

# Usmernenia



## **Usmernenia 8/2020 k zacielovaniu na používateľov sociálnych médií**

**Verzia 2.0**

**Prijaté 13. apríla 2021**

## Postupnosť verzií

Verzia 2.0	13. apríla 2021	Prijatie usmernení po verejnej konzultácii
Verzia 1.0	2. septembra 2020	Prijatie usmernení na účely verejnej konzultácie

## OBSAH

Obsah.....	3
1 Úvod .....	4
2 Rozsah pôsobnosti.....	5
3 Riziká pre práva a slobody používateľov vznikajúce v dôsledku spracúvania osobných údajov.....	6
4 Subjekty a úlohy .....	9
4.1 Používatelia .....	9
4.2 Poskytovatelia sociálnych médií.....	9
4.3 Subjekty vykonávajúce zacielenie .....	10
4.4 Ďalšie relevantné subjekty .....	11
4.5 Úlohy a povinnosti.....	11
5 Analýza rôznych mechanizmov zacielenia.....	13
5.1 Prehľad .....	13
5.2 Zacielenie na základe poskytnutých údajov .....	14
5.2.1 Údaje, ktoré poskytuje používateľ poskytovateľovi sociálnych médií .....	14
A. Úlohy .....	15
B. Právny základ.....	16
5.2.2 Údaje, ktoré poskytne používateľ platformy sociálnych médií subjektu vykonávajúcemu zacielenie.....	19
A. Úlohy .....	20
B. Právny základ.....	21
5.3 Zacielenie na základe pozorovaných údajov .....	21
5.3.1 Úlohy .....	22
5.3.2 Právny základ.....	23
5.4 Zacielenie na základe odvodených údajov .....	25
5.4.1 Úlohy .....	26
5.4.2 Právny základ.....	26
6 Transparentnosť a právo na prístup.....	27
6.1 Základné časti dohody a informácie, ktoré sa majú poskytnúť (článok 26 ods. 2 všeobecného nariadenia o ochrane údajov) .....	28
6.2 Právo na prístup (článok 15).....	30
7 Posúdenia vplyvu na ochranu údajov.....	31
8 Osobitné kategórie údajov .....	32
8.1 Čo tvorí osobitnú kategóriu údajov .....	32
8.1.1 Zjavné osobitné kategórie údajov .....	33
8.1.2 Údaje osobitných kategórií získané odvodením alebo kombináciou údajov .....	34

8.2	Výnimky z osobitných kategórií údajov, ktoré boli preukázateľne zverejnené podľa článku 9 ods. 2	36
9	Spoločné prevádzkovateľstvo a zodpovednosť.....	37
9.1	Dohoda spoločných prevádzkovateľov a určenie zodpovedností (článok 26 všeobecného nariadenia o ochrane údajov) .....	37
9.2	Úrovne zodpovednosti .....	39

## Európsky výbor pre ochranu údajov

so zreteľom na článok 70 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES,

### PRIJAL TIETO USMERNENIA

## 1 ÚVOD

1. Významným trendom v online prostredí za posledné desaťročie je vzostup sociálnych médií. Čoraz viac osôb využíva sociálne médiá na udržiavanie kontaktu s rodinou a priateľmi, na vytváranie sietí profesionálnych kontaktov alebo na spájanie sa s ľuďmi s rovnakými záujmami či názormi. Na účely týchto usmernení sa sociálne médiá chápu ako online platformy, ktoré umožňujú vytváranie sietí a komunít používateľov, ktorí si medzi sebou vymieňajú informácie a obsah.<sup>1</sup> Medzi kľúčové charakteristiky sociálnych médií možno zahrnúť schopnosť jednotlivcov zaregistrovať sa s cieľom vytvárať si vlastné „kontakty“ alebo „profily“, komunikovať medzi sebou prostredníctvom výmeny obsahu, ktorý vytvorila používateľia alebo niekto iný, rozvíjať kontakty a budovať siete s inými používateľmi.<sup>2</sup>
2. Mnohí poskytovatelia sociálnych médií v rámci svojho obchodného modelu ponúkajú ciele služby. Prostredníctvom cielejších služieb môžu fyzické alebo právnické osoby (ďalej len „subjekty vykonávajúce zacielenie“) [targeters] oznamovať používateľom sociálnych médií konkrétne správy súvisiace s komerčnými, politickými alebo inými záujmami.<sup>3</sup> Pre ciele služby je charakteristický vnímaný prienik medzi cieľovou osobou alebo skupinou a doručovanou správou. Základným predpokladom je, že čím je prienik väčší, tým je vyššia miera prijatia (konverzia), a tak je cielejšia kampaň účinnejšia (návrtnosť investícií).

---

<sup>1</sup> Medzi ďalšie funkcie sociálnych médií môžeme zaradiť napríklad personalizáciu, integráciu aplikácií, moduly sociálnych médií [social plug-ins], overovanie používateľov, analytiku a publikovanie. Funkcie sociálnych médií môžu prevádzkovatelia ponúkať samostatne alebo môžu byť integrované ako súčasť širšej ponuky služieb.

<sup>2</sup> Okrem „tradičných“ platforiem sociálnych médií môžu medzi sociálne médiá patriť napríklad aj: platformy na zoznamovanie, na ktorých sa zaregistrovaní používatelia prezentujú a hľadajú si partnerov, s ktorými by mohli mať v reálnom živote vzťah; platformy, na ktorých môžu registrovaní používatelia nahrávať svoje videá, komentovať ich a prepájať ich s videami iných osôb; alebo počítačové hry, ktoré môžu registrovaní používatelia hrať spoločne v skupinách, a môžu si pritom vymieňať informácie alebo deliť sa o skúsenosti a úspechy v rámci hry.

<sup>3</sup> Zacielenie [targeting] sa vymedzuje ako „akt nasmerovania alebo zamerania niečoho na konkrétnu skupinu osôb“ a „pokús zaujať osobu alebo skupinu alebo ich určitým spôsobom ovplyvniť“.

<https://www.collinsdictionary.com/dictionary/english/targeting>.

3. Mechanizmy zacielovania na používateľov sociálnych médií sú čoraz sofistikovanejšie. Organizácie teraz môžu pri zacielovaní na jednotlivcov využívať široký okruh kritérií. Tieto kritériá mohli vzniknúť na základe osobných údajov, ktoré používatelia aktívne poskytli alebo zdieľali, napríklad ich stav vzťahu. Kritériá zacielenia však čoraz častejšie vznikajú aj na základe osobných údajov, ktoré boli odpozorované alebo odvodené, či už poskytovateľom sociálnych médií alebo tretími stranami, a získané (agregované) platformou alebo inými subjektmi (napr. data brokermi) na účely podpory cielenej reklamy. Inak povedané, zacielovanie na používateľov sociálnych médií neznamená len akt „výberu“ jednotlivcov alebo skupín jednotlivcov, ktorí sú zamýšľanými príjemcami určitej správy („cieľová skupina“), ale zahŕňa celý proces vykonávaný skupinou zainteresovaných strán, ktorého výsledkom je doručenie osobitných odkazov jednotlivcom s kontami na sociálnych médiách.<sup>4</sup>
4. Vzhľadom na kombinovanie a analýzu údajov pochádzajúcich z rôznych zdrojov, ako aj na potenciálne citlivý charakter osobných údajov, ktoré sa v súvislosti so sociálnymi médiami spracúvajú<sup>5</sup>, vznikajú riziká, ktoré môžu ohroziť základné práva a slobody jednotlivcov. Z hľadiska ochrany údajov mnohé riziká súvisia s možnou nedostatočnou transparentnosťou a kontrolou používateľov. Pokiaľ ide o dotknuté osoby, spracúvanie osobných údajov, ktoré vedie k poskytnutiu cielenej správy, je často nejasné. Navyše môže zahŕňať nepredpokladané alebo neželané spôsoby použitia osobných údajov, čo vyvoláva otázky týkajúce sa nielen právnych predpisov o ochrane údajov, ale aj iných základných práv a slobôd. Nedávno sa zacielovaniu v rámci sociálnych médií začala venovať zvýšená pozornosť verejnosti a zvýšila sa regulačná kontrola v súvislosti s demokratickým rozhodovaním a volebnými procesmi.<sup>6</sup>

## 2 ROZSAH PÔSOBNOSTI

5. Na zacielovaní na používateľov sociálnych médií sa môže podieľať viacero rôznych subjektov, ktoré na účely týchto usmernení možno rozdeliť na štyri skupiny: poskytovatelia sociálnych médií, ich používatelia, subjekty vykonávajúce zacielenie a ďalšie subjekty, ktoré sa môžu podieľať na procese zacielovania. Význam správneho identifikovania úloh a povinností rôznych subjektov bol nedávno zdôraznený aj rozsudkami Súdneho dvora Európskej únie (SDEÚ) vo veciach Wirtschaftsakademie a Fashion ID.<sup>7</sup> Oba rozsudky svedčia o tom, že v dôsledku interakcie medzi poskytovateľmi sociálnych médií a inými subjektmi môžu vzniknúť spoločné povinnosti vyplývajúce z právnych predpisov EÚ o ochrane údajov.
6. Tieto usmernenia obsahujú pokyny súvisiace so zacielovaním na používateľov sociálnych médií, s prihliadnutím na judikatúru SDEÚ a ustanovenia všeobecného nariadenia o ochrane údajov týkajúce sa spoločných prevádzkovateľov a zodpovednosti, a to najmä pokiaľ ide o povinnosti subjektov vykonávajúcich zacielenie a poskytovateľov sociálnych médií. V prípade spoločných povinností sa

---

<sup>4</sup> Zobrazované správy zvyčajne tvoria obrázky a text, ale môžu obsahovať aj formáty videa a/alebo zvukové formáty.

<sup>5</sup> Osobné údaje spracúvané v kontexte sociálnych médií môžu predstavovať „osobitné kategórie osobných údajov“ podľa článku 9 všeobecného nariadenia o ochrane údajov, môžu sa týkať zraniteľných osôb alebo mať výrazný osobný charakter. Pozri aj usmernenia pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 týkajúce sa posúdenia vplyvu na ochranu údajov a stanovovania toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“, WP 248 rev. 01, s. 9.

<sup>6</sup> Pozri napríklad: [https://edpb.europa.eu/sites/default/files/files/file1/201902\\_edpb\\_statementonelections\\_sk.pdf](https://edpb.europa.eu/sites/default/files/files/file1/201902_edpb_statementonelections_sk.pdf); <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/>; [https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf); <https://www.personuvernd.is/information-in-english/greinar/nr/2880>.

<sup>7</sup> SDEÚ, rozsudok vo veci Wirtschaftsakademie, 5. júna 2018, C-210/16, ECLI:EU:C:2018:388; SDEÚ, rozsudok vo veci Fashion ID, 29. júla 2019, C-40/17, ECLI:EU:C:2019:629.

v týchto usmerneniach prostredníctvom praktických príkladov snažíme objasniť, ako by malo vyzerat ich rozdelenie medzi subjekty vykonávajúce zacielenie a poskytovateľov sociálnych médií.<sup>8</sup>

7. Hlavným cieľom týchto usmernení je preto objasniť úlohy a povinnosti poskytovateľa sociálnych médií a subjektu vykonávajúceho zacielenie. Na tento účel sú v usmerneniach identifikované aj potenciálne riziká pre práva a slobody jednotlivcov (oddiel 3), hlavné subjekty a ich úlohy (oddiel 4) a rieši sa v nich aj uplatňovanie kľúčových požiadaviek pri ochrane údajov (napr. zákonnosť a transparentnosť, posúdenie vplyvu na ochranu údajov atď.), ako aj kľúčové prvky dohôd medzi poskytovateľmi sociálnych médií a subjektmi vykonávajúcimi zacielenie.
8. Rozsah pôsobnosti týchto usmernení však zahŕňa vzťah medzi zaregistrovanými používateľmi sociálnej siete, jej poskytovateľmi a subjektmi vykonávajúcimi zacielenie. Do rozsahu pôsobnosti týchto usmernení nepatrí dôkladná analýza takých scenárov, ako je napr. prípad jednotlivcov, ktorí nie sú registrovaní u poskytovateľov sociálnych médií.

### 3 RIZIKÁ PRE PRÁVA A SLOBODY POUŽÍVATEĽOV VZNIKAJÚCE V DÔSLEDKU SPRACÚVANIA OSOBNÝCH ÚDAJOV

9. Vo všeobecnom nariadení o ochrane údajov sa zdôrazňuje, že je dôležité náležite zhodnotiť a zmierniť akékoľvek riziká pre práva a slobody jednotlivcov vyplývajúce zo spracúvania osobných údajov.<sup>9</sup> Mechanizmy, ktoré sa môžu využívať pri zacielení na používateľov sociálnych médií, ako aj súvisiace spracovateľské činnosti, ktoré umožňujú zacielenie, môžu predstavovať výrazné riziká. Účelom týchto usmernení nie je poskytnúť úplný zoznam možných rizík pre práva a slobody jednotlivcov. Napriek tomu však EDPB považuje za dôležité poukázať na niektoré typy rizík a poskytnúť viacero príkladov toho, ako sa môžu prejaviť.
10. Niektoré použitia osobných údajov v rámci zacielenia na používateľov sociálnych médií môžu byť v rozpore s primeranými očakávaniami jednotlivcov alebo môžu byť nad rámec týchto očakávaní, čím dochádza k porušeniu platných zásad a pravidiel ochrany údajov. Ak sociálne médiá kombinujú osobné údaje zo zdrojov tretích strán s údajmi, ktoré im poskytli používatelia jeho platformy, výsledkom môže byť použitie osobných údajov nad rámec ich pôvodného účelu a spôsobmi, ktoré jednotlivec nemohol rozumne predvídať. Súčasťou vytvárania profilov v súvislosti so zacielením môže byť vyvodzovanie záujmov alebo iných charakteristík, ktoré jednotlivec aktívne neposkytol, čím sa narúša jeho schopnosť vykonávať kontrolu nad svojimi osobnými údajmi.<sup>10</sup> Navyše nedostatočná transparentnosť týkajúca sa úlohy rôznych subjektov a použitých spracovateľských operácií môžu narušiť alebo skomplikovať výkon práv dotknutých osôb alebo mu úplne zabrániť.

---

<sup>8</sup> Tieto usmernenia platia bez toho, aby boli dotknuté usmernenia EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov prijaté 2. septembra 2020, ktoré sa týkajú rozdelenia povinností v iných kontextoch.

<sup>9</sup> Podľa článku 24 všeobecného nariadenia o ochrane údajov prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením, a to „s ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb“. Pozri aj usmernenia pracovnej skupiny zriadenej podľa článku 29 týkajúce sa posúdenia vplyvu na ochranu údajov a stanovovania toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“, WP 248 rev. 01, 4. októbra 2017.

<sup>10</sup> Pozri aj stanovisko Európskeho dozorného úradníka pre ochranu údajov (EDPS) k internetovej manipulácii, stanovisko 3/2018, 19. marca 2018, s. 15 („Pri používaní údajov z profilov na iné účely prostredníctvom algoritmov vzniká obava, že tieto údaje stratia svoj pôvodný kontext. Zmena účelu údajov môže ovplyvniť informačné súkromie osoby, ešte viac obmedziť kontrolu dotknutých osôb nad ich údajmi, a tým ešte viac ovplyvniť dôveru v digitálne prostredia a služby.“).

11. Druhý typ rizika sa týka možnosti diskriminácie a vylúčenia. Zacieľovanie na používateľov sociálnych médií môže zahŕňať kritériá, ktoré majú priame alebo nepriame diskriminačné účinky týkajúce sa rasového alebo etnického pôvodu jednotlivca, jeho zdravotného stavu či sexuálnej orientácie alebo iných chránených vlastností dotknutej osoby. Použitím takýchto kritérií v súvislosti s reklamou týkajúcou sa pracovných ponúk, bývania alebo úveru (pôžičiek, hypoték) sa môže znížiť viditeľnosť príležitostí pre osoby v rámci určitých skupín. Tento potenciál na diskrimináciu pri zacieľovaní vyplýva z toho, že zadávatelia reklamy môžu využiť obrovské množstvo rôznych osobných údajov (napr. údaje o demografii, správaní a záujmoch), ktoré sociálne médiá zhromažďujú o svojich používateľoch.<sup>11</sup> Z nedávneho výskumu vyplýva, že potenciál na vznik diskriminačných účinkov existuje aj vtedy, ak sa nepoužijú kritériá priamo súvisiace s osobitnými kategóriami osobných údajov v zmysle článku 9 všeobecného nariadenia o ochrane údajov.<sup>12</sup>
12. Druhá kategória rizík súvisí s potenciálnou možnou manipuláciou používateľov. Mechanizmy zacieľovania sa podľa definície používajú na ovplyvňovanie správania a rozhodnutí jednotlivcov, či už ide o ich rozhodnutia o nákupe v role spotrebiteľov alebo ich politické rozhodnutia ako občanov zapájajúcich sa do občianskeho života.<sup>13</sup> Niektoré postupy zacieľovania však môžu zájsť tak ďaleko, že narušia nezávislosť a slobodu osôb (napr. im budú ponúkať individualizované správy, v ktorých sa budú zneužívať, či dokonca zdôrazňovať určité zraniteľné miesta, osobné hodnoty či obavy). Analýzou obsahu zdieľaného cez sociálne siete sa napríklad môžu odhaliť informácie o emocionálnom stave (napr. prostredníctvom analýzy používania určitých kľúčových slov). Tieto informácie by sa mohli použiť na zacielenie osobitných správ na jednotlivca v konkrétnom čase, pri ktorých sa predpokladá, že bude voči nim otvorenejší, takže dôjde k nenápadnému ovplyvňovaniu jeho myšlienkového procesu, emócií a správania.<sup>14</sup>
13. Mechanizmy na zacieľovanie na používateľov sociálnych médií možno použiť aj na neprimerané ovplyvňovanie jednotlivcov v súvislosti s politickým diskurzom a demokratickými volebnými procesmi.<sup>15</sup> Zatiaľ čo „tradičné“ offline politické kampane sa zvyčajne snažia ovplyvniť správanie voličov prostredníctvom správ, ktoré sú vo všeobecnosti dostupné a dohľadateľné (overiteľné), pomocou dostupných internetových mechanizmov zacieľovania sa môžu politické strany a kampane zamerať na jednotlivých voličov prostredníctvom správ osobitne prispôbených konkrétnym potrebám, záujmom a hodnotám cieľovej skupiny.<sup>16</sup> Takéto zacielenie môže dokonca zahŕňať dezinformácie alebo správy, ktoré daní jednotlivci považujú za obzvlášť znepokojivé, takže je pravdepodobnejšie, že v nich vyvolajú určitú emóciu alebo reakciu. V prípade polarizujúcich alebo nepravdivých (dezinformačných) správ zameraných na konkrétne osoby pri ich nulovom alebo obmedzenom zasadení do kontextu alebo predstavení iných uhlov pohľadu môže použitie mechanizmov zacieľovania viesť k narušeniu demokratického volebného procesu.<sup>17</sup>

---

<sup>11</sup> T. Speicher a.o., Potential for Discrimination in Online Targeted Advertising, Výsledky 1. konferencie o spravodlivosti, zodpovednosti a transparentnosti, *Proceedings of Machine Learning Research* PMLR 81:5-19, 2018, <http://proceedings.mlr.press/v81/speicher18a.html>.

<sup>12</sup> Tamže.

<sup>13</sup> Stanovisko Európskeho dozorného úradníka pre ochranu údajov 3/2018, s. 18.

<sup>14</sup> Pozri *Experimental evidence of massive-scale emotional contagion through social networks*, Adam D. I. Kramer, Jamie E. Guillory a Jeffrey T. Hancock, *PNAS* 17. júna 2014, 111 (24) 8788-8790; po prvýkrát vydané 2. júna 2014 <https://doi.org/10.1073/pnas.1320040111>, k dispozícii na adrese: <https://www.pnas.org/content/111/24/8788> Adam D. I. Kramer Core Data Science Team, Facebook, Inc., Menlo Park, CA 94025.

<sup>15</sup> Pozri aj vyhlásenie Európskeho výboru pre ochranu údajov 2/2019 o používaní osobných údajov v priebehu politických kampaní, 13. marca 2019, s. 1.

<sup>16</sup> Úrad komisára pre informácie (ICO), *Democracy disrupted? Personal information and political influence* (Narušenie demokracie? Osobné údaje a politický vplyv), 10. júla 2018, s. 14.

<sup>17</sup> Pozri aj dokument Európskej komisie, Usmernenie Komisie o uplatňovaní práva Únie v oblasti ochrany údajov v kontexte volieb – Príspevok Európskej komisie k zasadnutiu lídrov 19. až 20. septembra 2018 v Salzburgu. Pozri

14. Rovnako aj využívanie algoritmov na určenie toho, ktorá informácia sa zobrazí ktorému používateľovi, môže nepriaznivo ovplyvniť pravdepodobnosť prístupu k diverzifikovaným zdrojom informácií vo vzťahu ku konkrétnej téme. To môže mať následne negatívne dôsledky pre pluralitu verejnej diskusie a prístup k informáciám.<sup>18</sup> Mechanizmy zacieľovania sa môžu využiť na zvýšenie viditeľnosti niektorých správ, zatiaľ čo iné sú zatlačené do úzadia. Potenciálny nepriaznivý vplyv sa môže prejavovať na dvoch úrovniach. Na jednej strane existujú riziká súvisiace s takzvanými „filtročnými bublinami“, v ktorých sú ľudia vystavení väčšinou rovnakým informáciám a stretávajú sa s užším okruhom názorov, čo vedie k zvýšenej politickej a ideologickej polarizácii.<sup>19</sup> Na strane druhej môžu mechanizmy zacieľovania vytvárať aj riziko „zahĺtenia informáciami“ [more-of-the-same], pri ktorom jednotlivci nemôžu prijať informované rozhodnutie, pretože majú príliš veľa informácií a nedokážu posúdiť, či sú dôveryhodné.
15. Osobné údaje, ktoré zbierajú poskytovatelia sociálnych médií, nemusia súvisieť len s činnosťami, ktoré vykonávajú jednotlivci v rámci samotnej platformy daného sociálneho média. Zacieľovanie na používateľov sociálnych médií na základe informácií vyplývajúcich z ich správania na internete alebo iných činností mimo platformy sociálnych médií môže v jednotlivcoch vyvolávať pocit, že ich správanie je systematicky monitorované. To môže mať odstrašujúci účinok na slobodu prejavu vrátane prístupu k informáciám.<sup>20</sup> Tieto účinky sa môžu ešte zhoršovať, ak sa pri zacielení využíva aj analýza obsahu, ktorý používatelia sociálnych médií zdieľajú. V prípade, že sú správy, príspevky a komentáre podrobované analýze na komerčné alebo politické účely, môže to viesť aj k autocenzúre.
16. Potenciálny negatívny vplyv zacielenia môže byť výrazne väčší v prípade zraniteľných kategórií osôb, napríklad u detí. Zacieľovanie môže ovplyvniť formovanie osobných preferencií a záujmov detí, čo v konečnom dôsledku môže ovplyvniť ich nezávislosť a právo na rozvoj. V odôvodnení 38 všeobecného nariadenia o ochrane údajov sa uvádza, že na využívanie osobných údajov detí na účely marketingu alebo vytvorenia osobného alebo používateľského profilu a získavanie osobných údajov o deťoch pri používaní služieb poskytovaných priamo dieťaťu by sa mala vzťahovať osobitná ochrana.<sup>21</sup>
17. Využívanie sociálnych médií v EÚ je rozšírené, keďže v roku 2019 bolo na sociálnych sieťach aktívnych 54 % ľudí vo veku 16 až 74 rokov. Táto miera účasti sa navyše v priebehu rokov neustále zvyšovala.<sup>22</sup> EDPB uznáva, že so zvyšovaním koncentrácie na trhu so sociálnymi médiami a zacieľovaním môžu stúpať aj riziká týkajúce sa práv a slobôd podstatného množstva osôb. Niektorí poskytovatelia sociálnych médií môžu byť napríklad schopní kombinovať väčšie množstvo rozmanitých osobných údajov, či už samostatne alebo v spolupráci s inými spoločnosťami. V dôsledku toho sa môže ďalej zvyšovať schopnosť ponúkať čoraz pokročilejšie ciele kampane. Tento aspekt je relevantný z hľadiska ochrany údajov (podrobnejšie profilovanie dotknutých osôb), ako aj z hľadiska práva hospodárskej súťaže (vzhľadom na bezkonkurenčné možnosti náhľadu získané pomocou platformy sa môže pre internetových predajcov stať „nevyhnutným obchodným partnerom“). Podľa EDPB tento stupeň trhovej a informačnej sily „môže ohroziť úroveň ochrany údajov a slobody spotrebiteľov digitálnych služieb“.<sup>23</sup>

---

aj L.M. Neudert a N.M. Marchal, Polarizácia a využitie technológií v politických kampaniach a komunikácii, Výskumná služba Európskeho parlamentu, 2019, s. 22 – 24.

<sup>18</sup> Pozri aj uznesenie Európskeho parlamentu z 3. mája 2018 o slobode a pluralite médií v Európskej únii.

<sup>19</sup> Stanovisko Európskeho dozorného úradníka pre ochranu údajov 3/2018, s. 7.

<sup>20</sup> Stanovisko Európskeho dozorného úradníka pre ochranu údajov 3/2018, s. 9. a Výbor odborníkov na pluralitu a transparentnosť v oblasti vlastníctva médií (MSI-MED), Internet a volebné kampane – Štúdiá o využívaní internetu vo volebných kampaniach, štúdiá Rady Európy DGI(2017)11, apríl 2018, s. 19 – 21.

<sup>21</sup> Pozri aj usmernenia pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, 6. februára 2018, WP 251 rev. 01, s. 29.

<sup>22</sup> <https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/edn-20200630-2>.

<sup>23</sup> Vyhlásenie EDPB o dosahu hospodárskej koncentrácie na ochranu údajov, k dispozícii na adrese: [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_statement\\_economic\\_concentration\\_sk\\_0.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_economic_concentration_sk_0.pdf).



18. Pravdepodobnosť a závažnosť spomínaných rizík bude okrem iného závisieť od povahy mechanizmu zacielenia a od toho, ako a na aké konkrétne účely sa použije. Prvkom, ktoré môžu ovplyvniť pravdepodobnosť a závažnosť rizík v súvislosti so zacielením na používateľov sociálnych médií, sa budeme podrobnejšie venovať v oddiele 7.

## 4 SUBJEKTY A ÚLOHY

### 4.1 Používatelia

19. Jednotlivci využívajú sociálne médiá v rôznych úlohách a na rôzne účely (napr. aby zostali v kontakte s priateľmi, na výmenu informácií o spoločných záujmoch alebo na hľadanie pracovných príležitostí). Pojem „používateľ“ sa zvyčajne používa na označenie osôb, ktoré sú zaregistrované v službe (t. j. ktoré majú „konto“ alebo „profil“). K mnohým službám sociálnych médií však môžu mať prístup aj osoby bez registrácie (t. j. bez toho, aby si vytvorili konto alebo profil).<sup>24</sup> Takéto osoby zvyčajne nemôžu využívať všetky funkcie alebo služby ponúkané osobám, ktoré sú zaregistrované u poskytovateľa sociálnych médií. Osoby registrované u poskytovateľov sociálnych médií, ale aj tie neregistrované, možno považovať za „dotknuté osoby“ v zmysle článku 4 bodu 1 všeobecného nariadenia o ochrane údajov, ak je daná osoba priamo alebo nepriamo identifikovaná alebo identifikovateľná.<sup>25</sup>
20. Od príslušnej služby sociálnych médií závisí, či sa osoby musia zaregistrovať pod svojim skutočným menom alebo môžu použiť prezývku alebo pseudonym. Aj v prípade politiky, pri ktorej sa nevyžaduje uvedenie skutočného mena, je vo všeobecnosti stále možné zacieliť na daného používateľa (alebo inak uplatniť osobitný výber), keďže väčšina typov zacielenia nie je založená na menách používateľov, ale na iných typoch osobných údajov, ako sú záujmy, sociografické údaje, správanie alebo iné identifikátory. Poskytovatelia sociálnych médií často nabádajú používateľov, aby uviedli svoje skutočné údaje, napríklad telefónne čísla.<sup>26</sup> Napokon treba poznamenať, že poskytovatelia sociálnych médií môžu umožniť aj zacielenie na osoby, ktoré u nich nemajú konto.<sup>27</sup>

### 4.2 Poskytovatelia sociálnych médií

21. Poskytovatelia sociálnych médií ponúkajú online služby, ktoré umožňujú vytváranie sietí a komunít používateľov, medzi ktorými prebieha výmena informácií a obsahu. Služby sociálnych médií sa zvyčajne ponúkajú cez webové prehliadače alebo špecializované aplikácie, ktoré si často najprv od používateľa vyžadujú súbor osobných údajov na účely vytvorenia používateľského „konta“ alebo „profilu“. Zároveň sa často používateľom ponúkajú súvisiace možnosti kontroly konta, prostredníctvom ktorých majú

---

<sup>24</sup> Osobné údaje a údaje využívané na profilovanie uchovávané poskytovateľmi sociálnych médií vo vzťahu k osobám, ktoré nie sú registrované u poskytovateľov sociálnych médií, sa niekedy označujú ako „tieňové profily“ [shadow profiles].

<sup>25</sup> Pozri aj odôvodnenie 26 („osobitný výber“) [singling out]. Pozri aj stanovisko 4/2007 pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 k pojmu osobné údaje, 20. júna 2007, WP 136, s. 12 a nasl.

<sup>26</sup> V niektorých prípadoch poskytovatelia sociálnych médií požadujú doplňujúcu dokumentáciu, aby si mohli overiť poskytnuté údaje, napríklad používateľov požiadajú o nahratie preukazu totožnosti alebo podobného dokumentu.

<sup>27</sup> Takéto zacielenie sa môže umožniť na základe online identifikátorov získaných zo zariadení, aplikácií, nástrojov a protokolov týchto osôb, ako sú adresy internetových protokolov, súbory cookie alebo iné identifikátory, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi a inými informáciami získanými zo serverov môžu použiť na vytvorenie profilov fyzických osôb a na ich identifikáciu. Pozri aj odôvodnenie 30 všeobecného nariadenia o ochrane údajov. Na základe tohto rozpoznávania sa na webových sídlach, ktoré daná osoba navštevuje, môžu zobrazovať ciele reklamy.

používateľia prístup k osobným údajom spracúvaným v súvislosti s využívaním konta a kontrolu nad nimi.

22. Poskytovateľ sociálnych médií určuje funkcie danej služby. V rámci toho určí, ktoré údaje sa spracúvajú, na aké účely, za akých podmienok, ako aj spôsob spracúvania osobných údajov. To umožňuje poskytovať služby sociálnych médií, ale pravdepodobne aj služby, ako je zacielenie, z ktorých môžu mať prospech obchodní partneri pôsobiaci v rámci platformy sociálnych médií alebo v spojitosti s ňou.
23. Poskytovateľ sociálnych médií má príležitosť zhromaždiť veľké množstvo osobných údajov týkajúcich sa správania a interakcií používateľov aj osôb, ktoré u neho nie sú registrované, vďaka čomu môže získať značný prehľad o sociálno-demografických charakteristikách, záujmoch a preferenciách používateľov. Je dôležité poznamenať, že takéto „prehľady“ založené na aktivitách používateľov často zahŕňajú odvodené [inferred or derived] osobné údaje. Keď napríklad používateľ reaguje na určitý obsah (napr. označí, že sa mu páči príspevok na sociálnych médiách alebo si pozrie video), poskytovateľ sociálnych médií môže túto akciu zaznamenať a odvodiť z toho, že danému používateľovi tento obsah vyhovoval.
24. Poskytovatelia sociálnych sietí čoraz častejšie zhromažďujú údaje nielen z činností na samotnej platforme, ale aj z činností vykonávaných mimo nej, pričom kombinujú údaje z viacerých online aj offline zdrojov s cieľom vygenerovať ďalšie informácie. Tieto údaje sa môžu kombinovať s osobnými údajmi, ktoré osoby aktívne poskytnú poskytovateľovi sociálnych médií (napr. meno používateľa, e-mailová adresa, miesto a telefónne číslo), ako aj s údajmi, ktoré im platforma „priradí“ (napr. jedinečné identifikátory).

### 4.3 Subjekty vykonávajúce zacielenie

25. Pojem „subjekty vykonávajúce zacielenie“ sa v týchto usmerneniach používa na označenie fyzických alebo právnických osôb, ktoré využívajú služby sociálnych médií na zameranie osobitných správ na určitú skupinu používateľov sociálnych médií na základe osobitných parametrov alebo kritérií.<sup>28</sup> Subjekty vykonávajúce zacielenie sa od ostatných používateľov sociálnych médií líšia tým, že svoje správy a/alebo cieľové skupiny vyberajú na základe odpozorovaných charakteristík, záujmov alebo preferencií dotknutých osôb, pričom tento postup sa niekedy označuje ako „mikrozacielenie“.<sup>29</sup> Subjekty vykonávajúce zacielenie môžu zacielenie využívať na presadzovanie obchodných, politických alebo iných záujmov. Typickým príkladom sú značky, ktoré využívajú sociálne médiá na propagáciu svojich výrobkov vrátane zvyšovania povedomia o značke. Politické strany čoraz častejšie využívajú sociálne médiá v rámci svojej stratégie kampaní. Charitatívne a iné neziskové organizácie takisto využívajú sociálne médiá na účely zacielenia správ na potenciálnych prispievateľov alebo na budovanie komunít.
26. Treba konštatovať, že zacielenie na používateľov sociálnych médií môže mať rôzne podoby. K zacieleniu môže napríklad dochádzať nielen zobrazením individualizovanej reklamy (napr. vo forme „bannera“ zobrazovaného v hornej alebo bočnej časti webovej stránky), ale aj zobrazením „informačného kanála“ [feed], „časovej osi“ alebo „príbehu“ používateľa na platforme sociálnych médií tak, že sa popri tomto obsahu generovanom používateľom zobrazí reklamný obsah. Zacielenie môže zahŕňať aj vytvorenie obsahu hostovaného poskytovateľom sociálnych médií (napr. prostredníctvom špecializovanej „stránky“ alebo na inom mieste v rámci sociálnych médií) alebo niekde inde (napr. na webových sídlach tretích strán). Subjekty vykonávajúce zacielenie môžu mať

---

<sup>28</sup> Spracúvanie osobných údajov fyzickou osobou v rámci výlučne osobnej alebo domácej činnosti nepatrí do rozsahu vecnej pôsobnosti všeobecného nariadenia o ochrane údajov [článok 2 ods. 2 písm. c)].

<sup>29</sup> Obyčajná výmena informácií na stránke sociálnych médií určenej pre širokú verejnosť (napr. informácie o otváracích hodinách) bez predchádzajúceho výberu cieľovej skupiny sa na účely týchto usmernení nepovažuje za „zacielenie“.

vlastné webové sídla a aplikácie, do ktorých môžu integrovať osobitné obchodné nástroje alebo funkcie sociálnych médií, napríklad moduly sociálnych médií, prihlasovanie cez sociálne médiá, alebo môžu využiť aplikačné programovacie rozhrania (API) alebo súpravy na vývoj softvéru (software development kit – SDK), ktoré ponúkajú poskytovatelia sociálnych médií.

#### 4.4 Ďalšie relevantné subjekty

27. Subjekty vykonávajúce zacielenie môžu priamo využívať mechanizmy zacielenia, ktoré ponúkajú poskytovatelia sociálnych médií, alebo môžu využívať služby iných subjektov, napríklad poskytovateľov marketingových služieb, reklamných sietí a búrz, platforiem pre odberateľov a dodávateľov, poskytovateľov správy údajov (DPMs) a spoločností zameraných na analýzu údajov. Tieto subjekty sú súčasťou komplexného a neustále sa vyvíjajúceho ekosystému online reklamy (niekedy označovaného ako „adtech“), ktorý zhromažďuje a spracúva údaje týkajúce sa jednotlivcov (vrátane používateľov sociálnych médií) napríklad tak, že sleduje ich činnosť v rámci rôznych webových sídel a aplikácií.<sup>30</sup>
28. Relevantnými subjektmi sú aj data brokeri a poskytovatelia správy údajov, ktorí zohrávajú dôležitú úlohu v zacielení na používateľov sociálnych médií. Data brokeri a poskytovatelia správy údajov sa od ostatných reklamno-technologických spoločností odlišujú tým, že spracúvajú nielen údaje získané pomocou sledovacích technológií, ale aj údaje z iných online aj offline zdrojov. Inak povedané, data brokeri a poskytovatelia správy údajov zoskupujú údaje získané z rôznych zdrojov, ktoré môžu potom predať ďalším zainteresovaným stranám zapojeným do procesu zacielenia.<sup>31</sup>
29. Hoci každý z týchto uvedených ďalších subjektov môže pri zacielení na používateľov sociálnych médií zohrávať dôležitú úlohu, tieto usmernenia sa zameriavajú na rozdelenie úloh poskytovateľov sociálnych médií a subjektov vykonávajúcich zacielenie a na ich povinnosti pri ochrane údajov. Podobné úvahy sa však môžu vzťahovať aj na ďalšie subjekty zapojené do ekosystému online reklamy, a to v závislosti od úlohy jednotlivých subjektov v procese zacielenia.

#### 4.5 Úlohy a povinnosti

30. V záujme objasnenia jednotlivých úloh a povinností poskytovateľov sociálnych médií a subjektov vykonávajúcich zacielenie je dôležité zohľadniť príslušnú judikatúru SDEÚ. V tomto smere sú obzvlášť relevantné rozsudky vo veci Wirtschaftsakademie (C-210/16), Jehovovi svedkovia (C-25/17) a Fashion ID (C-40/17).
31. Východiskovým bodom analýzy je právne vymedzenie pojmu prevádzkovateľ. Podľa článku 4 bodu 7 všeobecného nariadenia o ochrane údajov je prevádzkovateľ „fyzická alebo právnická osoba, [...] ktor[á] [sama] alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov“.
32. SDEÚ vo veci Wirtschaftsakademie rozhodol, že v prípade správcu [administrator] takzvanej „fanúšikovskej stránky“ na Facebooku je potrebné sa domnievať, že sa podieľa na určení účelov a prostriedkov spracúvania osobných údajov. Podľa podaní doručených SDEÚ správca v rámci vytvorenia fanúšikovskej stránky *nastaví parametre*, čo má vplyv na spracúvanie osobných údajov na účely *vypracovania štatistík* získaných na základe návštev fanúšikovskej stránky.<sup>32</sup> Pomocou filtrov, ktoré mu poskytuje spoločnosť Facebook, môže správca vymedziť kritériá, na základe ktorých majú byť

---

<sup>30</sup> Opis rôznych subjektov sa nachádza v stanovisku 2/2010 pracovnej skupiny zriadenej podľa článku 29 k behaviorálnej reklame online na strane 5. Stanovisko je k dispozícii na adrese:

[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171\\_sk.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_sk.pdf).

<sup>31</sup> Pozri Consumer Policy Research Centre, „A day in the life of data“ (Deň v živote údajov), k dispozícii na adrese: <http://cprc.org.au/publication/research-report-a-day-in-the-life-of-data/>.

<sup>32</sup> Rozsudok vo veci Wirtschaftsakademie, C-210/16, bod 36.

tieto štatistiky vypracované, ako aj vymedziť kategórie osôb, ktorých osobné údaje budú využívané spoločnosťou Facebook:

*„Správca fanúšikovskej stránky môže najmä požiadať o získanie – a teda o spracovanie – demografických údajov, ktoré sa týkajú jeho cieľovej skupiny, najmä tendencií týkajúcich sa veku, pohlavia, rodinného stavu a povolania, informácií o životnom štýle a záujmoch jeho cieľovej skupiny, ako aj informácií o nákupoch návštevníkov jeho stránky a ich nákupoch cez internet, kategóriách výrobkov alebo služieb, ktoré ich najviac zaujímajú, ako aj geografických údajov, ktoré umožňujú správcovi fanúšikovskej stránky zistiť, kde má ponúkať špeciálne akcie a organizovať podujatia a všeobecne čo najlepšie zamieriť svoju ponuku informácií.“*

33. Keďže nastavenie parametrov závisí okrem iného od cieľovej skupiny správcu, „ako aj cieľov riadenia alebo podpory [jeho] činností“, správca sa podieľa aj na určení účelov spracúvania osobných údajov.<sup>33</sup> Preto sa správca považoval za prevádzkovateľa spoluzodpovedného za spracúvanie osobných údajov návštevníkov svojej „stránky“ spoločne s poskytovateľom sociálnych médií.

34. Ako sa ďalej podrobnejšie uvádza v oddiele 9 týchto usmernení, prevádzkovatelia sa môžu na spracúvaní osobných údajov podieľať v rôznych fázach a stupňoch. Za týchto okolností treba mieru zodpovednosti každého z nich hodnotiť z hľadiska všetkých relevantných okolností prejednávanej veci:

*„[E]xistencia spoločnej zodpovednosti neznamena nevyhnutne rovnakú zodpovednosť rôznych subjektov, ktorých sa týka spracovanie osobných údajov. Tieto subjekty môžu byť naopak zapojené do tohto spracovania v rôznych fázach a stupňoch, takže mieru zodpovednosti každého z nich treba hodnotiť z hľadiska všetkých relevantných okolností prejednávanej veci.“<sup>34</sup>*

35. Okrem toho, že SDEÚ dospel k záveru, že správca stránky koná ako prevádzkovateľ spoločne so spoločnosťou Facebook, konštatoval zároveň aj to, že v prejednávanej veci treba zastávať názor, že spoločnosť Facebook určuje *predovšetkým* účely a prostriedky spracúvania osobných údajov používateľov Facebooku, ako aj osôb, ktoré navštívili fanúšikovské stránky umiestnené na Facebooku.<sup>35</sup>

36. Vo veci Fashion ID SDEÚ rozhodol, že správcu internetovej stránky [website operator] možno považovať za prevádzkovateľa, ak na svojom webovom sídle umiestni modul sociálnej siete Facebook, ktorý spôsobuje poskytnutie osobných údajov návštevníka stránky v prospech spoločnosti Facebook z prehliadača tohto návštevníka.<sup>36</sup> Označenie správcu internetovej stránky ako prevádzkovateľa je však obmedzené na operáciu alebo všetky operácie, pri ktorých skutočne určuje ich účely a prostriedky spracúvania. V tejto prejednávanej veci sa SDEÚ domnieval, že správca internetovej stránky dokáže v spojení so spoločnosťou Facebook určovať len účely a prostriedky zberu a poskytovania osobných údajov návštevníkov jeho internetovej stránky. V dôsledku toho SDEÚ rozhodol, že v prípade umiestnenia modulu sociálnych médií na internetovej stránke je zodpovednosť jej správcu:

*„obmedzená na operáciu alebo všetky operácie spracovania osobných údajov, pri ktorých skutočne určuje účely a prostriedky, t. j. operácie zberu a prenosu predmetných údajov.“<sup>37</sup>*

37. SDEÚ je presvedčený, že správca internetovej stránky nie je prevádzkovateľom v prípade následných<sup>38</sup> operácií spracúvania osobných údajov, ktoré vykonáva spoločnosť Facebook po tom, čo sú jej

<sup>33</sup> Rozsudok vo veci Wirtschaftsakademie, C-210/16, bod 39.

<sup>34</sup> Rozsudok vo veci Wirtschaftsakademie, C-210/16, bod 43; rozsudok vo veci Jehovahi svedkovia, C-25/17, bod 66; a rozsudok vo veci Fashion ID, C-40/17, bod 70.

<sup>35</sup> Rozsudok vo veci Wirtschaftsakademie, C-210/16, bod 30.

<sup>36</sup> Rozsudok vo veci Fashion ID, C-40/17, bod 75 a nasledujúce body a bod 107.

<sup>37</sup> Rozsudok vo veci Fashion ID, C-40/17, bod 107.

<sup>38</sup> Následné spracúvanie je akákoľvek spracovateľská operácia alebo súbor spracovateľských operácií, ktoré nasledujú (alebo sa vykonávajú) po získaní údajov. V spoločnosti Fashion ID sa týmto pojmom označujú

postúpené, keďže správca internetovej stránky nemohol na základe umiestnenia modulov sociálnych médií určovať účely a prostriedky týchto operácií.

*„Naopak, vzhľadom na uvedené informácie sa na prvý pohľad javí ako vylúčené, že by Fashion ID určovala účely a prostriedky neskorších operácií spracovania osobných údajov, ktoré vykonáva Facebook Ireland po tom, čo sú jej postúpené, takže Fashion ID nemôže byť považovaná za prevádzkovateľa s ohľadom na tieto operácie [...]“.<sup>39</sup>*

38. V prípade spoločného prevádzkovateľstva [joint controllership] majú prevádzkovatelia podľa článku 26 ods. 1 všeobecného nariadenia o ochrane údajov povinnosť uzavrieť dohodu, v ktorej transparentne určia svoje príslušné zodpovednosti za plnenie tohto nariadenia, najmä pokiaľ ide o vykonávanie práv dotknutej osoby, a svoje povinnosti poskytovať informácie uvedené v článkoch 13 a 14 nariadenia.
39. V nasledujúcich oddieloch sú prostredníctvom konkrétnych príkladov objasnené úlohy subjektov vykonávajúcich zacielenie a poskytovateľov sociálnych médií vo vzťahu k rôznym mechanizmom zacielenia. Osobitná pozornosť sa venuje najmä tomu, ako sa v tejto súvislosti uplatňujú požiadavky zákonnosti a obmedzenia účelu. Potom nasleduje analýza požiadaviek týkajúcich sa transparentnosti, posúdení vplyvu na ochranu údajov a spracúvania osobitných kategórií údajov. Na záver sa usmernenia zaoberajú povinnosťou spoločných prevádzkovateľov uzavrieť primeranú dohodu podľa článku 26 všeobecného nariadenia o ochrane údajov, v ktorej sa zohľadní miera zodpovednosti subjektu vykonávajúceho zacielenie a poskytovateľa sociálnych médií.

## 5 ANALÝZA RÔZNYCH MECHANIZMOV ZACIEĽOVANIA

### 5.1 Prehľad

40. Zacielenie na používateľov sociálnych médií môže prebiehať na základe poskytnutých, pozorovaných alebo odvodených údajov alebo ich kombinácie:
- a) **Zacielenie na osoby na základe poskytnutých [provided] údajov** – „Poskytnuté údaje“ sú informácie, ktoré dotknutá osoba aktívne poskytne poskytovateľovi sociálnych médií a/alebo subjektu vykonávajúcemu zacielenie.<sup>40</sup> Napríklad:
- )] Používateľ sociálnych médií môže v opise svojho používateľského profilu uviesť svoj vek. Poskytovateľ sociálnych médií môže zase povoliť zacielenie na základe tohto kritéria.
  - )] Subjekt vykonávajúcí zacielenie môže informácie, ktoré mu poskytne dotknutá osoba, využiť na zacielenie konkrétne na túto osobu, napríklad prostredníctvom údajov o zákazníkoch (napr. zoznamu e-mailových adries), ktoré priradí k údajom už

---

spracovateľské operácie, ktoré vykonáva spoločnosť Facebook po tom, ako sú jej postúpené, a v prípade ktorých by sa spoločnosť Fashion ID nemala považovať za spoločného prevádzkovateľa (pretože sa prakticky nepodieľa na určovaní účelov a prostriedkov tohto spracúvania).

Následné spracúvanie na iné účely ako tie, na ktoré boli osobné údaje získané, je povolené len vtedy, ak sú dodržané podmienky článku 6 ods. 4 všeobecného nariadenia o ochrane údajov týkajúce sa ďalšieho spracúvania. Ak napríklad online predajca získa údaje týkajúce sa adresy bydliska osoby, následné spracúvanie by spočívalo v ich uchovávaní alebo neskoršom vymazaní týchto informácií. Ak sa však tento online predajca neskôr rozhodne tieto osobné údaje spracúvať, aby obohatil profil dotknutej osoby na účely zacielenia, znamenalo by to ďalšie spracúvanie v zmysle článku 6 ods. 4 všeobecného nariadenia o ochrane údajov, keďže ide o spracúvanie na iné účely ako tie, na ktoré boli údaje pôvodne získané.

<sup>39</sup> Rozsudok vo veci Fashion ID, C-40/17, bod 76.

<sup>40</sup> Pracovná skupina na ochranu údajov zriadená podľa článku 29, Usmernenia k právu na prenosnosť údajov, WP 242 rev. 01, 5. apríla 2017, s. 10.

uchovávaným v rámci platformy sociálnych médií, čo povedie k zacieleniu reklamy na všetkých používateľov zodpovedajúcich zadaným kritériám<sup>41</sup>.

- b) **Zacielenie na základe pozorovaných [observed] údajov** – Zacielenie na používateľov sociálnych médií môže prebiehať aj na základe pozorovaných údajov.<sup>42</sup> Pozorované údaje sú údaje, ktoré dotknutá osoba poskytne na základe používania služby alebo zariadenia.<sup>43</sup> Na konkrétneho používateľa sociálnych médií možno zacieliť napríklad na základe:
- J jeho aktivity na samotnej platforme sociálnych médií (napr. obsahu, ktorý používateľ zdieľal, ktorý si prezeral alebo ktorý označil, že sa mu páči),
  - J použitia zariadení, na ktorých bola spustená aplikácia sociálnych médií (napr. súradnice GPS, mobilné telefónne číslo),
  - J údajov získaných externým vývojárom aplikácie prostredníctvom aplikačných programovacích rozhraní (API) alebo súprav na vývoj softvéru (SDK), ktoré ponúkajú poskytovatelia sociálnych médií,
  - J získavania údajov pomocou webových sídel tretích strán, ktoré obsahujú moduly sociálnych médií alebo pixely,
  - J údajov získaných prostredníctvom tretích strán (napr. strán, s ktorými bola dotknutá osoba v interakcii, kúpila si od nich nejaký produkt, zriadila si vernostné karty) alebo
  - J údajov získaných prostredníctvom služieb, ktoré ponúkajú spoločnosti vlastnené alebo riadené poskytovateľom sociálnych médií.
- c) **Zacielenie na základe odvodených [inferred] údajov** – „Ovodené údaje“ vytvára prevádzkovateľ na základe údajov poskytnutých dotknutou osobou alebo na základe svojho pozorovania.<sup>44</sup> Poskytovateľ sociálnych médií alebo subjekt vykonávajúci zacielenie napríklad môže odvodiť, že osobu pravdepodobne zaujíma určitá činnosť alebo výrobok na základe jej správania na internete a/alebo sieťových prepojení.

## 5.2 Zacielenie na základe poskytnutých údajov

### 5.2.1 Údaje, ktoré poskytuje používateľ poskytovateľovi sociálnych médií

41. Jednotlivé osoby môžu pri používaní sociálnych médií o sebe aktívne poskytnúť množstvo informácií. Pri vytváraní konta (alebo „profilu“) na sociálnych médiách sa poskytuje viacero atribútov, ktoré môžu zahŕňať meno, dátum narodenia, pohlavie, miesto bydliska, jazyk atď. V závislosti od povahy platformy sociálnych médií môžu používatelia uviesť ďalšie informácie, ako je stav vzťahu, záujmy alebo súčasné zamestnanie. Osobné údaje, ktoré používatelia sociálnych médií poskytnú, môže poskytovateľ

<sup>41</sup> Pozri napríklad rozhodnutie Vyššieho správneho súdu spolkovej krajiny Bavorsko (Nemecko), Beschluss v.26.09.2018 – 5 CS 18.1157, [www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-25018](http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-25018).

<sup>42</sup> Pracovná skupina zriadená podľa článku 29 vo svojom stanovisku 2/2010 k behaviorálnej reklame online uviedla, že „[r]ozoznávame dva prístupy k vytváraniu profilov: i) Prediktívne profily sú stanovené na základe zhrnutia pozorovaní správania jednotlivcov a kolektívneho správania v čase, najmä sledovaním navštívených stránok, prezeranej reklamy alebo reklamy, na ktorú bolo kliknuté. ii) Explicitné profily sú vytvorené z osobných údajov, ktoré poskytujú samotné dotknuté osoby webovej službe, ako napr. pri registrácii“ (Pracovná skupina na ochranu údajov zriadená podľa článku 29, stanovisko 2/2010 k behaviorálnej reklame online, WP 171, s. 7).

<sup>43</sup> Pracovná skupina na ochranu údajov zriadená podľa článku 29, Usmernenia k právu na prenosnosť údajov, WP 242 rev. 01, 5. apríla 2017, s. 10.

<sup>44</sup> Tamže.

sociálnych médií použiť na vytvorenie kritérií, na základe ktorých môže subjekt vykonávajúci zacielenie adresovať používateľom sociálnych médií osobitné správy.

Príklad 1:

Spoločnosť X predáva pánske topánky a chce spropagovať svoju zimnú kolekciu. V rámci svojej reklamnej kampane sa chce zamerať na mužov vo veku 30 až 45 rokov, ktorí vo svojom profile na sociálnych médiách uviedli, že sú nezadaní. Príslušné kritériá zacielenia ponúkané poskytovateľom sociálnych médií pritom využíva ako parametre na identifikáciu cieľovej skupiny, ktorej sa má reklama zobrazovať. Okrem toho subjekt vykonávajúci zacielenie uvádza, že sa má reklama používateľom sociálnych médií zobrazovať vtedy, keď používajú službu sociálnych médií v čase medzi 17.00 a 20.00 h. Poskytovateľ sociálnych médií na účely zacielenia na používateľov sociálnych médií na základe osobitných kritérií vopred určil, ktoré typy osobných údajov sa majú použiť na vytvorenie týchto kritérií zacielenia a ktoré kritériá by sa mali ponúkať. Po zobrazení reklamy poskytovateľ sociálnych médií zároveň oznamuje subjektu vykonávajúcemu zacielenie určité štatistické informácie (napr. správu o demografickom zložení osôb, ktoré na reklamu reagovali).

#### A. Úlohy

42. V príklade 1 sa na určovaní účelu a prostriedkov spracúvania osobných údajov podieľajú subjekt vykonávajúci zacielenie aj poskytovateľ sociálnych médií. To vedie k zobrazeniu reklamy cieľovej skupine.
43. Pokiaľ ide o určenie *účelu*, spoločnosť X a poskytovateľ sociálnych médií spoločne určia účel spracúvania, ktorým je zobrazenie konkrétnej reklamy skupine jednotlivcov (v tomto prípade používateľom sociálnych médií) predstavujúcim cieľovú skupinu, a to tak, že vyberú dostupné kritériá zacielenia spojené s týmito používateľmi s cieľom osloviť skupinu, ktorá by mohla mať o produkt záujem, a poskytnúť jej relevantnejší reklamný obsah. Okrem toho z tejto jednej spracovateľskej operácie vyplýva vzájomný prospech pre spoločnosť X aj poskytovateľa sociálnych médií, čo je ďalším indikátorom toho, že účely, ktoré sledujú, sú neoddeliteľne prepojené.<sup>45</sup>
44. Pokiaľ ide o určenie *prostriedkov*, subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií spoločne určia prostriedky, ktoré sa použijú pri zacielení. Subjekt vykonávajúci zacielenie sa na určení týchto prostriedkov podieľa tým, že sa rozhodne využiť služby ponúkané poskytovateľom sociálnych médií<sup>46</sup> a požiada ho, aby sa zamerlal na skupinu osôb na základe určitých kritérií (t. j. vekové rozpätie, stav vzťahu, načasovanie zobrazenia).<sup>47</sup> Týmto spôsobom subjekt vykonávajúci zacielenie vymedzí kritériá, ktorými sa zacielenie riadi, a určí kategórie osôb, ktorých osobné údaje sa majú použiť. Na druhej strane poskytovateľ sociálnych médií sa rozhodol spracúvať osobné údaje svojich

<sup>45</sup> Pozri usmernenia EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov („Okrem toho ak subjekty nemajú rovnaký účel spracúvania, spoločné prevádzkovateľstvo možno podľa judikatúry SDEÚ potvrdiť aj vtedy, keď zapojené subjekty sledujú účely, ktoré sú úzko prepojené alebo sa dopĺňajú. Môže ísť napríklad o vzájomný prospech vyplývajúci z rovnakej spracovateľskej operácie, ak sa všetky zapojené subjekty podieľajú na určení účelov a prostriedkov príslušnej spracovateľskej operácie“).

<sup>46</sup> Pozri usmernenia EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov („Okrem toho ak sa subjekt rozhodne použiť na vlastné účely nástroj alebo iný systém vyvinutý iným subjektom, ktorý umožňuje spracúvanie osobných údajov, s veľkou pravdepodobnosťou to povedie k spoločnému rozhodovaniu o prostriedkoch, ktoré tieto subjekty pri spracúvaní použijú. Vyplýva to z veci Fashion ID, v ktorej SDEÚ dospel k záveru, že tým, že spoločnosť Fashion ID umiestnila na svoju internetovú stránku tlačidlo Páči sa mi to, ktoré spoločnosť Facebook sprístupnila pre správcov internetových stránok, uplatnila rozhodujúci vplyv vo vzťahu k operáciám, ktorých súčasťou je zber a poskytnutie osobných údajov návštevníkov jej internetovej stránky v prospech spoločnosti Facebook, a tým určila prostriedky ich spracúvania spoločne so spoločnosťou Facebook“).

<sup>47</sup> V tejto súvislosti pozri vec Wirtschaftsakademie, C-210/16, bod 39, ECLI:EU:C:2018:388.

používateľov tak, aby vytvoril kritériá zacielenia, ktoré sprístupňuje subjektu vykonávajúcemu zacielenie.<sup>48</sup> V tejto súvislosti poskytovateľ sociálnych médií prijal určité rozhodnutia týkajúce sa základných [essential] prostriedkov spracúvania, napríklad ktoré kategórie údajov sa majú spracúvať, ktoré kritériá zacielenia ponúknuť a kto by mal mať prístup k osobným údajom (a k akým typom), ktoré sa spracúvajú vo vzťahu ku konkrétnej cieľovej kampani.<sup>49</sup>

45. Pre úplnosť EDPB konštatuje, že poskytovateľ sociálnych médií sa nepovažuje za sprostredkovateľa v zmysle článku 4 bodu 8 všeobecného nariadenia o ochrane údajov.<sup>50</sup> V príklade 1 môže poskytovateľ sociálnych médií použiť kritériá zacielenia, ktoré vytvoril s použitím osobných údajov používateľa, na ďalšie spracovateľské operácie, čo dokazuje, že ho nemožno považovať za sprostredkovateľa. Navyše sa zdá, že poskytovateľ sociálnych médií nespracúva údaje výhradne v mene spoločnosti X a v súlade s jej pokynmi.
46. Spoločná kontrola [joint control] zo strany subjektu vykonávajúceho zacielenie a poskytovateľa sociálnych médií sa vzťahuje len na tie spracovateľské operácie, v prípade ktorých prakticky spoločne určujú ich účely a prostriedky. Týka sa aj spracúvania osobných údajov vyplývajúceho z výberu relevantných kritérií zacielenia a zobrazenia reklamy cieľovej skupine. Zároveň sa vzťahuje aj na spracúvanie osobných údajov, ktoré vykonáva poskytovateľ sociálnych médií s cieľom podať subjektu vykonávajúcemu zacielenie správu o výsledkoch cieľovej kampane. Spoločná kontrola sa však nevzťahuje na operácie, ktoré zahŕňajú spracúvanie osobných údajov v iných fázach ešte pred výberom príslušných kritérií zacielenia alebo po dokončení zacielenia a podaní správy (napr. vytvorenie nových kritérií zacielenia poskytovateľom sociálnych médií na základe dokončených cieľových kampaní) a pri ktorých sa subjekt vykonávajúci zacielenie nepodieľal na určovaní účelov a prostriedkov. Podobne poskytovateľ sociálnych médií sa v podstate nezúčastňuje vo fáze plánovania cieľovej kampane až do chvíle, keď s ním subjekt vykonávajúci zacielenie nadviaže kontakt.<sup>51</sup>
47. Uvedená analýza sa nemení ani v prípade, ak subjekt vykonávajúci zacielenie zadá len parametre cieľovej skupiny a nemá prístup k osobným údajom dotknutých používateľov. Pravdaže, v prípade, ak ide o spoluzodpovednosť viacerých subjektov za to isté spracúvanie, nevyžaduje sa, aby mal každý z nich prístup k dotknutým osobným údajom.<sup>52</sup> EDPB pripomína, že samotný prístup k osobným údajom nie je požiadavkou na odvodenie spoločnej zodpovednosti.<sup>53</sup>

## B. Právny základ

48. Obe strany (poskytovateľ sociálnych médií a subjekt vykonávajúci zacielenie) musia ako spoloční prevádzkovatelia vedieť preukázať existenciu právneho základu (článok 6 všeobecného nariadenia o ochrane údajov) na odôvodnenie spracúvania osobných údajov, za ktoré je každý z týchto prevádzkovateľov zodpovedný. EDPB pripomína, že medzi jednotlivými právnymi základmi všeobecného nariadenia o ochrane údajov neexistuje žiadna konkrétna hierarchia. Prevádzkovateľ

---

<sup>48</sup> Rovnako pozri aj vec Fashion ID, C-40/17, bod 80: „*tieto operácie spracovania sa uskutočňovali v hospodárskom záujme tak spoločnosti Fashion ID, ako aj spoločnosti Facebook Ireland, pre ktorú skutočnosť, že má prístup k týmto údajom na svoje vlastné obchodné účely, predstavuje protiplnenie za výhodu, ktorú ponúka spoločnosti Fashion ID.*“

<sup>49</sup> Pozri stanovisko 1/ 2010.

<sup>50</sup> Pozri usmernenia EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov.

<sup>51</sup> Pozri aj rozsudok vo veci Fashion ID, C-40/17, bod 74, („*uvedenú fyzickú alebo právnickú osobu [nemožno] považovať za prevádzkovateľa v zmysle uvedeného ustanovenia za predchádzajúce alebo neskoršie operácie v postupe spracovania, pri ktorých neurčuje účely ani prostriedky.*“) a bod 101.

<sup>52</sup> Rozsudok vo veci Wirtschaftsakademie, C-210/16, bod 38 – ECLI:EU:C:2018:388; rozsudok vo veci Jehovahi svedkovia, C-25/17, bod 69 – ECLI:EU:C:2018:551.

<sup>53</sup> Rozsudok SDEÚ z 10. júla 2018 (C-25/17, body 68 až 72).



musí zabezpečiť, aby vybraný právny základ zodpovedal cieľu a kontextu danej spracovateľskej operácie. Identifikácia primeraného právneho základu sa viaže na princípy spravodlivosti a obmedzenia účelu.<sup>54</sup>

49. Vo všeobecnosti existujú dva právne základy, ktorými by bolo možné zdôvodniť spracúvanie údajov na účely zacielenia na používateľov sociálnych médií: súhlas dotknutej osoby [článok 6 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov] alebo oprávnené záujmy [článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov]. Prevádzkovateľ musí vždy zvážiť, ktorý právny základ je primeraný vzhľadom na dané okolnosti. Vo vzťahu k poskytovateľom sociálnych médií nemožno článok 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov považovať za právny základ pre online reklamu, pretože touto reklamou sa nepriamo financuje poskytovanie ich služieb.<sup>55</sup> To isté platí aj pre subjekt vykonávajúci zacielenie, keďže zacielenie na používateľov sociálnych médií nemožno považovať za neoddeliteľný aspekt žiadnej služby, ani nie je potrebné na účely plnenia zmluvy uzavretej s používateľom.<sup>56</sup> Hoci individualizácia obsahu môže za určitých okolností predstavovať neoddeliteľný a očakávaný prvok určitých online služieb<sup>57</sup>, ťažko možno v súvislosti so zacielením na používateľov sociálnych médií aplikovať článok 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov, ako je ukázané aj v príkladoch v týchto usmerneniach.<sup>58</sup>
50. Pokiaľ ide o právny základ postavený na oprávnenom záujme, EDPB pripomína, že SDEÚ vo veci Fashion ID pripomenul, že na to, aby spracúvanie osobných údajov bolo založené na oprávnenom záujme, musia byť splnené tri kumulatívne podmienky, a to <sup>59</sup> i) sledovanie oprávneného záujmu prevádzkovateľom alebo tretími stranami, ktorým sú údaje oznámené, ii) nevyhnutnosť spracúvania osobných údajov na realizáciu sledovaného oprávneného záujmu a iii) podmienka, že neprevažujú základné práva a slobody osoby, ktorej sa ochrana údajov týka. SDEÚ zároveň uviedol, že v prípade spoločného prevádzkovateľstva „je potrebné, aby každý z týchto prevádzkovateľov sledoval uvedenými operáciami spracovania legitímny záujem [...], aby tieto operácie boli z jeho pohľadu odôvodnené“.<sup>60</sup>
51. Pokiaľ ide o príklad 1, subjekt vykonávajúci zacielenie by mohol svoj oprávnený záujem považovať za hospodársky záujem dosiahnuť lepšiu propagáciu svojich výrobkov prostredníctvom zacielenia na sociálnych médiách. Poskytovateľ sociálnych médií by sa mohol domnievať, že jeho oprávneným záujmom je dosiahnuť predajom reklamného priestoru ziskovosť služby sociálnych médií. To, či subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií môže použiť ako právny základ článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov závisí od toho, či sú splnené všetky tri kumulatívne podmienky, ako nedávno pripomenul SDEÚ. Aj ak subjekt vykonávajúci zacielenie a poskytovateľ

<sup>54</sup> Pozri bod 18 usmernení 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám, verzia 2.0, 8. októbra 2019, k dispozícii na adrese [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines-art-6-1-b-adopted-after-public-consultation-sk.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art-6-1-b-adopted-after-public-consultation-sk.pdf).

<sup>55</sup> Pozri body 52 a 53 usmernení 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám, verzia 2.0, 8. októbra 2019, k dispozícii na adrese [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines-art-6-1-b-adopted-after-public-consultation-sk.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art-6-1-b-adopted-after-public-consultation-sk.pdf).

<sup>56</sup> Nevyhnutnosť neexistuje v prípade, že by subjekt vykonávajúci zacielenie využil služby poskytovateľa sociálnych médií napriek priamemu zmluvnému vzťahu so zákazníkom, ktorý znamená možnosť priamej reklamy.

<sup>57</sup> Pozri s. 15 usmernení 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám, verzia 2.0, 8. októbra 2019, k dispozícii na adrese [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines-art-6-1-b-adopted-after-public-consultation-sk.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art-6-1-b-adopted-after-public-consultation-sk.pdf).

<sup>58</sup> Usmernenia 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám, bod 57.

<sup>59</sup> SDEÚ, rozsudok vo veci Fashion ID, 29. júla 2019, C-40/17, bod 95 – ECLI:EU:C:2019:629.

<sup>60</sup> Tamtiež, bod 97.

sociálnych médií považujú svoje hospodárske záujmy za oprávnené, nemusí to nevyhnutne znamenať, že sa môžu skutočne odvolávať na článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov.

52. V rámci druhej časti testu vyváženosti [balancing test] musia spoloční prevádzkovatelia stanoviť, že spracúvanie údajov je nevyhnutné na dosiahnutie týchto oprávnených záujmov. Na to, aby bolo spracúvanie naozaj „nevyhnutné“, musí existovať prepojenie medzi spracúvaním a sledovanými záujmami. Táto požiadavka „nevyhnutnosti“ je relevantná najmä v súvislosti s uplatňovaním článku 6 ods. 1 písm. f), aby sa zabezpečilo, že spracúvanie údajov založené na oprávnených záujmoch nepovedie k príliš širokému výkladu nevyhnutnosti spracúvania údajov. Podobne ako v iných prípadoch to znamená, že by sa malo posúdiť, či sú k dispozícii iné prostriedky vhodné na rovnaký účel, ktoré predstavujú menší zásah.<sup>61</sup>
53. Tretím krokom pri posudzovaní toho, či sa subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií môžu odvolávať na článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov ako na právny základ na účely spracúvania osobných údajov, je test vyváženosti [balancing exercise], ktorým sa určí, či nad daným oprávneným záujmom neprevažujú základné práva a slobody dotknutej osoby.<sup>62</sup>
54. EDPB pripomína, že v prípade, ak sa chce prevádzkovateľ odvolať na oprávnený záujem, je potrebné venovať dôkladnú pozornosť povinnosti transparentnosti a právu namietať. Než sa začne so spracúvaním údajov, dotknuté osoby by mali mať možnosť namietať proti spracúvaniu svojich údajov na určené účely. Používatelia sociálnych médií by mali mať k dispozícii nielen možnosť namietať proti zobrazovaniu cielenej reklamy pri prístupe k platforme, ale aj kontrolné mechanizmy, ktorými sa zabezpečí, že sa po vznesení námietky ich osobné údaje už viac nebudú spracúvať na účely zacielenia.
55. Ak sa chce subjekt vykonávajúci zacielenie odvolať na oprávnený záujem, mal by za seba jednotlivcom umožniť jednoduchým spôsobom vopred vyjadriť námietku proti jeho používaniu sociálnych médií na zacielenie. Ak subjekt vykonávajúci zacielenie nemá žiadnu priamu komunikáciu s dotknutou osobou, mal by aspoň zaistiť, aby dotknutá osoba mohla v rámci platformy sociálnych médií účinne využiť svoje právo na predbežnú námietku [right to prior objection]. Subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií by ako spoloční prevádzkovatelia mali objasniť, ako sa v súvislosti so spoločnou dohodou bude dodržiavať právo jednotlivcov namietať (ako aj iné práva) (pozri oddiel 6). Ak sa v rámci testu vyváženosti ukáže, že záujmy alebo základné práva a slobody dotknutých osôb prevažujú nad oprávneným záujmom poskytovateľa sociálnych médií a subjektu vykonávajúcemu zacielenie, článok 6 ods. 1 písm. f) nemožno použiť.
56. Pokiaľ ide o právny základ založený na súhlase, prevádzkovateľ musí mať na pamäti, že jasne existujú situácie, v ktorých by spracúvanie údajov bez platného súhlasu dotknutých osôb bolo protizákonné [článok 6 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov]. Pracovná skupina zriadená podľa článku 29 sa napríklad predtým domnievala, že pre prevádzkovateľov by bolo ťažké zdôvodniť použitie oprávnených záujmov ako právneho základu pre intruzívne profilovanie a postupy sledovania na

---

<sup>61</sup> Stanovisko 06/2014 pracovnej skupiny zriadenej podľa článku 29 k pojmu legitímne záujmy [legitimate interests] prevádzkovateľa podľa článku 7 smernice 95/46/ES, WP217, 9. apríla 2014, s. 29.

<sup>62</sup> Pri posudzovaní vplyvu na záujmy, základné práva a slobody dotknutej osoby je v súvislosti so zacielením na používateľov sociálnych médií obzvlášť dôležité zohľadniť tieto aspekty: i) účely zacielenia, ii) úroveň podrobnosti použitých kritérií zacielenia (napr. zoširoka opísaná kohorta, napr. „ľudia so záujmom o anglickú literatúru“ alebo podrobnejšie kritériá umožňujúce segmentáciu a zacielenie na detailnejšej úrovni), iii) typ (a kombinácia) použitých kritérií zacielenia (t. j. či sa zacielenie vo vzťahu k dotknutým osobám zameriava len na drobný aspekt alebo má komplexnejší charakter) a iv) povaha (citlivosť), objem a zdroj údajov použitých na vytvorenie kritérií zacielenia. Pozri stanovisko 06/2014 pracovnej skupiny zriadenej podľa článku 29 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES, WP 217, 9. apríla 2014, [https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217\\_sk.pdf](https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217_sk.pdf).

marketingové alebo reklamné účely, napríklad tie, ktoré zahŕňajú sledovanie jednotlivcov na viacerých webových sídlach, lokalitách, zariadeniach, službách alebo data-brokeringu.<sup>63</sup>

57. Súhlas so spracúvaním údajov je platný len vtedy, ak spĺňa podmienky stanovené v článku 4 ods. 11 a v článku 7 všeobecného nariadenia o ochrane údajov. Vo všeobecnosti môže súhlas slúžiť ako primeraný právny základ len vtedy, keď má dotknutá osoba možnosť kontroly a skutočnej voľby. Ak je súhlas súčasťou nezmeniteľných podmienok, nepovažuje sa za daný slobodne. Súhlas musí byť konkrétny, informovaný a jednoznačný a dotknuté osoby musia mať možnosť ho odmietnuť alebo odvolať bez nepriaznivých následkov.<sup>64</sup>
58. Súhlas [článok 6 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov] by bolo možné dosiahnuť, ak budú splnené všetky podmienky na udelenie platného súhlasu. EDPB pripomína, že získaním súhlasu navyše nezakazuje ani sa žiadnym spôsobom neobmedzuje povinnosť prevádzkovateľa dodržiavať zásady spracúvania údajov uvedené vo všeobecnom nariadení o ochrane údajov, osobitne v článku 5, týkajúce sa spravodlivosti, nevyhnutnosti a primeranosti, ako aj kvality údajov. Aj keď je spracúvanie osobných údajov založené na súhlase dotknutej osoby, týmto súhlasom sa neopravňuje zacielenie, ktoré je neprimerané alebo nespravodlivé.<sup>65</sup>
59. A napokon EDPB zastáva názor, že spracúvanie osobných údajov opísané v príklade 1 nemožno odôvodniť na základe článku 6 ods. 1 písm. b), a to ani zo strany sociálnej platformy, ani zo strany subjektu vykonávajúceho zacielenie.<sup>66</sup>

#### 5.2.2 Údaje, ktoré poskytne používateľ platformy sociálnych médií subjektu vykonávajúcemu zacielenie

60. Pri zacielení sa môžu použiť aj údaje, ktoré poskytne dotknutá osoba subjektu vykonávajúcemu zacielenie, a ten následne získané údaje použije na zacielenie na dotknutú osobu na sociálnych médiách. K zacieleniu „na základe zoznamu“ [list-based] dochádza, keď subjekt vykonávajúci zacielenie nahrá už existujúce zoznamy osobných údajov (napr. e-mailové adresy alebo telefónne čísla), aby ich poskytovateľ sociálnych médií mohol porovnať s informáciami na platforme. Poskytovateľ sociálnych médií v takom prípade porovná údaje nahraté subjektom vykonávajúcim zacielenie s údajmi, ktoré už má, a akýchkoľvek používateľov, ktorí zodpovedajú kritériám, pridá do cieľovej skupiny (t. j. do „klastra“ osôb, ktorým sa bude na platforme sociálnych médií zobrazovať reklama) alebo ich z nej vylúči. Poskytovateľ sociálnych médií môže zároveň subjektu vykonávajúcemu zacielenie povoliť, aby daný zoznam pred dokončením skontroloval, takže k určitému spracúvaniu údajov dôjde ešte pred vytvorením cieľovej skupiny.

#### Príklad 2:

Pani Jonesová sa obráti na banku X, aby si dohodla stretnutie v súvislosti s možnou hypotékou, pretože kupuje dom. Stretnutie v banke si dohodne cez e-mail. Po stretnutí sa pani Jonesová rozhodne, že sa

<sup>63</sup> Stanovisko pracovnej skupiny zriadenej podľa článku 29 k profilovaniu a k automatizovanému individuálnemu rozhodovaniu, WP 251 rev. 01, s. 15; pozri aj stanovisko WP29 k legitímnym záujmom, s. 32 a 48: „Celkovo nie je legitímny záujem spoločnosti vyvážený s ochranou základných práv používateľov a nemalo by sa vychádzať z článku 7 písm. f) ako právneho dôvodu na spracovanie. Vhodnejší dôvod na použitie by bol článok 7 písm. a), pokiaľ by boli splnené podmienky platného súhlasu.“

<sup>64</sup> Pozri usmernenia pracovnej skupiny zriadenej podľa článku 29 k súhlasu podľa nariadenia 2016/679, WP 259 rev. 01.

<sup>65</sup> Pozri usmernenia pracovnej skupiny zriadenej podľa článku 29 k súhlasu podľa nariadenia 2016/679, WP259, rev. 01, s. 3 až 4.

<sup>66</sup> Pozri usmernenia 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám, verzia 2.0, 8. októbra 2019, k dispozícii na adrese [https://edpb.europa.eu/sites/edpb/files/files/file1/edpb\\_guidelines-art-6-1-b-adopted-after-public-consultation-sk.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art-6-1-b-adopted-after-public-consultation-sk.pdf).

nestane zákazníkom banky. Banka napriek tomu pridala e-mailovú adresu pani Jonesovej do svojej zákazníckej e-mailovej databázy. Banka potom použije túto e-mailovú databázu tak, že umožní poskytovateľovi sociálnych médií, aby porovnal jej zoznam e-mailových adries s adresami z platformy sociálnych médií, aby mohol prostredníctvom tejto platformy zacieliť na dotknuté osoby a ponúknuť im kompletnú škálu finančných služieb.

#### Príklad 3:

Pán Lopez je zákazníkom banky X už skoro rok. Na začiatku banke X poskytol svoju e-mailovú adresu a banka ho pri tej príležitosti informovala, že: a) jeho e-mailová adresa bude použitá na propagáciu ponúk súvisiacich s bankovými službami, ktoré už používa, a b) môže proti tomuto spracúvaniu údajov kedykoľvek namietať. Banka pridala jeho e-mailovú adresu do svojej zákazníckej e-mailovej databázy. Následne banka túto e-mailovú databázu použila na zacielenie na svojich zákazníkov na platforme sociálnych médií, aby im ponúkla kompletnú škálu finančných služieb.<sup>67</sup>

### A. Úlohy

61. V týchto príkladoch subjekt vykonávajúci zacielenie, t. j. banka, vystupuje ako prevádzkovateľ, keďže určuje účely a prostriedky spracúvania tým, že aktívne získava, spracúva a poskytuje osobné údaje dotknutých osôb poskytovateľovi sociálnych médií na reklamné účely. Poskytovateľ sociálnych médií zas koná ako prevádzkovateľ, pretože prijal rozhodnutie použiť osobné údaje získané od používateľa sociálnych médií (t. j. e-mailovú adresu, ktorú používateľ zadal pri vytváraní konta), aby umožnil subjektu vykonávajúcemu zacielenie zobrazovať reklamu špecifickej skupine osôb.
62. Spoločné prevádzkovateľstvo existuje vo vzťahu k spracovateľským operáciám, pre ktoré poskytovateľ sociálnych médií a subjekt vykonávajúci zacielenie spoločne určujú účely a prostriedky, v tomto prípade nahrať jedinečných identifikátorov súvisiacich s cieľovou skupinou, porovnanie údajov, výber kritérií zacielenia a následné zobrazovanie reklamy, ako aj podávanie správ v súvislosti s cieľovou kampaňou.<sup>68</sup>
63. V oboch prípadoch, teda pri získavaní e-mailovej adresy pani Jonesovej aj pána Lopeza, banka vystupuje ako výlučný prevádzkovateľ. Poskytovateľ sociálnych médií sa žiadnym spôsobom nepodieľa na určovaní prostriedkov a účelov tohto získavania údajov. Spoločné prevádzkovanie sa začína poskytnutím osobných údajov a ich súbežným prevzatím zo strany poskytovateľa sociálnych médií. Ďalej pokračuje zobrazovaním cieľenej reklamy a (vo väčšine prípadov) sa končí po dokončení nasledujúcej fázy podávania správ. V niektorých prípadoch možno spoločné prevádzkovateľstvo ešte predĺžiť až do fázy vymazania údajov, pokiaľ sa subjekt vykonávajúci zacielenie naďalej podieľa na určovaní účelov a prostriedkov.

---

<sup>67</sup> V situáciách, keď sa e-mailové adresy používajú na posielanie priameho marketingu používateľom, musia prevádzkovatelia zohľadniť aj ustanovenia článku 13 smernice o súkromí a elektronických komunikáciách.

<sup>68</sup> Určenie účelov a prostriedkov spracúvania údajov zo strany subjektu vykonávajúceho zacielenie a poskytovateľa sociálnych médií je podobné (hoci nie rovnaké) ako v príklade 1. Nahrať zoznamu e-mailových adries a určením ďalších kritérií zacielenia subjekt vykonávajúci zacielenie vymedzí kritériá, ktorými sa zacielenie riadi, a určí kategórie osôb, ktorých osobné údaje sa majú použiť. Poskytovateľ sociálnych médií takisto rozhoduje o tom, či osobné údaje sa majú spracúvať, a to tým, že povoľuje spracúvanie konkrétnych kategórií údajov, určuje, ktoré kritériá zacielenia ponúknuť a kto by mal mať prístup k osobným údajom (a k akým typom) spracúvaným vo vzťahu ku konkrétnej cieľenej kampani. Spoločný účel týchto spracovateľských operácií sa podobá na účel identifikovaný v príklade 1, konkrétne zobrazenie konkrétnej reklamy skupine jednotlivcov (v tomto prípade používateľom sociálnych médií), ktorí predstavujú cieľovú skupinu.

64. Dôvodom, prečo banka koná ako výlučný prevádzkovateľ pri získavaní e-mailovej adresy od pani Jonesovej a pána Lopeza je, že toto získavanie údajov prebieha ešte pred cieľnou kampaňou (a nie je s ňou neoddeliteľne prepojené). Preto je v tomto prípade potrebné rozlišovať medzi úvodným súborom spracovateľských operácií, pri ktorom je banka výlučným prevádzkovateľom, a následným spracúvaním údajov, na ktoré sa vzťahuje spoločná kontrola. Zodpovednosť banky sa nevzťahuje na operácie po dokončení zacielenia a podania správ, v prípade ktorých sa subjekt vykonávajúci zacielenie nepodieľal na určovaní účelov a prostriedkov a poskytovateľ sociálnych médií v nich vystupuje ako výlučný prevádzkovateľ.

## B. Právny základ

65. Pre Príklad 2 článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov nepredstavuje primeraný právny základ, ktorým by bolo možné v tomto prípade odôvodniť spracúvanie údajov, vzhľadom na kontext, v akom boli osobné údaje poskytnuté. Pani Jonesová sa v skutočnosti obrátila na banku s jediným cieľom – dohodnúť si stretnutie, po ktorom oznámila, že nemá v úmysle využiť služby ponúkané bankou. Preto sa dá povedať, že pani Jonesová logicky neočakáva, že sa jej osobné údaje použijú na účely zacielenia („opätovné zacielenie“) [re-targeting]. Okrem toho test zlučiteľnosti [compatibility test] podľa článku 6 ods. 4 všeobecného nariadenia o ochrane údajov by pravdepodobne viedol k záveru, že toto spracúvanie nie je zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané.
66. V príklade 3 sa môže subjekt vykonávajúci zacielenie pri spracúvaní údajov odvolať na oprávnený záujem, okrem iného vzhľadom na to, že: a) pán Lopez bol informovaný o tom, že jeho e-mailová adresa sa môže použiť na účely reklamy cez sociálne médiá na služby súvisiace so službou, ktorú dotknutá osoba používa; b) reklama sa týka služieb podobných tým, ktoré pán Lopez už využíva, a c) pán Lopez mal možnosť namietat ešte pred spracúvaním jeho údajov, teda vo chvíli, keď banka získala jeho osobné údaje. EDPB by však rád objasnil, že splnenie informačných povinností vyplývajúcich z článkov 13 a 14 všeobecného nariadenia o ochrane údajov a zváženie záujmov, ktoré sa má vykonať podľa článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov, predstavujú dva rôzne súbory povinností. Preto samotné splnenie informačných povinností podľa článkov 13 a 14 všeobecného nariadenia o ochrane údajov nie je opatrením na zvýšenie transparentnosti, ktoré sa má zohľadniť pri zvažovaní záujmov podľa článku 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov.

### 5.3 Zacielenie na základe pozorovaných údajov

67. Existuje niekoľko spôsobov, ktorými môžu poskytovatelia sociálnych médií sledovať správanie svojich používateľov. Sledovanie je možné napr. prostredníctvom samotných služieb sociálnych médií alebo na externých webových sídlach pomocou modulov sociálnych médií alebo pixelov.

#### Príklad 4: Zacielenie na základe pixelov

Pán Schmidt si prezerá internet a chce si kúpiť batoh. Navštívi webové sídlo BestBags.com, pozrie si viacero položiek, ale rozhodne sa nič nekúpiť. Správca sídla BestBags.com chce zacieliť na používateľov sociálnych médií, ktorí navštívili jeho webové sídlo a nič si nekúpili. Preto na webové sídlo umiestni tzv. „sledovací pixel“ [tracking pixel]<sup>69</sup>, ktorý sprístupnil poskytovateľ sociálnych médií. Keď pán Schmidt

<sup>69</sup> Sledovacie pixely sú tvorené zlomkami kódu, ktoré sú integrované na webovom sídle subjektu vykonávajúceho zacielenie. Keď osoba otvorí webové sídlo subjektu vykonávajúceho zacielenie vo svojom prehliadači, prehliadač automaticky odošle serveru poskytovateľa sociálnych médií žiadosť o získanie sledovacieho pixelu. Keď sa sledovací pixel stiahne, poskytovateľ sociálnych médií zvyčajne môže monitorovať reláciu používateľa (t. j. správanie jednotlivca na daných webových sídlach). Pozorované údaje sa môžu využiť napríklad na pridanie používateľa sociálnych médií do konkrétnej cieľovej skupiny.

opustí webové sídlo BestBags.com a prihlási sa do svojho konta na sociálnych médiách, začnú sa mu zobrazovať reklamy na batohy, ktoré zvažoval pri prezeraní sídla BestBags.com.

#### Príklad 5: Geografické zacielenie

Pani Michuová si do smartfónu nainštalovala aplikáciu poskytovateľa sociálnych médií. Počas dovolenky sa prechádza po Paríži. Poskytovateľ sociálnych médií prostredníctvom GPS funkcií jej smartfónu získava priebežné informácie o jej polohe<sup>70</sup> na základe povolení, ktoré mu boli udelené pri inštalácii aplikácie. Pani Michuová je ubytovaná v hoteli vedľa pizzerie. Pizzeria využíva funkciu geografického zacielenia, ktorú ponúka poskytovateľ sociálnych médií na zacielenie na osoby nachádzajúce sa vo vzdialenosti do 1 km od pizzerie po prvýkrát za posledných šesť mesiacov. Keď si pani Michuová vo svojom smartfóne otvorí aplikáciu tohto poskytovateľa sociálnych médií, zobrazí sa jej reklama z pizzerie, rozhodne sa, že je hladná, a cez webové sídlo reštaurácie si kúpi pizzu.

#### Príklad 6:

Pani Ghorbaniová si vytvorí konto na platforme sociálnych médií. Počas registrácie sa jej zobrazí otázka, či súhlasí so spracúvaním jej osobných údajov na účely zobrazovania cieľenej reklamy na stránke jej sociálnych médií na základe údajov, ktoré priamo poskytne poskytovateľovi sociálnych médií (napr. jej vek, pohlavie a poloha), ako aj na základe jej aktivity na iných webových sídlach mimo platformy sociálnych médií, ktoré využívajú súbory cookie. Je informovaná, že tieto údaje sa budú získavať prostredníctvom modulov sociálnych médií alebo sledovacích pixelov, dostane presný opis postupov a informáciu, že na zacielení sa podieľajú ďalšie subjekty, ktoré spoločne zodpovedajú za dodržiavanie všeobecného nariadenia o ochrane údajov. Tieto informácie obsahujú aj vysvetlenie, že svoj súhlas môže kedykoľvek odvolať, a dostane odkaz na zásady ochrany osobných údajov. Keďže pani Ghorbaniová má záujem o cieľenú reklamu na svojej stránke sociálnych médií, súhlasí s podmienkami. Všetky súbory cookie sa ukladajú alebo získavajú až po tom, ako pani Ghorbaniová udelí svoj súhlas.

Neskôr navštívi webové sídlo „Thelatesthotnews.com“, ktoré má integrované tlačidlo sociálnych médií. Na pravom okraji obrazovky sa zobrazí malý, ale dobre viditeľný banner so žiadosťou o súhlas s poskytnutím jej osobných údajov poskytovateľovi sociálnych médií prostredníctvom súborov cookie a modulov sociálnych médií. Správca webového sídla vykonal technické opatrenia na to, aby sa platforme sociálnych médií nepreniesli žiadne osobné údaje bez jej súhlasu.

### 5.3.1 Úlohy

68. V Príklad 4 subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií spoločne určili účely a prostriedky spracúvania osobných údajov, ktoré viedli k zobrazovaniu reklamy páňovi Schmidtovi.
69. Pokiaľ ide o určovanie účelu, BestBags.com a poskytovateľ sociálnych médií spoločne určili účel spracúvania údajov, ktorým je zobrazenie konkrétnej reklamy na platforme sociálnych médií osobám predstavujúcim cieľovú skupinu. Prostredníctvom pixelu umiestneného na sídle BestBags.com získava toto sídlo rozhodujúci vplyv na prostriedky spracúvania údajov. Bez umiestnenia tohto pixelu by nedošlo k získaniu a poskytnutiu osobných údajov návštevníkov webového sídla poskytovateľovi sociálnych médií. Na druhej strane poskytovateľ sociálnych médií vytvoril a ponúka softvérový kód (pixel), ktorý vedie k automatickému získavaniu, poskytovaniu a hodnoteniu osobných údajov na obchodné účely v prospech poskytovateľa sociálnych médií. V dôsledku toho existuje spoločné

<sup>70</sup> Poskytovateľ sociálnych médií môže byť zároveň schopný určiť polohu používateľov na základe iných údajových bodov vrátane IP adresy, informácií o Wi-Fi z mobilných zariadení alebo údajov odvodených od informácií používateľov (napr. ak uvedú svoju polohu v príspevku na platforme).

prevádzkovateľstvo z hľadiska získavania osobných údajov a ich poskytovania pomocou pixelov, ako aj porovnávaní a následného zobrazovania reklamy pánovi Schmidtovi na sociálnej platforme, a každého podávania správ v súvislosti s cieľovou kampaňou. Z podobných dôvodov existuje spoločné prevádzkovateľstvo aj v príklade 6.

70. V príklade 5 má pizzeria rozhodujúci vplyv na spracúvanie osobných údajov tým, že vymedzuje parametre zacielenia reklamy v súlade so svojimi obchodnými potrebami (napr. otváracie hodiny pizzerie a geografická poloha osôb v blízkosti pizzerie v tomto čase), a preto ju treba považovať za subjekt, ktorý sa podieľa na určovaní účelov a prostriedkov spracúvania údajov. Na druhej strane poskytovateľ sociálnych médií získal informácie o polohe pani Michuovej (pomocou GPS), na základe ktorých môže využiť reklamu cielenú podľa lokality. V dôsledku toho existuje spoločná kontrola zo strany subjektu vykonávajúceho zacielenie a platformy sociálnych médií vo vzťahu k získavaniu a analýze údajov o polohe pani Michuovej, ako aj k zobrazeniu reklamy s cieľom zacieliť túto reklamu na ňu (ako na osobu nachádzajúcu sa vo vzdialenosti do 1 km od pizzerie po prvýkrát za posledných šesť mesiacov).

### 5.3.2 Právny základ

71. V prvom rade, keďže príklady 4, 5 a 6 sa týkajú použitia súborov cookie, je potrebné zohľadniť požiadavku vyplývajúcu z článku 5 ods. 3 smernice o súde a elektronických komunikáciách.
72. V tomto smere treba pripomenúť, že podľa článku 5 ods. 3 smernice o súde a elektronických komunikáciách sa požaduje, aby používatelia ešte pred udelením súhlasu dostali jasné a komplexné informácie, okrem iného o účeloch spracúvania<sup>71</sup>, s veľmi malým počtom výnimiek.<sup>72</sup> Jasné a komplexné informácie znamenajú, že používateľ môže jednoducho určiť následky súhlasu, ktorý môže poskytnúť, a zabezpečiť, že bude poskytnutý informovaný súhlas.<sup>73</sup> V dôsledku toho bude prevádzkovateľ musieť informovať dotknuté osoby o všetkých relevantných účeloch spracúvania – vrátane akéhokoľvek následného spracúvania osobných údajov získaných na základe prístupu k údajom v koncovom zariadení.
73. Súhlas získaný na účely zavedenia sledovacích technológií je platný len vtedy, ak spĺňa podmienky stanovené v článku 7 všeobecného nariadenia o ochrane údajov.<sup>74</sup> Súhlas napríklad nie je platne daný vtedy, keď je použitie súborov cookie povolené začiarkavacím políčkcom, ktoré bolo vopred označené poskytovateľom služby a ktorého označenie musí používateľ zrušiť, aby odmietol dať svoj súhlas.<sup>75</sup> V súlade s odôvodnením 32 úkony ako posúvanie alebo potiahnutie prstom cez webové sídlo alebo podobná činnosť používateľa za žiadnych okolností nespĺňajú požiadavku jednoznačného a potvrdzujúceho úkonu: takéto úkony môžu byť ťažko odlišiteľné od inej činnosti alebo interakcie používateľa, a preto ani nie je možné konštatovať, že bol získaný jednoznačný súhlas. Okrem toho bude v takom prípade ťažké umožniť používateľovi odvolať súhlas rovnako jednoduchým spôsobom, akým bol poskytnutý.<sup>76</sup>
74. Každý (spoločný) prevádzkovateľ, ktorý chce použiť súhlas ako právny základ, musí zabezpečiť získanie platného súhlasu. V rozsudku vo veci Fashion ID SDEÚ zdôrazňuje, že je dôležité zaistiť efektívnu

<sup>71</sup> SDEÚ, rozsudok vo veci Planet 49 GmbH, C-673/17, bod 73.

<sup>72</sup> Pozri stanovisko 5/2019 týkajúce sa vzájomného pôsobenia medzi smernicou o súde a elektronických komunikáciách a všeobecným nariadením o ochrane údajov, najmä pokiaľ ide o príslušnosť, úlohy a právomoci orgánov pre ochranu osobných údajov. Pozri aj Súdny dvor Európskej únie, rozsudok vo veci Fashion ID, C-40/17, body 89 až 91.

<sup>73</sup> Tamže, bod 74.

<sup>74</sup> Usmernenia EDPB 05/2020 k súhlasu podľa nariadenia 2016/679, verzia 1.1, s. 6.

<sup>75</sup> SDEÚ, rozsudok vo veci Planet 49, C-637/17, bod 57.

<sup>76</sup> Usmernenia EDPB 05/2020 k súhlasu podľa nariadenia 2016/679, verzia 1.1, s. 19.

a včasnú ochranu práv dotknutých osôb a že súhlas by sa nemal poskytovať len spoločnému prevádzkovateľovi, ktorý sa podieľa na neskoršej fáze spracúvania. Platný súhlas treba získať ešte pred spracúvaním, čo znamená, že (spoloční) prevádzkovatelia musia posúdiť, kedy a ako tieto informácie poskytnúť používateľovi a získať jeho súhlas. Inak povedané, to, ktorý zo spoločných prevádzkovateľov by mal zodpovedať za získanie tohto súhlasu, závisí od toho, kto z nich ako prvý prichádza do kontaktu s dotknutou osobou. Vzhľadom na to, že v príklade 6 k uloženiu súborov cookie a spracúvaníu osobných údajov dochádza vo chvíli vytvorenia konta, poskytovateľ sociálnych médií musí získať platný súhlas ešte pred uložením reklamných súborov cookie.

75. EDPB zároveň pripomína, že v prípade, keď sa o požadovaný súhlas opierajú viacerí (spoloční) prevádzkovatelia, alebo ak sa údaje majú prenášať iným prevádzkovateľom alebo majú byť spracúvané inými prevádzkovateľmi, ktorí sa chcú opierať o pôvodný súhlas, všetky tieto organizácie by mali byť vymenované.<sup>77</sup> Ak vo chvíli, keď poskytovateľ sociálnych médií žiada o súhlas, ešte nie sú známi všetci spoloční prevádzkovatelia, bude potrebné, aby sa súhlas pre poskytovateľa sociálnych médií doplnil o ďalšie informácie a súhlas získaný správcom webového sídla, na ktorom je umiestnený modul sociálnych médií (t. j. *Thelatesthotnews.com* v príklade 6).
76. EDPB zdôrazňuje, že súhlas, ktorý musí správca webového sídla získať na účely poskytnutia osobných údajov, ktoré spúšťa jeho webové sídlo (vložením modulu sociálneho média), sa týka len operácie alebo súboru operácií spracúvania osobných údajov, pri ktorých tento prevádzkovateľ skutočne určuje účely a prostriedky<sup>78</sup>. Tým, že správca webového sídla, t. j. napríklad *Thelatesthotnews.com* v príklade 6, získa súhlas, nezakazuje ani sa žiadnym spôsobom neobmedzuje povinnosť poskytovateľa sociálnych médií zaistiť, aby dotknutá osoba poskytla platný súhlas so spracúvaním údajov, za ktoré tento poskytovateľ ako spoločný prevádzkovateľ zodpovedá<sup>79</sup>, ako aj s každým následným [subsequent] alebo ďalším [further] spracúvaním, ktoré vykonáva a pre ktoré neurčuje účely a prostriedky spoločne so správcom webového sídla (napr. neskoršie operácie profilovania na účely zacielenia).
77. Okrem toho každé následné spracúvanie osobných údajov vrátane osobných údajov získaných pomocou súborov cookie, modulov sociálnych médií alebo pixelov je zákonné len vtedy, ak má právny základ v článku 6 všeobecného nariadenia o ochrane údajov.<sup>80</sup> Pokiaľ ide o právny základ spracúvania v príkladoch 4, 5 a 6, EDPB je presvedčený, že oprávnený záujem nemôže slúžiť ako právny základ, keďže zacielenie je založené na monitorovaní správania jednotlivcov na webových sídlach a miestach pomocou sledovacích technológií.<sup>81</sup>
78. Preto za týchto okolností je pravdepodobné, že primeraným právnym základom pre akékoľvek následné spracúvanie podľa článku 6 všeobecného nariadenia o ochrane údajov bude takisto súhlas dotknutej osoby. Pri hodnotení súladu s článkom 6 všeobecného nariadenia o ochrane údajov je samozrejme potrebné zohľadniť, že spracúvanie ako celok zahŕňa osobitné činnosti, v prípade ktorých

<sup>77</sup> Usmernenia EDPB 05/2020 k súhlasu podľa nariadenia 2016/679, verzia 1.1, s. 16, odsek 65.

<sup>78</sup> Rozsudok vo veci Fashion ID, 29. júla 2019, C-40/17, ECLI:EU:C:2019:629, body 100 až 101.

<sup>79</sup> To platí tým skôr, že v prípade väčšiny nástrojov zacielenia práve sociálne médiá vykonávajú operácie čítania z koncového zariadenia používateľa alebo zápisu naň, keďže získavajú osobné údaje na účely cielenej reklamy. Preto poskytovateľ sociálnych médií zodpovedá za získanie platného súhlasu.

<sup>80</sup> Stanovisko 5/2019 týkajúce sa vzájomného pôsobenia medzi smernicou o súkromí a elektronických komunikáciách a všeobecným nariadením o ochrane údajov, najmä pokiaľ ide o príslušnosť, úlohy a právomoci orgánov pre ochranu osobných údajov, bod 41.

<sup>81</sup> Stanovisko pracovnej skupiny zriadenej podľa článku 29 k profilovaniu a k automatizovanému individuálnemu rozhodovaniu, WP 251 rev. 01, s. 15; pozri aj stanovisko WP29 k legitímnym záujmom, s. 32 a 48: „Celkovo nie je legitímny záujem spoločnosti vyvážený s ochranou základných práv používateľov a nemalo by sa vychádzať z článku 7 písm. f) ako právneho dôvodu na spracúvanie. Vhodnejší dôvod na použitie by bol článok 7 písm. a), pokiaľ by boli splnené podmienky platného súhlasu.“



sa zákonodarca EÚ snažil stanoviť dodatočnú ochranu.<sup>82</sup> Prevádzkovatelia musia pri určovaní vhodného právneho základu zohľadniť vplyv na práva dotknutých osôb, s cieľom dodržať zásadu spravodlivosti.<sup>83</sup>

#### 5.4 Zacielenie na základe odvodených údajov

79. Odvodené údaje sú údaje vytvorené prevádzkovateľom na základe údajov poskytnutých dotknutou osobou (bez ohľadu na to, či ide o údaje získané sledovaním, alebo či ich aktívne poskytla dotknutá osoba, alebo o ich kombináciu).<sup>84</sup> Závery o dotknutých osobách môže odvodzovať poskytovateľ sociálnych médií aj subjekt vykonávajúci zacielenie.
80. Poskytovateľ sociálnych médií môže byť napríklad schopný na základe dlhodobého monitorovania správania svojich používateľov v rámci sociálnych médií aj mimo nich (napr. navštívené stránky, čas strávený na jednotlivých stránkach, počet opakovaných pripojení k danej stránke, vyhľadávané výrazy, sledované hypertextové odkazy, označenia „Páči sa mi to“) odvodiť informácie o záujmoch a iných charakteristikách používateľa sociálnych médií. Rovnako subjekt vykonávajúci zacielenie môže byť schopný odvodiť údaje o konkrétnych osobách a využiť tieto znalosti pri zacielení na ne a zobrazovaní reklamy na ich stránke sociálnych médií.

##### Príklad 7:

Pani Deluccová často označuje, že sa jej páčia fotky diel impresionistického maliara Pataolita, ktoré na svojej stránke sociálnych médií uverejňuje umelecká galéria Beautifulart. Múzeum Z chce v rámci pripravovanej výstavy prilákať osoby, ktoré sa zaujímajú o impresionistické maľby. Múzeum Z využije tieto kritériá zacielenia, ktoré mu ponúkne poskytovateľ sociálnych médií: „záujem o impresionizmus“, pohlavie, vek a miesto pobytu. Pani Deluccovej sa v dôsledku toho na jej stránke sociálnych médií zobrazí cielená reklama múzea Z týkajúca sa pripravovanej výstavy tohto múzea.

##### Príklad 8:

Pán Leon na svojej stránke sociálnych médií uviedol, že sa zaujíma o šport. Stiahol si do mobilu aplikáciu, aby mohol sledovať aktuálne výsledky svojich obľúbených športových podujatí, nastavil si v prehliadači v laptope ako domovskú stránku [www.livesportsresults.com](http://www.livesportsresults.com) a na stolovom počítači v práci často vyhľadáva najnovšie športové výsledky na internete. Zároveň navštevuje aj mnohé webové sídla s online hazardnými hrami. Poskytovateľ sociálnych médií sleduje aktivitu pána Leona na internete cez jeho rôzne zariadenia, t. j. laptop, mobilný telefón a stolový počítač. Na základe tejto aktivity a všetkých informácií, ktoré mu pán Leon poskytol si poskytovateľ sociálnych médií odvodí, že bude mať záujem o internetové stávky. Okrem toho platforma sociálnych médií vytvorila kritériá zacielenia, ktoré umožňujú spoločnostiam zacieliť na ľudí so sklonsmi k impulzívnosti a s nižším príjmom. Internetová stávková spoločnosť [bestpaydayloans](http://bestpaydayloans.com) chce zacieliť na používateľov, ktorí majú záujem o stávky a je u nich pravdepodobné, že budú uzatvárať veľa stávok. Preto zvolí kritériá zacielenia ponúkané poskytovateľom sociálnych médií, aby zacielenila na skupinu, ktorej sa má reklama zobrazovať.

<sup>82</sup> Stanovisko 5/2019 týkajúce sa vzájomného pôsobenia medzi smernicou o súde a elektronických komunikáciách a všeobecným nariadením o ochrane údajov, najmä pokiaľ ide o príslušnosť, úlohy a právomoci orgánov pre ochranu osobných údajov, bod 41.

<sup>83</sup> Európsky výbor pre ochranu údajov, [usmernenia 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b\) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám](#), verzia 2.0, 8. októbra 2019, bod 1.

<sup>84</sup> Pozri aj usmernenia pracovnej skupiny na ochranu údajov zriadenej podľa článku 29 k právu na prenosnosť údajov, WP 242 rev. 01, 5. apríla 2017, s. 10.

#### 5.4.1 Úlohy

81. Pokiaľ ide o určenie úloh jednotlivých subjektov, EDPB konštatuje: v príklade 7 existuje spoločné prevádzkovateľstvo zo strany múzea Z a poskytovateľa sociálnych médií, ktoré sa týka spracúvania osobných údajov na účely cielenej reklamy, s ohľadom na získavanie týchto údajov prostredníctvom funkcie „Páči sa mi to“ na platforme sociálnych médií a analýzu, ktorú vykonáva poskytovateľ sociálnych médií, aby mohol subjekt vykonávajúci zacielenie ponúknuť kritériá zacielenia („záujem o impresionizmus“), zodpovedajúce účelu konečného zobrazenia reklamy.<sup>85</sup>
82. V príklade 8 existuje spoločná kontrola zo strany sídla bestpaydayloans a poskytovateľa sociálnych médií vo vzťahu k spoločne stanoveným spracovateľským operáciám, v tomto prípade ide o výber kritérií zacielenia a následné zobrazovanie reklamy, ako aj akékoľvek podávanie správ vo vzťahu k cielenej kampani.

#### 5.4.2 Právny základ

83. Súčasťou zacielenia na používateľov sociálnych médií na základe odvodených údajov na účely reklamy často býva profilovanie.<sup>86</sup> Pracovná skupina zriadená podľa článku 29 už skôr objasnila, že podľa všeobecného nariadenia o ochrane údajov je profilovanie automatizované spracúvanie osobných údajov s cieľom vyhodnotiť osobné aspekty, a predovšetkým zanalyzovať alebo predvídať aspekty týkajúce sa jednotlivcov, pričom dodala, že „[p]oužitie slova ‚vyhodnotenie‘ naznačuje, že profilovanie zahŕňa určitú formu posúdenia alebo úsudku o osobe.“<sup>87</sup> Profilovanie môže byť zákonné so zreteľom na právny základ v článku 6 ods. 1 všeobecného nariadenia o ochrane údajov, s viazanosťou na platnosť tohto právneho základu.
84. Na príklad 7 sa vzťahuje článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách, keďže na zobrazenie reklamy o maliarovi Pataolitovi na stránke pani Deluccovej je potrebná operácia čítania/zápisu, aby sa jej označenie „Páči sa mi to“ priradilo k informáciám, ktoré o nej poskytovateľ sociálnych médií mal už predtým. Na tieto operácie bude preto potrebný súhlas.
85. Pokiaľ ide o príklad 8, EDPB pripomína, že v prípade automatizovaného rozhodovania, ktoré má právne účinky alebo podobným spôsobom výrazne ovplyvňuje dotknutú osobu, prevádzkovatelia môžu podľa článku 22 všeobecného nariadenia o ochrane údajov využiť tieto výnimky:
- ) výslovný súhlas dotknutej osoby,
  - ) nevyhnutnosť automatizovaného rozhodnutia na uzavretie alebo plnenie zmluvy alebo
  - ) povolenie právom Únie alebo členského štátu, ktorému prevádzkovateľ podlieha.
86. Pracovná skupina zriadená podľa článku 29 už konštatovala, že „[v] mnohých typických prípadoch nebude mať rozhodnutie predstaviť cielenú reklamu založenú na profilovaní podobne významný účinok na jednotlivcov (...). Je však možné, že takéto rozhodnutie môže mať podobne významný účinok na jednotlivcov v závislosti od konkrétnych charakteristík prípadu vrátane:

---

<sup>85</sup> Pokiaľ ide o stránky sociálnych médií, podmienky spoločného prevádzkovateľstva môžu byť splnené aj vo vzťahu k štatistickým informáciám, ktoré poskytovateľ sociálnych médií poskytuje správcovi stránky: pozri rozhodnutie SDEÚ C-210/16, Wirtschaftsakademie.

<sup>86</sup> EDPB konštatuje, že k profilovaniu mohlo dôjsť aj v predchádzajúcich prípadoch.

<sup>87</sup> Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, WP 251 rev. 01, s. 7.

- ) dotieravosti procesu profilovania vrátane sledovania jednotlivcov naprieč rôznymi webovými sídlami, zariadeniami a službami,
- ) očakávaní a želaní dotknutých jednotlivcov,
- ) spôsobu, akým je reklama poskytovaná, alebo
- ) využitia znalostí o zraniteľnosti cieľových dotknutých osôb.<sup>88</sup>

87. Ak je pravdepodobné, že profilovanie vykonávané poskytovateľom sociálnych médií „podobne významne [ovplyvní]“ dotknutú osobu, vzťahuje sa naň článok 22. Prevádzkovateľ (alebo prípadne spoloční prevádzkovatelia) musí posúdiť, či zacielenie „podobne významne [ovplyvní]“ dotknutú osobu vykonať v každom prípade so zreteľom na osobitné skutočnosti zacielenia.
88. Za podobných okolností, ako sú opísané v príklade 8, môže zobrazovanie reklám na internetové stávkovanie patriť do rozsahu pôsobnosti článku 22 všeobecného nariadenia o ochrane údajov (zacielenie na finančne zraniteľné osoby, ktoré majú záujem o internetové stávky, ktoré môžu potenciálne významne a nepriaznivo ovplyvniť ich finančnú situáciu). Preto by v súlade s článkom 22 bolo potrebné získať výslovný súhlas. Okrem toho použitie sledovacích techník má za následok uplatnenie článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, z čoho vyplýva požiadavka predchádzajúceho súhlasu. A napokon EDPB pripomína, že spracúvanie je zákonné len vtedy, ak prevádzkovateľ posudzuje každú situáciu individuálne, a že získaním súhlasu sa neznižujú ostatné povinnosti dodržať požiadavky spravodlivosti, nevyhnutnosti, primeranosti a kvality údajov uvedené v článku 5 všeobecného nariadenia o ochrane údajov.

## 6 TRANSPARENTNOSŤ A PRÁVO NA PRÍSTUP

89. V článku 5 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov sa uvádza, že osobné údaje sa vo vzťahu k dotknutej osobe spracúvajú zákonným spôsobom, spravodlivo a transparentne. V článku 5 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov sa zároveň uvádza, že osobné údaje sa získavajú na konkrétne určené, výslovne uvedené a legitímne účely. Články 12, 13 a 14 všeobecného nariadenia o ochrane údajov obsahujú špecifické ustanovenia týkajúce sa povinností transparentnosti prevádzkovateľa. A napokon v odôvodnení 39 sa uvádza, že „[p]re fyzické osoby by malo byť transparentné, že sa získavajú, používajú, konzultujú alebo inak spracúvajú osobné údaje, ktoré sa ich týkajú, ako aj to, v akom rozsahu sa tieto osobné údaje spracúvajú alebo budú spracúvať“.<sup>89</sup>
90. Informácie predkladané dotknutým osobám v súvislosti so spôsobom, akým sa ich osobné údaje spracúvajú, by mali byť v každom prípade stručné, transparentné, zrozumiteľné a v ľahko dostupnej forme a mali by využívať jasný a zrozumiteľný jazyk.
91. EDPB pripomína, že samotné použitie slova „reklama“ nestačí na informovanie používateľov o tom, že je ich aktivita monitorovaná na účely cielenej reklamy. Osobám by sa malo transparentne oznámiť, aké typy spracovateľských činností sa vykonávajú a čo to pre dotknutú osobu znamená v praxi. Sociálna platforma alebo subjekt vykonávajúci zacielenie by mali ľahko zrozumiteľným jazykom informovať dotknuté osoby o tom, ak sa vytvorí profil na základe ich správania na internete na platforme alebo na webovom sídle subjektu vykonávajúceho zacielenie, pričom sa používateľom poskytnú informácie o typoch osobných údajov, ktoré sa získavajú na účely vytvorenia takéhoto profilu a ktoré v konečnom

<sup>88</sup> Usmernenia pracovnej skupiny zriadenej podľa článku 29 k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, WP 251 rev. 01, s. 22.

<sup>89</sup> Pozri usmernenia pracovnej skupiny zriadenej podľa článku 29 k transparentnosti podľa nariadenia 2016/679, WP 260 rev. 01, 11. apríla 2018, [https://ec.europa.eu/newsroom/Article29/item-detail.cfm?item\\_id=622227](https://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=622227).

dôsledku umožňujú subjektom vykonávajúcim zacielenie realizovať zacielenie a zobrazovať behaviorálnu reklamu.<sup>90</sup> Používateľom by sa mali relevantné informácie zobrazovať priamo na obrazovke, interaktívnou formou a v primeraných alebo potrebných prípadoch prostredníctvom viacvrstvových oznámení.<sup>91</sup>

## 6.1 Základné časti dohody a informácie, ktoré sa majú poskytnúť (článok 26 ods. 2 všeobecného nariadenia o ochrane údajov)

92. Podľa článku 26 ods. 1 všeobecného nariadenia o ochrane údajov spoloční prevádzkovatelia „[t]ransparentne určia svoje príslušné zodpovednosti za plnenie povinností podľa tohto nariadenia, najmä pokiaľ ide o vykonávanie práv dotknutej osoby, a svoje povinnosti poskytovať informácie uvedené v článkoch 13 a 14, a to formou vzájomnej dohody, pokiaľ nie sú príslušné zodpovednosti prevádzkovateľov určené právom Únie alebo právom členského štátu, ktorému prevádzkovatelia podliehajú. V dohode sa môže určiť kontaktné miesto pre dotknuté osoby“.
93. Zásada transparentnosti je ďalej vyjadrená aj povinnosťou vyplývajúcou z článku 26 ods. 2 všeobecného nariadenia o ochrane údajov poskytnúť základné časti dohody o spoločnom prevádzkovateľstve dotknutým osobám. V článku 26 všeobecného nariadenia o ochrane údajov sa vyžaduje, aby spoloční prevádzkovatelia prijali primerané opatrenia a zaistili, aby boli dotknuté osoby informované o rozdelení zodpovedností.
94. Informácie poskytované dotknutým osobám musia v zásade zahŕňať všetky aspekty spracovateľských operácií, za ktoré sú spoloční prevádzkovatelia spoločne zodpovední. Dotknuté osoby majú samozrejme nárok dostať všetky informácie (vrátane informácií o plánovanom následnom spracúvaní, ak je predmetom spoločného prevádzkovateľstva), aby mali k dispozícii spravodlivé a primerané informácie. V rámci spoločnej dohody je konkrétne potrebné zabezpečiť, aby dotknutá osoba mala k dispozícii informácie požadované podľa článkov 13 a 14 všeobecného nariadenia o ochrane údajov vrátane údajov o spoločných alebo úzko prepojených účeloch, dobe uchovávaní, poskytovaní tretím stranám atď., ktoré je potrebné dotknutej osobe oznámiť pri získavaní údajov alebo pred začiatkom ich spracúvania. V dohode je potrebné jasne stanoviť, kto v tomto ohľade nesie zodpovednosť. V záujme splnenia týchto požiadaviek musí takáto dohoda obsahovať (alebo odkazovať na) jasné a komplexné informácie týkajúce sa spracúvania, na ktoré sa vzťahuje, s prípadnými vysvetleniami jednotlivých fáz spracúvania a subjektov, ktoré ho vykonávajú.<sup>92</sup>
95. Hoci obaja spoloční prevádzkovatelia majú v prípade spoločnej zodpovednosti povinnosť informovať, môžu sa vzájomne dohodnúť, že jeden z nich bude mať za úlohu podávať úvodné informácie dotknutým osobám, najmä v prípadoch, ak s nimi pred spracúvaním komunikuje len jeden z prevádzkovateľov, napríklad prostredníctvom svojho webového sídla.<sup>93</sup> Výmena informácií, ktoré sa majú poskytnúť dotknutej osobe, by mala byť neoddeliteľnou súčasťou spoločnej dohody (napr. ako príloha). Ak jeden zo spoločných prevádzkovateľov nemá všetky podrobné informácie, pretože napríklad nepozná presnú technickú realizáciu spracovateľských činností, druhý spoločný prevádzkovateľ mu poskytne všetky potrebné informácie, aby mu umožnil poskytnúť dotknutej osobe úplné informácie podľa článkov 13 a 14 všeobecného nariadenia o ochrane údajov.

---

<sup>90</sup> Pozri usmernenia EDPB k transparentnosti podľa nariadenia 2016/679.

<sup>91</sup> Usmernenia pracovnej skupiny zriadenej podľa článku 29 k súhlasu podľa nariadenia 2016/679, WP 259 rev. 01, body 24 a 35.

<sup>92</sup> Stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“ [processor], WP 169, s. 28.

<sup>93</sup> SDEÚ, Fashion ID, body 102 a 105.

96. EDPB konštatuje, že prevádzkovatelia nenesú priamu zodpovednosť za poskytnutie informácií požadovaných podľa článkov 13 a 14 všeobecného nariadenia o ochrane údajov vo vzťahu k ďalším spracovateľským operáciám, ak tieto operácie nepatria do rozsahu spoločného prevádzkovateľstva. Preto subjekt vykonávajúci zacielenie priamo nezodpovedá za poskytovanie informácií týkajúcich sa akéhokoľvek ďalšieho spracúvania, ktoré vykonáva platforma sociálnych médií.<sup>94</sup>
97. EDPB však zdôrazňuje, že spoločný prevádzkovateľ, ktorý má v úmysle osobné údaje ďalej používať, má špecifické informačné povinnosti vo vzťahu k tomuto ďalšiemu spracúvaniu, ak sa naň nevzťahuje spoločná zodpovednosť, podľa článku 14 ods. 4 všeobecného nariadenia o ochrane údajov, ako aj povinnosti zachovať zlučiteľnosť ďalšieho spracúvania podľa článku 6 ods. 4. Subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií sa napríklad môžu dohodnúť, že subjekt vykonávajúci zacielenie poskytne určité informácie v mene poskytovateľa sociálnych médií. Poskytovateľ sociálnych médií však naďalej nesie konečnú zodpovednosť za to, aby dotknutá osoba dostala relevantné informácie týkajúce sa všetkých spracovateľských činností, ktoré má poskytovateľ pod kontrolou.

V príklade 3 (pán Lopez, ktorému sa na stránke sociálnych médií zobrazuje zacielená reklama na banku X po tom, ako táto banka nahrala jeho e-mailovú adresu poskytovateľovi sociálnych médií) musí banka pána Lopeza informovať, že jeho e-mailová adresa sa prostredníctvom poskytovateľa sociálnych médií použije na propagáciu ponúk súvisiacich s bankovými službami. Každé ďalšie spracúvanie zo strany poskytovateľa sociálnych médií musí byť zákonné a zlučiteľné s účelmi, na ktoré banka údaje získala.

Okrem toho, ak má poskytovateľ sociálnych médií v úmysle e-mail pána Lopeza ďalej spracúvať na iný účel, musí predtým zabezpečiť, aby pán Lopez dostal informácie požadované podľa článku 14 ods. 4 všeobecného nariadenia o ochrane údajov.

Poskytovateľ sociálnych médií a banka sa môžu dohodnúť, že banka poskytne pánovi Lopezovi relevantné informácie v mene poskytovateľa sociálnych médií. Aj v takom prípade však poskytovateľ sociálnych médií naďalej nesie konečnú zodpovednosť za to, aby dotknutá osoba dostala relevantné informácie týkajúce sa všetkých spracovateľských činností, za ktoré zodpovedá (samotný) poskytovateľ. Táto povinnosť neplatí vtedy, ak pána Lopeza o tomto spracúvaní už informovala banka, podľa článku 14 ods. 5 písm. a) všeobecného nariadenia o ochrane údajov.

Tieto povinnosti transparentnosti nie sú v relevantných prípadoch dotknuté osobitnými povinnosťami, ktoré sa vzťahujú na právny základ.

98. Každý spoločný prevádzkovateľ zodpovedá za sprístupnenie základných častí dohody dotknutej osobe. V praxi by základné časti dohody mali byť dostupné priamo na platforme, mal by na ne byť odkaz v zásadách ochrany osobných údajov platformy a mali by byť priamo dostupné prostredníctvom odkazu, napríklad na stránke subjektu vykonávajúceho zacielenie na platforme sociálnych médií alebo cez odkazy typu „prečo sa mi zobrazuje táto reklama?“.

<sup>94</sup> Ako sa objasňuje v usmerneniach EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov, každý prevádzkovateľ má zodpovednosť zabezpečiť, aby sa údaje ďalej nespracúvali spôsobom, ktorý nie je kompatibilný s účelmi, na ktoré ich prevádzkovateľ vykonávajúci výmenu údajov pôvodne získal. Osvedčeným postupom by malo byť to, že prevádzkovateľ, ktorý má v úmysle spracúvať osobné údaje na ďalšie účely, poskytne druhému prevádzkovateľovi, ktorý poskytuje osobné údaje, dostatočné prostriedky, aby mohol zistiť, či je toto spracúvanie založené na právnom základe, ktorým je pravdepodobne súhlas, a či boli dotknuté osoby náležite informované. Subjekt vykonávajúci zacielenie by tak získal istotu, že prenos údajov poskytovateľovi sociálnych médií je zákonný.

## 6.2 Právo na prístup (článok 15)

99. Prevádzkovatelia musia používateľom umožniť jednoduchým spôsobom a v plnom rozsahu uplatniť ich práva dotknutých osôb. Dotknutá osoba by mala mať k dispozícii ľahko použiteľný a účinný nástroj, ktorý by jej umožňoval kedykoľvek bez problémov uplatniť všetky jej práva, najmä právo na vymazanie, právo namietat' a právo na prístup podľa článku 15 všeobecného nariadenia o ochrane údajov.<sup>95</sup> Nasledujúce body sú zamerané na to, kto a akým spôsobom by mal zohľadňovať právo na prístup v súvislosti so zacielením na používateľov sociálnych médií.<sup>96</sup>
100. Vo všeobecnosti na účely splnenia požiadaviek článku 15 ods. 1 všeobecného nariadenia o ochrane údajov a zaistenia úplnej transparentnosti by prevádzkovatelia mohli chcieť zväziť zavedenie mechanizmu, prostredníctvom ktorého si dotknuté osoby môžu pozrieť svoj profil vrátane podrobností o informáciách a zdrojoch použitých na ich vypracovanie. Dotknutá osoba by mala mať možnosť zistiť identitu subjektu vykonávajúceho zacielenie a prevádzkovatelia by jej mali umožniť prístup k informáciám o zacielení vrátane použitých kritérií zacielenia a iných informácií požadovaných podľa článku 15 všeobecného nariadenia o ochrane údajov.<sup>97</sup>
101. Pokiaľ ide o druh prístupu, ktorý sa má dotknutým osobám poskytnúť, v odôvodnení 63 sa uvádza, že „[a]k je to možné, prevádzkovateľ by mal môcť poskytnúť prístup na diaľku k bezpečnému systému, ktorý by dotknutej osobe zabezpečil priamy prístup k jej osobným údajom.“ Osobitné charakteristiky poskytovateľov sociálnych médií, ako je online prostredie či existencia používateľského konta, poskytujú možnosť jednoducho udeliť dotknutej osobe prístup na diaľku k osobným údajom, ktoré sa ich týkajú, v súlade s článkom 15 ods. 1 a 2 všeobecného nariadenia o ochrane údajov. Prístup na diaľku možno v tomto prípade považovať za „najprimeranejšie opatrenie“ v zmysle článku 12 ods. 1 všeobecného nariadenia o ochrane údajov, aj vzhľadom na to, že ide o typickú situáciu, v ktorej „veľký počet účastníkov a technologická zložitosť činnosti sťažujú dotknutej osobe zistiť a pochopiť, či osobné údaje, ktoré sa jej týkajú, boli získané, kým a na aké účely“ (pozri odôvodnenie 58, v ktorom sa „online reklama“ výslovne uvádza ako konkrétny príklad). Okrem toho by sa zacieleným používateľom sociálnych médií na základe ich žiadosti mala poskytnúť kópia osobných údajov, ktoré sa ich týkajú, v súlade s článkom 15 ods. 3 všeobecného nariadenia o ochrane údajov.
102. Podľa článku 15 ods. 1 písm. c) všeobecného nariadenia o ochrane údajov by používateľ mal mať prístup najmä k týmto informáciám: „príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie“. Podľa článku 4 bodu 9 je „príjemca“ fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Subjekt vykonávajúci zacielenie nemusí nevyhnutne byť „príjemcom“ osobných údajov (pozri príklad 1), keďže mu nemusia byť poskytnuté osobné údaje, ale štatistiky o zacielených zákazníkoch v agregovanej alebo

<sup>95</sup> Článok 15 ods. 1 a 2 všeobecného nariadenia o ochrane údajov obsahuje podrobný prehľad informácií, ktoré sa majú poskytnúť dotknutej osobe, ktorá požiada o prístup k svojim údajom. Článok 15 ods. 3 a 4 všeobecného nariadenia o ochrane údajov upravuje právo získať kópiu.

<sup>96</sup> Pozri usmernenia EDPB k transparentnosti podľa nariadenia 2016/679, s. 35.

<sup>97</sup> Podrobnosti o informáciách poskytovaných podľa článku 15 všeobecného nariadenia o ochrane údajov v súvislosti s profilovaním sa nachádzajú v usmerneniach pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29, WP 251 rev. 01, s. 17 („Článok 15 dáva dotknutej osobe právo získať podrobnosti o všetkých osobných údajoch použitých na profilovanie vrátane kategórií údajov použitých na vytvorenie profilu. Okrem všeobecných informácií o spracúvaní podľa článku 15 ods. 3 je prevádzkovateľ povinný sprístupniť údaje použité ako vstup na vytvorenie profilu, ako aj informácie o profile a podrobnosti o tom, do ktorých segmentov bola dotknutá osoba umiestnená“). Je dôležité, aby takéto informácie boli prispôsobené konkrétnej situácii dotknutej osoby a aby dopĺňali informácie poskytnuté na základe článkov 1 a 14.

anonymizovanej podobe, napr. ako súčasť jeho kampane alebo v rámci preskúmania výkonnosti takejto kampane. V každom prípade, pokiaľ subjekt vykonávajúci zacielenie koná ako spoločný prevádzkovateľ, musí sa takto predstaviť aj používateľovi sociálnych médií.

103. Hoci článok 15 všeobecného nariadenia o ochrane údajov nie je výslovne identifikovaný v článku 26 ods. 1 tohto nariadenia, odkazuje sa v ňom na všetky „zodpovednosti za plnenie povinností“ v rámci všeobecného nariadenia o ochrane údajov, čo zahŕňa aj článok 15 tohto nariadenia.
104. Aby mohli dotknuté osoby uplatňovať svoje práva účinným a ľahko dostupným spôsobom, v rámci dohody medzi poskytovateľom sociálnych médií a subjektom vykonávajúcim zacielenie sa môže pre dotknuté osoby určiť jednotné kontaktné miesto. Spoloční prevádzkovatelia sa môžu v podstate slobodne dohodnúť medzi sebou, kto by mal byť zodpovedný za odpovede na žiadosti dotknutých osôb a za ich plnenie, nemôžu však dotknutej osobe uprieť možnosť uplatniť svoje práva voči každému z nich (článok 26 ods. 3 všeobecného nariadenia o ochrane údajov). Preto musia subjekty vykonávajúce zacielenie a poskytovatelia sociálnych médií zabezpečiť zavedenie vhodného mechanizmu, vďaka ktorému by dotknutá osoba mala čo najjednoduchší prístup k svojim osobným údajom (vrátane použitých kritérií zacielenia) a všetkým informáciám stanoveným v článku 15 všeobecného nariadenia o ochrane údajov.

## 7 POSÚDENIA VPLYVU NA OCHRANU ÚDAJOV

105. Pred začiatkom plánovaných operácií zacielenia by v zásade obaja spoloční prevádzkovatelia mali skontrolovať zoznam spracovateľských operácií, ktoré „pravdepodobne povedú k vysokému riziku“, ktorý bol prijatý na vnútroštátnej úrovni podľa článku 35 ods. 4 a odôvodnení 71, 75 a 91 všeobecného nariadenia o ochrane údajov, aby určili, či zvolené zacielenie nezodpovedá niektorému typu spracovateľských operácií, na ktoré sa vzťahuje požiadavka vykonať posúdenie vplyvu na ochranu údajov. Pri posudzovaní, či plánované operácie zacielenia „pravdepodobne povedú k vysokému riziku“ a či je potrebné vykonať posúdenie vplyvu na ochranu údajov, by sa mali zohľadniť aj kritériá identifikované v usmerneniach týkajúcich sa posúdenia vplyvu na ochranu údajov<sup>98</sup>, ako aj zoznamy druhov spracovateľských operácií, ktoré podliehajú požiadavke na posúdenie vplyvu na ochranu údajov, vypracované dozornými orgánmi (podľa článku 35 ods. 4).
106. V niektorých prípadoch môže povaha inzerovaného výrobku alebo služby, obsah správy alebo spôsob zobrazovania reklamy mať na jednotlivcov vplyv, ktorý je potrebné bližšie posúdiť. Môže sa to stať napríklad pri výrobkoch zameraných na zraniteľné osoby. Dodatočné riziká môžu vzniknúť v závislosti od účelov reklamnej kampane a jej miery narušenia, alebo ak je súčasťou zacielenia aj spracúvanie získaných alebo odvodených osobných údajov.
107. Okrem povinností výslovne uvedených v článku 26 ods. 1 všeobecného nariadenia o ochrane údajov by mali spoloční prevádzkovatelia pri určovaní svojich povinností zvážiť aj iné povinnosti. Ako sa uvádza v usmerneniach EDPB týkajúcich sa posúdenia vplyvu na ochranu údajov, „[k]eď spracovateľská operácia zahŕňa spoločných prevádzkovateľov, musia si presne vymedziť svoje povinnosti“.
108. V dôsledku toho musia obaja spoloční prevádzkovatelia posúdiť, či je posúdenie vplyvu na ochranu údajov potrebné. Ak je toto posúdenie potrebné, obaja nesú zodpovednosť za splnenie tejto povinnosti. EDPB pripomína, že posúdenie vplyvu na ochranu údajov by sa malo vzťahovať na celé spracúvanie osobných údajov, takže sa na jeho realizácii v zásade musia podieľať obaja spoloční prevádzkovatelia. V tejto súvislosti musia obaja prevádzkovatelia zaistiť, aby mali dostatočnú úroveň

---

<sup>98</sup> Pozri usmernenia EDPB týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenia toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“, wp248rev.0.

informácií o spracúvaní, aby mohli príslušné posúdenie vplyvu na ochranu údajov vykonať.<sup>99</sup> Z toho vyplýva, že „[k]aždý prevádzkovateľ by mal vyjadriť svoje potreby a vymeniť si užitočné informácie bez toho, aby vyzradil tajomstvá (napr. ochranu obchodných tajomstiev, duševné vlastníctvo, dôverné obchodné informácie) alebo zverejnil zraniteľné miesta“.<sup>100</sup>

109. V praxi je možné, aby sa spoloční prevádzkovatelia rozhodli, že jeden z nich bude mať za úlohu vykonať posúdenia vplyvu na ochranu údajov ako také. Malo by sa to uviesť aj v spoločnej dohode bez toho, aby bola dotknutá existencia spoločnej zodpovednosti ako takej. Samozrejme, môže sa stať, že jeden z prevádzkovateľov sa nachádza v lepšej pozícii na posúdenie určitých spracovateľských operácií. Tento prevádzkovateľ môže napríklad v závislosti od kontextu mať vyššiu úroveň kontroly a znalosti procesu zacielenia, najmä pokiaľ ide o koncovú fázu použitého systému, alebo prostriedkov spracúvania.
110. Súčasťou každého posúdenia vplyvu na ochranu údajov musia byť opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu so všeobecným nariadením o ochrane údajov s ohľadom na práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka. Ak identifikované riziká nemožno dostatočne riešiť (t. j. zvyškové riziká sú naďalej vysoké), spoloční prevádzkovatelia majú obaja povinnosť zabezpečiť predchádzajúcu konzultáciu s príslušnými dozornými orgánmi. Ak by zacielenie porušovalo všeobecné nariadenie o ochrane údajov, najmä z dôvodu nedostatočnej identifikácie alebo zmiernenia rizík, nemalo by sa vykonať.

Príklad 9:

Politická strana Letschangetheworld chce vyzvať používateľov sociálnych médií, aby v nadchádzajúcich voľbách hlasovali za konkrétneho politického kandidáta. Chcú sa zamerať na starších ľudí z vidieckych oblastí krajiny, ktorí pravidelne chodia do kostola a za posledné dva roky nevycestovali nikam do zahraničia.

111. Zo strany platformy sociálnych médií a politickej strany existuje spoločné prevádzkovateľstvo na účely priradenia profilu a zobrazenia cielenej reklamy. Oba subjekty, politická strana Letschangetheworld aj platforma sociálnych médií musia posúdiť, či je potrebné vykonať posúdenie vplyvu na ochranu údajov. V tomto prípade majú obaja dostatočnú znalosť kritérií používaných na zacielenie na osoby na to, aby videli, že spracúvanie údajov môže viesť k vysokému riziku.
112. Ak je potrebné posúdenie vplyvu na ochranu údajov, v spoločnej dohode by sa malo uviesť, ako ho prevádzkovatelia vykonajú a ako sa zabezpečí relevantná výmena vedomostí. V tomto príklade môže platiť, že platforma sociálnych médií má lepšiu pozíciu na to, aby posúdila určité spracovateľské operácie, keďže politická strana len vyberá všeobecné kritériá zacielenia.

## 8 OSOBITNÉ KATEGÓRIE ÚDAJOV

### 8.1 Čo tvorí osobitnú kategóriu údajov

<sup>99</sup> EDPB zdôrazňuje, že posúdenie vplyvu na ochranu údajov nie je potrebné, ak sú povaha, rozsah, kontext a účely spracúvania veľmi podobné spracúvaniu, pre ktoré sa už posúdenie vplyvu na ochranu údajov vykonalo. V takých prípadoch možno použiť výsledky posúdenia vplyvu na ochranu údajov pre podobné spracúvania, pozri usmernenia pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenia toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“, WP 248 rev. 01, s. 12.

<sup>100</sup> Tamže, s. 8.



113. Všeobecným nariadením o ochrane údajov sa poskytuje osobitná ochrana pre osobné údaje, ktoré sú mimoriadne citlivé vo vzťahu k základným právam a slobodám. Takéto údaje sú vymedzené v článku 9 všeobecného nariadenia o ochrane údajov ako osobitné kategórie osobných údajov a zahŕňajú údaje o zdraví, rasovom a etnickom pôvode, biometrii, náboženskom alebo filozofickom presvedčení, politickom názore, členstve v odborových organizáciách, sexuálnom živote alebo sexuálnej orientácii.
114. Prevádzkovatelia môžu osobitné kategórie údajov spracúvať len vtedy, ak sú schopní splniť jednu z podmienok stanovených v článku 9 ods. 2 všeobecného nariadenia o ochrane údajov, napríklad získať výslovný súhlas dotknutej osoby alebo dané údaje dotknutá osoba preukázateľne zverejnila. Okrem podmienok v článku 9 všeobecného nariadenia o ochrane údajov sa spracúvanie osobitných kategórií údajov musí opierať o právny základ stanovený v článku 6 tohto nariadenia a musí sa vykonávať v súlade so základnými princípmi stanovenými v článku 5 tohto nariadenia.
115. Spracúvanie osobitných kategórií osobných údajov je ďalej relevantné vtedy, keď sa posudzujú primerané opatrenia podľa článkov 24, 25, 28 a 32 všeobecného nariadenia o ochrane údajov, ale aj na určenie toho, či je potrebné vykonať posúdenie vplyvu na ochranu údajov podľa článku 35 všeobecného nariadenia o ochrane údajov a či je potrebné vymenovať zodpovednú osobu podľa článku 37 tohto nariadenia.
116. V súvislosti so sociálnymi médiami a zacielením je potrebné určiť, či spracúvanie osobných údajov zahŕňa „osobitné kategórie údajov“ a či takéto údaje spracúva poskytovateľ sociálnych médií, subjekt vykonávajúci zacielenie alebo obaja. Ak sa spracúvajú osobitné kategórie osobných údajov, je potrebné určiť, či a za akých podmienok môžu poskytovateľ sociálnych médií a subjekt vykonávajúci zacielenie tieto údaje zákonne spracúvať.
117. Ak poskytovateľ sociálnych médií spracúva osobitnú kategóriu údajov na účely zacielenia, musí pre toto spracúvanie nájsť právny základ v článku 6 všeobecného nariadenia o ochrane údajov a odvolať sa na výnimku v článku 9 ods. 2 tohto nariadenia, ako je napríklad výslovný súhlas podľa článku 9 ods. 2 písm. a) tohto nariadenia. Ak subjekt vykonávajúci zacielenie zapojí poskytovateľa sociálnych médií a požaduje od neho, aby pri zacielení na používateľov použil osobitnú kategóriu údajov, subjekt vykonávajúci zacielenie bude za spracúvanie tejto osobitnej kategórie údajov zodpovedný spoločne s poskytovateľom sociálnych médií.
118. Nasledujúca právna analýza je venovaná rôznym situáciám, v ktorých môže dôjsť k takémuto spracúvaniu, a ich právnym dôsledkom.

#### 8.1.1 Zjavné osobitné kategórie údajov

119. Na niektoré spracúvané osobné údaje sa jasne vzťahuje vymedzenie osobitných kategórií údajov, napr. v prípade priameho vyhlásenia o tom, že je niekto členom určitej politickej strany alebo náboženského združenia.

##### Príklad 10:

Pani Flora na svojom profile na sociálnych médiách jasne uvádza, že je členkou politickej strany GreenestPlanet. Environmentálna organizácia Long live the Earth chce zacieliť na používateľov sociálnych médií, ktorí sú členmi politickej strany GreenestPlanet, aby im mohla posilať ciele správy.

120. V príklade 10 poskytovateľ sociálnych médií a environmentálna organizácia vystupujú ako spoloční prevádzkovatelia.<sup>101</sup> Keď environmentálna organizácia požaduje od poskytovateľa sociálnych médií zacielenie na používateľov na základe ich politického názoru, obaja prevádzkovatelia sa podieľajú na spracúvaní osobitných kategórií údajov vymedzených v článku 9 všeobecného nariadenia o ochrane údajov. Spracúvanie týchto údajov je podľa článku 9 ods. 1 v zásade zakázané. Poskytovateľ sociálnych médií aj environmentálna organizácia preto musia byť schopní odvolať sa na niektorú z výnimiek spracúvania podľa článku 9 ods. 2. Okrem toho musia obaja zabezpečiť právny základ podľa článku 6. S ohľadom na výnimky uvedené v článku 9 ods. 2 sa zdá, že jedinými uplatniteľnými výnimkami v tejto situácii by bolo získať výslovný súhlas dotknutých osôb podľa článku 9 ods. 2 písm. a) všeobecného nariadenia o ochrane údajov alebo vychádzať z toho, že pani Flora tieto osobné údaje preukázateľne zverejnila podľa článku 9 ods. 2 písm. e) tohto nariadenia.

### 8.1.2 Údaje osobitných kategórií získané odvodením alebo kombináciou údajov

121. Predpoklady alebo odvodenia v súvislosti s osobitnou kategóriou údajov, napríklad pravdepodobnosť, že osoba bude voliť určitú stranu po tom, ako navštívila stránku hlásajúcu liberálne názory, takisto predstavujú osobitnú kategóriu osobných údajov. Podobne, ako už uviedol EDPB, „[p]rofilovanie môže vytvoriť údaje osobitných kategórií vyvodením z údajov, ktoré samé osebe nie sú údajmi osobitnej kategórie, ale stanú sa takými v kombinácii s inými údajmi. Napríklad zdravotný stav niekoho je možné vyvodiť zo záznamu jeho nákupu potravín v kombinácii s údajmi o kvalite a energetickom obsahu potravín“.<sup>102</sup>
122. Napríklad spracúvanie samotného konštatovania alebo jedného lokalizačného údaju svedčiaco o tom, že používateľ (raz alebo niekoľkokrát) navštívil miesto, na ktoré zvyčajne chodia ľudia s určitým náboženským presvedčením, sa vo všeobecnosti a samo o sebe nebude považovať za spracúvanie osobitnej kategórie údajov. O spracúvaní osobitných kategórií údajov však možno hovoriť v prípade, že sa tieto údaje skombinujú s inými údajmi, alebo s ohľadom na súvislosti, v ktorých sa tieto údaje spracúvajú, či na účely, na ktoré sa používajú.

#### Príklad 11:

Pán Novák má v profile svojho konta na sociálnych médiách uvedené len všeobecné informácie ako meno a bydlisko, ale z jeho aktualizácie statusu vyplýva, že často chodí na omše do mestského kostola. O niečo neskôr chce mestský kostol zacieliť náboženské odkazy na svojich návštevníkov, a motivovať tak kresťanov, aby sa zúčastňovali na zhromaždeniach. Použitie osobných údajov z aktualizácie statusu pána Nováka na účely zacielenia za týchto okolností predstavuje spracúvanie osobitných kategórií osobných údajov.

123. Ak poskytovateľ sociálnych médií alebo subjekt vykonávajúci zacielenie používa pozorované údaje na kategorizáciu používateľov v súvislosti s určitým náboženským, filozofickým alebo politickým presvedčením, túto kategorizáciu treba zjavne považovať za spracúvanie osobitnej kategórie osobných údajov – bez ohľadu na to, či je správna/pravdivá alebo nie. Pokiaľ kategorizácia umožňuje zacielenie na základe osobitnej kategórie údajov, nezáleží na tom, ako je označená.

#### Príklad 12:

Pán Sifuentes vo svojom profile na sociálnych médiách poskytuje informácie v podobe pravidelných aktualizácií statusu, nahlásení sa atď. Vyplýva z nich, že sa pravidelne zúčastňuje na aktivitách, ktoré organizuje Hnutie pre myseľ, telo a ducha. Hoci pán Sifuentes neuvádza žiadne výslovné vyhlásenie

<sup>101</sup> Pozri analýzu v kapitole 5.2.1.

<sup>102</sup> Usmernenia pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, WP 251 rev. 01, s. 15.

o svojom filozofickom presvedčení, z kombinácie všetkých jeho aktualizácií, označení „Páči sa mi to“, nahlásení a podobných údajov určité filozofické presvedčenie výrazne vyplýva.

Príklad 13:

Poskytovateľ sociálnych médií využíva informácie, ktoré pani Allgrovová aktívne poskytuje na svojej profilovej stránke na sociálnych médiách o svojom veku, záľubách a adrese, a kombinuje ich s pozorovanými údajmi o webových sídlach, ktoré navštívila, a veciach, ktoré označila, že sa jej páčia na platforme sociálnych médií. Poskytovateľ sociálnych médií na základe týchto údajov vyvodí, že pani Allgrovová podporuje ľavicovú liberálnu politiku a zaradí ju do kategórie zacielenia „zaujíma sa o ľavicovú liberálnu politiku“, pričom túto kategóriu sprístupní subjektom vykonávajúcim zacielenie na účely cielennej reklamy.

124. V príklade 12 z množstva dostupných informácií a absencie opatrení na prevenciu zacielenia na základe údajov osobitných kategórií vyplýva, že tu dochádza k spracúvaniu osobitných kategórií údajov. Samotná skutočnosť, že poskytovateľ sociálnych médií spracúva množstvo údajov, ktoré potenciálne možno použiť na odvodenie osobitných kategórií údajov, však automaticky neznamená, že sa na toto spracúvanie vzťahuje článok 9 všeobecného nariadenia o ochrane údajov. Článok 9 sa uplatňuje len vtedy, keď spracúvanie údajov zo strany poskytovateľa sociálnych médií vedie k odvodeniu osobitných kategórií údajov a poskytovateľ sociálnych médií neprijal opatrenia, aby zabránil odvodeniu takýchto údajov alebo ich použitiu na účely zacielenia. V každom prípade, zo spracúvania veľkého množstva osobných údajov o používateľovi môžu vyplývať osobitné riziká pre práva a slobody fyzických osôb, ktoré je potrebné riešiť zavedením primeraných bezpečnostných opatrení, ako sa stanovuje v článku 32 všeobecného nariadenia o ochrane údajov, ako aj zohľadnením výsledkov posúdenia vplyvu na ochranu údajov, ktoré je potrebné vykonať podľa článku 35 tohto nariadenia.
125. V príklade 13 ponuka a použitie kategórie zacielenia „zaujíma sa o ľavicovú liberálnu politiku“ predstavuje spracúvanie osobitných kategórií údajov, keďže táto kategória by sa ľahko dala použiť ako zástupná na zacielenie na osoby s ľavicovým liberálnym politickým presvedčením. Ak poskytovateľ sociálnych médií priradí používateľovi odvodený politický názor, predstavuje to spracúvanie osobitnej kategórie údajov. Na účely článku 9 všeobecného nariadenia o ochrane údajov nie je podstatné, či používateľ skutočne podporuje ľavicovú liberálnu politiku. Takisto nie je podstatné, že v označení kategórie zacielenia sa uvádza „zaujíma sa o...“ a nie „podporuje...“, keďže používateľ je na základe odvodených politických záujmov zaradený do kategórie zacielenia.

Príklad 14:

Pán Svenson si urobí test profesijných predpokladov, ktorý zahŕňa psychologické hodnotenie a ktorý vyvinula spoločnosť YourPerfectJob. Tento test je dostupný na platforme sociálnych médií a využíva aplikačné programovacie rozhranie (API) poskytovateľa sociálnych médií. Spoločnosť YourPerfectJob získa jeho údaje o vzdelaní, stavu zamestnanosti, veku, záľubách, príspevkoch, e-mailovej adrese a prepojeniach. Spoločnosť YourPerfectJob tieto údaje získa cez API v súlade s „povoleniami“, ktoré pán Svenson udelil prostredníctvom svojho konta na sociálnych médiách. Uvedeným účelom aplikácie je predpovedať optimálnu kariérnu dráhu pre konkrétneho používateľa.

Spoločnosť YourPerfectJob tieto údaje bez vedomia alebo schválenia poskytovateľa sociálnych médií používa na odvodenie množstva osobných aspektov vrátane osobnostných charakteristík, psychologického profilu a politických presvedčení. Spoločnosť YourPerfectJob sa neskôr rozhodne využiť tieto informácie na zacielenie na pána Svensona v mene politickej strany, pričom použije funkciu

zacielenia poskytovateľa sociálnych médií s využitím e-mailu bez toho, aby pridala akékoľvek ďalšie kritériá ponúkané poskytovateľom sociálnych médií.

V príklade 14 spracúva osobitné kategórie osobných údajov subjekt vykonávajúci zacielenie, nie však poskytovateľ sociálnych médií. Posúdenie a identifikácia politického presvedčenia pána Svensona v skutočnosti prebieha bez účasti poskytovateľa sociálnych médií.<sup>103</sup> Okrem uplatnenia všeobecného zákazu podľa článku 9 všeobecného nariadenia o ochrane údajov predstavuje zacielenie uvedené v príklade 14 porušenie požiadaviek spravodlivosti, transparentnosti a obmedzenia účelu. Pán Svenson v skutočnosti nie je náležite informovaný o skutočnosti, že osobné údaje, ktoré sa na neho vzťahujú, budú spracúvané na účely politického zacielenia, ktoré navyše zdanlivo nie je zlučiteľné s testom profesionálnych predpokladov.

126. Hoci spracovateľské činnosti poskytovateľa sociálnych médií v príklade 14 nezodpovedajú spracúvaniu osobitných kategórií údajov v zmysle článku 9 všeobecného nariadenia o ochrane údajov, poskytovateľ sociálnych médií je zodpovedný za to, aby do tohto spracúvania začlenil potrebné záruky, na účely splnenia požiadaviek všeobecného nariadenia o ochrane údajov a ochrany údajov dotknutých osôb v súlade s článkami 24 a 25 všeobecného nariadenia o ochrane údajov.

## 8.2 Výnimky z osobitných kategórií údajov, ktoré boli preukázateľne zverejnené podľa článku 9 ods. 2

127. Podľa článku 9 ods. 2 písm. e) všeobecného nariadenia o ochrane údajov sa povoľuje spracúvanie osobitnej kategórie údajov v prípade, ak tieto údaje dotknutá osoba preukázateľne zverejnila. Výraz „preukázateľne“ znamená, že na túto výnimku sa možno odvolať, len ak je splnená vysoko stanovená hranica. EDPB pripomína, že prítomnosť len jedného prvku nemusí vždy byť dostatočným argumentom na stanovenie toho, že dotknutá osoba údaje „preukázateľne“ zverejnila. Ak chcú prevádzkovatelia doložiť, že dotknutá osoba jasne preukázala úmysel údaje zverejniť, v praxi môže byť potrebné zvážiť kombináciu týchto alebo iných prvkov, a je potrebné posúdiť každý prípad jednotlivo. Pri tomto posudzovaní môže byť relevantné zohľadniť nasledujúce aspekty:

- i) predvolené nastavenia platformy sociálnych médií (t. j. či dotknutá osoba vykonala konkrétny krok, aby zmenila tieto predvolené nastavenia súkromia na verejné); alebo
- ii) povahu platformy sociálnych médií – t. j. či je táto platforma neoddeliteľne spojená s myšlienkou nadväzovania kontaktov s blízkymi známymi dotknutej osoby alebo intímnych vzťahov (napríklad online platformy na zoznamovanie) alebo je jej účelom nadväzovanie širších medziľudských vzťahov, napr. pracovných vzťahov, mikrobloggerovanie, spoločné využívanie médií, či ide o sociálne platformy na výmenu online recenzií atď.; alebo

<sup>103</sup> V príklade 14 nedochádza v momente získavania osobných údajov k spoločnému prevádzkovateľstvu medzi poskytovateľom sociálnych médií a spoločnosťou YourPerfectJob, keďže v tejto fáze spracúvania spoločne neurčili účely získavania osobných údajov a ich následného alebo ďalšieho spracúvania na účely spoločnosti YourPerfectJob. EDPB by rád pripomenul, že analýzu úloh a zodpovedností treba vykonávať pre každý prípad jednotlivo a že záver pre tento konkrétny prípad sa nevzťahuje na žiadnu ďalšiu prácu, ktorú môže EDPB vykonávať v súvislosti s API. Samozrejme, situácia by bola iná, ak by sa poskytovateľ sociálnych médií okrem sprístupnenia osobných údajov podieľal aj na určení účelu, ktorý chce spoločnosť YourPerfectJob dosiahnuť. V každom prípade stále existuje spoločné prevádzkovateľstvo medzi subjektom vykonávajúcim zacielenie a poskytovateľom sociálnych médií v súvislosti s použitím zacielenia na základe zoznamu.

iii) dostupnosť stránky, na ktorej sú uverejnené citlivé údaje (t. j. či sú tieto informácie verejne dostupné alebo je potrebné si na prístup k nim napríklad najprv vytvoriť konto); alebo

iv) viditeľnosť informácií, ktoré dotknutú osobu upozorňujú na verejnú povahu informácií, ktoré uverejnia (t. j. či je napríklad na stránke neustále zverejnený banner alebo či tlačidlo na zverejnenie obsahuje informáciu, že údaje budú sprístupnené širokej verejnosti...); alebo

v) či dotknutá osoba zverejnila citlivé údaje sama alebo či boli zverejnené treťou stranou (napr. fotografie zverejnené priateľom, ktoré odhaľujú citlivé informácie), alebo či boli odvodené.

128. EDPB pripomína, že prítomnosť len jedného prvku nemusí vždy byť dostatočným argumentom na stanovenie toho, že dotknutá osoba údaje „preukázateľne“ zverejnila. Ak chcú prevádzkovatelia doložiť, že dotknutá osoba jasne preukázala úmysel údaje zverejniť, v praxi môže byť potrebné zvážiť kombináciu týchto alebo iných prvkov.

#### Príklad 15:

Pán Jansen si vytvoril konto na mikrobloggerovej platforme sociálnych médií. Pri vyplňaní informácií v profile uviedol, že je homosexuál. Keďže je konzervatívny, rozhodol sa pridať do konzervatívnych skupín, s vedomím, že pri prihlasovaní bol upozornený na to, že správy, ktoré na platforme napíše, sú verejné. Konzervatívna strana chce využiť nástroje zacielenia, ktoré ponúkajú sociálne médiá, na zacielenie na ľudí s rovnakou politickou príslušnosťou a sexuálnou orientáciou, ako pán Jansen.

129. Keďže sexuálna orientácia členov je štandardne „súkromná“ a pán Jansen nepodnikol žiadne kroky, aby ju zverejnil, nemožno túto informáciu považovať za preukázateľne zverejnenú. Okrem toho neboli preukázateľne zverejnené ani údaje o jeho politickej príslušnosti, a to napriek i) povahe mikrobloggerovej platformy sociálnych médií, ktorá slúži na výmenu informácií so širokou verejnosťou, a ii) skutočnosti, že bol informovaný o verejnom charaktere správ, ktoré zverejní na fórach. Navyše hoci sa pridal do verejných fór súvisiacich s konzervativizmom, tieto citlivé údaje nemožno použiť na zacielenie, pretože ide o dedukciu platformy sociálnych médií o politickej príslušnosti pána Jansena, ktorý nemal konkrétny úmysel tieto údaje preukázateľne zverejniť, navyše sa môže ukázať, že táto dedukcia nie je pravdivá. Preto na neho nemožno zacieliť na základe údajov o politickej príslušnosti. Inak povedané, pri posudzovaní toho, či dotknutá osoba údaje preukázateľne zverejnila, je potrebné zohľadniť okolnosti každého konkrétneho prípadu.<sup>104</sup>

## 9 SPOLOČNÉ PREVÁDZKOVATEĽSTVO A ZODPOVEDNOSŤ

### 9.1 Dohoda spoločných prevádzkovateľov a určenie zodpovedností (článok 26 všeobecného nariadenia o ochrane údajov)

130. V článku 26 ods. 1 všeobecného nariadenia o ochrane údajov sa požaduje, aby spoloční prevádzkovatelia v dohode transparentným spôsobom určili svoje príslušné zodpovednosti za plnenie povinností podľa tohto nariadenia, vrátane už spomínaných požiadaviek transparentnosti.
131. Pokiaľ ide o rozsah, EDPB sa domnieva, že v dohode medzi subjektmi vykonávajúcimi zacielenie a poskytovateľmi sociálnych médií by sa mali zahrnúť všetky spracovateľské operácie, za ktoré sú

<sup>104</sup> Pracovná skupina zriadená podľa článku 29 objasnila vo svojom stanovisku k niektorým kľúčovým otázkam smernice o presadzovaní práva (WP 258, 29. 11. 2017, s. 10), že výraz „preukázateľne zverejnené dotknutou osobou“ sa musí vykladať tak, aby to znamenalo, že dotknutá osoba si bola vedomá toho, že príslušné údaje budú verejne prístupné, teda každému, a to aj orgánom, a preto „[v] prípade pochybností by sa mal použiť úzky výklad...“

spoločne zodpovední (t. j. na ktoré sa vzťahuje spoločná kontrola). Ak subjekty vykonávajúce zacielenie a poskytovatelia sociálnych médií uzavrujú dohodu, ktorá je len povrchná a neúplná, porušujú podmienku zachovania súladu s povinnosťami, ktoré im vyplývajú z článku 26 všeobecného nariadenia o ochrane údajov.

V príklade 4 by napríklad dohoda mala obsahovať celý proces spracúvania osobných údajov, na ktorý sa vzťahuje spoločné prevádzkovateľstvo, t. j. od získania osobných údajov prostredníctvom sledovacieho pixelu v čase, keď pán Schmidt navštívi webové sídlo BestBags.com, až po zobrazenie reklamy na stránke sociálnych médií, ako aj akékoľvek prípadné podávanie správ o cielej kampani.

132. Aby mohli poskytovateľ sociálnych médií a subjekt vykonávajúci zacielenie vytvoriť komplexnú dohodu, musia vedieť o tom, či dochádza k spracovateľským operáciám osobitných údajov, a musia o nich mať dostatočne podrobné informácie. Dohoda medzi subjektom vykonávajúcim zacielenie a poskytovateľom sociálnych médií by preto mala obsahovať (alebo odkazovať na) všetky informácie potrebné na to, aby mohli obe strany splniť svoje záväzky podľa všeobecného nariadenia o ochrane údajov vrátane povinnosti zachovania súladu s princípmi podľa článku 5 ods. 1 tohto nariadenia a povinnosti preukázať tento súlad podľa článku 5 ods. 2 tohto nariadenia.
133. Ak sa napríklad prevádzkovateľ chce odvolať na článok 6 ods. 1 písm. f) všeobecného nariadenia o ochrane údajov ako na právny základ, musí okrem iného poznať rozsah spracúvania údajov, aby dokázal posúdiť, či nad záujmami prevádzkovateľa neprevažujú základné práva a slobody dotknutých osôb. Takéto posúdenie nemožno vykonať bez dostatočných informácií týkajúcich sa spracúvania. Je potrebné neustále zdôrazňovať, že je dôležité do spoločnej dohody zahrnúť potrebné informácie alebo odkazy na ne, a to najmä v situáciách, keď znalosti o informáciách potrebných pre obe strany na zachovanie súladu so všeobecným nariadeniami o ochrane údajov a prístup k týmto informáciám má takmer výlučne jedna zo strán.

V príklade 1, kde spoločnosť X posudzuje, či môže použiť oprávnený záujem ako právny základ na zacielenie na mužov vo veku 30 až 45 rokov, ktorí uviedli, že sú nezadaní, je napríklad potrebné, aby mala táto spoločnosť prístup k dostatku informácií o spracúvaní, ktoré vykonáva platforma sociálnych médií, a to napríklad vrátane informácií o doplňujúcich opatreniach (napr. právo na predbežnú námietku) zavedených platformou sociálnych médií, aby zabezpečila, že nad oprávnenými záujmami neprevažujú záujmy alebo základné práva a slobody dotknutej osoby.

134. Aby sa zaistilo účinné dodržiavanie práv dotknutej osoby, EDPB zastáva názor, že v spoločnej dohode medzi subjektmi vykonávajúcimi zacielenie a poskytovateľmi sociálnych médií ako spoločnými prevádzkovateľmi by sa mal uvádzať aj účel spracúvania a príslušný právny základ. Hoci všeobecné nariadenie o ochrane údajov nebráni spoločným prevádzkovateľom použiť pre rôzne spracovateľské operácie rôzne právne základy, ak je to možné, odporúča sa pre konkrétny nástroj zacielenia a účel použiť rovnaký právny základ. Ak by každá fáza spracúvania prebiehala na inom právnom základe, uplatňovanie práv by sa stalo pre dotknuté osoby nevykonateľné (napr. v jednej fáze by platilo právo na prenosnosť údajov, v inej zas právo namietať).
135. Keďže subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií sú ako prevádzkovatelia obaja zodpovední za zaistenie toho, aby sa dodržal princíp obmedzenia účelu, mali by v tomto ohľade v spoločnej dohode zaviesť primerané ustanovenia.

Ak chce napríklad subjekt vykonávajúci zacielenie použiť osobné údaje, ktoré mu poskytla dotknutá osoba, na zacielenie na sociálne médiá, musí prijať primerané opatrenia, aby zabezpečil, že tieto poskytnuté údaje poskytovateľ sociálnych médií ďalej nepoužije spôsobom nezlučiteľným s týmito účelmi, pokiaľ na to nezíska platný súhlas dotknutej osoby podľa článku 6 ods. 4 všeobecného nariadenia o ochrane údajov.

V príklade 3 by banka X mala zabezpečiť, aby spoločná dohoda s platformou sociálnych médií obsahovala primerané ustanovenia o tom, že e-mailová adresa pána Lopeza sa bez jeho súhlasu nepoužije na iné účely ako na zobrazovanie reklamy s ponukami súvisiacimi s bankovými službami, ktoré už používa.

Poskytovateľ sociálnych médií musí zároveň zaistiť, že použitie údajov na účely zacielenia zo strany subjektov vykonávajúcich zacielenie je v súlade s princípmi obmedzenia účelu, transparentnosti a zákonnosti.

136. Medzi ďalšie povinnosti, ktoré by subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií mali zväžiť v súvislosti so spoločnou dohodou, patria: iné všeobecné zásady ochrany údajov obsiahnuté v článku 5 všeobecného nariadenia o ochrane údajov, bezpečnosť spracúvania, špecificky navrhnutá a štandardná ochrana údajov, upozornenia na porušenia ochrany osobných údajov a ich oznamovanie, posúdenie vplyvu na ochranu údajov, využitie sprostredkovateľov a prenosy do tretích krajín.

Napríklad v príklade 13 by sa v spoločnej dohode malo uviesť, ktorý z prevádzkovateľov vykoná posúdenie vplyvu na ochranu údajov a zabezpečí relevantnú výmenu vedomostí. Inak povedané, politická strana Letschangetheworld by mala zabezpečiť, aby mala pri vykonávaní posúdenia vplyvu na ochranu údajov dostatočnú úroveň informácií, napríklad o bezpečnostných opatreniach, ktoré zaviedla platforma sociálnych médií.

137. A napokon spoločná dohoda medzi poskytovateľom sociálnych médií a subjektom vykonávajúcim zacielenie musí obsahovať konkrétne informácie o tom, ako sa v praxi splnia povinnosti vyplývajúce zo všeobecného nariadenia o ochrane údajov. Ak nie je jasné, akým spôsobom sa tieto povinnosti splnia, najmä vo vzťahu k právam dotknutých osôb, bude sa to považovať za porušenie článku 26 ods. 1 všeobecného nariadenia o ochrane údajov zo strany subjektu vykonávajúceho zacielenie a poskytovateľa sociálnych médií. Navyše v takýchto prípadoch nebudú mať obaja (spoloční) prevádzkovatelia zavedené vhodné technické a organizačné opatrenia, aby zaistili a boli schopní preukázať, že spracúvanie sa vykonáva v súlade so všeobecným nariadením o ochrane údajov, čo sa bude považovať za porušenie ich povinností podľa článku 5 ods. 2 a článku 24.

## 9.2 Úrovne zodpovednosti

138. EDPB konštatuje, že subjekty vykonávajúce zacielenie, ktoré chcú použiť nástroje zacielenia ponúkané poskytovateľom sociálnych médií, sa môžu stretnúť s tým, že budú musieť dodržať vopred vymedzené opatrenia, bez možnosti o nich rokovať alebo vykonávať úpravy (podmienky „ber alebo nechaj tak“). EDPB sa domnieva, že takáto situácia nevyvracia spoločnú zodpovednosť poskytovateľa sociálnych médií a subjektu vykonávajúceho zacielenie a nemôže slúžiť na to, aby zbavila niektorú stranu jej povinností vyplývajúcich zo všeobecného nariadenia o ochrane údajov. Obe strany spoločnej dohody sú zároveň povinné zabezpečiť, aby rozdelenie zodpovednosti náležite a praktickým, pravdivým a transparentným spôsobom zodpovedalo ich jednotlivým úlohám a vzťahom s dotknutými osobami.
139. Je dôležité zdôrazniť, že dohoda uzavretá podľa článku 26 všeobecného nariadenia o ochrane údajov nemôže prevažovať nad právnymi záväzkami, ktoré vznikajú (spoločnému) prevádzkovateľovi. Zatiaľ

čo článkom 26 všeobecného nariadenia o ochrane údajov sa stanovuje, že prevádzkovatelia „určia svoje príslušné zodpovednosti za plnenie povinností“ podľa tohto nariadenia, každý prevádzkovateľ je v zásade naďalej zodpovedný za súlad postupov spracúvania. Znamená to, že každý prevádzkovateľ okrem iného nesie zodpovednosť za súlad so zásadami stanovenými v článku 5 ods. 1 všeobecného nariadenia o ochrane údajov vrátane princípu zákonnosti stanoveného v článku 5 ods. 1 písm. a) tohto nariadenia.

140. Miera zodpovednosti subjektu vykonávajúceho zacielenie a poskytovateľa sociálnych médií vo vzťahu ku konkrétnym povinnostiam sa však môže líšiť. SDEÚ vo veci Wirtschaftsakademie konštatoval, že „[e]xistencia spoločnej zodpovednosti neznamená nevyhnutne rovnakú zodpovednosť rôznych subjektov, ktorých sa týka spracovanie osobných údajov. [...] tieto subjekty môžu byť naopak zapojené do tohto spracovania v rôznych fázach a stupňoch, takže mieru zodpovednosti každého z nich treba hodnotiť z hľadiska všetkých relevantných okolností prejednávanej veci“.<sup>105</sup>
141. Inak povedané, hoci obaja spoloční prevádzkovatelia zodpovedajú za dodržiavanie povinností podľa všeobecného nariadenia o ochrane údajov a hoci dotknutá osoba môže uplatniť svoje práva voči každému z nich, úroveň zodpovednosti treba posudzovať podľa ich skutočnej úlohy v rámci spracúvania údajov. Vo veci Google Spain SDEÚ objasnil, že prevádzkovateľ musí „v rámci svojich zodpovedností, kompetencií a možností“ zaručiť, že spracúvanie osobných údajov spĺňa požiadavky právnych predpisov EÚ o ochrane údajov.<sup>106</sup>
142. Pokiaľ ide o posudzovanie úrovne zodpovednosti subjektov vykonávajúcich zacielenie a poskytovateľov sociálnych médií, môže byť relevantných niekoľko faktorov, napríklad schopnosť ovplyvniť spracúvanie na praktickej úrovni, ako aj skutočná alebo predpokladaná vedomosť každého zo spoločných prevádzkovateľov. Zároveň je dôležité presne stanoviť, v ktorej fáze spracúvania nesú subjekt vykonávajúci zacielenie a poskytovateľ sociálnych médií zodpovednosť za tento proces a v akom rozsahu.<sup>107</sup>

V príklade 1 spoločnosť X vytvára reklamnú kampaň, aby sa používateľom, ktorí zodpovedajú konkrétnym kritériám zacielenia, mohli na platforme sociálnych médií zobrazovať reklamy na túto spoločnosť. Hoci však stanovuje parametre reklamnej kampane, nezískava žiadne osobné údaje, nemá k nim prístup ani nie je vôbec v priamom kontakte s dotknutou osobou. Každý z týchto prvkov môže byť relevantný pri posudzovaní úrovne (alebo „stupňa“) zodpovednosti subjektu vykonávajúceho zacielenie a poskytovateľa sociálnych médií v prípade, že je identifikované porušenie všeobecného nariadenia o ochrane údajov (napr. v prípade nedostatočnej transparentnosti voči dotknutej osobe alebo nezabezpečení zákonnosti spracúvania). Ako už bolo uvedené, bez ohľadu na uvedené majú obe strany povinnosť prijať vhodné opatrenia na to, aby splnili požiadavky podľa všeobecného nariadenia o ochrane údajov a chránili údaje dotknutých osôb pred nezákonným spracúvaním.

V príklade 3, ktorý zahŕňa zacielenie na základe zoznamu, je situácia mierne odlišná od príkladu 1. V prípade 3 banka na úvod získala osobné údaje a poskytla ich s poskytovateľom sociálnych médií na účely zacielenia. V takom prípade subjekt vykonávajúci zacielenie v rámci spracúvania údajov dobrovoľne zapríčinil fázu získania a poskytnutia. Pri posudzovaní úrovne zodpovednosti

<sup>105</sup> Rozsudok SDEÚ únie z 5. júna 2018 vo veci Wirtschaftsakademie, C-210/16, bod 43.

<sup>106</sup> Pozri aj SDEÚ, C-131/12, Google Spain („zodpovednosti, kompetencie a možnosti“).

<sup>107</sup> EDPB sa domnieva, že v rôznych prípadoch posúdenie založené na uvedených kritériách (napr. údaje použité na určenie kritérií zacielenia, priradenie dotknutej osoby, získanie súhlasu) s veľkou pravdepodobnosťou povedie k výsledku, že poskytovateľ sociálnych médií má väčší skutočný vplyv na spracúvanie, a preto má vyššiu úroveň zodpovednosti, v závislosti od konkrétnych použitých mechanizmov zacielenia.



jednotlivých subjektov treba vziať do úvahy každý z týchto prvkov a náležite ho zohľadniť v podmienkach spoločnej dohody.

Podobne aj v príklade 4 v prípade zacielenia na základe pixelov treba zohľadniť, že správca webového sídla umožňuje poskytnutie osobných údajov poskytovateľovi sociálnych médií. Spoločnosť BestBags.com v tomto prípade integruje na svoje sídlo sledovací pixel, aby mohla na pána Schmidta zacieliť svoju kampaň napriek tomu, že sa rozhodol nič nekúpiť<sup>108</sup>. Webové sídlo sa preto aktívne podieľa na získavaní a poskytovaní údajov. Poskytovateľ sociálnych médií má však ako spoločný prevádzkovateľ takisto povinnosť prijať vhodné opatrenia na to, aby splnil požiadavky všeobecného nariadenia o ochrane údajov a chránil údaje dotknutých osôb pred nezákonným spracúvaním. Ak je v tomto prípade potrebný súhlas dotknutej osoby, spoloční prevádzkovatelia by sa mali dohodnúť na spôsobe, akým chcú tento súhlas v praxi získať.

143. Pokiaľ ide o posúdenie úrovne zodpovednosti poskytovateľa sociálnych médií, EDPB konštatuje, že niekoľko mechanizmov zacielenia je založených na profilovaní a/alebo iných spracovateľských činnostiach, ktoré predtým vykonal poskytovateľ sociálnych médií. Poskytovateľ sociálnych médií rozhoduje o spracúvaní osobných údajov svojich používateľov tak, aby vytvoril kritériá zacielenia, ktoré sprístupňuje subjektom vykonávajúcim zacielenie. V tejto súvislosti poskytovateľ sociálnych médií nezávisle prijal určité rozhodnutia týkajúce sa spracúvania, napríklad ktoré kategórie údajov sa majú spracúvať, ktoré kritériá zacielenia ponúknuť a kto by mal mať prístup k osobným údajom (a k akým typom), ktoré sa spracúvajú vo vzťahu ku konkrétnej cieľovej kampani. Než poskytovateľ sociálnych médií začne ponúkať služby zacielenia, musí zabezpečiť, aby tieto spracovateľské činnosti boli v súlade so všeobecným nariadením o ochrane údajov.
144. Príklady uvedené v predchádzajúcich odsekoch sú ukážkou toho, aké dôležité je jasne prideliť zodpovednosti v rámci spoločnej dohody medzi poskytovateľmi sociálnych médií a subjektmi vykonávajúcimi zacielenie. Hoci v podmienkach tejto dohody by sa mala vždy zohľadňovať úroveň zodpovednosti každého zo subjektov, komplexná dohoda, v ktorej sa náležite zohľadňuje úloha a schopnosti oboch strán, je potrebná nielen z hľadiska súladu s článkom 26 všeobecného nariadenia o ochrane údajov, ale aj na účely splnenia ďalších pravidiel a zásad tohto nariadenia.
145. A napokon EDPB konštatuje, že pokiaľ podmienky spoločnej dohody medzi poskytovateľom sociálnych médií a subjektom vykonávajúcim zacielenie nie sú záväzné pre dozorné orgány, môžu tieto orgány uplatňovať svoje kompetencie a právomoci voči ktorémukoľvek spoločnému prevádzkovateľovi, ak tento spoločný prevádzkovateľ patrí do pôsobnosti daného dozorného orgánu.

---

<sup>108</sup> Keďže spoločnosť BestBags.com integrovala na svoje webové sídlo sledovací pixel sociálnych médií, má zároveň povinnosť dodržiavať požiadavky smernice o súde a elektronických komunikáciách týkajúce sa tohto nástroja, a vzhľadom na to, že pixel zároveň prispieva k spracúvaniu osobných údajov, je dôležité ho zohľadniť aj pri určovaní úrovne zodpovednosti.