. példa: Az interfész egy váltókapcsolót használ, lehetővé téve a felhasználók számára a hozzájárulás megadását vagy visszavonását. A kapcsoló kialakításának módja azonban nem teszi egyértelművé, hogy melyik helyzetben van, és hogy a felhasználó hozzájárulását adta-e vagy sem. A kapcsoló helyzete valójában nem passzol a színével. Ha a kapcsoló a jobb oldalon van, ami általában a funkció aktiválásához („bekapcsolás”) kapcsolódik, a kapcsoló színe piros, ami általában azt jelenti, hogy a funkció ki van kapcsolva. Ezzel szemben, amikor a kapcsoló a bal oldalon van, ami általában azt jelenti, hogy a funkció ki van kapcsolva, a kapcsoló háttérszíne zöld, ami általában aktív opciót jelent.



⁵⁷ Lásd a 2002/58/EK irányelv 2. cikkének f) pontját, valamint az Európai Adatvédelmi Testület 5/2019. sz. véleményét az elektronikus hírközlési adatvédelmi irányelv és az általános adatvédelmi rendelet közötti kölcsönhatásról, különösen az adatvédelmi hatóságok illetékessége, feladatai és hatásköre tekintetében, elfogadva 2019. március 12-én, 14. pont, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_hu.

⁵⁸ Lásd az 1. használati esetet (32–49. pont) vagy a 1. használati eset mellékletben felsorolt példáinak számait.

102. Az **egymásnak ellentmondó információk** megadása a hozzájárulás megszerzésekor homályossá és érthetlenné teszi az információkat. A fenti példa egy olyan esetet szemlélteti, amikor a vizuális információ kétértelmű. Amikor ilyen kapcsolókkal találkozunk, a felhasználók bizonytalanok abban, hogy hozzájárulásukat adták-e vagy sem. Az általános adatvédelmi rendelet 4. cikkének (11) pontjával összefüggésben értelmezett 7. cikkének (2) bekezdése értelmében a hozzájárulás nem tekinthető egyértelműnek, ha a vizuális jelöléseket oly módon cserélik fel, vagy olyan színekben jelenítik meg, amelyek ellentmondanak a tényleges beállításnak – lásd a 26. példát, amely csak egy zavaros illusztrációt tartalmaz a kapcsolókról –, az nem tekinthető egyértelműnek. **Egymásnak ellentmondó információk** szöveges úton is megadhatók, amint az lentebb látható.

27. példa: A közösségimédia-szolgáltató ellentmondásos információkat szolgáltat a felhasználóknak: bár a tájékoztatás először azt állítja, hogy névjegyeiket hozzájárulásuk nélkül nem importálják, egy felugró tájékoztató ablak egyidejűleg elmagyarázza, hogy a névjegyek mégis importálásra kerülnek.

Akadályozás – Megtévesztő tevékenység (I. melléklet, az ellenőrző lista 4.4.3. pontja)

103. Amellett, hogy **egymásnak ellentmondó információkat** bocsátanak rendelkezésre, az adatkezelők olyan információkat is közzétehetnek, amelyek azáltal tévesztik meg a felhasználókat, hogy nem felelnek meg az elvárásaiknak. **Megtévesztő tevékenységnek** azt nevezzük, ha a felhasználók rendelkezésére álló információk és tevékenységek közötti eltérés arra készíti őket, hogy megtegyenek valamit, amit egyébként nem akartak megtenni. A felhasználók elvárásai és a kapott információk közötti különbség visszatárhathatja őket attól, hogy folytassák a műveletet.

28. példa: A felhasználó közösségimédia-hírfolyamát böngészi. Ennek során reklámokat jelenítenek meg számára. Egy hirdetés felkeltette az érdeklődését, és kíváncsi arra, hogy az oldal miért mutatja azt neki, ezért a hirdetés jobb alsó sarkában található „?” jelre kattint. Ez megnyit egy felugró ablakot, amely megmagyarázza, hogy a felhasználó miért látja ezt a konkrét hirdetést, és felsorolja a célkiválasztási kritériumokat. Arról is tájékoztatja, hogy visszavonhatja a célzott hirdetésekhez való hozzájárulását, és egy erre mutató hivatkozást is tartalmaz. Amikor a felhasználó rákattint erre a hivatkozásra, az átirányítja őt egy teljesen másik weboldalra, amely általános magyarázatot ad arra vonatkozóan, hogy mi a hozzájárulás, és hogyan kell azt kezelni.

104. A fenti eset olyan tartalomra példa, amely nem felel meg a felhasználók elvárásainak. Amikor a felhasználó rákattint a hivatkozásra, azt várja, hogy az majd átirányítja őt egy olyan oldalra, amely lehetővé teszi számára, hogy közvetlenül visszavonja hozzájárulását. Az oldal, ahova ehelyett jut, ezt nem teszi lehetővé számára, és nem határozza meg, hogy milyen konkrét módon vonhatja vissza hozzájárulását a közösségimédia-platfomra. A felhasználó által feltételezetten és ténylegesen talált információk közötti eltérés összezavarja és elbizonytalanítja a további teendők tekintetében. A legrosszabb esetben azt is gondolhatja, hogy nem vonhatja vissza hozzájárulását. A **megtévesztő tevékenységek** nem tekinthetők átláthatónak az általános adatvédelmi rendelet 12. cikkének (1) bekezdésében előírtak szerint. Továbbá, ha a visszavonást a hozzájárulás gyűjtésének módjával hasonlítjuk össze, ez a gyakorlat sértheti az általános adatvédelmi rendelet 7. cikkének (3) bekezdését, ha a hozzájárulás visszavonása nehezebbnek bizonyul, mint a hozzájárulás megadása.

105. Ha a közösségimédia-szolgáltatók arról tájékoztatják a felhasználókat, hogy egy lépésük bizonyos következményekkel járhat, és a lépés valójában más eredményhez vezet, ez **megetvesztő tevékenységnek** minősül, amint azt a következő példa is mutatja.

29. példa: A közösségimédia-fiók azon részében, ahol a felhasználók megoszthatják gondolataikat, képeiket stb., meg kell erősíteniük, hogy meg kívánják-e osztani ezt a tartalmat, miután begépeltek vagy feltöltötték azt. A felhasználók választhatnak egy „Igen, kérem” és egy „Nem, köszönöm” gomb között. Miután azonban a második gombra kattintva úgy döntenek, hogy nem osztják meg a tartalmat másokkal, a tartalom közzétételre kerül közösségimédia-fiókjukon.

106. Az előző példához hasonlóan ez az információ nem átlátható, és elveszi a felhasználóktól a választás lehetőségét. Még ha a felhasználók gyorsan észlelik is a közzétételt, és törlik azt, az adatokat elutasításuk ellenére kezelték, és mások számára elérhetővé tették azokat. Ennél is rosszabb példa, ha az adatkezelés nem vagy csak nehezen vagy információtechnológia ismeretek megléte esetén észlelhető a felhasználók számára, mivel arra a közösségimédia-platform háttérében kerül sor.

ii. Interfészalapú megoldások

107. A fenti két megetvesztő tervezési megoldáson kívül ebben a használati esetben többnyire az interfészalapú megoldások relevánsak.

Átugrás – Figyelemelterelés (I. melléklet, az ellenőrző lista 4.2.2. pontja)

108. Amikor egy adatvédelmi vonatkozású intézkedést vagy információt egy másik, az adatvédelemhez kapcsolódó vagy ahhoz nem kapcsolódó elemmel állítanak versenybe, ha a felhasználók ezt a lehetőséget választják, akkor valószínűleg megfelelnek a másíkról, még akkor is, ha az volt az eredeti szándékuk. Ez az **figyelemelterelés** megetvesztő megoldás, amelyet eseti alapon kell értékelni.

30. példa: A közösségimédia-platform egyik süti bannerje szerint „Egy finom sütihez csak vajra, cukorra és lisztre van szükséged. Tekintsd meg kedvenc receptünket itt: [link]. Mi is használunk süteket. További információk találhatsz a sütikre vonatkozó szabályzatunkban [link].”, mellette egy „OK” gomb található.

109. A humor nem használható fel a potenciális kockázatok valótlan bemutatására és a tényleges információk érvénytelenítésére. Ebben a példában előfordulhat, hogy a felhasználók csak az első linkre kattintanak, elolvassák a süti receptjét, majd rákattintanak az „OK” gombra. Amellett, hogy nem teszi lehetővé a felhasználók számára a hozzájárulás megtagadását, ez a példa jól szemlélteti azt az esetet, amikor a hozzájárulás nem feltétlenül megfelelő tájékoztatáson alapul. Az „OK” gombra kattintva a felhasználók azt gondolhatják, hogy csak a sütikről, mint süttött finomságokról szóló szórakoztató üzenetet csuknak be, és nem veszik figyelembe a „süti” kifejezés technikai jelentését. Ez az eset nem minősül az általános adatvédelmi rendelet 4. cikkének 11. pontjával összefüggésben értelmezett 7. cikkének (2) bekezdése értelmében vett tájékoztatáson alapuló hozzájárulásnak.
110. Az általános adatvédelmi rendelet 7. cikkének (2) bekezdése továbbá kimondja, hogy a hozzájárulás iránti kérelemnek egyértelműen megkülönböztethetőnek kell lennie más ügyektől. Ezért szükséges, hogy az adatvédelmi információkat ne árnyékolják be más összefüggések. Ebben a példában a „süti” homonimákon alapuló szójáték miatt a sütődei kontextus háttérbe szoríthatja az adatvédelmi

kontextust. Ahhoz, hogy az információk egyértelműen megkülönböztethetők legyenek, a felhasználók számára az érvényes hozzájárulás megadásához szükséges releváns információknak feltűnőnek kell lenniük, nem lehetnek **bújtatottan közzétéve**, és nem keveredhetnek más ügyekkel vagy jelentésekkel. Nem szabad összemosni az adatvédelmi információkat és az egyéb tartalmakat, ellenkező esetben a felhasználók figyelme eltérülhet a személyes adataik kezelésének tényleges következményeiről. Ezen előfeltételek megvalósításakor a tervezőknek némi mozgásteret kell biztosítani ahhoz, hogy az információk vonzóvá váljanak.

Akadályozás – Zsákutca (I. melléklet, az ellenőrző lista 4.4.1. pontja)

111. Az összezavarás vagy a figyelem elterelése nem az egyetlen lehetséges hatás, amely a megtévesztő tervezési megoldásokkal elérhető, amikor a hozzájárulásról van szó. Különösképpen, a **zsákutca** megoldás többféle módon befolyásolhatja az általános adatvédelmi rendelet 4. cikkének 11. pontjával összefüggésben értelmezett 7. cikkében meghatározott hozzájárulási feltételeket.

31. példa: A felhasználó kezelni kívánja a közösségimédia-platfornak hozzájárulás alapján adott engedélyeket. A beállítások között meg kell találnia az említett konkrét intézkedésekhez kapcsolódó beállításokban egy oldalt, és le kívánja tiltani személyes adatai kutatási célú megosztását. Amikor a felhasználó ki akarja venni a pipát a jelölőnégyzetből, a felület szintjén semmi sem történik, és azt a benyomása támadhat, hogy a hozzájárulás nem vonható vissza.

112. Ebben a konkrét példában a **zsákutca** megtévesztő megoldás sértheti az általános adatvédelmi rendelet 7. cikkének (3) bekezdését, mivel a felhasználó láthatóan nem tudja visszavonni a személyes adatai kutatási célú kezeléséhez való hozzájárulását, mivel az erre szolgáló eszköz nyilvánvalóan nem működik. Ha a felhasználók tevékenységét nem regisztrálják megfelelően a rendszerben, az általános adatvédelmi rendelet 7. cikke (3) bekezdésének megsértése figyelhető meg. Ha a döntést valójában regisztrálja a rendszer, az a tény, hogy az interfész nem tükrözi a felhasználók tevékenységét, úgy tekinthető, hogy nem felel meg az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában foglalt tisztességes eljárás elvének. Ha egy felület látszólag a hozzájárulás megfelelő kezelésének eszközeit kínálja, lehetővé téve a felhasználók számára a hozzájárulás megadását vagy a korábban adott hozzájárulás visszavonását, de ez a cselekvés semmilyen vizuális hatást nem vált ki, az félrevezető a felhasználó számára, és zavart, sőt frusztrációt okoz. El kell kerülni a rendszer állapota és a felület által továbbított információk közötti eltérést, mivel ez általánosságban akadályozhatja a felhasználókat a személyes adataik feletti rendelkezésben.
113. Számos adatkezelési tevékenység több felet is érint, például egy másik (közös) adatkezelőt vagy adatfeldolgozót a mellett az adatkezelő vagy adatfeldolgozó mellett, akivel az érintett közvetlen kapcsolatban áll.

32. példa: Egy közösségimédia-szolgáltató együttműködik harmadik felekkel felhasználói személyes adatainak kezelése érdekében. Az adatvédelmi szabályzatában anélkül tünteti fel e harmadik felek listáját, hogy hivatkozást biztosítsa azok adatvédelmi szabályzataihoz, és csupán azt mondja a felhasználóknak, hogy keressék fel a harmadik felek weboldalait, hogy tájékozódjanak arról, hogy ezek a szervezetek hogyan kezelik az adatokat, valamint hogy gyakorolják jogaikat.

114. A **zsákutca** megtévesztő tervezési gyakorlat e példája azt mutatja, hogyan nehezítik meg a felhasználók számára az adatkezelésre vonatkozó információkhoz való hozzáférést. Mivel valószínűleg nem kapnak

meg minden releváns információt az adatkezelésről, úgy tekinthető, hogy az ilyen gyakorlat sérti az általános adatvédelmi rendelet 12. cikkének (1) bekezdésében foglalt, a könnyen hozzáférhető formában történő tájékoztatásra vonatkozó követelményeket. Ha ezt a gyakorlatot a hozzájárulás gyűjtésével kapcsolatos tájékoztatás vonatkozásában alkalmazzák, az sértheti a tájékoztatáson alapuló hozzájárulásra vonatkozó, az általános adatvédelmi rendelet 4. cikkének 11. pontjával összefüggésben értelmezett 7. cikkének (2) bekezdésében meghatározott követelményeket, mivel a tájékoztatás elérése túlságosan nehéz lenne, így az érintettek nem lennének teljes mértékben tisztában döntésük következményeivel.

Akadályozás – Indokolatlanul hosszú folyamatok (I. melléklet, az ellenőrző lista 4.4.2. pontja)

115. Az általános adatvédelmi rendelet 7. cikkének (3) bekezdése kimondja, hogy a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását. Az Európai Adatvédelmi Testület az (EU) 2016/679 rendelet szerinti hozzájárulásról szóló 5/2020. sz. iránymutatása tovább részletezi a kérdést, kimondva, hogy a hozzájárulás megadásának és visszavonásának azonos módon kell rendelkezésre állnia. Ez azt jelenti, hogy ugyanazt a felületet kell használni, de azt is jelenti, hogy a hozzájárulás visszavonására szolgáló mechanizmusoknak könnyen hozzáférhetőnek kell lenniük, például egy hivatkozás vagy ikon segítségével, amely a közösségimédia-platform használata során bármikor elérhető.

33. példa: A közösségimédia-szolgáltató nem ad közvetlen lehetőséget a célzott hirdetések céljából történő adatkezelés visszavonásához, noha a hozzájáruláshoz csak egy kattintásra van szükség.

116. A hozzájárulás visszavonásához szükséges idő vagy az ahhoz szükséges kattintások száma felhasználható annak értékelésére, hogy azt valóban könnyű-e elérni. Az ***indokolatlanul hosszú folyamatok*** megtévesztő tervezési megoldásnak a felhasználói útvonal során történő alkalmazása – amint azt a 33. példa mutatja – ellentétes ezekkel az elvekkel, így sérti az általános adatvédelmi rendelet 7. cikkének (3) bekezdését.

Túlterhelés – Adatvédelmi útvesztő (I. melléklet, az ellenőrző lista 4.1.2. pontja)

117. Amint azt a hozzájárulásról szóló 5/2020. sz. iránymutatás kiemeli, az érintettek számára tájékoztatást kell nyújtani a hozzájáruláson alapuló adatkezelésről annak érdekében, hogy tájékoztatáson alapuló döntést hozhassanak⁵⁹. Ennek hiányában a hozzájárulás nem tekinthető érvényesnek. Ugyanez az iránymutatás továbbfejleszti a tájékoztatás ismertetésének módjait, meghatározva, hogy ehhez többszintű tájékoztatás is felhasználható. Ugyanakkor, amint az a 2a. használati esetből⁶⁰ is kiderül, a közösségimédia-szolgáltatóknak ügyelniük kell arra, hogy elkerüljék az ***adatvédelmi útvesztő*** megtévesztő tervezési megoldást, amikor a hozzájárulás iránti kérelemmel kapcsolatos tájékoztatást többszintű módon adják meg. Ha egyes információkat túlságosan nehéz megtalálni, mivel az érintetteknek több oldalon vagy dokumentumon kellene megkeresniük azokat, az ilyen információk biztosításával gyűjtött hozzájárulás nem tekinthető tájékoztatáson alapulónak, ami ellentétes az általános adatvédelmi rendeletnek az általános adatvédelmi rendelet 4. cikkének 11. pontjával

⁵⁹ A hozzájárulásról szóló 5/2020. sz. iránymutatás, 62–64. pont.

⁶⁰ Lásd a fenti 79–81. pontot.

összefüggésben értelmezett 7. cikkével. Következésképpen ez azt jelentené, hogy a hozzájárulás érvénytelen, és a közösségimédia-szolgáltató megsérti az általános adatvédelmi rendelet 6. cikkét.

34. példa: A hozzájárulás visszavonására vonatkozó információk egy olyan hivatkozásról érhetőek el, amely csak a fiókjuk minden egyes részének és a közösségimédia-hírfolyamukon megjelenő hirdetésekhez kapcsolódó információk átnézésével érhető el.

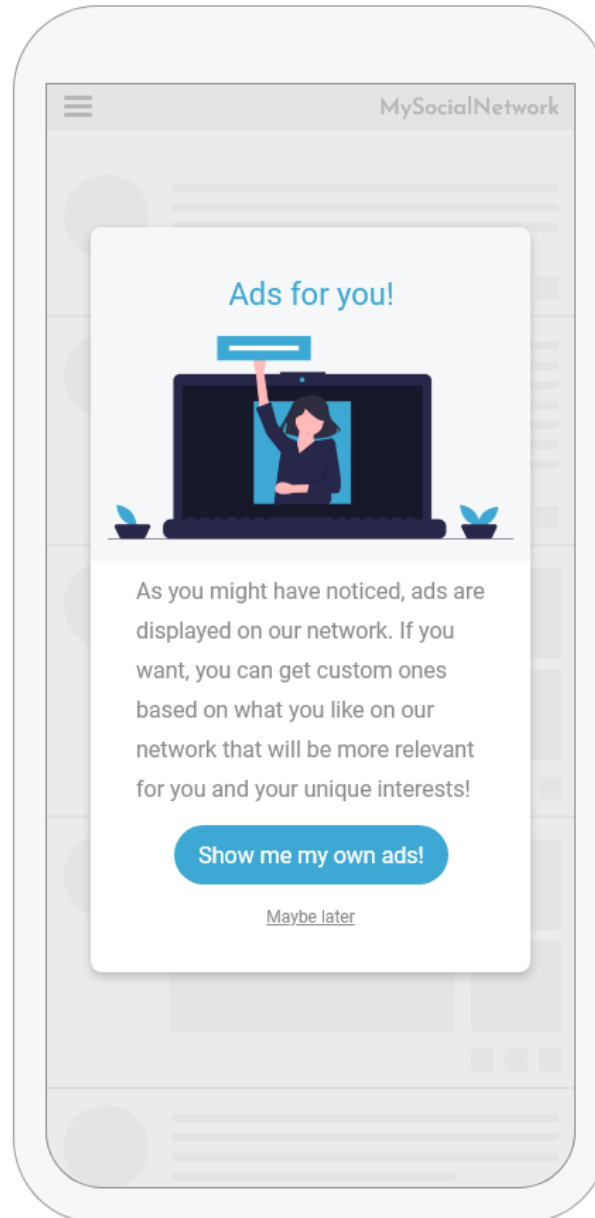
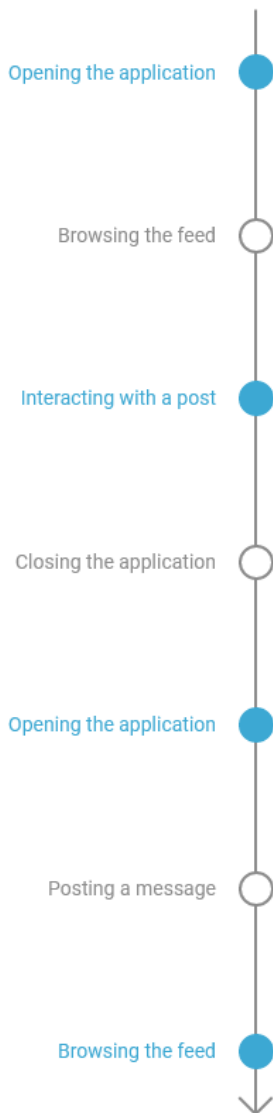
118. Amint azt a fent ismertetett forgatókönyv mutatja, az **adatvédelmi útvesztő** megtévesztő tervezési megoldás a hozzájárulás megszerzését követően is okozhat problémát, ha nem tartja tiszteletben az általános adatvédelmi rendelet 7. cikke (3) bekezdésének negyedik mondatában foglalt feltételt, amely kimondja, hogy a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását. Ez kimondottan annak tudható be, hogy a hozzájárulás visszavonásának folyamata több lépést foglal magában, mint a hozzájárulás megadásának megerősítését kifejező cselekedet. Mivel az adott információ az érintett számára még csak könnyen sem hozzáférhető, hiszen az oldal különböző részein van szétszórva, sérül az általános adatvédelmi rendelet 12. cikkének (1) bekezdésében meghatározott elv.

Túlterhelés – Folyamatos noszogatás (I. melléklet, az ellenőrző lista 4.1.1. pontja)

119. A **folyamatos noszogatás**, ha olyan felhasználók esetében alkalmazzák, akik nem járultak hozzá személyes adataik meghatározott célból történő kezeléséhez, akadályozzák a közösségi média rendszeres használatát. Ez azt jelenti, hogy a felhasználók nem tagadhatják meg a hozzájárulást, így nem is vonhatják vissza anélkül, hogy hátrányt szenvednének. Ez ellentétes a hozzájárulásnak az általános adatvédelmi rendelet 4. cikkének 11. pontjával összefüggésben értelmezett 7. cikke szerinti önkéntesség feltételével, amely szerint a hozzájárulás az érintettek akaratának önkéntes kinyilvánítását jelenti, amellyel beleegyezésüket fejezik ki az őket érintő személyes adatok kezeléséhez. Az általános adatvédelmi rendelet (42) preambulumbekzdésének ötödik mondata azt is kimondja, hogy a hozzájárulás nem tekinthető önkéntesnek, ha a felhasználók nem rendelkeznek valós vagy szabad választási lehetőséggel. Ezt az Európai Adatvédelmi Testület hozzájárulásról szóló iránymutatása is alátámasztja, amely leírja, hogy a hozzájárulás nem érvényes, ha az érintettek nem rendelkeznek valódi választási lehetőséggel vagy hozzájárulásra kényszerítve érzik magukat a rájuk gyakorolt nem megfelelő nyomást vagy befolyást gyakorló bármely olyan elem miatt, amely megakadályozza, hogy szabad akaratukat gyakorolják⁶¹. Mivel a **folyamatos noszogatás** ilyen nyomást válthat ki, ez sérti az önkéntes hozzájárulás elvét. Továbbá, mivel nem valószínű, hogy a felhasználók hozzájárulását követően a közösségimédia-szolgáltató rendszeresen (pl. minden alkalommal, amikor ismét bejelentkeznek fiókjukba) felajánlja a hozzájárulás visszavonásának lehetőségét, ez a megtévesztő tervezési megoldás sértheti az általános adatvédelmi rendelet 7. cikke (3) bekezdésének negyedik mondatát, amely előírja, hogy a hozzájárulás visszavonásának ugyanolyan egyszerűnek kell lennie, mint a megadásának („tükrözési hatás”).

⁶¹ A hozzájárulásról szóló 5/2020. sz. iránymutatás, 13–14. pont.

Timeline of the user interactions where the pop-up is displayed



35. példa: Ebben a példában, amikor a felhasználók létrehozzák felhasználói fiókjukat, megkérdezik tőlük, hogy elfogadják-e, hogy adataikat személyre szabott reklámok küldése céljából kezeljék. Amennyiben a felhasználók nem járulnak hozzá adataik ilyen célú kezeléséhez, a közösségi oldal használata során rendszeresen megjelenik számukra a fent látható ablak, amely megkérdezi, hogy szeretnének-e személyre szabott hirdetéseket. Az ablak megakadályozza őket a közösségi hálózat használatában. Mivel rendszeresen megjelenik, ez a **folyamatos noszogatás** valószínűleg arra készíti az abba belefáradó felhasználókat, hogy hozzájáruljanak a személyre szabott hirdetésekhöz. Ezen az interfészen továbbá a **bújtatott közzététel** megtévesztő megoldást⁶² is alkalmazták, mivel a hirdetések elfogadására irányuló művelet sokkal feltűnőbb, mint az elutasítási lehetőség.

⁶² Lásd a 49. pontot vagy a lenti melléklet 4.3.2. részét.

120. Emellett az adatkezelő megsértheti az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja szerinti tisztességes eljárás elvét is. Tekintettel arra, hogy a fenti példában a felhasználók a fiókjuk létrehozásakor nem járultak hozzá egyértelműen személyes adataik célzott hirdetések céljából történő kezeléséhez, az egyértelmű elutasítás állandó megkérdőjelezése megterhelő. Ezt a felhasználók által a regisztrációs folyamat során tett egyértelmű lépést most folyamatosan megkérdőjelezzik. A felhasználói élmény ebből eredő romlása jelentősen növeli annak valószínűségét, hogy a felhasználók egy idő után elfogadják a célzott hirdetést, pusztán azért, hogy ne kérdezzék meg őket minden alkalommal, amikor bejelentkeznek a fiókjukba, és használni kívánják a közösségimédia-platformot. Ebben az esetben a hozzájárulás megtagadása közvetlen hatással van a felhasználóknak nyújtott szolgáltatás minőségére és a szerződés teljesítésének feltételére.

c. Bevált gyakorlatok

Eszközök közötti konzisztencia: Ha a közösségimédia-platform különböző eszközökön (pl. számítógépen, okostelefonon stb.) keresztül érhető el, az adatvédelemmel kapcsolatos beállításokat és információkat a különböző verziókban ugyanazon a helyen kell elhelyezni, és azoknak ugyanazonok az útvonalakon és interfészelemekeken (menü, ikonok stb.) keresztül kell elérhetőnek lenniük.

Változásfigyelés és összehasonlítás: A fogalom meghatározást lásd az 1. használati esetről (29. o.).

Koherens megfogalmazás: A fogalom meghatározást lásd az 1. használati esetről (29. o.).

Fogalom meghatározások: A fogalom meghatározást lásd az 1. használati esetről (29. o.).

Példák használata: A fogalom meghatározást lásd az 1. használati esetről (29. o.).

Ragadós navigáció: A fogalom meghatározást lásd a 2a. használati esetről (36. o.).

Vissza az oldal tetejére: A fogalom meghatározást lásd a 2a. használati esetről (36. o.).

Értesítések: A fogalom meghatározást lásd a 2c. használati esetről (41. o.).

A következmények magyarázata: A fogalom meghatározást lásd a 2c. használati esetről (41. o.).

3b. használati eset: Az adatvédelmi beállítások kezelése

a. A kontextus leírása

121. A regisztrációs folyamat befejezését követően és közösségimédia-fiókjuk teljes életciklusa alatt lehetővé kell tenni a felhasználók számára, hogy módosítsák adatvédelmi beállításukat.
122. Függetlenül attól, hogy a felhasználók rendelkeznek-e előzetes ismeretekkel általában az adatvédelemről, és konkrétan az általános adatvédelmi rendeletről, és függetlenül attól, hogy odafigyelnek-e arra, hogy milyen személyes adatokat kívánnak vagy nem kívánnak megosztani és mások számára elérhetővé tenni, mindannyian jogosultak arra, hogy a közösségi média használata során átlátható módon tájékoztatást kapjanak lehetőségeikről.
123. A felhasználók rengeteg személyes adatot osztanak meg a közösségimédia-platformokon. A közösségimédia-platformok gyakran arra ösztönzik őket, hogy rendszeresen még több adatot osszanak meg. Bár elképzelhető, hogy a felhasználók meg akarják osztani életük pillanatait, részt kívánnak venni egy adott kérdéssről folytatott vitában, vagy – akár szakmai, akár személyes okokból – bővíteni kívánják kapcsolati hálójukat, biztosítani kell számukra azokat az eszközöket is, amelyek segítségével Elfogadott

szabályozhatják, hogy személyes adataik egyes részeit kik láthatják. A beállítások megváltoztatásához szükséges lépések számának megsokszorozódása elkerülhető egy olyan adatvédelmi irányítópult kialakításával, amely lehetővé teszi a beállítások központosítását és a felhasználói adatok feletti könnyebb rendelkezést.

b. Vonatkozó jogi rendelkezések

124. A fent említettek⁶³ szerint a személyes adatok kezelésére vonatkozó egyik fő elvként az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja előírja, hogy a személyes adatokat jogszerűen, tisztességesen és – ami e tekintetben különösen fontos – átlátható módon kell kezelni („jogszerűség, tisztességes eljárás és átláthatóság”). Az általános adatvédelmi rendelet 5. cikkének (2) bekezdése szerinti elszámoltathatóság elve szerint az adatkezelőknek be kell mutatniuk, hogy milyen intézkedéseket tesznek annak érdekében, hogy adatkezelési tevékenységeiket ne csak jogszerűvé és tisztességesé, hanem átláthatóvá is tegyék. Emellett az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja szerinti adattakarékosság, valamint a 25. cikk szerinti beépített és alapértelmezett adatvédelem elvei is relevánsak ebben a használati esetben.

c. Megtévészto tervezési megoldások

i. Tartalomalapú megoldások

125. Az első probléma, amellyel a felhasználók ebben az összefüggésben találkozhatnak, az, hogy hol találják meg ténylegesen az adatvédelemmel kapcsolatos beállításokat. A felhasználók elolvashatják az adatvédelmi nyilatkozatot, majd dönthetnek úgy, hogy változtatásokat hajtanak végre személyes adataik kezelésével kapcsolatban. Ez az igény a nyilatkozat elolvasása nélkül is felmerülhet bennük, csupán a közösségi média rendszeres használata révén, például ha felismerik, hogy egy a közösségimédia-platformon közzétett információt (pl. egy tengerparti fotó a családdal) egy nem kívánatos csoporttal (pl. munkatársakkal) is megosztanak. Mindenesetre az átláthatóság elve megköveteli, hogy a beállítási lehetőségek könnyen hozzáférhetőek és érthetőek legyenek. Ez úgy érhető el, hogy az adatbeállításokat és az adatvédelmi beállításokat egy helyen központosítják egy magától értetődő URL-cím, például [kozossegi-oldal.com]/adatbeallitasok cím alatt.
126. Ezzel a kérdéssel kapcsolatban számos olyan tervezési megoldás létezik, amelyek megnehezítik a felhasználók számára a beállítások megtalálását. A közösségimédia-platformok tervezőinek ezért ügyelniük kell ezekre a megtévészto tervezési megoldásokra.

Túlterhelés – Túl sok választási lehetőség (I. melléklet, az ellenőrző lista 4.1.3. pontja)

127. Az adatvédelmi beállításoknak könnyen hozzáférhetőnek és logikusan elrendezettnek kell lenniük. Az azonos adatvédelmi szemponthoz kapcsolódó beállításokat lehetőleg egyben, egy jól látható helyen kell elhelyezni. Ellenkező esetben a felhasználóknak túl sok oldalt kell megnézniük és áttekíteniük, ami túlterheli őket az adatvédelmi preferenciáik beállításai során. A **túl sok választási lehetőséggel** szembesülve ugyanis előfordulhat, hogy nem tudnak választani, vagy átsiklanak néhány beállításon, esetleg végül feladják, vagy nem találják meg adatvédelmi preferenciáik beállításait. Ez sérti az átláthatóság és a tisztességes eljárás elvét. Nevezetesen sértheti az általános adatvédelmi rendelet 12. cikkének (1) bekezdését, mert vagy nehezen elérhetővé tesz egy konkrét, az adatvédelemmel

⁶³ Lásd a fenti 1., 9., 10., 14–16. pontot.

kapcsolatos beállítást, mivel az több oldalon van szétszórva, vagy nem teszi egyértelművé a felhasználók számára biztosított különböző lehetőségek közötti különbséget.

36. példa: A felhasználók valószínűleg nem tudják, mit kell tenniük, ha egy közösségimédia-platform menüje több, adatvédelemmel foglalkozó lapot tartalmaz, úgy mint: „*adatvédelem*”, „*biztonság*”, „*tartalom*”, „*a magánélet védelme*”, „*az Ön preferenciái*”.

128. Ebben a példában a fülek címei nem jelzik egyértelműen, hogy a tartalomfelhasználók mire számíthatnak a kapcsolódó oldalon, vagy hogy ezek mindegyike az adatvédelemhez kapcsolódik, különösen, mivel az egyik lap kifejezetten ezt a nevet viseli. Ez azzal a kockázattal járhat, hogy a felhasználók nem tudnak változtatásokat eszközölni. Ha például a felhasználók korlátozni vagy bővíteni kívánják azoknak a személyeknek a számát, akik láthatják az általuk feltöltött képeket, a fülek nevei alapján a „*biztonság*” fülre kattinthatnak, ha úgy gondolják, hogy biztonsági kockázatot jelent, ha az adataik nyilvánosan hozzáférhetőek; a „*tartalom*” fülre, ha bejegyzésük láthatóságát kívánják beállítani; vagy a „*magánélet védelme*” fülre, mivel ez a konkrét fogalom közvetlenül kapcsolódik ahhoz, hogy az emberek mit akarnak megosztani másokkal. Ez azt jelenti, hogy ezek a címek nem elég egyértelműek a felhasználók által elérni kívánt tevékenységek tekintetében. Különösen az „*adatvédelem*” és a „*magánélet védelme*” kifejezéseket használják gyakran szinonimákként, és ezért különösen zavaróak, ha különböző szakaszokként jelennek meg.

Sötétben hagyás – Egymásnak ellentmondó információk (I. melléklet, az ellenőrző lista 4.6.2. pontja)

129. Amint az a 12. példában már bemutatásra került, és a következő példa részletesebben is szemlélteti, a felhasználók az adatvédelmi beállítások keretében ***egymásnak ellentmondó információkat*** is kaphatnak.

37. példa: X felhasználó kikapcsolja a földrajzi helymeghatározás hirdetési célú használatát. Miután rákattintott a kapcsolóra, a következő üzenet jelenik meg: „*Kikapcsoltuk a földrajzi helymeghatározást, de a földrajzi helyzetedre vonatkozó adatokat továbbra is használni fogjuk.*”

Túlterhelés – Adatvédelmi útvesztő (I. melléklet, az ellenőrző lista 4.1.2. pontja)

130. Ha a felhasználók megváltoztatnak egy adatvédelmi beállítást, a tisztességes eljárás elve azt is megköveteli a közösségimédia-szolgáltatótól, hogy tájékoztassa a felhasználókat más, hasonló beállításokról. Ha ezek a beállítások a közösségimédia-platform különböző, össze nem kapcsolt oldalain vannak szétszórva, a felhasználók egy vagy több, személyes adataik egy-egy aspektusa feletti rendelkezésre szolgáló lehetőséget valószínűleg nem fognak észrevenni. A felhasználók arra számíthatnak, hogy az egymással összefüggő beállításokat egymás mellett találják meg.

38. példa: A kapcsolódó témaköröket, például az adatoknak a közösségimédia-szolgáltató által harmadik felekkel való megosztására – és fordítva – vonatkozó beállítások nem ugyanazon vagy egymáshoz közeli helyeken, hanem a beállítások menü különböző fülein érhetők el.

131. Nincs univerzális megközelítés, amikor arról van szó, hogy a közösségimédia-platformok felhasználói átlagosan hány lépést tartanak elviselhetőnek a beállítások megváltoztatása során. Ugyanakkor a
- Elfogadott

lépések nagyobb száma eltántoríthatja a felhasználókat a módosítás véglegesítésétől, vagy előfordulhat, hogy szem előtt tévesztik annak egyes részeit, különösen akkor, ha több módosítást szeretnének végrehajtani. A felhasználók akaratának ily módon történő akadályozása sérti a tisztességes eljárásnak az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában foglalt elveit. Emellett a beállítások módosítása szorosan kapcsolódik az érintettek jogainak gyakorlásához⁶⁴. Az adatokkal kapcsolatos beállítások módosítása, például a felhasználói név módosítása vagy a diplomaszerezés évének törlése a helyesbítéshez való jog, illetve a törléshez való jog gyakorlásának tekinthető az adott adatok tekintetében. A szükséges lépések számának ezért a lehető legalacsonyabbnak kell lennie. Bár ez eltérő lehet, a lépések túlzott száma akadályozza a felhasználókat, és ezért sérti a tisztességes eljárás elvét, valamint az általános adatvédelmi rendelet 12. cikkének (1) és (2) bekezdését.

Összezavarás – Nyelvi akadályok (I. melléklet, az ellenőrző lista 4.5.4. pontja)

132. Az átlátható információk tekintetében a közösségimédia-platformok tervezőinek arra is ügyelniük kell, hogy elkerüljék a 2a. használati esetben felsorolt tartalomalapú megtévesztő tervezési megoldásokat, például a **nyelvi akadályokat**. Ha a beállítási oldalakat (vagy azok egy részét) nem teszik elérhetővé azon a nyelven, amelyet a felhasználó a közösségimédia-platformhoz választott, az megnehezíti számára, hogy megértse, mit változtathat meg, és így beállíthassa preferenciáit.

Összezavarás – Következtelen interfész (I. melléklet, az ellenőrző lista 4.5.3. pontja)

133. Ebben az összefüggésben egy másik probléma akkor merül fel, amikor a közösségimédia-platformok adatvédelmi szempontból kedvező döntéseket kínálnak a felhasználóknak, de erről nem tájékoztatják őket egyértelműen. Ez akkor fordulhat elő, ha a közösségimédia-platform hirtelen eltér a szokásos tervezési megoldásától. Ilyen **következtelen interfész** akkor fordul elő, ha egy interfész nem konzisztens a különböző kontextusokban, vagy nem felel meg a felhasználók elvárásainak. Ezek a különbségek oda vezethetnek, hogy a felhasználók nem találják meg a kívánt beállítást vagy információt, vagy megszokásból lépnek interakcióba a felület valamelyik elemével, még akkor is, ha ez az interakció olyan adatvédelmi döntést eredményez, amelyet a felhasználók nem akarnak.

39. példa: A közösségimédia-platformon tízből kilenc adatvédelmi beállítási opció az alábbi sorrendben jelenik meg:

- a legszigorúbb opció (azaz a legkevesebb adat megosztása másokkal),
- korlátozott opció, de nem annyira szigorú, mint az első opció,

– a legkevésbé szigorú opció (azaz a legtöbb adat megosztása másokkal).

A platform felhasználói megszokták, hogy adatvédelmi beállításai ebben a sorrendben jelennek meg. Az utolsó beállításnál azonban nem ez a sorrend érvényesül, ahol a felhasználók születésnapjainak láthatósága a következő sorrendben jelenik meg:

- Mutassa a teljes születésnapomat: 1929. január 15. (= a legkevésbé szigorú opció)
- Csak a napot és a hónapot mutassa: január 15. (= korlátozott opció, de nem a legszigorúbb opció)

⁶⁴ Lásd lent a 4. és 5. használati esetet, azaz ezen iránymutatás 3.4. és 3.5. részét.

– Ne mutassa másoknak a születésnapomat (= a legszigorúbb opció).

134. A példában az utolsó beállítás három választási lehetősége a korábbi beállításoktól eltérő sorrendben szerepel. Azok a felhasználók, akik korábban módosították más beállításait, valószínűleg megszokták a beállítások tizből kilenc esetben használt „szokásos” sorrendjét. Az utolsó beállításnál már annyira hozzászoktak ehhez a sorrendhez, hogy ösztönösen az első opciót választják, feltételezve, hogy az a legkorlátozóbb. Az egyik adatvédelmi beállítás opcióinak a többitől eltérő elrendezése ugyanazon közösségimédia-platformon **következtelen interfésznek** minősül, mivel a felhasználók által megszokottakkal és elvárásaikkal játszik. Ez zavart okozhat, vagy elhitetheti a felhasználókkal, hogy az általuk kívánt lehetőséget választották, holott valójában nem ez a helyzet.

ii. Interfészalapú megoldások

135. A második probléma, amellyel az adatvédelmi beállításokkal kapcsolatban találkozhatunk, az, hogy a beállítások sérthetik az alapértelmezett adatvédelem elvét. Az általános adatvédelmi rendelet 25. cikkének (1) bekezdése előírja az adatkezelők számára, hogy az adatvédelmi elvek – például az adattakarékosság (az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja) – megvalósítását célzó megfelelő intézkedéseket hajtsanak végre. Ezeket a rendelkezéseket nem tartják tiszteletben, ha a személyes adatok megosztására vonatkozó beállítások közül a legkevésbé invazív lehetőség helyett a leginvazívabbat jelölik ki előre.

Átugrás – Megtévesztő biztonság (1. melléklet, az ellenőrző lista 4.2.1. pontja)

40. példa: A „számomra látható”, a „legközelebbi barátaim számára látható”, a „valamennyi ismerősöm számára látható” és a „nyilvános” adatmegjelenítési lehetőségek közül a „valamennyi ismerősöm számára látható” középső opció van előre beállítva. Ez azt jelenti, hogy a velük kapcsolatban álló valamennyi felhasználó láthatja hozzászólásaikat, valamint a közösségimédia-platformra való regisztrációhoz megadott valamennyi információt, például e-mail-címüket vagy születési dátumukat.

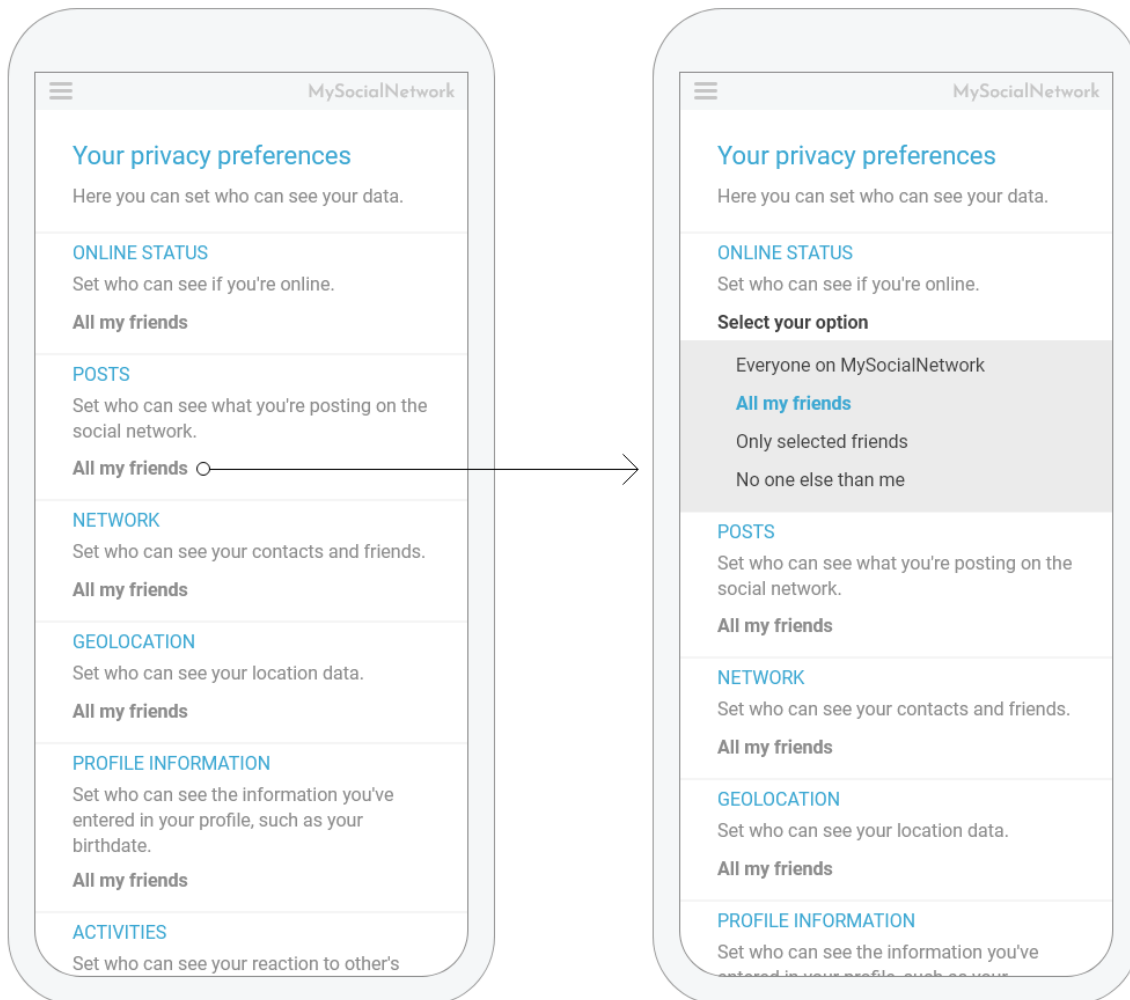
136. A közösségimédia-szolgáltatók azzal érvelhetnek, hogy a legkevésbé invazív beállítás megghiúsítaná az adott közösségimédia-platform felhasználóinak célját, például azt, hogy ismeretlenek találjanak rájuk, hogy új barátot, partnert vagy munkát találjanak. Bár ez igaz lehet bizonyos beállítások esetén, a közösségimédia-szolgáltatóknak szem előtt kell tartaniuk, hogy az a tény, hogy a felhasználók bizonyos adatokat feltöltenek a hálózatra, nem jelenti az adatok másokkal való megosztásához való hozzájárulást⁶⁵. Amennyiben a közösségimédia-szolgáltatók eltérnek az alapértelmezett adatvédelemtől, ügyelniük kell arra, hogy erről megfelelően tájékoztassák a felhasználókat. Ez azt jelenti, hogy a felhasználóknak tudniuk kell, mi az alapértelmezett beállítás, hogy vannak kevésbé invazív lehetőségek, és hogy a platformon hol tudnak módosításokat végezni. Az adott példában ez azt jelenti, hogy ha a „*legközelebbi barátaim számára látható*” opció van előre beállítva a felhasználók által a közösségi médiaplatformon aktívan közzétett hozzájárulásokhoz, meg kell mutatni nekik, hogy hol módosíthatják ezt a beállítást. A láthatóságnak a „*valamennyi ismerősöm számára látható*” (vagy akár a nagyközönség számára látható) opcióra történő előzetes beállítása azonban **megtévesztő biztonságnak** minősül, különösen akkor, ha olyan adatokra alkalmazzák, amelyeket a közösségimédia-szolgáltató a fiók létrehozásához kér a felhasználóktól, mint például az e-mail-cím vagy a születési

⁶⁵ Például születési idejük, lásd a fenti 58. pontot.

dátum. Az 1. használati eset 55. pontjában leírtak szerint ez a gyakorlat sérti az általános adatvédelmi rendelet 25. cikkének (2) bekezdését.

Megkavarás – Bújtatott közzététel (1. melléklet, az ellenőrző lista 4.3.2. pontja)

137. A **bújtatott közzététel** és a **megettévesztő biztonság** megettévesztő tervezési megoldások könnyen kombinálhatók, amikor az adatvédelemmel kapcsolatos opciók kiválasztásáról van szó, amint azt a 9. példa szemlélteti a regisztrációs folyamat esetében, illetve amint a lenti példa mutatja, amikor a felhasználók a közösségi média használata során akarják megváltoztatni adatvédelmi preferenciáikat.



41. példa: Ebben a példában, amikor a felhasználók az adataik láthatóságát szeretnék kezelni, az „*adatvédelmi preferenciák*” fülre kell menniük. Itt található az információk, amelyekre vonatkozóan beállíthatják preferenciáikat. Az információk megjelenítésének módja azonban nem teszi magától értetődővé, hogy hogyan kell módosítani a beállításokat. A felhasználóknak valójában a jelenlegi láthatósági opcióra kell kattintaniuk ahhoz, hogy hozzáférjenek egy legördülő menükhöz, amelyből kiválaszthatják az általuk preferált opciót.

138. Bár a preferenciák módosítása elérhető ezen a fülön, az **bújtatottan van közzétéve**, mivel a legördülő menü nem látható közvetlenül a felhasználók számára, akiknek rá kell jönniük, hogy az aktuális opcióra kattintva fog megnyílni valami. Valójában nincs olyan megszokott vizuális elem (aláhúzott szöveg, lefelé mutató nyíl), ami az interakció lehetőségére és a legördülő menü megnyitására utalna. Ez a konkrét gyakorlat tisztességtelen a felhasználókkal szemben, és hozzájárulhat az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában foglalt tisztességes eljárás elvének Elfogadott

általános megsértéséhez. Ezenkívül, ha az opciók alapértelmezés szerint előre ki lennének jelölve, a **megtévésző biztonság** megtévésző tervezési megoldás – a fenti 128. pontban leírtak szerint – szintén megfigyelhető lenne.

Összefoglalás – Váratlan szövegkörnyezetbe helyezés (I. melléklet, az ellenőrző lista 4.5.2. pontja)

139. **Váratlan szövegkörnyezetbe helyezésre** akkor kerül sor, ha az adatvédelmi vonatkozású információk vagy beállítások egy olyan oldalon találhatóak, amely kívül esik a kontextuson, így a felhasználók valószínűleg nem találják meg azokat, mivel nem lenne intuitív az adott oldalon keresniük őket.

42. példa: Az adatvédelmi beállításokat nehéz megtalálni a felhasználói fiókban, mivel az első szinten nincs olyan menüfejezet, amelynek neve vagy címe a megfelelő helyre irányítaná a felhasználót. A felhasználóknak meg kell nyitniuk más almenüt, például a „*Biztonság*” almenüt.

140. Ebben a példában a felhasználókat semmi nem irányítja az adatvédelmi beállításokhoz, mivel a szolgáltató nem használ érdemi és egyértelmű kifejezéseket annak jelzésére, hogy ezek hol találhatóak a közösségimédia-platfomon. A „*Biztonság*” kifejezés valójában csak töredékét fedi le annak, ami az adatvédelmi beállításoktól elvárható. Ezért a felhasználók számára nem magától értetődő, hogy ebben a menüben keressék ezeket a beállításokat. Az átláthatóság hiánya a kelleténél nehezebbé teszi az információkhoz való hozzáférést, és az általános adatvédelmi rendelet 12. cikkének (1) bekezdésébe, valamint adott esetben az általános adatvédelmi rendelet 12. cikkének (2) bekezdésébe ütközőnek tekinthető, amennyiben ezek a beállítások valamely jog gyakorlásához kapcsolódnak.

43. példa: A beállítás megváltoztatása akadályokba ütközik, mivel a közösségimédia-platfom asztali verziójában a változások regisztrálására szolgáló „*mentés*” gomb nem látható az összes lehetőségénél, hanem csak az almenü tetején. A felhasználók valószínűleg figyelmen kívül hagyják azt, és tévesen azt feltételezik, hogy beállításai automatikusan mentésre kerülnek, ezért a „*mentés*” gombra való kattintás nélkül váltanak át egy másik oldalra. Ez a probléma nem fordul elő az alkalmazásban és a mobil verzióban. Ezért ez további zavart okoz azon felhasználók számára, akik a mobil verzióról, illetve az alkalmazásról váltanak az asztali verzióra, mivel azt hihetik, hogy csak a mobilverzióban vagy az alkalmazásban módosíthatják a beállításait.

141. Ha a felhasználók megtalálták az adatvédelmi beállításokat és elvégzik a módosításokat, nem szabad őket ebben meggátolni. Miután a felhasználók elvégeztek egy módosítást, a mentés módjának nyilvánvalónak kell lennie, akár azonnal megtörténik, amint a felhasználók módosítanak egy beállítást, akár a felület egy adott elemére, például egy „*mentés*” gombra kattintva kell megerősíteni azt. Emellett az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja szerinti tisztességes eljárás elve megköveteli, hogy a közösségimédia-szolgáltatók a platformjuk egészén következetesek legyenek, különösen a különböző eszközökön átívelően. Ez a követelmény nem teljesül, ha az interfész a fenti példákban leírt megtévésző tervezési megoldást használ.

d. Bevált gyakorlatok

Adatvédelmi címtár: A menü különböző szakaszai közötti könnyű tájékozódás érdekében a felhasználók számára biztosítani kell egy könnyen hozzáférhető oldalt, ahonnan az összes adatvédelmi vonatkozású művelet (pl. beállítások) és tájékoztatás hozzáférhető. Ez az oldal elhelyezhető a közösségimédia-szolgáltató fő navigációs menüjében, a felhasználói fiókban, az adatvédelmi szabályzatban stb.

Csoportosított opciók: Az azonos adatkezelési célt szolgáló lehetőségek egy helyen történő elhelyezése annak érdekében, hogy a felhasználók könnyebben módosíthassák azokat, miközben továbbra is lehetőséget kapnak arra, hogy részletesebb változtatásokat hajtsanak végre. Ha a közösségimédia-platformok csoportosított opciókat kínálnak, ezek nem tartalmazhatnak váratlan vagy egymáshoz nem kapcsolódó elemeket (például különböző célú elemeket). Ha az adatkezeléshez hozzájárulásra van szükség, a csoportosított opcióknak összhangban kell lenniük az Európai Adatvédelmi Testület hozzájárulásról szóló iránymutatásával, különösen annak 42–44. pontjával.

Hivatkozások: a fogalommeghatározást lásd az 1. használati esetről (22. o.) (*pl. amikor a felhasználók tájékoztatást kapnak az adatkezelés valamely aspektusáról, felkéri őket arra, hogy a vonatkozó adatpreferenciáikat a megfelelő beállítás oldalon / irányítópulton határozzák meg*).

Magától értetődő URL cím: az adatvédelmi beállításokhoz vagy tájékoztatáshoz kapcsolódó oldalakon olyan webcímet kell használni, amely egyértelműen tükrözi azok tartalmát. Az adatvédelmi beállításokat központosító oldal URL-je lehet például [kozossegi-oldal.com]/adatbeallitasok.

Koherens megfogalmazás: A fogalommeghatározást lásd az 1. használati esetről (22. o.).

Fogalommeghatározások: A fogalommeghatározást lásd az 1. használati esetről (22. o.).

Példák használata: A fogalommeghatározást lásd az 1. használati esetről (22. o.).

Ragadós navigáció: A fogalommeghatározást lásd a 2a. használati esetről (28. o.).

Értesítések: A fogalommeghatározást lásd a 2c. használati esetről (32. o.).

A következmények magyarázata: A fogalommeghatározást lásd a 2c. használati esetről (32. o.).

Eszközök közötti konzisztencia: A fogalommeghatározást lásd a 3a. használati esetről (39. o.).

3.4 Jogérvényesítés a közösségi médiában: Az érintettek jogai

4. használati eset: Hogyan biztosíthatók megfelelő funkciók az érintettek jogainak gyakorlásához?

a. A kontextus leírása

142. A közösségimédia-platform használata azt jelenti, hogy a közösségimédia-szolgáltató által kitűzött célok mentén használjuk funkcióit. Ez azt is jelenti továbbá, hogy a felhasználók gyakorolhatják adatvédelmi jogaikat. Ezek az adatvédelem és a saját információk feletti rendelkezés kulcsfontosságú elemei, függetlenül attól, hogy az adatok az érintett által tudatosan és közvetlenül rendelkezésre bocsátott adatok, az érintett által a szolgáltatás vagy készülék használatával rendelkezésre bocsátott, megfigyelt adatok, vagy az érintett által rendelkezésre bocsátott adatok elemzéséből következtetett adatok⁶⁶. A platformon keresztül áramló személyes adatok mennyisége megköveteli, hogy a felhasználók világos és intuitív módon rendelkezhessenek adataik felett az általános adatvédelmi rendeletben biztosított jogok segítségével. Az Európai Adatvédelmi Testület több iránymutatásban is elmagyarázta ezeket a fogalmakat⁶⁷. A jogok gyakorlásának a platform használatának kezdetétől a

⁶⁶ Lásd a 29. cikk szerinti munkacsoport az (EU) 2016/679 rendelet szerinti, az adathordozhatósághoz való jogról szóló iránymutatását, WP242rev.01, 10. o., <https://ec.europa.eu/newsroom/article29/items/611233/en>.

⁶⁷ Az adatok hordozhatóságáról szóló iránymutatás és az Európai Adatvédelmi Testület 5/2019. sz. iránymutatása az elfeledtetéshez való jog kritériumairól az általános adatvédelmi rendelet hatálya alá eső, keresőmotorokkal kapcsolatos ügyekben (1. rész) – nyilvános konzultációt követően elfogadott változat,

befejezéséig, sőt bizonyos esetekben még azt követően is biztosítottak kell lennie, hogy a felhasználók úgy döntöttek, hogy elhagyják a platformot, és az adatkezelő még nem törölte az adataikat. A platformot nem használók számára ugyancsak lehetővé kell tenni, hogy gyakorolhassák az érintetteknek az adataik kezelésével kapcsolatos jogait. Természetesen egyes esetekben az adatkezelés jogalapjától függően nem minden érintetti jog áll rendelkezésre. A közösségimédia-szolgáltatóknak ezért egyértelműen indokolnia kell, hogy bizonyos jogok miért nem érvényesek, és egyes jogok miért korlátozhatók. Amint azt fentebb és az előző fejezetekben említettük, a jogok alkalmazását érvényre kell juttatni. A jogok gyakorlásának megkönnyítése érdekében az automatizálást és a közösségimédia-platformok egyéb funkcióit is fel kell használni.

b. Vonatkozó jogi rendelkezések

143. Az általános adatvédelmi rendelet hét különböző jogot ír le, amelyeket az érintettek bizonyos feltételek mellett (pl. az adatkezelés jogalapja stb.) gyakorolhatnak. Az általános adatvédelmi rendelet 15. cikke lehetővé teszi az érintettek számára, hogy megtudják, hogy személyes adataik kezelése folyamatban van-e, és hogy azokhoz hozzáférést kapjanak, azaz hogy további információkat szerezzenek az adatkezelésről, valamint hogy másolatot kapjanak az említett adatokról. Az általános adatvédelmi rendelet 16. cikke részletezi a helyesbítéshez való jogot, amely lehetővé teszi az érintettek számára, hogy aktualizálják az adatkezelő által kezelt személyes adataikat. Az általános adatvédelmi rendelet 17. cikke szerinti törléshez való jog lehetővé teszi az érintettek számára, hogy kérésükre az adatkezelő törölje a rájuk vonatkozó személyes adatokat. Az adatkezelés korlátozásához való, az általános adatvédelmi rendelet 18. cikke szerinti jog lehetővé teszi az érintettek számára, hogy ideiglenesen leállítsák személyes adataik kezelését. Az általános adatvédelmi rendelet 20. cikke bevezeti az adathordozhatósághoz való jogot, amely lehetővé teszi az érintettek számára, hogy megkapják személyes adataikat és továbbítsák azokat egy másik adatkezelőnek⁶⁸. Az érintetteknek az általános adatvédelmi rendelet 21. cikkében meghatározottak szerint joguk van ahhoz is, hogy tiltakozzanak személyes adataik kezelése ellen. Végezetül az általános adatvédelmi rendelet 22. cikke biztosítja az érintettek számára azt a jogot, hogy ne terjedjen ki rájuk a kizárólag automatizált adatkezelésen alapuló döntések hatálya.⁶⁹
144. Az Európai Adatvédelmi Testület hangsúlyozza, hogy e jogok közül nem mindegyik vonatkozik minden egyes közösségimédia-platformra, a személyes adatok kezelésének jogalapjától és céljaitól, valamint a nyújtott szolgáltatások típusától függően. A különbségeket az adatkezelőnek az általános adatvédelmi rendelet 12. cikkével összhangban meg kell magyaráznia. Ez azt jelenti, hogy az alkalmazandó jogokra vonatkozó tájékoztatásnak tömörnek és a felhasználók számára egyértelműnek kell lennie, beleértve azt is, hogy bizonyos jogok miért nem alkalmazandók. Egy ilyen magyarázat korlátozhatná a felhasználókkal folytatott kommunikáció mennyiségét, amikor ezen jogok némelyikét megpróbálják gyakorolni. A jog gyakorlásának a 12. cikk (2) bekezdésével összhangban egyszerűnek és elérhetőnek kell lennie, és a választ az általános adatvédelmi rendelet 12. cikkének (3) bekezdésében előírtak szerint indokolatlan késelem nélkül meg kell adni. Hasonlóképpen, a közösségimédia-platformnak indokolnia kell, hogy bizonyos kérések miért nem teljesíthetők, és tájékoztatást kell nyújtania arról, hogy az általános adatvédelmi rendelet 12. cikkének (4) bekezdése szerint az érintett panaszt nyújthat

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbsearchengines_afterpublicconsultation_hu.pdf.

⁶⁸ Ezt a jogot tovább részletezi az adatok hordozhatóságáról szóló iránymutatás.

⁶⁹ Lásd még a 29. cikk szerinti munkacsoport iránymutatását az automatizált döntéshozatallal és a profilalkotással kapcsolatban az (EU) 2016/679 rendelet alkalmazásához, wp251rev.01, 19. és az azt követő oldalak, <https://ec.europa.eu/newsroom/article29/items/612053/en>.

be a kijelölt felügyeleti hatósághoz. Így a következő megtévesztő tervezési megoldások nem feltétlenül alkalmazhatók a fent említett jogok mindegyikére. A törléshez való jogot a következő fejezet tárgyalja részletesen.

c. **Megtévesztő tervezési megoldások**

i. **Tartalomalapú megoldások**

Akadályozás – Zsákutca (I. melléklet, az ellenőrző lista 4.4.1. pontja)

145. A **zsákutca** megtévesztő tervezési megoldás közvetlenül befolyásolhatja a jogok gyakorlásához való könnyű hozzáférést. Ha egy jog gyakorlásának eszközeire mutató hivatkozások nem működnek, vagy hiányoznak a jog gyakorlásának módjára vonatkozó egyértelmű magyarázatok, a felhasználók nem tudják megfelelően gyakorolni azt, ami sérti az általános adatvédelmi rendelet 12. cikkének (2) bekezdését.

44. példa: Amikor a felhasználók az adatvédelmi nyilatkozatban az „Élek a hozzáférési jogommal” gombra kattintanak, az átirányítja őket a profiljukra, amely nem tartalmaz a jog gyakorlásához kapcsolódó funkciókat.

146. A megtévesztő tervezési megoldásra vonatkozó fent említett példa rámutat arra, hogy egyértelmű és intuitív módon kell biztosítani a felhasználók számára az általános adatvédelmi rendelet 12. cikkének (1) és (2) bekezdése szerinti jogaik gyakorlását, mivel máskülönben esetleg nem tudnák azokat gyakorolni. Nem elegendő megerősíteni a felhasználók számára, hogy rendelkeznek az érintetteknek az általános adatvédelmi rendelet 12. cikkének (1) bekezdésében (beleértve a kommunikáció módját) és különösen az általános adatvédelmi rendelet 13. cikke (2) bekezdésének b) pontjában és 14. cikke (2) bekezdésének c) pontjában előírt jogaival. Azt is lehetővé kell tenni a számukra, hogy egyszerűen gyakorolhassák azokat, lehetőleg a platform interfészébe ágyazva, például egy erre a célra szolgáló űrlap biztosításával. Ez a platformmal kapcsolatos felhasználói élményt is pozitívabbá tenné – látva, hogy a szolgáltató erőfeszítéseket tett annak érdekében, hogy alkalmazkodjon a felhasználóknak a személyes adatok jogszerű kezelésére és az adataik feletti rendelkezésre vonatkozó elvárásaihoz azáltal, hogy a jogok gyakorlását a szolgáltatás egyéb funkcióival kombinálja. Ha a közösségimédia-platformszolgáltatás lehetővé teszi a kétirányú kommunikációt a felhasználók között, valamint az adatkezelő és a felhasználók között, nincs ok arra, hogy az adatkezelő az érintettek kérelmeinek megkönnyítése érdekében kommunikációs csatornáját egy külön kommunikációs eszközre, például e-mailre korlátozza. Ugyanakkor az érintetteket nem szabad arra kényszeríteni, hogy az adatkezelővel való kommunikáció céljából a platformra jöjjenek⁷⁰. Emellett az adatkezelők nem korlátozhatják az érintett ezen jogát a másolathoz való jogra, ehelyett gondoskodniuk kell arról, hogy az általános adatvédelmi rendelet 15. cikkének (1) bekezdésében említett információkat is az adataikhoz hozzáférést kérő felhasználók rendelkezésére bocsássák.⁷¹

Összevadás – Nyelvi akadályok (I. melléklet, az ellenőrző lista 4.5.4. pontja)

⁷⁰ Lásd az Európai Adatvédelmi Testület 1/2022. sz. iránymutatását az érintettek jogairól – hozzáférési jog, 136. pont, 1.0. verzió, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.

⁷¹ Lásd az Európai Adatvédelmi Testület 1/2022. sz. iránymutatásának 131., 142. és 145. pontját.

45. példa: Az érintett jogainak gyakorlásával kapcsolatos hivatkozásra kattintva a szolgáltatással ellentétben a következő információk nem a felhasználók országának hivatalos nyelvén (nyelvein) kerülnek megadásra. Ehelyett a felhasználókat egy angol nyelvű oldalra irányítják át.

147. Szem előtt tartva az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja és 12. cikkének (1) bekezdése szerinti átláthatóság elvét, a felhasználóknak egyértelmű és világos, érthető módon kell megkapniuk a jogaikra vonatkozó valamennyi információt. Ennek kapcsolódnia kell a felhasználók tartózkodási helyéhez és a szolgáltatásnyújtás helye szerinti országban vagy joghatóságban használt nyelvhez is. Az a tény, hogy a felhasználók megerősítik, hogy képesek idegen nyelvet használni, nem mentesíti az adatkezelőt kötelezettségei alól. Ugyanez vonatkozik arra az esetre is, ha a felhasználók tevékenységéből kikövetkeztethető, hogy más nyelveken is értenek. A tájékoztatásnak relevánsnak és hasznosnak kell lennie a jogukat gyakorló felhasználók számára.

Sötétben hagyás – Félreérthető megfogalmazás vagy tájékoztatás (I. melléklet, az ellenőrző lista

4.6.3. pontja)

148. Az érintettek jogaival összefüggésben a felhasználók a ***félreérthető megfogalmazás vagy tájékoztatás*** megtévesztő tervezési megoldással is szembesülhetnek, amint azt a következő példa mutatja.

46. példa: A közösségimédia-platform nem mondja ki kifejezetten, hogy az EU-ban a felhasználóknak jogukban áll panaszt benyújtani egy felügyeleti hatósághoz, hanem csak megemlíti, hogy egyes országokban – anélkül, hogy részleteznék, mely országokban – vannak olyan adatvédelmi hatóságok, amelyekkel a közösségi médiaszolgáltató együttműködik a panaszok tekintetében.

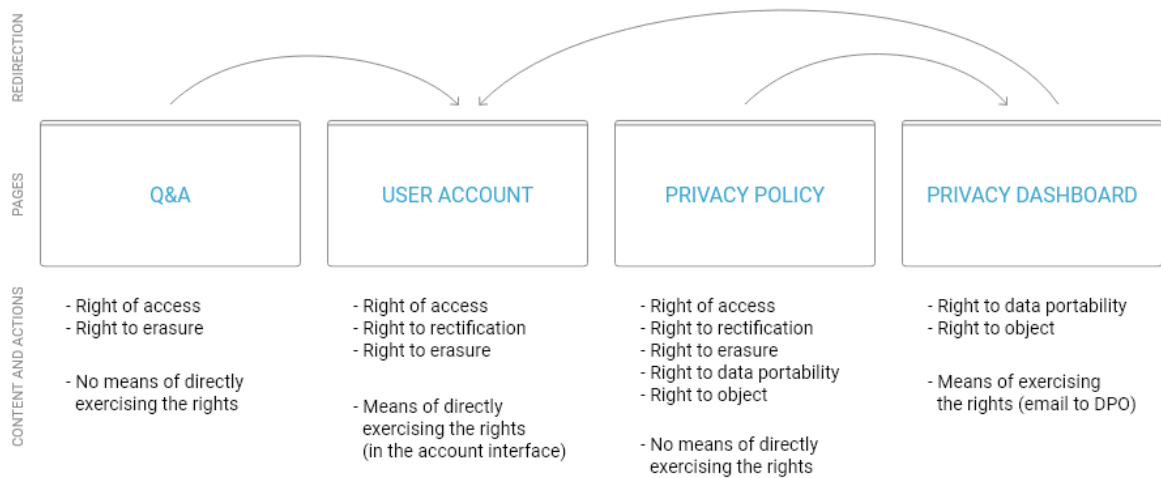
149. A közösségimédia-szolgáltatóknak azt is szem előtt kell tartaniuk, hogy az érintettek jogaikról való tájékoztatása során elkerüljék a ***félreérthető megfogalmazás vagy tájékoztatás*** megtévesztő tervezési megoldást. Az átláthatóság elvét sérti, ha a felhasználókat olyan módon tájékoztatják, amely elbizonytalanítja őket az adataik kezelésének módjával, illetve azzal kapcsolatban, hogy miként rendelkezhetnek adataik felett, és ezáltal hogyan gyakorolhatják jogukat. Emellett a félreérthető megfogalmazás nem tömör, amint azt az általános adatvédelmi rendelet 12. cikkének (1) bekezdése előírja, és az érintetteknek nyújtott tájékoztatást hiányossá teheti, ami az általános adatvédelmi rendelet 13. cikke megsértésének tekinthető. A fent említett példa az általános adatvédelmi rendelet 13. cikke (2) bekezdése d) pontjának megsértését is mutatja, amely előírja az adatkezelők számára, hogy tájékoztassák az érintetteket a felügyeleti hatósághoz címzett panasz benyújtásának jogáról. Következésképpen ez az általános adatvédelmi rendelet 12. cikkének (2) bekezdésével is ellentétes, mivel a közösségimédia-szolgáltató nem segíti elő a panasztételhez való jog gyakorlását.

ii. Interfészalapú megoldások

Túlterhelés – Adatvédelmi útvesztő (I. melléklet, az ellenőrző lista 4.1.2. pontja)

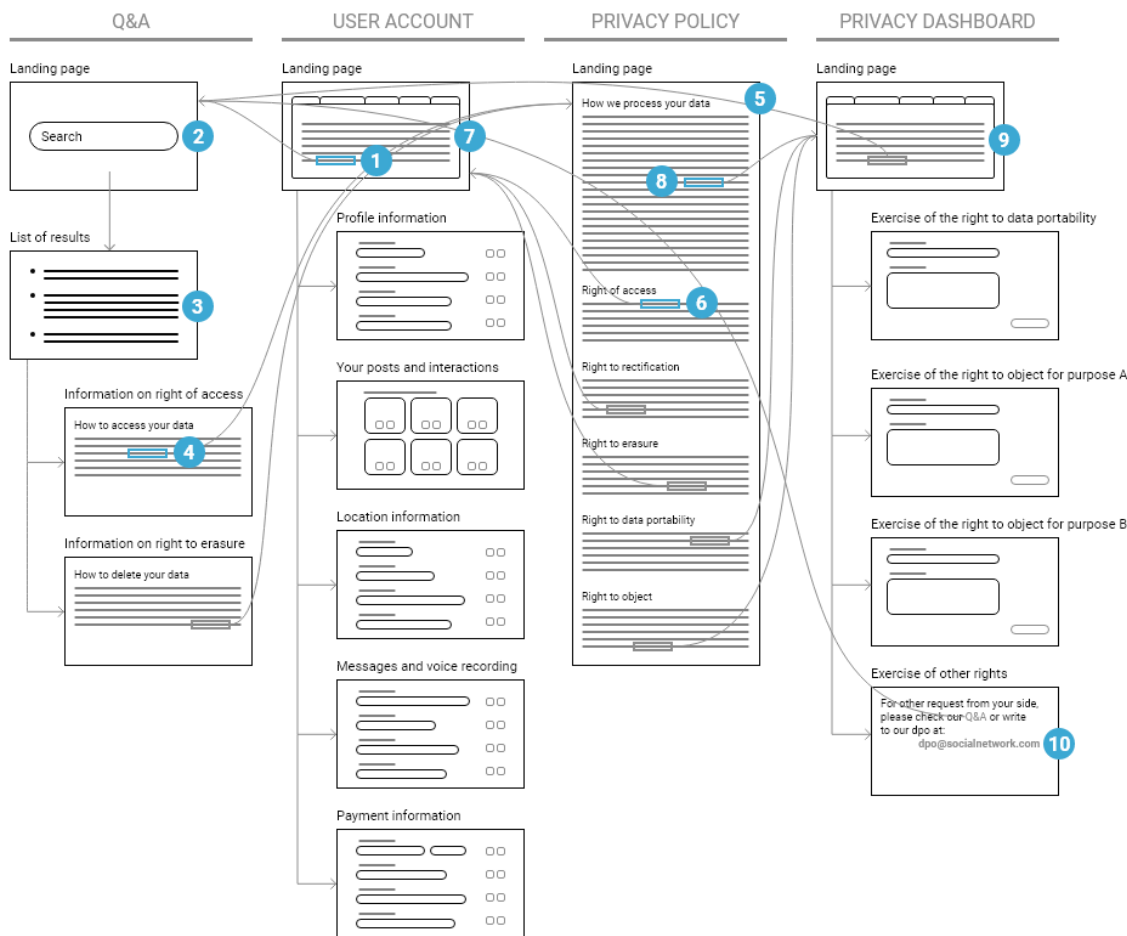
150. A 3b. használati esetben korábban ismertetetteknek megfelelően a vonatkozó adatvédelmi információk megszerzéséhez szükséges lépések száma nem lehet túlzott mértékű, ahogyan az

érintettek jogainak érvényesítéséhez szükséges lépések száma sem⁷². Így a felhasználóknak mindig gyorsan el kell tudniuk jutni a joggyakorlási oldalra, függetlenül attól, hogy milyen kiindulópontból érkeztek, és hogy a közösségimédia-platfromon hol található ez a funkció. A közösségimédia-szolgáltatóknak ezért alaposan át kell gondolniuk, hogy a felhasználók milyen különböző helyzetekben kívánhatják gyakorolni jogaikat, és ennek megfelelően kell kialakítaniuk a hozzáférést ahhoz a helyhez, ahol ezt megtehetik. Ez azt jelenti, hogy egy közösségimédia-platfromon több útvonal is létrehozható és rendelkezésre bocsátható az érintett jogainak eléréséhez. Mindazonáltal minden egyes útvonalnak elő kell segítenie a jogok gyakorlását, és egyik sem akadályozhatja a többi útvonalat. Ellenkező esetben ezt a 47. és 48. példa által szemléltetett **adatvédelmi útvesztő** megtévesztő tervezési megoldásnak kell tekinteni, ami ellentétes az általános adatvédelmi rendelet 12. cikkének (2) bekezdésével.



47. példa: Az adatvédelmi jogokkal kapcsolatos információk itt legalább négy oldalon érhetők el. Bár az adatvédelmi szabályzat valamennyi jogról tájékoztatást nyújt, nem irányít át az egyes jogokra vonatkozó oldalakra. Ezzel szemben, amikor a felhasználók felkeresik fiókjukat, nem találnak semmilyen információt az általuk gyakorolható jogok némelyikéről. Ez az **adatvédelmi útvesztő** arra kényszeríti a felhasználókat, hogy több oldalt is átnézzenek annak érdekében, hogy megtalálják az egyes jogok gyakorlásának helyét, és a böngészéstől függően előfordulhat, hogy nem ismerik meg az összes őket megillető jogot.

⁷² Lásd a fenti 123. pontot.



48. példa: Ebben a példában a felhasználó aktualizálni kívánja személyes adatainak egy részét, de nem talál erre módot felhasználói fiókjában. Rákattint egy hivatkozásra (1), amely átirányítja a Kérdések és válaszok oldalra, ahol begépel a kérdést (2). Több találat is megjelenik (3), amelyek közül néhány a hozzáférési és törlési joggal kapcsolatos. Az összes találat ellenőrzése után rákattint (4) a „Hogyan férhetsz hozzá az adataidhoz?” oldalon található linkekre. Ez visszaviszi őt az adatvédelmi szabályzathoz (5). Ott további jogokkal kapcsolatos információkat talál. Ezen információk elolvasása után a helyesbítéshez való jog gyakorlásához kapcsolódó hivatkozásra kattint (6), amely átirányítja őt a felhasználói fiókjához (7). Elégedetlenül visszatér az adatvédelmi szabályzathoz, és rákattint a „Kérelem elküldése” című általános hivatkozásra (8). Ez a felhasználót adatvédelmi irányítópultjához (9) viszi. Mivel úgy tűnik, hogy a rendelkezésre álló lehetőségek egyike sem felel meg az igényeinek, a felhasználó az „egyéb jogok gyakorlása” című oldalra (10) megy, ahol végül megtalálja a kapcsolattartási címet.

151. Mindkét példa a jogok gyakorlásának különösen hosszadalmas és fárasztó útvonalt szelmléti. Ha a különböző jogok gyakorlásának eszközei nem ugyanazon a helyen találhatóak, de rendelkezésre áll egy, az érintett valamennyi jogát felsoroló oldal, a legutolsónak pontosan ezekre a különböző helyekre kell átirányítania, nem pedig csak az egyikre vagy azok egy részére, amint azt a 47. példa szelmléti. A

másik példa egy olyan útvonalat mutat be, ahol a felhasználók nem találják meg az általuk kívánt konkrét jog, nevezetesen a helyesbítéshez való jog egyszerű gyakorlásának módját, mivel az a hely, ahol ez általában történik, azaz a felhasználói fiók, nem biztosítja az ehhez szükséges eszközt. Ha más módot keresnek e jog gyakorlására, nem találnak egy konkrétan megfelelő lehetőséget, és kénytelenek az adatvédelmi irányítópulton megadott általános eszközhöz fordulni.

152. Ha egy jog gyakorlásához több útvonalat is kialakítottak, a felhasználók számára mindig könnyűvé kell tenni az érintettek jogairól szóló áttekintés megtalálását. Az adatvédelmi szabályzatoknak egyértelműnek kell lenniük, és az olyan oldalak egyik kapujaként szolgálhatnak, ahol a felhasználók gyakorolhatják jogaikat. Ennek a dokumentumnak tartalmaznia kell az összes alkalmazandó jogot. Ha jogi vagy technikai korlátok miatt valamelyik nem áll rendelkezésre, ezt is meg kell indokolni a felhasználók megfelelő tájékoztatása érdekében. Az adatkezelési műveletek – akár azok alapja, akár az adatkezelők által elfogadott biztosítékok miatti – korlátozásának megértése nemcsak a felhasználók számára hasznos. Korlátozza azokat az eseteket is, amikor a közösségimédia-szolgáltatónak magyarázatot kell adnia arra, hogy miért nem tud eleget tenni a felhasználók által benyújtott, az érintetti jogokra vonatkozó kérelemnek.

Megkavarás – Bújtatott közzététel (I. melléklet, az ellenőrző lista 4.3.2. pontja)

153. A felhasználók azon képességének befolyásolása, hogy elérjék azt a helyet, ahol jogaikat gyakorolhatják, úgy is megvalósítható, hogy a kapcsolódó információkat vagy hivatkozásokat nehezen láthatóvá tesszük a **bújtatott közzététel** megtévesztő tervezési megoldás alkalmazásával.

49. példa: Az adatvédelmi szabályzat „hozzáférési jog” alcím alatti bekezdése kifejti, hogy a felhasználóknak az általános adatvédelmi rendelet 15. cikkének (1) bekezdése értelmében joguk van a tájékoztatáshoz. Ugyanakkor csak annyit említ meg, hogy a felhasználók másolatot kaphatnak személyes adataikról. Az általános adatvédelmi rendelet 15. cikkének (3) bekezdése szerinti hozzáférési jog másolati elemének gyakorlásához nincs látható közvetlen hivatkozás. Ehelyett kissé aláhúzzák a „Másolatot kaphat személyes adatairól” szöveg első három szavát. Ha a felhasználó ezen szavak fölé viszi a kurzort, egy kis szövegdoboz jelenik meg, amely a beállításokra mutató hivatkozást tartalmaz.

154. Az előző szakaszt kiegészítve, az adatkezelő által a jogok gyakorlása céljából létrehozott eszközöknek könnyen hozzáférhetőnek kell lenniük. Ezt a szabályt nem szabad alábecsülni. Az adatkezelő fent leírt intézkedése kizárólag a felhasználókat megillető jogok gyakorlásának akadályozására irányuló erőfeszítésnek tekinthető, ami sérti az általános adatvédelmi rendelet 12. cikkének (2) bekezdését. Az adatkezelők – indokaiktól függetlenül – nem akadályozhatják meg az ilyen kérést. Egy konkrét esetben a felügyeleti hatóság általi alaposabb vizsgálat esetén ez hozzájárulhat az általános adatvédelmi rendelet megsértéséhez, ami az adatkezelő szankcionálásához vezethet.

Összevadás – Következtelen interfész (I. melléklet, az ellenőrző lista 4.5.3. pontja)

50. példa: A közösségimédia-platform különböző verziókat kínál (asztali, alkalmazás, mobil böngésző). Az egyes verziókban a (hozzáféréshez/kifogáshoz stb. vezető) beállítások eltérő szimbólummal jelennek meg, ami összevadásra a különböző változatok között váltó felhasználókat.

155. Ha a felhasználók különböző eszközökön olyan interfészekkel találkoznak, amelyek ugyanazt az információt különböző vizuális jelölések révén közvetítik, valószínűleg több idejükbe kerül, vagy nehezebben találják meg az egyik eszköztől ismert beállításokat a másik eszközön. A fenti példában ez annak tudható be, hogy a felületek különböző szimbólumokat vagy ikonokat használnak, amelyek a felhasználókat a beállításokra irányítják. A felhasználók ily módon történő összezavarása ellentétesnek tekinthető az érintettek jogainak az általános adatvédelmi rendelet 12. cikkének (2) bekezdésében meghatározott elősegítésével.

Akadályozás – Indokolatlanul hosszú folyamatok (I. melléklet, az ellenőrző lista 4.4.2. pontja)

156. Végezetül az általános adatvédelmi rendelettel ellentétesnek tekinthető minden olyan próbálkozás, amely arra irányul, hogy a jog gyakorlását a **szükségesnél hosszabbá** tegye.

51. példa: Amikor a *felhasználók* úgy döntenek, hogy törlik középiskolájuk nevét és helyét, vagy egy olyan eseményre való hivatkozást, amelyen részt vettek és megosztottak, felugrik egy második ablak, amely a döntés megerősítését kéri („*Tényleg ezt akarod? Miért szeretnéd ezt megtenni?*”).

157. Az adatvédelmi szabályzat rétegeinek mennyiségéhez (2a. használati eset) és a beállítások eléréséhez vagy megváltoztatásához szükséges lépések számához (3b. használati eset) hasonlóan a felhasználók által a jog gyakorlása érdekében végrehajtandó lépések vagy kattintások száma nem lehet túlzott mértékű. Ez természetesen az adatkezelő által végzett műveletek összetettségétől függ, figyelembe véve az adott kontextust. Észszerűtlen lenne azonban arra kötelezni a felhasználókat, hogy nagyszámú szükségtelen műveletet hajtsanak végre jogaik gyakorlása érdekében. A felhasználókat nem szabad olyan további kérdésekkel eltántorítani, mint például, hogy valóban élni akarnak-e ezzel a joggal, vagy hogy mi az oka a kérésüknek. A legtöbb esetben lehetővé kell tenni számukra, hogy egyszerűen gyakorolhassák jogaikat, anélkül, hogy megkérdőjeleznék motivációjukat. A fenti példában bemutatott ilyen gyakorlatok ellentétesek az általános adatvédelmi rendelet 12. cikkének (2) bekezdésével, mivel az adatkezelő szükségtelen lépésekkel akadályozza a jogok gyakorlását. Ez természetesen nem zárja ki annak lehetőségét, hogy az adatkezelő a szolgáltatás javítása érdekében utólag további kérdéseket tegyen fel. A kérdést utólag feltéve kizárólag a felhasználók akaratától függ, hogy megválaszolják-e, és nem lenne összetéveszthető a jog gyakorlására vonatkozó követelménnyel.

d. Bevált gyakorlatok

A jogok gyakorlására szolgáló űrlap: a felhasználók általános adatvédelmi rendelethez fűződő jogai gyakorlásának elősegítése érdekében egy erre a célra szolgáló űrlapot lehet biztosítani, amely segíti őket jogaik megértésében, és amely iránymutatást nyújt számukra az ilyen típusú kérelmek benyújtásához.

Hivatkozások: a fogalommeghatározást lásd az 1. használati esetről (22. o.) (*pl. a felhasználói fiók törlésére mutató hivatkozás biztosítása a felhasználói fiókban*).

Koherens megfogalmazás: A fogalommeghatározást lásd az 1. használati esetről (22. o.).

Fogalommeghatározások: A fogalommeghatározást lásd az 1. használati esetről (22. o.).

Példák használata: A fogalommeghatározást lásd az 1. használati esetről (22. o.).

Ragadós navigáció: A fogalommeghatározást lásd a 2a. használati esetről (28. o.).

A következmények magyarázata: A fogalommeghatározást lásd a 2c. használati esetről (32. o.).

Eszközök közötti konzisztencia: A fogalommeghatározást lásd a 3a. használati esetről (39. o.).

Adatvédelmi címtár: A fogalommeghatározást lásd a 3b. használati esetről (45. o.).

Az adatvédelmi ellenőrzések kapcsolata: A fogalommeghatározást lásd a 3b. használati esetről (45. o.).

3.5 Viszlát, és minden jót: a közösségimédia-fiók bezárása

5. használati eset: a fiók szüneteltetése / az összes személyes adat törlése

a. A kontextus és a vonatkozó jogi rendelkezések leírása

158. A felhasználói fiók életciklusának vége azt a helyzetet írja le, amikor a felhasználók úgy döntenek, hogy elhagyják a közösségi hálózatot. Ebben a helyzetben a felhasználók általában úgy döntenek, hogy véglegesen elhagyják a közösségimédia-platformot. Ugyanakkor gyakran arra is lehetőségük van, hogy csak ideiglenesen szüneteltessék a fiókot és függesszék fel a szolgáltatást. A két döntés jogi következményei eltérőek, és az alábbiakban kerülnek ismertetésre.

i. A fiók végleges törlése

159. A közösségimédia-platform végleges elhagyására vonatkozó döntést az általános adatvédelmi rendelet 17. cikke (1) bekezdésének a) pontja szerinti törléshez való joggal jár együtt. Ebben az összefüggésben a törlésre angolul a „deletion” szót gyakrabban használják, mint az a) pontban használt szinonimáját („erasure”).
160. A „törlés” kifejezést az általános adatvédelmi rendelet 17. cikke jogilag nem határozza meg, és azt csak az általános adatvédelmi rendelet 4. cikkének 2. pontja említi az adatkezelés egyik formájaként. A törlés általánosságban úgy értelmezhető, hogy a törlendő adatokban korábban megtestesült, az érintettre vonatkozó információkat (gyakorlatilag) nem lehet érzékelni. A törlést követően a szóban forgó információ senki számára nem lehet aránytalan erőfeszítés nélkül észlelhető.
161. Az anonimizálás egy másik módja annak, hogy tartósan megszűnjön a személyhez fűződő kapcsolat. Más szóval az anonimizálási technikák alkalmazásának célja annak biztosítása, hogy az érintettet többé ne lehessen azonosítani. Az anonimizálás azt is jelenti, hogy az adatvédelmi jog elvei – például a célhoz kötöttség elve – már nem alkalmazandók (lásd a (26) preambulumbekzdés negyedik és ötödik mondatát).
162. Az általános adatvédelmi rendelet 12. cikkének (2) bekezdése szerint az adatkezelőnek elő kell segítenie az érintettek 15–22. cikk szerinti jogainak a gyakorlását. E követelmény szerint az érintettek jogainak érvényesítése elé sem lényegi, sem alaki akadályok nem állíthatók. Ezért, ha a törléshez való jog gyakorlását valódi ok nélkül megnehezítik, az az általános adatvédelmi rendelet megsértésének minősül. Bár indokolt, hogy a közösségimédia-szolgáltatók objektíven elmagyarázzák a következményeket, például az összes személyes adat törlését, és felkérjék az érintetteket, hogy erősítsék meg döntésüket⁷³, a szükségtelen akadályokat ebben a használati esetben is el kell kerülni. Ebből például az következik, hogy a felhasználók fióktörlési kérelme és a fiók tényleges törlése közötti türelmi időnek arányosnak kell lennie. Ez az idő tehát nem lehet túlzottan hosszú, figyelembe véve az azonnali törlés elmaradásához vezető technikai okokat, valamint azt a rövid időt, amely alatt a felhasználók azt követően, hogy elindították a fióktörlési folyamatot, meggondolhatják magukat a fiók törlése tekintetében. Bár tiszteletben kell tartani, hogy a felhasználók szabadon meggondolhatják magukat, a közösségimédia-szolgáltatók nem kísérelhetik meg előidézni ezt a döntést a felhasználók visszatérésre való ösztönzésével, ami szintén a felhasználók törléshez való jogának akadályozását jelentené. A türelmi idő alatt a törlési folyamat bizonyos esetekben megszakadhat, például ha a felhasználó ismét bejelentkezik. Ha a törlés nem hajtható végre, a felhasználót tájékoztatni kell erről és fel kell világosítani azzal kapcsolatban, hogyan tudja befejezni a törlést.
163. A közösségimédia-platform elhagyására vonatkozó döntést az általános adatvédelmi rendelet 17. cikke (1) bekezdésében meghatározott törlés következményeit vonja maga után. Ha az érintett az adott fiók

⁷³ Az érintett egyéb jogaival ellentétesen, lásd a fenti 154. pontot.

törlését kéri, a közösségimédia-platform adatkezelőjének törölnie kell az adatokat. Mindazonáltal bizonyos adatok bizonyos ideig megőrizhetők a közösségimédia-platfromon, amennyiben az általános adatvédelmi rendelet 17. cikkének (3) bekezdése alkalmazandó. Az általános adatvédelmi rendelet 17. cikkének (3) bekezdésében felsorolt kivételeket megszorítóan kell értelmezni, és azok csak a rendelkezés e részében kifejezetten megnevezett esetekben alkalmazandók. Az adatkezelő által az általános adatvédelmi rendelet 17. cikkének (3) bekezdése alapján hivatkozott bármely kivételt és a vonatkozó adatmegőrzést az adatkezelőnek indokolnia kell, például, hogy a nemzeti jog előírja az adatkezelő számára, hogy közérdeken alapuló kényszerítő okokból, a véleménynyilvánítás és a tájékozódás szabadságához való alapvető jog gyakorlása vagy adózási okok miatt tárolja az érintettre vonatkozó információkat. Magától értetődik, hogy az ilyen fennmaradó adatokat a közösségimédia-szolgáltató csak belsőleg tárolja, és azok nem lehetnek nyilvánosan láthatók más felhasználók számára. Az általános adatvédelmi rendelet 17. cikkének (3) bekezdése szerinti kivétel azonban semmiképpen sem teszi lehetővé a közösségimédia-szolgáltató számára, hogy a törlés iránti kérelmét követően a felhasználó által tervezettnél hosszabb ideig fenntartsa az érintett fiókját.

164. A fiók törlésére irányuló kérelemtől függetlenül, ha a felhasználók az általános adatvédelmi rendelet 7. cikkének (3) bekezdése alapján visszavonják hozzájárulásukat, a hozzájárulás alapján szolgáltatott adataiknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének a) pontja szerinti kezelésére már nem kerülhet sor. Ebben az esetben bizonyos körülmények között továbbra is sor kerülhet egyéb adatkezelési műveletekre, amennyiben a közösségimédia-szolgáltató az általános adatvédelmi rendelet 6. cikkének (1) bekezdése szerinti egyéb jogalapokra támaszkodik.
165. Ha azonban a felhasználók fiókjuk törlését kérik, a mögöttes jogalaptól függetlenül további adatkezelésre nem kerülhet sor, kivéve, ha az általános adatvédelmi rendelet 17. cikkének (3) bekezdésében tételesen felsorolt kivételek valamelyike alkalmazandó. Ebben az összefüggésben fontos szem előtt tartani, hogy a megőrzés a fent említett minimális tárolásra korlátozódik.
166. Az általános adatvédelmi rendelet 25. cikkének (1) bekezdése szerint az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell végrehajtania az adatvédelmi elvek gyakorlati megvalósítása érdekében. A beépített és alapértelmezett adatvédelemről szóló 4/2019. sz. iránymutatás szerint a technikai és szervezési intézkedések tágabb értelmezés szerint bármely olyan módszert vagy eszközt jelenthetnek, amelyet az adatkezelő az adatkezelés során alkalmazhat. A megfelelés azt jelenti, hogy az intézkedéseknek a tervezett cél teljesítéséhez kell igazodniuk, azaz hatékonyan kell érvényesíteniük az adatvédelmi elveket. A megfelelés követelménye tehát szorosan kapcsolódik a hatékonyság követelményéhez⁷⁴.

⁷⁴ Az Európai Adatvédelmi Testület 4/2019. sz. iránymutatása a 25. cikk szerinti beépített és alapértelmezett adatvédelemről, 6. o., 8. pont.

ii. A fiók szüneteltetése

167. Alternatív megoldásként a felhasználóknak lehetőségük van arra, hogy ideiglenesen deaktiválják fiókjukat, ami lehetővé teszi számukra, hogy fiókjuk végleges törlése nélkül egy bizonyos időre elhagyják a közösségi médiát. Ebben az esetben a fiók átmenetileg le van tiltva, és a profilt, a képeket, a hozzászólásokat és a reakciókat mindaddig elrejtik, amíg a felhasználó újra nem aktiválja fiókját, pl. azáltal, hogy ismét bejelentkezik. A törléshez képest a fő különbség az, hogy a személyes adatok megmaradnak a közösségi hálózaton, és a felhasználók új regisztráció nélkül újraaktiválhatják a fiókot.
168. A fióktörlés folyamatát megkezdő felhasználók azt tapasztalhatják, hogy a fiók szüneteltetése opció van előre kijelölve. Bár azoknak a felhasználóknak, akik még nem szeretnék véglegesen törölni fiókjukat, hasznos lehet, hogy felkínálják számukra a szüneteltetés opciót, a közösségimédia-szolgáltatók nem írhatnak elő ilyen megfontolási időt a felhasználók számára, különösen nem előre kijelölés révén. A közösségimédia-szolgáltató azáltal, hogy lehetőséget kínál a deaktiválásra, észszerű elvárásokat ébreszt a felhasználókban arra vonatkozóan, hogy személyes adataikat ne ugyanolyan módon kezeljék, mint a fiók aktív használata során, és hogy a közösségimédia-szolgáltató a személyes adatok feldolgozását ezen időszak alatt a szigorúan szükséges szintre csökkentse. A felhasználók arra számíthatnak, hogy adataikat nem vagy nem teljes mértékben kezelik meghatározott célokból, például azáltal, hogy profiljukat olyan harmadik felek weboldalain tett látogatásokkal bővítik, amelyek arra alkalmas célzasi vagy nyomon követési eszközöket használnak. Amellett, hogy átlátható módon tájékoztatják a felhasználókat a felhasználói fiókjuk szüneteltetésének következményeiről, az ilyen szüneteltetés alatt végzett adatkezelésnek érvényes jogalapra kell támaszkodnia.
169. Az általános adatvédelmi rendelet 6. cikke (1) bekezdésének a) pontja szerinti hozzájáruláson alapuló adatkezelés tekintetében a közösségimédia-szolgáltatónak figyelembe kell vennie, hogy a felhasználók várakozásai szerint a regisztráció során vagy azt követően megadott hozzájárulás csak a fiók aktív használata során végzett adatkezelésre terjed ki. Az Európai Adatvédelmi Testület elismeri, hogy a hozzájárulás időtartama a kontextustól, az eredeti hozzájárulás hatályától és az érintett elvárásaitól függ⁷⁵. Bár az általános adatvédelmi rendeletben nem szerepel konkrét határidő a hozzájárulás időtartamára vonatkozóan, az érvényesség a kontextustól, az eredeti hozzájárulás hatályától és az érintett elvárásaitól függ⁷⁶. Ha az adatkezelési műveletek jelentősen megváltoznak vagy módosulnak, akkor az eredeti hozzájárulás tovább már nem érvényes⁷⁷. Az Európai Adatvédelmi Testület bevált gyakorlatként azt ajánlja, hogy a hozzájárulást megfelelő időközönként frissítsék⁷⁸. Valamennyi információ megadása szintén segít annak biztosításában, hogy az érintett tájékozott maradjon az adatai felhasználásának módját és a jogai gyakorlásának módját illetően⁷⁹. Ebben az esetben ismét be kell szerezni a hozzájárulást⁸⁰, és minden vonatkozó követelménynek teljesülnie kell.
170. Az általános adatvédelmi rendelet 6. cikke (1) bekezdésének f) pontja alkalmazásakor az érintett észszerű elvárásait is figyelembe kell venni (lásd a (47) preambulumbekendést). Különösen azt kell megvizsgálni, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. A felhasználók azonban arra számíthatnak, hogy a deaktiválás ideje alatt csak a szükséges adatkezelésre kerül sor. Ezenkívül a közösségimédia-szolgáltató csak akkor hivatkozhat a jogos érdekre, ha a jogos érdek vizsgálatának

⁷⁵ A hozzájárulásról szóló 5/2020. sz. iránymutatás, 110. pont.

⁷⁶ A hozzájárulásról szóló 5/2020. sz. iránymutatás, 110. pont.

⁷⁷ A hozzájárulásról szóló 5/2020. sz. iránymutatás, 110. pont.

⁷⁸ A hozzájárulásról szóló 5/2020. sz. iránymutatás, 111. pont.

⁷⁹ A hozzájárulásról szóló 5/2020. sz. iránymutatás, 111. pont.

⁸⁰ A hozzájárulásról szóló 5/2020. sz. iránymutatás, 110. pont.

valamennyi lépése teljesül, beleértve a mérlegelést is. Az érintett bármely nyomós érdekét vagy alapvető jogait és szabadságait eseti alapon kell értékelni.

171. Mivel a deaktiválás során a szerződéses kötelezettségek is nagyrészt felfüggesztésre kerülnek, az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja értelmében az adatkezelési műveletekre csak korlátozott mértékben van szükség. Csak a felhasználók adatainak a reaktiválásra vagy törlésre vonatkozó végső döntésig történő tárolása tekinthető szükségesnek.
172. Tekintettel arra, hogy minden korábbi adatkezelés egy aktív fiókra irányult, további tájékoztatást kell nyújtani a deaktiválás alatti adatkezelésről, ha az nem szerepel az általános adatvédelmi rendelet 13. és 14. cikke szerinti általános tájékoztatásban. Ez az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja szerinti átláthatóság és tisztességes eljárás, valamint az általános adatvédelmi rendelet 5. cikke (1) bekezdésének b) pontja szerinti célhoz kötöttség elvéből következik. A deaktiválást követő adatkezelést az érintett megfelelő tájékoztatásának kell kísérnie. Ezért a közösségimédia-szolgáltatónak átfogóan tájékoztatnia kell a felhasználókat a szüneteltetés során történő tényleges adatkezelésről és annak céljairól, és szükség esetén új hozzájárulást kell beszereznie.

b. Megtévészto tervezési megoldások

i. Tartalomalapú megoldások

Túlterhelés – Adatvédelmi útvesztő (I. melléklet, az ellenőrző lista 4.1.2. pontja)

173. Ebben a használati esetben az **adatvédelmi útvesztő** megtévészto tervezési megoldás fordul elő, amikor a felhasználókat több helyen elszórt, nagy mennyiségű információval árasztják el, hogy megakadályozzák őket abban, hogy töröljék fiókjukat, ahogy az alábbi példa is mutatja. Bár e lépés előtt valóban kívánatos néhány további információ, például annak feltüntetése, hogy a felhasználók a törlés előtt hozzáférnek az adataikhoz, az általános, nem kapcsolódó információk már nem kulcsfontosságúak. A felhasználókat nem szabad szükségtelenül hátráltatni e lépés megtételében.

52. példa: A felhasználók a törléshez való jogot szeretnék megtalálni. Elő kell hívniuk a fiókbeállításokat, meg kell nyitniuk egy „a magánélet védelme” (privacy) elnevezésű almenüt, és teljesen le kell görgetniük az oldal aljáig, hogy megtalálják a fiók törléséhez vezető hivatkozást.

Felkavarás – Érzelmű befolyásolás (I. melléklet, az ellenőrző lista 4.3.1. pontja)

53. példa: Az első információs szinten a felhasználókat csak a fiókjuk törlésének negatív következményeiről tájékoztatják (pl. „mindent örökre elveszítesz” vagy „a barátaid el fognak felejteni”).

174. Míg a szerződéses jogviszony megszüntetésével kapcsolatos sajnálkozás társadalmi szempontból megfelelőnek tűnik, és ezért jogi értelemben nehezen megragadható, a fiókjukat törölő felhasználók által okozott állítólagos negatív következmények átfogó leírása akadályozza döntésüket, ha az a fenti példához hasonlóan a kimaradástól való félelemre (fear of missing out, FOMO) épít, ami a fiók törlésére vonatkozó döntést különösen súlyosnak tünteti fel. Az ilyen **érzelmű befolyásolás**, amely azzal fenyegeti a felhasználókat, hogy a fiókjuk törlése esetén magukra maradnak, sérti az általános adatvédelmi rendelet 12. cikkének (2) bekezdése szerinti, az érintettek jogai gyakorlásának elősegítésére vonatkozó kötelezettséget, valamint az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontja szerinti tisztességes eljárás elvét.

Sötétben hagyás – Félreérthető megfogalmazás vagy tájékoztatás (I. melléklet, az ellenőrző lista 4.6.3. pontja)

175. A közösségimédia-fiók törlésével összefüggésben a felhasználók a **félreérthető megfogalmazás vagy tájékoztatás** megtévesztő tervezési megoldással is szembesülhetnek, amint azt a következő példa mutatja.

54. példa: Amikor a felhasználók törlik felhasználói fiókjukat, nem kapnak tájékoztatást arról, hogy a fiók törlése után mennyi ideig őrzik meg adataikat. Ami még rosszabb, hogy a törlési folyamat egyetlen pontján sem tájékoztatják a felhasználókat arról, hogy a „*személyes adataik egy részét*” a fiók törlése után is tárolhatják. Saját maguknak kell kikeresniük ezt az információkat a különböző elérhető információforrásokból.

55. példa: A felhasználók csak a fiókjukban elérhető „*Viszlát*” vagy „*Deaktiválás*” elnevezésű hivatkozásokon keresztül törölhetik fiókjukat.

176. Ezekben a példákban a hivatkozásokhoz használt szövegezés nem utal egyértelműen arra a tényre, hogy a felhasználókat a fióktörlési folyamatra fogják átirányítani. Ehelyett a felhasználók valószínűleg más funkciókra gondolnak, például a következő használatig történő kijelentkezésre vagy fiókjuk deaktiválására. Ez az általános adatvédelmi rendelet 12. cikke (2) bekezdésének megsértéseként értelmezhető, amely kimondja, hogy az adatkezelőknek elő kell segíteniük az érintettek jogainak gyakorlását. A közösségimédia-platform azáltal, hogy zavart kelt a felhasználóknak a hivatkozással kapcsolatos elvárásaiban, nem segíti elő teljes mértékben a törléshez való jog gyakorlását. Az ilyen kétértelmű szavak más összefüggésben történő használata sértheti az általános adatvédelmi rendelet olyan rendelkezéseit, mint az általános adatvédelmi rendelet 7. cikke, és ezáltal az általános adatvédelmi rendelet 17. cikke (1) bekezdésének b) pontja.

ii. Interfészalapú megoldások

Átugrás – Megtévesztő biztonság (I. melléklet, az ellenőrző lista 4.2.1. pontja)

56. példa: Fiókjuk törlése során a felhasználók két választási lehetőséget kapnak: Törölhetik, illetve szüneteltethetik fiókjukat. Alapértelmezés szerint a szüneteltetés opció van kijelölve.

177. Az első, a fiók törlésére vonatkozó opció a felhasználó valamennyi személyes adatának törlését eredményezi, ami azt jelenti, hogy a közösségimédia-platform a továbbiakban nem rendelkezik ezekkel az adatokkal, kivéve az általános adatvédelmi rendelet 17. cikkének (3) bekezdésében foglalt átmeneti kivétel hatálya alá tartozó adatokat. Ezzel szemben a második opcióval, a felhasználói fiók használatának szüneteltetésével a közösségimédia-szolgáltató minden személyes adatot megtart és potenciálisan kezel. Ez szükségszerűen nagyobb kockázatot jelent az érintett számára, például ha adatvédelmi incidens történik, és a közösségimédia-szolgáltató által továbbra is tárolt adatokhoz hozzáférnek, illetve lemásolják, továbbítják vagy más módon kezelik azokat. A szüneteltetési opció alapértelmezett kijelölése valószínűleg arra ösztönzi a felhasználókat, hogy ezt válasszák ahelyett, hogy az eredeti szándék szerint törölnék a fiókjukat. Ezért az e példában ismertetett gyakorlat az általános adatvédelmi rendelet 12. cikke (2) bekezdése megsértésének tekinthető, mivel az ebben az esetben nem segíti elő a törléshez való jog gyakorlását, sőt, megpróbálja eltántorítani a felhasználókat attól.

Átugrás – Figyelemelterelés (I. melléklet, az ellenőrző lista 4.2.2. pontja)

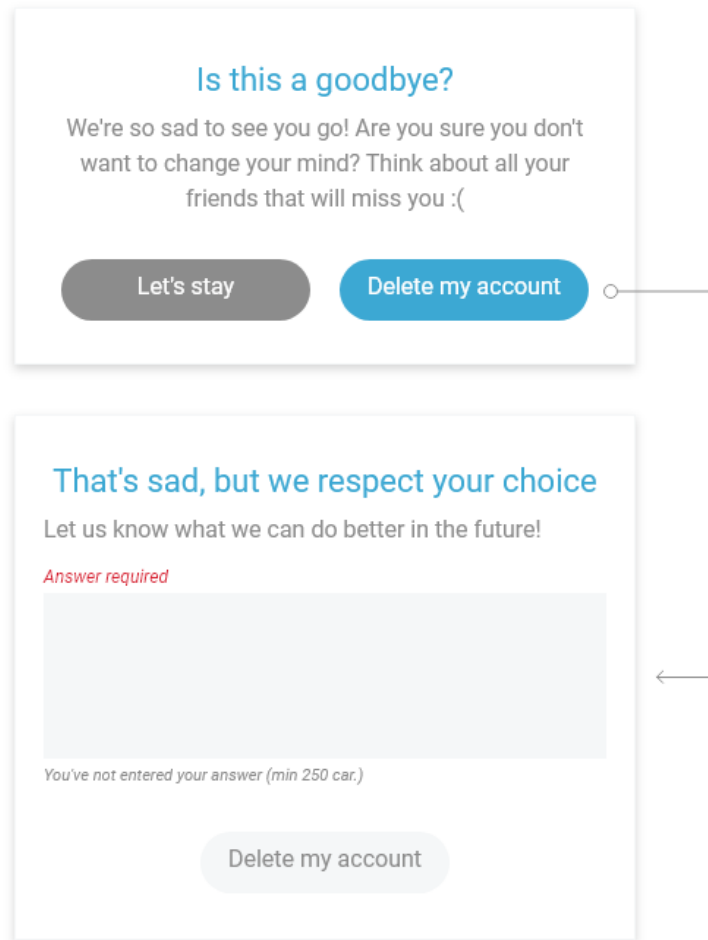
178. Fontos lehetőség lehet, ha a felhasználók számára lehetővé teszik adataik letöltését, amikor jelzik a fiókjuk törlésére irányuló szándékukat. A fiókjuk törlését követően személyes adataikat bizonyos idő elteltével törlik. Ez azt jelenti, hogy ha nem kapnak másolatot személyes adataikról, akkor teljesen elveszítik azokat. Ennek az opciónak a bemutatása azonban a **figyelemelterelés** megtévesztő tervezési megoldást jelentheti, amint azt az alábbi példa mutatja.

57. példa: A „Törölöm a fiókom” gombra kattintva a felhasználóknak lehetőségük nyílik arra, hogy a fiók törlése előtt letöltsék adataikat, ami a hordozhatósághoz való jogot valósítja meg. Az információk letöltésére kattintva a felhasználókat átirányítják a letöltési információk oldalra. Azt követően azonban, hogy a felhasználók eldöntötték, mit és hogyan töltsenek le, nem irányítják tovább őket a törlési folyamatra.

179. A fenti példában úgy tekinthető, hogy a letöltési lehetőség megvalósításának módja nem segíti elő a fiók törléséhez kapcsolódó törléshez való jog gyakorlását. Miután a felhasználók letöltötték adataikat, az oldal nem viszi vissza őket a törlési folyamatba. Ahhoz, hogy visszatérjenek ahhoz, többször kell kattintaniuk. Valamely jog gyakorlásának ily módon történő akadályozása sérti az általános adatvédelmi rendelet 12. cikkének (2) bekezdését. Ezen túlmenően egy olyan eszköz biztosítása, amely lehetővé teszi a törlési folyamat könnyű elérését az adatok letöltése után, egyszerűen kivitelezhető. E tekintetben megállapítható, hogy az általános adatvédelmi rendelet 25. cikkének (1) bekezdésében foglalt, a megfelelő technikai és szervezési intézkedések végrehajtására vonatkozó kötelezettséget a közösségi oldal nem tartja tiszteletben, mivel a felhasználók nem tudják folytatni jogaik hatékony gyakorlását.

Akadályozás – Indokolatlanul hosszú folyamatok (I. melléklet, az ellenőrző lista 4.4.2. pontja)

180. Amint azt a 4. használati eset részletesen kifejti, valamely jog gyakorlásához bármilyen nem releváns lépés hozzáadása ellentétes lehet az általános adatvédelmi rendelet rendelkezéseivel, különösen a 12. cikk (2) bekezdésével. Ez arra a pillanatra vonatkozik, amikor a felhasználók fiókjukat törölni kívánják, mivel ez sértene az ilyen kérelemhez kapcsolódó törléshez való jogot.



58. példa: Ebben a példában a felhasználók először egy a fiókjuk törlését megerősítő párbeszédpanel látnak, miután rákattintottak a megfelelő hivatkozásra vagy gombra a fiókjukban. Annak ellenére, hogy a párbeszédpanelben van némi **érzelmi befolyásolás**, ez a lépés biztonsági intézkedésnek tekinthető annak érdekében, hogy a felhasználók ne töröljék fiókjukat, ha félrekattintanak a fiókjukban. Amikor azonban a felhasználók a „Törölöm a fiókom” gombra kattintanak, egy második párbeszédpanellel találkoznak, amelyben arra kéri őket, hogy szövegesen írják le, hogy miért kívánják felszámolni a fiókot. Mindaddig, amíg nem írtak be valamit a szövegdobozba, nem törölhetik fiókjukat, mivel a művelethez tartozó gomb inaktív és szürke. Ez a gyakorlat az **indokoltnál hosszabbá** teszi a fióktörlés folyamatát, különösen mivel az, hogy a felhasználókat arra kéri, írják le, hogy miért akarják felszámolni a fiókjukat, extra erőfeszítést és időt igényel, aminek nem kellene kötelezőnek lennie a fiók törléséhez.

181. Amint azt már korábban említettük, valamely jog gyakorlása során a felhasználók nem kötelezhetőek arra, hogy olyan kérdésekre válaszoljanak, amelyek nem kapcsolódnak magához a jog gyakorlásához. Az, ha meg kell indokolniuk döntésüket, vagy ki kell fejteniük, hogyan lehetne javítani a közösségimédia-platfomot, nem tartozik ebbe a kategóriába. Az illusztrált példában ez a probléma még súlyosabb, mivel az érintetteknek be kell gépelniük a választ, ahelyett, hogy előre elkészített javaslatok közül választhatnának, ami még nagyobb terhet jelent számukra, mivel a választ teljes

mértékben nekik kell megszövegezniük. Egy ilyen mechanizmus egyes felhasználókat teljesen kizárhat jogaik gyakorlásától, amennyiben nem érzik elég felkészültnek magukat a válasz megírásához.

182. Ez azonban nem jelenti azt, hogy az előre kidolgozott válaszok listájának hozzáadása a fiók törlésének folyamatához elfogadható lépés lenne. Ez különösen akkor igaz, ha ezek a válaszok a felhasználókat terhelő további lépésekhez és intézkedésekhez kapcsolódnak, amint azt az alábbi példa mutatja.

59. példa: A közösségimédia-szolgáltató kötelezővé teszi a felhasználók számára, hogy egy legördülő menüből kiválasztott válasz segítségével válaszolják meg az arra vonatkozó kérdést, hogy miért kívánják törölni fiókjukat. A felhasználók számára úgy tűnik, hogy e kérdés megválaszolása (látszólag) lehetővé teszi számukra, hogy elérjék a kívánt műveletet, azaz a fiók törlését. A válasz kiválasztását követően egy felugró ablak jelenik meg, amely megmutatja a felhasználóknak, hogyan tudják megoldani a válaszban szereplő problémát. A kérdés-válasz folyamat ezért lelassítja a felhasználók fióktörlési folyamatát.

183. Amellett, hogy a fiók törlése különösen hosszadalmassá válik, a **figyelemelterelés** mechanizmus célja, hogy a felhasználókat eltérítse a fiókjuk törlésétől azáltal, hogy megoldást kínál a közösségimédia-platform elhagyását kiváltó okra. Ezek akadályozzák a törléshez való jog gyakorlását, és ezáltal visszatartják az érintetteket jogaik gyakorlásától.

Összefoglalás – Váratlan szövegkörnyezetbe helyezés (I. melléklet, az ellenőrző lista 4.5.2. pontja)

184. Végezetül, a **váratlan szövegkörnyezetbe helyezés** megtévesztő tervezési megoldással is találkozhatunk, amikor a felhasználó törölni kívánja fiókját.

60. példa: Az XY közösségimédia-platformon a fiók deaktiválásához vagy törléséhez vezető hivatkozás „Az Ön XY adatai” fülön található.

185. Általánosságban elmondható, hogy a közösségimédia-platform adatvédelmi kérdésekkel foglalkozó oldalának vagy az oldal egy szakaszának címeként használt kifejezéseknek egyértelműen tükrözniük kell az ott szereplő információ vagy ellenőrzés jellegét. Az átlagos felhasználók valószínűleg nem kapcsolják össze a fiókjuk törlésére vagy deaktiválására irányuló műveleteket az adatkezeléssel. Az előző példában a felhasználók nem számítanak a fiókjuk törlésére szolgáló funkcióra „Az Ön XY adatai” elnevezésű oldalon, ami az információ megtekintésére és esetleges felülvizsgálatára utal. Ehelyett egy „Általános” vagy egy „A fiókom törlése” elnevezésű oldalt keresnének. Ezért a felhasználók szempontjából az opciók egy a kontextusból kiragadott környezetbe vannak elhelyezve, ami nem felel meg várakozásaiknak.

61. példa: A fiók törlésére szolgáló tényleges fül az „a fiók egy funkciójának törlése” szakaszban található.

186. Ebben a példában a felhasználók tévesen úgy értelmezhetik a szakasz címét, mintha az csupán egyes funkciók módosítására szolgáló hely lenne. A felhasználók ezért nem számítanak arra, hogy ott találják a teljes fiók törlésének lehetőségét. Ez megnehezíti számukra, hogy megtalálják a megfelelő hivatkozást a teljes fiók törléséhez.

187. A fenti két példában bemutatott **váratlan szövegkörnyezetbe helyezés** megtévesztő tervezési megoldás az általános adatvédelmi rendelet 12. cikke (2) bekezdése megsértésének tekinthető, mivel
- Elfogadott

a felhasználók nehézségekbe ütköznek a törléshez való joguk gyakorlására szolgáló hely megtalálása során.

c. Bevált gyakorlatok

Koherens megfogalmazás: A fogalom meghatározást lásd az 1. használati esetről (29. o.).

Fogalom meghatározások: A fogalom meghatározást lásd az 1. használati esetről (29. o.).

Példák használata: A fogalom meghatározást lásd az 1. használati esetről (29. o.).

A következmények magyarázata: A fogalom meghatározást lásd a 2c. használati esetről (41. o.).

Eszközök közötti konzisztencia: A fogalom meghatározást lásd a 3a. használati esetről (57. o.).

Az Európai Adatvédelmi Testület részéről

az elnök

(Andrea Jelinek)

4 I. MELLÉKLET: A MEGTÉVESZTŐ TERVEZÉSI MEGOLDÁSOK KATEGÓRIÁINAK ÉS TÍPUSAINAK JEGYZÉKE

Az alábbi jegyzék áttekintést nyújt a megtévesztő tervezési megoldások kategóriáiról és a megtévesztő tervezési megoldások egyes kategóriákon belüli típusairól. Felsorolja továbbá az általános adatvédelmi rendeletnek a megtévesztő tervezési megoldások különböző típusainak szempontjából leginkább jelentéssel bíró rendelkezéseit. Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének a) pontjában meghatározott tisztességes adatkezelés elve kiindulópontként szolgál annak megállapítására, hogy vannak-e megtévesztő tervezési megoldások. A tisztességes eljárás elve átfogó jellegű, és egyetlen megtévesztő tervezési megoldás sem felel meg annak, függetlenül attól, hogy megfelelnek-e más adatvédelmi elveknek⁸¹.

A jegyzék minden egyes megoldás esetében tartalmazza a példák és a kapcsolódó használati esetek számát is, hogy az olvasók gyorsan megtalálhassák azokat.

Fontos megjegyezni, hogy ez a jegyzék nem teljes körű, ezért megtévesztő tervezési megoldások előfordulhatnak olyan használati esetekben is, amelyekre vonatkozóan az iránymutatás szövege nem tartalmaz példát az adott megtévesztő tervezési megoldástípusra.

4.1 Túlterhelés

A felhasználók elárasztása kérések, információk, opciók vagy lehetőségek sokaságával annak érdekében, hogy visszatartsák őket a folytatástól, és rávegyék őket bizonyos adatkezelési gyakorlatok megtartására vagy elfogadására.

4.1.1 Folyamatos noszogatás⁸²

A felhasználók rábírása arra, hogy az adatkezelés céljaihoz szükségesnél több személyes adatot adjanak meg, vagy hogy hozzájáruljanak adataik más célú felhasználásához azáltal, hogy újra és újra adatok szolgáltatására vagy az adatkezelés valamely új céljához való hozzájárulásra kéri őket. Ezek az ismétlődő felszólítások egy vagy több eszközön keresztül is bekövetkezhetnek. A felhasználók végül valószínűleg beadják a derekukat, miután belefáradtak abba, hogy minden egyes alkalommal, amikor a platformot használják, vissza kell utasítaniuk a kérést, ami megzavarja őket annak használatában.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *célhoz kötöttség: 5. cikk, (1) bekezdés, b) pont,*
- *önkéntes hozzájárulás: 7. cikk, a 4. cikk 11. pontjával összefüggésben,*
- *kifejezett hozzájárulás: 7. cikk, (2) bekezdés.*

Példák: 1. használati eset, 1., 2. példa; 3a. használati eset, 34. példa (illusztráció).

⁸¹ Lásd ezen iránymutatás fenti 9. pontját.

⁸² Ez a megoldás szorosan összefügg a szakirodalomban található, úgynevezett „zaklatás” (nagging) megoldással.

4.1.2 Adatvédelmi útvesztő

Amikor a felhasználók bizonyos információkhoz szeretnének hozzájutni, egy adott beállítást szeretnének használni, vagy valamelyik érintetti jogot szeretnék gyakorolni, különösen nehéz megtalálniuk azt, mivel – átfogó és teljes körű áttekintés hiányában – túl sok oldalt kell átvizsgálniuk ahhoz, hogy hozzájussanak a megfelelő információhoz vagy beállításhoz. A felhasználók valószínűleg feladják, vagy átsiklanak a vonatkozó információ vagy beállítás felett.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *az átláthatóság elve: 5. cikk, (1) bekezdés, a) pont és átlátható tájékoztatás: 12. cikk, (1) bekezdés,*
- *a tisztességes eljárás elve: 5. cikk, (1) bekezdés, a) pont,*
- *könnyen hozzáférhető információ: 12. cikk, (1) bekezdés,*
- *egyszerű hozzáférés a jogokhoz: 12. cikk, (2) bekezdés,*
- *tájékoztatáson alapuló hozzájárulás: 7. cikk, a 4. cikk 11. pontjával összefüggésben.*

Példák: 2a. használati eset, 17. példa; 3a. használati eset, 33. példa; 3a. használati eset, 37. példa; 4. használati eset; 47. példa (illusztráció) és 48. példa (illusztráció); 5. használati eset, 51. példa.

4.1.3 Túl sok választási lehetőség

A felhasználók számára (túl) sok választási lehetőség biztosítása. A választási lehetőségek nagy mennyisége miatt a felhasználók nem tudnak döntést hozni, vagy figyelmen kívül hagynak bizonyos beállításokat, különösen, ha nem áll rendelkezésükre megfelelő információ. Ez arra készítheti őket, hogy végül feladják vagy elmulasztják adatvédelmi preferenciáik vagy jogaik beállítását.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *az átláthatóság és a tisztességes eljárás elve: 5. cikk, (1) bekezdés, a) pont,*
- *átlátható tájékoztatás: 12. cikk, (1) bekezdés.*

Példák: 3a. használati eset, 35. példa.

4.2 Átugrás

Az interfész vagy a felhasználói útvonal oly módon történő megtervezése, hogy a felhasználók megfedkezzenek az adatvédelmi szempontokról vagy azok egy részéről, illetve eszközbe se jussanak azok.

4.2.1 Megtévesztő biztonság

Alapértelmezés szerint a leginkább adatinvazív funkció és opció van engedélyezve. Az alapértelmezett hatás miatt, amely arra ösztönzi az egyéneket, hogy megtartsák az előre kiválasztott opciót, a felhasználók valószínűleg akkor sem változtatnak ezeken, ha lehetőségük van rá.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *beépített és alapértelmezett adatvédelem*: 25. cikk, (1) bekezdés,
- *hozzájárulás*: 4. cikk, 11. pont és 6. cikk (alapértelmezett hozzájáruláson alapuló adatkezelés indításának jogellenes gyakorlata).

Példák: 1. használati eset, 9. példa; 3b. használati eset; 39. és 40. példa (illusztráció); 5. használati eset, 55. példa.

4.2.2 Figyelemelterelés

Az adatvédelemmel kapcsolatos intézkedés vagy információ egy másik, az adatvédelemhez kapcsolódó vagy ahhoz nem kapcsolódó elemmel kerül versenybe. Amikor a felhasználók ezt a figyelemelterelő lehetőséget választják, valószínűleg megfelelnek a másiktól, még akkor is, ha az volt az eredeti szándékuk.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *az átláthatóság és a tisztességes eljárás elve*: 5. cikk, (1) bekezdés, a) pont,
- *átlátható tájékoztatás*: 12. cikk, (1) bekezdés,
- *a jogok gyakorlása*: 12. cikk, (2) bekezdés.

Példák: 2c. használati eset, 25. példa; 3a. használati eset, 29. példa; 5. használati eset, 56. és 58. példa.

4.3 Felkavarás

A felhasználók döntéseinek az érzelmeikre való apellálással vagy vizuális ösztönzéssel történő befolyásolása.

4.3.1 Érzelmi befolyásolás⁸³

A szövegek vagy vizuális elemek (például stílus, színek, képek stb.) oly módon történő használata, ami az információt a felhasználóknak vagy nagyon pozitív perspektívából közvetíti, így a felhasználók jól, biztonságban vagy megjutalmazva érzik magukat, vagy rendkívül negatív perspektívából, ami miatt a felhasználók szoronganak, bűnösnek vagy büntetve érzik magukat. A felhasználók érzelmi állapotának ily módon történő befolyásolása olyan cselekvésre készíti őket, amely ellentétes az adatvédelmi érdekeikkel.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *az átláthatóság és a tisztességes eljárás elve*: 5. cikk, (1) bekezdés, a) pont,
- *átlátható tájékoztatás*: 12. cikk, (1) bekezdés,

⁸³ Ez a megoldás szorosan összefügg az „*érzelmekkel való játszadozás*” tervezési megoldással, amely megtalálható többek között kormányközi szervezetek jelentéseiben, mint például: az Európai Bizottság Jogértvényesülési és Fogyasztópolitikai Főigazgatósága, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Bogliacino, F., et al.: *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report* (Viselkedéstudományi tanulmány a digitális környezetben tapasztalható tisztességtelen kereskedelmi gyakorlatokról: sötét megoldások és manipulatív személyre szabási gyakorlatok: zárójelentés), az Európai Unió Kiadóhivatala, 2022, <https://data.europa.eu/doi/10.2838/859030> és OECD (2022): „Dark commercial patterns” (Sötét kereskedelmi megoldások), *Documents de travail de l'OCDE sur l'économie numérique*, n° 336., Éditions OCDE, Párizs, <https://doi.org/10.1787/44f5e846-en>.

- *a jogok gyakorlása*: 12. cikk, (2) bekezdés,
- *a gyermek hozzájárulása*: 8. cikk,
- *tájékoztatáson alapuló hozzájárulás*: 7. cikk, a 4. cikk 11. pontjával összefüggésben.

Példák: 1. használati eset, 4., 5. és 6. példa; 5. használati eset, 52. példa.

4.3.2 Bújtatott közzététel

Olyan vizuális stílus vagy technika használata a tájékoztatáshoz vagy az adatvédelmi beállításokhoz, amely a felhasználókat a kevésbé szigorú és ezáltal invazívabb lehetőségek felé tereli.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *a tisztességes eljárás elve*: 5. cikk, (1) bekezdés, a) pont,
- *önkéntes hozzájárulás*: 7. cikk, a 4. cikk 11. pontjával összefüggésben,
- *világos tájékoztatás*: 12. cikk, (1) bekezdés,
- *a jogok gyakorlása*: 12. cikk, (2) bekezdés.

Példák: 1. használati eset, 8. példa, 3a. használati eset, 34. példa (illusztráció); 3a. használati eset, 40. példa (illusztráció); 4. használati eset, 48. példa.

4.4 Akadályozás⁸⁴

A felhasználók akadályozása vagy gátolása az információszerzésben vagy adataik kezelésben azáltal, hogy megnehezítik vagy lehetetlenné teszik a művelet végrehajtását.

4.4.1 Zsákutca

Miközben a felhasználók információt keresnek vagy a beállításokat keresik, végül nem találják meg azokat, mivel az átirányító hivatkozás vagy nem működik, vagy egyáltalán nincs is. A felhasználók nem tudják elvégezni a műveletet.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *könnyen hozzáférhető információ*: 12. cikk, (1) bekezdés,
- *a jogok gyakorlása*: 12. cikk, (2) bekezdés,
- *beépített és alapértelmezett adatvédelem*: 25. cikk, (1) bekezdés.

Példák: 1. használati eset, 10. és 11. példa; 2a. használati eset, 18. példa; 3a. használati eset, 30., 31. példa; 4. használati eset, 43. példa.

⁸⁴ Ez a kategória szorosan kapcsolódik a Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph és Toombs Austin L. (2018) által meghatározott és ismertetett „Obstruction” (akadályozás) elnevezésű stratégiához. The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canada) (CHI '18). ACM, New York, NY, USA, 534. cikk, 14. oldal. <https://doi.org/10.1145/3173574.3174108>.

4.4.2 Indokolatlanul hosszú folyamatok

Amikor a felhasználók az adatvédelemmel kapcsolatos ellenőrzést próbálnak aktiválni, de a felhasználói útvonal úgy van kialakítva, hogy a felhasználóknak több lépést kell végrehajtaniuk, mint ahány lépés az adatinvazív opciók aktiválásához szükséges. Ez valószínűleg visszatartja őket az ilyen ellenőrzés aktiválásától.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *könnyen hozzáférhető információ:* 12. cikk, (1) bekezdés,
- *a jogok gyakorlása:* 12. cikk, (2) bekezdés,
- *tiltakozáshoz való jog:* 21. cikk, (1) bekezdés,
- *hozzájárulás visszavonása:* 7. cikk, (3) bekezdés,
- *beépített és alapértelmezett adatvédelem:* 25. cikk, (1) bekezdés.

Példák: 1. használati eset, 7. példa; 3a. használati eset, 32. példa; 4. használati eset, 50. példa; 5. használati eset; 57. példa (illusztráció) és 58. példa.

4.4.3 Megtévesztő tevékenységek

A felhasználók rendelkezésére álló információk és tevékenységek közötti eltérés, ami arra készíti őket, hogy megtegyenek valamit, amit egyébként nem akartak megtenni. A felhasználók elvárásai és a kapott információk közötti különbség visszatartja őket attól, hogy folytassák a műveletet.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *átlátható tájékoztatás:* 12. cikk, (1) bekezdés,
- *tisztességes adatkezelés:* 5. cikk, (1) bekezdés, a) pont,
- *tájékoztatáson alapuló hozzájárulás:* 7. cikk, (2) bekezdés, a 4. cikk 11. pontjával összefüggésben.

Példák: 1. használati eset, 3. példa; 3a. használati eset, 28. példa.

4.5 Összezavarás

Az interfész kialakítása esetleges és következtelen, ami megnehezíti a felhasználók számára, hogy megismerjék az adatkezelés jellegét, megfelelő döntést hozzanak az adataikról, és megtalálják a különböző beállítások helyét.

4.5.1 A hierarchia hiánya

Az adatvédelemre vonatkozó információk nélkülözik a hierarchiát, emiatt az információk több helyen is előfordulnak, és többféleképpen kerülnek bemutatásra. A felhasználókat valószínűleg összezavarja ez a redundancia, és nem értik teljesen, hogyan kezelik adataikat, és hogyan rendelkezhetnek azok felett.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *könnyen hozzáférhető információ:* 12. cikk, (1) bekezdés,
- *a jogok gyakorlása:* 12. cikk, (2) bekezdés.

Példák: 2a. használati eset, 13. és 14. példa.

4.5.2 Váratlan szövegkörnyezetbe helyezés

Az adatvédelmi információk vagy beállítások egy olyan oldalon találhatóak, amely kívül esik a kontextuson. A felhasználók valószínűleg nem találják meg az információkat vagy a beállításokat, mivel nem lenne intuitív az adott oldalon keresniük azokat.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *könnyen hozzáférhető információ:* 12. cikk, (1) bekezdés,
- *átlátható tájékoztatás:* 12. cikk, (1) bekezdés,
- *a jogok gyakorlása:* 12. cikk, (2) bekezdés.

Példák: 3a. használati eset, 41–42. példa; 5. használati eset, 59. és 60. példa.

4.5.3 Következetlen interfész

Az interfész nem konzisztens a különböző kontextusokban (pl. az adatvédelmi menü nem ugyanazokat az elemeket jeleníti meg a mobilon és az asztali számítógépen), vagy nem felel meg a felhasználók elvárásainak (pl. olyan opció, amelynek helyét felcserélték egy másik opció helyével). Ezek a különbségek oda vezethetnek, hogy a felhasználók nem találják meg a kívánt beállítást vagy információt, vagy megszokásból lépnek interakcióba a felület valamelyik elemével, még akkor is, ha ez az interakció olyan adatvédelmi döntést eredményez, amelyet a felhasználók nem akarnak.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *könnyen hozzáférhető információ:* 12. cikk, (1) bekezdés,
- *a jogok gyakorlása:* 12. cikk, (2) bekezdés.

Példák: 3a. használati eset, 39. példa; 4. használati eset, 50. példa.

4.5.4 Nyelvi akadályok

Az adatvédelemmel kapcsolatos információkat a szolgáltatással ellentétben nem annak az országnak a hivatalos nyelvén vagy nyelvein adják meg, ahol a felhasználók élnek. Ha a felhasználók nem ismerik azt a nyelvet, amelyen az adatvédelmi információkat biztosítják, azokat nem fogják tudni könnyen elolvasni, és ezért nem lesznek tisztában személyes adataik kezelésének módjával.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *tisztességes adatkezelés:* 5. cikk, (1) bekezdés, a) pont,
- *érthető információk:* 12. cikk, (1) bekezdés, 13. cikk és 14. cikk,
- *világosan és közérthetően megfogalmazott tájékoztatás:* 12. cikk, (1) bekezdés, 13. cikk és 14. cikk.

Példák: 2a. használati eset, 16. példa; 3a. használati eset; 26. példa (illusztráció) és 27. példa; 4. használati eset, 44. példa.

4.6 Sötétben hagyás

Az interfészt olyan kialakítása, hogy elrejtse az információkat vagy az adatvédelmi beállításokat, vagy hogy a felhasználókat bizonytalanságban tartsa az adataik kezelésének módjával és az azok feletti rendelkezéssel kapcsolatosan.

4.6.1 Egymásnak ellentmondó információk

Olyan információk átadása a felhasználóknak, amelyek valamilyen módon ellentmondanak egymásnak. A felhasználók valószínűleg bizonytalanok lesznek a tekintetben, hogy mit kell tenniük, és milyen következményekkel járnak cselekedeteik, ezért valószínűleg nem tesznek semmit, és megtartják az alapértelmezett beállításokat.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *tisztességes adatkezelés:* 5. cikk, (1) bekezdés, a) pont,
- *átlátható tájékoztatás:* 12. cikk, (1) bekezdés,
- *tájékoztatáson alapuló hozzájárulás:* 7. cikk (2) bekezdés, a 4. cikk 11. pontjával összefüggésben.

Példák: 2a. használati eset, 12. példa; 2c. használati eset, 20. példa; 3a. használati eset, 36. példa.

4.6.2 Félreérthető megfogalmazás vagy tájékoztatás

Félreérthető és homályos kifejezések használata a felhasználók tájékoztatása során. A felhasználók valószínűleg bizonytalanok maradnak az adatkezelés módját, illetve azt illetően, hogy miként rendelkezhetnek személyes adataik felett.

Az általános adatvédelmi rendelet érintett rendelkezései:

- *tisztességes adatkezelés:* 5. cikk, (1) bekezdés, a) pont,
- *átlátható tájékoztatás:* 12. cikk, (1) bekezdés,
- *világosan és közérthetően megfogalmazott tájékoztatás:* 12. cikk, (1) bekezdés,
- *tájékoztatáson alapuló hozzájárulás:* 7. cikk (2) bekezdés, a 4. cikk 11. pontjával összefüggésben,
- *hiányos információk:* 13. cikk,
- *az adott használati esettől függő egyedi rendelkezések, például a 2c. használati esetről a 34. cikk.*

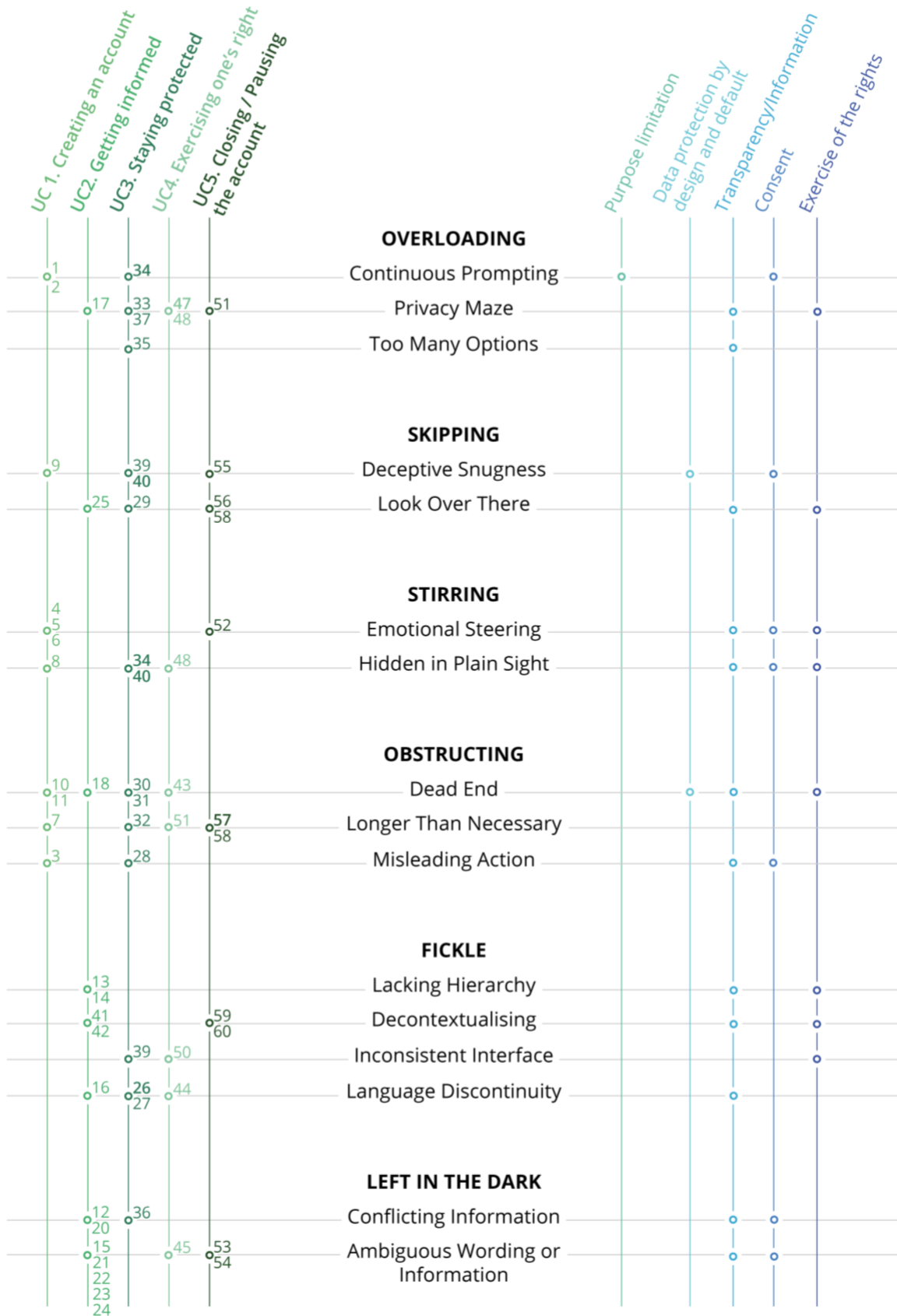
Példák: 2a. használati eset, 15. példa; 2c. használati eset, 21., 22., 23. és 24. példa; 4. használati eset, 45. példa; 5. használati eset, 53. és 54. példa.

LIFECYCLE

DECEPTIVE DESIGN OVERVIEW

GDPR PROVISIONS

All deceptive design go against the fairness principle



5 II. MELLÉKLET: BEVÁLT GYAKORLATOK

Az alábbi jegyzék áttekintést nyújt az iránymutatásban, az egyes használati esetek végén ismertetett bevált gyakorlatokról. Ezek felhasználhatók olyan felhasználói felületek kialakítására, amelyek elősegítik az általános adatvédelmi rendelet hatékony végrehajtását. Ezek a bevált gyakorlatok jelenthetik az első lépést ahhoz, hogy a felhasználók szabványosított módon rendelkezzenek adataik felett és gyakorolhassák jogaikat.

Hivatkozások: A felhasználók számára adataik és adatvédelmi beállítások kezeléséhez gyakorlati segítséget nyújtó információkra, műveletekre vagy beállításokra mutató hivatkozásoknak mindenhol elérhetőnek kell lenniük, ahol a kapcsolódó információkkal vagy tapasztalatokkal találkozhatnak (pl. az adatvédelmi szabályzat vonatkozó részeire átirányító hivatkozások; pl. az adatvédelmi nyilatkozatban minden egyes adatvédelmi információhoz olyan hivatkozásokat kell beszúrni, amelyek közvetlenül a közösségimédia-platform kapcsolódó adatvédelmi oldalaira irányítanak; hivatkozás biztosítása a felhasználók számára jelszavuk visszaállításához; ha a felhasználók tájékoztatást kapnak az adatkezelés valamely aspektusáról, felkérjük őket arra, hogy a vonatkozó adatpreferenciáikat a megfelelő beállítás oldalon/irányítópulton határozzák meg; a felhasználói fiók törlésére mutató hivatkozás biztosítása a felhasználói fiókban).

Csoportosított opciók: Az azonos adatkezelési célt szolgáló lehetőségek egy helyen történő elhelyezése annak érdekében, hogy a felhasználók könnyebben módosíthassák azokat, miközben továbbra is lehetőséget kapnak arra, hogy részletesebb változtatásokat hajtsanak végre. Ha a közösségimédia-platformok csoportosított opciókat kínálnak, ezek nem tartalmazhatnak váratlan vagy egymáshoz nem kapcsolódó elemeket (például különböző célú elemeket). Ha az adatkezeléshez hozzájárulásra van szükség, a csoportosított opcióknak összhangban kell lenniük az Európai Adatvédelmi Testület hozzájárulásról szóló iránymutatásával, különösen annak 42–44. pontjával.

Elérhetőségek: Az adatvédelmi szabályzatban egyértelműen fel kell tüntetni az adatvédelmi kérések kezelésére szolgáló vállalati kapcsolattartási címet. Ennek egy olyan részben kell szerepelnie, ahol a felhasználók számíthatnak rá, például az adatkezelő személyazonosságára vonatkozó részben, a jogokkal kapcsolatos részben vagy az elérhetőségek részben.

A felügyeleti hatóság elérése: A felügyeleti hatóság konkrét megnevezésének feltüntetése, valamint a hatóság honlapjára vagy a panasz benyújtásához kapcsolódó weboldalra mutató hivatkozás. Ennek az információnak egy olyan részben kell szerepelnie, ahol a felhasználók számíthatnak rá, például a jogokkal kapcsolatos részben.

Az adatvédelmi szabályzat áttekintése: Az adatvédelmi szabályzat elején/tetején meg kell jeleníteni egy (összecsukható) tartalomjegyzéket címsorokkal és alcímekkel, amelyek az adatvédelmi nyilatkozat különböző szakaszait mutatják. Az egyes szakaszok nevei egyértelműen a pontos tartalomhoz vezetnek a felhasználót, és lehetővé teszik számára, hogy gyorsan beazonosítsa és elérje a keresett részt.

Változásfigyelés és összehasonlítás: Az adatvédelmi nyilatkozat módosítása esetén a korábbi változatok hozzáférhetővé tétele a verzió dátumával együtt, valamint a változások kiemelése.

Koherens megfogalmazás: A weboldal ugyanazokat a kifejezéseket és meghatározásokat használja ugyanazon adatvédelmi kérdések kapcsán. Az adatvédelmi szabályzatban használt kifejezéseknek meg kell egyezniük a platform többi részén használt kifejezésekkel.

Fogalommeghatározások: Ismeretlen vagy technikai szavak vagy szakzsargon használata esetén a közérthető nyelven megfogalmazott fogalommeghatározás segíti a felhasználókat abban, hogy megértsék a rendelkezésükre bocsátott információkat. A fogalommeghatározás közvetlenül a szövegben is megadható, amikor a felhasználók a szó fölé viszik a kurzort, illetve glosszáriumban is közzétehető.

Kontrasztos adatvédelmi elemek: Az adatvédelemmel kapcsolatos elemek vagy intézkedések vizuálisan feltűnővé tétele egy olyan felületen, amely nem közvetlenül a témával foglalkozik. Például, amikor nyilvános üzenetet tesznek közzé a platformon, a földrajzi helymeghatározás társítása feletti rendelkezésnek közvetlenül elérhetőnek és jól láthatónak kell lennie.

Adatvédelem a csatlakozáskor: Közvetlenül a fiók létrehozását követően a közösségimédia-szolgáltató az adatvédelemmel kapcsolatos pontokat épít bele a bemutatási élménybe, hogy a felhasználók zökkenőmentesen felfedezhessék és beállíthassák preferenciáikat. Ez történhet például úgy, hogy első ismerősük hozzáadása vagy első bejegyzésük megosztása után kéri fel őket, hogy határozzák meg adatvédelmi preferenciáikat.

Példák használata: Az adatkezelés célját egyértelműen és pontosan feltüntető kötelező információk mellett példákkal lehet szemléltetni egy konkrét adatkezelést, hogy az a felhasználók számára kézzelfoghatóbbá váljon.

Ragadós navigáció: Egy adatvédelemmel kapcsolatos oldal megtekintése során a tartalomjegyzék folyamatosan megjeleníthető a képernyőn, lehetővé téve a felhasználók számára, hogy mindig be tudják tájolni magukat az oldalon, és gyorsan navigálhassanak a tartalomban a horgonyhivatkozásoknak (anchor links) köszönhetően.

Vissza az oldal tetejére: Az oldal alján vagy az ablak alján ragadós elemként el lehet helyezni egy „vissza az oldal tetejére” gombot, hogy megkönnyítse a felhasználók számára az oldalon való navigációt.

Értesítések: Az értesítések felhasználhatók arra, hogy felhívják a felhasználók figyelmét a személyes adatok kezelésével kapcsolatos szempontokra, változásokra vagy kockázatokra (pl. *adatvédelmi incidens esetén*). Ezek az értesítések többféle módon is megvalósíthatók, például bejövő üzenetek, felugró ablakok, a weboldal tetején elhelyezett rögzített szalaghirdetések stb. révén.

A következők magyarázata: Ha a felhasználók egy adatvédelmi ellenőrzést kívánnak be- vagy kikapcsolni, vagy hozzájárulásukat akarják adni vagy vissza kívánják vonni azt, semleges módon kell tájékoztatni őket az ilyen intézkedések következményeiről.

Eszközök közötti konzisztencia: Ha a közösségimédia-platform különböző eszközökön (pl. számítógépen, okostelefonon stb.) keresztül érhető el, az adatvédelemmel kapcsolatos beállításokat és információkat a különböző verziókban ugyanazon a helyen kell elhelyezni, és azoknak ugyanazonok az útvonalakon és interfészelemeken (menü, ikonok stb.) keresztül kell elérhetőnek lenniük.

Adatvédelmi címtár: A menü különböző szakaszai közötti könnyű tájékozódás érdekében a felhasználók számára biztosítani kell egy könnyen hozzáférhető oldalt, ahonnan az összes adatvédelmi vonatkozású művelet és tájékoztatás hozzáférhető. Ez az oldal elhelyezhető a közösségimédia-szolgáltató fő navigációs menüjében, a felhasználói fiókban, az adatvédelmi szabályzatban stb.

Háttér-információk: A teljes körű adatvédelmi szabályzat mellett a legmegfelelőbb időpontban rövid információmorzsákat lehet biztosítani a felhasználóknak, hogy konkrét és folyamatos tájékoztatást kapjon adatainak kezeléséről.

Magától értetődő URL cím: Az adatvédelmi beállításokhoz vagy tájékoztatáshoz kapcsolódó oldalakon olyan webcímet kell használni, amely egyértelműen tükrözi azok tartalmát. Az adatvédelmi beállításokat központosító oldal URL-je lehet például [kozossegi-oldal.com]/adatbeallitasok.

A jogok gyakorlására szolgáló űrlap: A felhasználók általános adatvédelmi rendelethez fűződő jogai gyakorlásának elősegítése érdekében egy erre a célra szolgáló űrlapot lehet biztosítani, amely segíti őket jogaik megértésében, és amely iránymutatást nyújt számukra az ilyen típusú kérelmek benyújtásához.