



**00264/10/SK
WP 169**

Stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“

prijaté 16. februára 2010

Táto pracovná skupina bola zriadená podľa článku 29 smernice 95/46/ES. Je nezávislým európskym poradným orgánom pre ochranu údajov a súkromia. Jej úlohy sú definované v článku 30 smernice 95/46/ES a článku 15 smernice 2002/58/ES.

Úlohy sekretariátu poskytuje riaditeľstvo D (základné práva a občianstvo) Európskej komisie, Generálne riaditeľstvo pre spravodlivosť, slobodu a bezpečnosť, B-1049 Brusel, Belgicko, kancelária č. LX-46 01/190.

Internetová stránka: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

OBSAH

Zhrnutie	1
I. Úvod	2
II. Všeobecné poznámky a politické otázky	3
II.1. Úloha pojmov	4
II.2. Príslušný kontext	6
II.3. Niektoré najväčšie výzvy	7
III. Analýza definícií	7
III.1. Vymedzenie pojmu prevádzkovateľ	7
III.1.a) Úvodný prvok: „určuje“	8
III.1.b) Tretí prvok: „účely a prostriedky spracovania“	12
III.1.c) Prvý prvok: „fyzickú alebo právnickú osobu, alebo akýkoľvek iný orgán“	14
III.1.d) Druhý prvok: „sám, alebo v spojení s inými“	17
III.2. Vymedzenie pojmu spracovateľ	24
III.3. Vymedzenie pojmu tretia strana	30
IV. Závery	31

Zhrnutie

Pojem prevádzkovateľ údajov (pôvodne označovaný aj ako „kontrolór“) a jeho vzájomný vzťah s pojmom spracovateľ údajov zohrávajú rozhodujúcu úlohu pri uplatňovaní smernice 95/46/ES, pretože určujú, kto má niesť zodpovednosť za dodržiavanie pravidiel ochrany údajov, ako si môžu dotknuté osoby uplatniť svoje práva, ktoré vnútroštátne právne predpisy sú uplatniteľné a ako účinne môžu pracovať orgány na ochranu údajov.

Organizačná diferenciacia vo verejnom a súkromnom sektore, vývoj IKT a globalizácia spracovania údajov, zvyšujú zložitosť spôsobu spracovania osobných údajov a vyžadujú si ujasnenie týchto pojmov s cieľom zabezpečiť účinné uplatňovanie a dodržiavanie pravidiel v praxi.

Pojem prevádzkovateľ je nezávislý v tom zmysle, že by sa mal vykladať najmä podľa právnych predpisov Spoločenstva o ochrane údajov, a funkčný v tom zmysle, že jeho cieľom je prideliť zodpovednosť tam, kde je aj skutočný vplyv, a preto je založený skôr na faktickej ako na formálnej analýze.

Definícia uvedená v smernici obsahuje tri základné stavebné prvky:

- osobné hľadisko („*fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán*“),
- možnosť spoločnej kontroly („*ktorý sám, alebo v spojení s inými*“), a
- základné prvky na odlišenie prevádzkovateľa od ostatných aktérov („*určuje účely a prostriedky spracovania osobných údajov*“).

Analýza týchto stavebných prvkov vedie k niekoľkým záverom, ktoré sú zhrnuté v odseku IV tohto stanoviska.

V tomto stanovisku sa analyzuje aj pojem spracovateľ, ktorého existencia závisí od rozhodnutia prevádzkovateľa, ktorý sa môže rozhodnúť spracovať údaje vo svojej vlastnej organizácii, alebo poveriť externú organizáciu vykonaním všetkých činností spracovania alebo ich časti. Na kvalifikáciu spracovateľa je potrebné splniť dve základné podmienky, na jednej strane, musí ísť o samostatný právnický subjekt nezávislý od prevádzkovateľa a na druhej strane, tento subjekt musí spracovávať osobné údaje v mene prevádzkovateľa.

Pracovná skupina si uvedomuje ťažkosti súvisiace s uplatňovaním definícií smernice v zložitom prostredí, v ktorom je možné predpokladať veľké množstvo scenárov, v ktorých prevádzkovatelia a spracovatelia vystupujú samostatne alebo spoločne, s rôznymi stupňami samostatnosti a zodpovednosti.

Pracovná skupina vo svojej analýze zdôrazňuje potrebu prideliť zodpovednosť takým spôsobom, aby sa dostatočne zabezpečilo dodržiavanie pravidiel ochrany údajov v praxi. Nenašla však dôvod domnievať sa, že by už v tomto ohľade súčasné rozlíšenie medzi prevádzkovateľom a spracovateľom nebolo relevantné a nedalo by sa s ním pracovať.

Pracovná skupina preto dúfa, že vysvetlenie, ktoré ponúka v tomto stanovisku, doplnené o konkrétne príklady každodennej praxe orgánov na ochranu údajov, prispeje k účinnému usmerneniu na ceste k výkladu týchto ústredných definícií smernice.

Pracovná skupina pre ochranu jednotlivcov so zreteľom na spracovanie osobných údajov,

ktorá bola zriadená smernicou Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995,

so zreteľom na článok 29 a článok 30 ods. 1 písm. a) a ods. 3 uvedenej smernice a článok 15 ods. 3 smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002,

so zreteľom na svoj rokovací poriadok,

prijala toto stanovisko:

I. Úvod

Pojem prevádzkovateľ údajov a jeho vzájomný vzťah s pojmom spracovateľ údajov zohrávajú rozhodujúcu úlohu pri uplatňovaní smernice 95/46/ES, pretože určujú, kto má niesť zodpovednosť za dodržiavanie pravidiel ochrany údajov a ako si môžu dotknuté osoby uplatniť svoje práva v praxi. Pojem prevádzkovateľ údajov je nevyhnutný aj pre určenie uplatniteľných vnútroštátnych právnych predpisov a účinné vykonávanie dozorných úloh, ktorými sú poverené orgány na ochranu údajov.

Z tohto dôvodu je najdôležitejšie, aby presný význam týchto pojmov a kritériá ich správneho používania boli dostatočne jasné a aby ich v členských štátoch chápali rovnakým spôsobom všetci aktéri, ktorí sa podieľajú na vykonávaní smernice a uplatňovaní, hodnotení a presadzovaní vnútroštátnych ustanovení, ktoré zabezpečujú jej účinnosť.

Objavili sa náznaky, že prinajmenšom v súvislosti s niektorými hľadiskami týchto pojmov môže chýbať úplná jasnosť, ale aj niekoľko rozdielnych názorov aktérov v rôznych členských štátoch, ktoré môžu viesť k odlišným výkladom tých istých zásad a definícií zavedených na účely harmonizácie na európskej úrovni. Z tohto dôvodu sa pracovná skupina zriadená podľa článku 29 rozhodla, že v rámci svojho strategického pracovného programu na roky 2008 – 2009 bude venovať osobitnú pozornosť vypracovaniu dokumentu, v ktorom stanoví spoločný prístup k týmto otázkam.

Pracovná skupina si uvedomuje, že konkrétne používanie pojmov prevádzkovateľ údajov a spracovateľ údajov sa stáva čoraz zložitejším. Najväčší podiel má na tom narastajúca zložitosť prostredia, v ktorom sa tieto pojmy používajú, a najmä rastúca tendencia, v súkromnom aj verejnom sektore, smerom k organizačnej diferenciacii v kombinácii s vývojom IKT a globalizáciou, a to spôsobom, v dôsledku ktorého môžu vzniknúť nové a závažné problémy, ktorých výsledkom môže byť niekedy nižšia úroveň ochrany dotknutých osôb.

Aj keď sa ustanovenia smernice sformulovali technologicky neutrálne a doposiaľ úspešne odolávali vyvíjajúcim sa súvislostiam, spomínaná zložitosť môže skutočne viesť k neistote, pokiaľ ide o pridelenie zodpovednosti a rozsah uplatniteľných vnútroštátnych zákonov. Tieto neistoty môžu mať záporný účinok na dodržiavanie pravidiel ochrany údajov v kritických oblastiach a na účinnosť zákona o ochrane údajov ako celku. Pracovná skupina už rieši niektoré z týchto problémov v súvislosti s konkrétnymi otázkami¹, no v súčasnosti považuje za dôležité poskytnúť pokročilejšie usmernenia a konkrétny návod s cieľom zabezpečiť konzistentný a harmonizovaný prístup.

¹ Pozri napríklad stanovisko 10/2006 k spracúvaniu osobných údajov Spoločnosťou pre celosvetovú medzibankovú finančnú telekomunikáciu (SWIFT), prijaté 22. novembra 2006 (WP 128), a novšie stanovisko 5/2009 k sociálnym sieťam online, prijaté 12. júna 2009 (WP 163).

Preto sa pracovná skupina v tomto stanovisku – podobným spôsobom ako v predchádzajúcom stanovisku k pojmu osobné údaje² – rozhodla poskytnúť určité ujasnenie a niekoľko konkrétnych príkladov³ v súvislosti s pojmami prevádzkovateľ údajov a spracovateľ údajov.

II. Všeobecné poznámky a otázky politiky

Smernica priamo odkazuje na pojem prevádzkovateľ v niekoľkých ustanoveniach. Pojmy „prevádzkovateľ“ a „spracovateľ“ sú definované v článku 2 písm. d) a písm. e) smernice 95/46/ES (ďalej len „smernica“) takto:

„Prevádzkovateľ“ znamená fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán, ktorý sám alebo v spojení s inými určuje účely a prostriedky spracovania osobných údajov; tam, kde sú účely a prostriedky spracovania stanovené vnútroštátnymi zákonmi a nariadeniami, alebo zákonmi a nariadeniami Spoločenstva, ten, kto spracovanie riadi, alebo konkrétne kritéria pre jeho menovanie môžu byť navrhnuté na základe vnútroštátneho práva alebo práva Spoločenstva;

„Spracovateľ“ znamená fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán, ktorý spracúva osobné údaje v mene prevádzkovateľa.

Tieto definície sa utvorili počas rokovaní o návrhu smernice v prvej polovici 90-tych rokov 20. storočia a pojem „prevádzkovateľ“ sa pôvodne prevzal z dohovoru Rady Európy č. 108 prijatého v roku 1981. Počas týchto rokovaní sa udialo niekoľko významných zmien.

V prvom rade, pojem „prevádzkovateľ súboru“ z dohovoru č. 108 sa nahradil pojmom „prevádzkovateľ“ v súvislosti so „spracovaním osobných údajov“. Ide o široký pojem vymedzený v článku 2 písm. b) smernice, ktorý znamená „akúkoľvek operáciu alebo súbor operácií, ktoré sa s osobnými údajmi vykonávajú, či už automatickými prostriedkami alebo nie, ako je zber, zaznamenávanie, organizácia, uskladnenie, úprava alebo nahradenie, vyhľadávanie, nahliadnutie, používanie, odhalenie prenosom, šírenie alebo sprístupnenie iným spôsobom, upravenie alebo kombinácia, blokovanie, vymazanie alebo zničenie.“ Pojem „prevádzkovateľ“ sa tak prestal používať vo vzťahu k statickému predmetu („súboru“), ale začal sa týkať činností odzrkadľujúcich životný cyklus informácií od ich zberu po ich zničenie, a na to bolo potrebné pozerieť sa podrobne a v celistvosti („operáciu alebo súbor operácií“). Hoci v mnohých prípadoch mohol byť výsledok rovnaký, pojem sa takto rozšíril a získal omnoho dynamickejší význam a rozsah.

Ďalšie zmeny sa týkali zavedenia možnosti „spoločnej kontroly“ („sám, alebo v spojení s inými“), podmienky, že prevádzkovateľ „určí účely a prostriedky spracovania osobných údajov“ a koncepcie, podľa ktorej sa o tomto určení môže rozhodnúť na základe vnútroštátnych právnych predpisov, právnych predpisov Spoločenstva, alebo iným spôsobom. Smernicou sa zároveň zaviedol pojem „spracovateľ“, ktorý sa v dohovore

² Stanovisko 4/2007 ku koncepcii osobných údajov, prijaté 20. júna 2007 (WP 136).

³ Tieto príklady vychádzajú zo súčasnej vnútroštátnej alebo európskej praxe a mohli byť upravené alebo spracované s cieľom zabezpečiť lepšie pochopenie.

č. 108 nenachádza. V tomto stanovisku sa postupne podrobne analyzujú tieto a ďalšie zmeny.

II.1. Úloha pojmov

Kým v dohovore č. 108 plní pojem prevádzkovateľ (súboru) veľmi obmedzenú úlohu⁴, v smernici je to úplne inak. V článku 6 ods. 2 sa explicitne stanovuje, že „Úlohou prevádzkovateľa je zaistiť, aby sa vyhovelo odseku 1“. Tento odsek odkazuje na hlavné zásady týkajúce sa kvality údajov vrátane zásady uvedenej v článku 6 ods. 1 písm. a), že „osobné údaje musia byť spracované spravodlivo a zákonne“. V praxi to znamená, že všetky ustanovenia, ktorými sa stanovujú podmienky zákonného spracovania, sa v podstate vzťahujú na prevádzkovateľa, aj keď to nie je vždy jasne vyjadrené.

Ustanovenia o právach dotknutej osoby na informácie o osobných údajoch, prístup k nim, ich opravu, vymazanie a zablokovanie a o práve namietať proti ich spracovaniu (články 10 – 12 a 14), sa navyše sformulovali takým spôsobom, aby sa vytvorili povinnosti pre prevádzkovateľa. Prevádzkovateľ plní ústrednú úlohu aj v ustanoveniach o oznamovaní a predbežnej kontrole (články 18 – 21). Nakoniec by nemalo byť prekvapením ani to, že prevádzkovateľ sa považuje za zodpovedného v zásade za akúkoľvek ujmu v dôsledku nezákonného spracovania (článok 23).

To znamená, že prvotnou a najdôležitejšou úlohou pojmu prevádzkovateľ je určiť, kto má niesť zodpovednosť za dodržiavanie pravidiel ochrany údajov a ako si môžu dotknuté osoby uplatniť svoje práva v praxi⁵. Inými slovami: prideliť zodpovednosť.

Významne sa to týka smernice, ktorej prvým cieľom je „ochraňovať jednotlivcov vzhľadom na spracovanie osobných údajov“. Tento cieľ je možné dosiahnuť a uplatniť v praxi iba vtedy, ak tí, ktorí sú zodpovední za spracovanie údajov, môžu byť právnymi a inými spôsobmi dostatočne stimulovaní, aby vykonali všetky opatrenia nevyhnutné na zabezpečenie tejto ochrany v praxi. Potvrďuje to článok 17 ods. 1 smernice, podľa ktorého prevádzkovateľ zabezpečí „zavedenie vhodných technických a organizačných opatrení na ochranu osobných údajov pred náhodným alebo nezákonným poškodením alebo náhodnej strate, zmene, neoprávnenému prezradeniu alebo sprístupneniu, najmä, kde spracovanie obsahuje prenos údajov cez sieť a proti všetkým iným nezákonným formám spracovania.“

Prostriedky na stimuláciu zodpovednosti môžu byť proaktívne a reakčné. V prvom prípade sa nimi musí zabezpečiť účinné vykonávanie opatrení na ochranu údajov a dostatočné spôsoby zodpovednosti prevádzkovateľov. V druhom prípade môžu zahŕňať občianskoprávnú zodpovednosť a sankcie s cieľom zabezpečiť, aby sa vynahradila každá vzniknutá ujma a vykonali sa primerané opatrenia na nápravu všetkých chýb alebo priestupkov.

⁴ Nepoužíva sa v žiadnych podstatných ustanoveniach okrem článku 8 písm. a) v súvislosti s právom byť informovaný (zásadou transparentnosti). Prevádzkovateľ ako zodpovedná strana je viditeľný iba v určitých častiach odôvodnenia.

⁵ Pozri aj odôvodnenie 25 smernice 95/46/ES: „keďže zásady ochrany sa musia na jednej strane odrážať v povinnostiach kladených na osoby, verejné úrady, podniky, agentúry alebo iné orgány zodpovedné za spracovanie, najmä pokiaľ ide o kvalitu údajov, technické zabezpečenie, oznámenia kontrolným orgánom, a okolnosti, za ktorých sa môže vykonávať spracovanie a na druhej strane v práve delegovanom na jednotlivcov, o ktorých sa údaje spracovávajú, aby boli informovaní, že sa uskutočňuje spracovanie, aby sa pozreli na údaje, aby žiadali opravy a, aby za určitých okolností mali námietky proti spracovaniu.“

Pojem prevádzkovateľ je zároveň základným prvkom pri určení skutočnosti, čie vnútroštátne právne predpisy sú uplatniteľné na operáciu spracovania alebo súbor operácií spracovania. Základné pravidlo uplatniteľných právnych predpisov podľa článku 4 ods. 1 písm. a) smernice hovorí, že každý členský štát uplatňuje svoje vnútroštátne ustanovenia na „spracovanie osobných údajov, ak (...) sa vykonáva v kontexte činností ustanovenia prevádzkovateľa na území členského štátu“. Toto ustanovenie pokračuje takto: „keď je tá istá inštitúcia, ktorá riadi spracovanie, ustanovená na území niekoľkých členských štátov, musí prijať nevyhnutné opatrenia, aby zaistila, že každé z týchto ustanovení je v súlade so záväzkami, ktoré predpisuje uplatniteľnosť vnútroštátneho práva“. To znamená, že aj to, kde sú usadené pobočky prevádzkovateľa, rozhoduje o tom, ktoré vnútroštátne predpisy, prípadne aj viaceré rôzne uplatniteľné vnútroštátne predpisy, sú uplatniteľné a o spôsobe, ako vzájomne súvisia⁶.

Nakoniec treba poznamenať, že pojem prevádzkovateľ sa objavuje v mnohých ustanoveniach smernice ako prvok ich rozsahu alebo osobitnej podmienky uplatnenej podľa nich: napríklad v článku 7 sa stanovuje, že osobné údaje je možné spracovať iba ak: „c) spracovanie je nevyhnutné pre dodržanie právneho záväzku, ktorého subjektom je prevádzkovateľ, e) spracovanie je nevyhnutné na splnenie úlohy vykonávanej vo verejnom záujme alebo v uplatňovaní oficiálneho poverenia zverného prevádzkovateľovi alebo tretej strane, ktorej sa údaje odhalia, alebo f) spracovanie je nevyhnutné pre účely legitímnych záujmov, ktoré plní prevádzkovateľ alebo tretia strana alebo strany, ktorým sú údaje odhalené, s výnimkou, ak takéto záujmy sú prevýšené ...“. Identita prevádzkovateľa je tiež významný prvok informácií pre dotknutú osobu, ktoré sa vyžadujú podľa článku 10 a článku 11.

Pojem „spracovateľ“ plní dôležitú úlohu v kontexte dôveryhodnosti a bezpečnosti spracovania (články 16 – 17), pretože slúži na identifikáciu povinností tých, ktorí sú užšie zapojení do spracovania osobných údajov, tých, ktorí buď priamo podliehajú právomoci prevádzkovateľa, alebo konajú inak v jeho mene. Rozdiel medzi „prevádzkovateľom“ a „spracovateľom“ slúži najmä na odlišenie tých, ktorí nesú zodpovednosť ako prevádzkovateľ (prevádzkovatelia), od tých, ktorí iba konajú v ich mene. Opäť ide predovšetkým o otázku pridelenia zodpovednosti. Odtiaľ môžu prameniť ďalšie následky, buď v súvislosti s uplatniteľnými právnymi predpismi alebo v inej súvislosti.

V prípade spracovateľa existuje ďalší následok, jednako pre prevádzkovateľa, jednako pre spracovateľa, že podľa článku 17 smernice sú použiteľným právom pre bezpečnosť spracovania vnútroštátne právne predpisy členského štátu, v ktorom má spracovateľ sídlo⁷.

Nakoniec, ako je stanovené v článku 2 písm. f), „tretia strana“ znamená *akúkoľvek fyzickú alebo právnickú osobu, štátny orgán, agentúru alebo akýkoľvek iný orgán ako dotknutú osobu, ten, kto spracovanie riadi, spracovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo spracovateľom poverené spracovať údaje*.“ Prevádzkovateľ a spracovateľ a ich zamestnanci sa preto považujú za „vnútorný kruh spracovania údajov“ a nevzťahujú sa na nich osobitné ustanovenia o tretích stranách.

⁶ Pracovná skupina plánuje prijať samostatné stanovisko k „uplatniteľným právnym predpisom“ počas roka 2010. Keď inštitúcie a orgány Spoločenstva spracúvajú osobné údaje, posúdenie kontroly je významné aj v súvislosti s možným uplatnením nariadenia (ES) 45/2001 alebo iných príslušných právnych nástrojov EÚ.

⁷ Pozri článok 17 ods. 3 druhá zarážka: „povinnosti ako definuje právo členského štátu, v ktorom má spracovateľ sídlo, tiež musia pripadať spracovateľovi.“

II.2. Príslušný kontext

V dôsledku vývoja a rôznych vplyvov v príslušnom prostredí sa tieto otázky stali naliehavejšími a zložitejšími ako v minulosti. V čase podpísania dohovoru č. 108 a vo veľkej miere aj v období prijatia smernice 95/46/ES bol kontext spracovania údajov ešte pomerne jasný a jednoznačný, dnes tomu tak už nie je.

Je to v prvom rade zapríčinené rastúcou tendenciou smerom k organizačnej diferenciacii v najvýznamnejších sektoroch. V súkromnom sektore viedlo rozdelenie finančných alebo iných rizík k neustálej diverzifikácii podnikov, ktorá sa ešte posilňuje fúziami a akvizíciami. Vo verejnom sektore prebieha podobná diferenciacia v kontexte decentralizácie alebo rozdeľovania politických oddelení a výkonných agentúr. V oboch sektoroch sa kladie čoraz väčší dôraz na rozvoj dodávateľských reťazcov alebo poskytovania služieb medzi organizáciami a na využívanie subdodávateľov alebo externých poskytovateľov služieb (outsourcing) s cieľom využiť špecializáciu a možné úspory z rozsahu. Výsledkom je rast rôznych služieb ponúkaných poskytovateľmi služieb, ktorí sami seba často nepovažujú za zodpovedných. Pre organizačné rozhodnutia spoločností (a ich zmluvných dodávateľov alebo subdodávateľov) sa môžu príslušné databázy nachádzať v jednej alebo vo viacerých krajinách v rámci Európskej únie alebo mimo nej.

Vývoj informačných a komunikačných technológií („IKT“) vo veľkej miere uľahčuje tieto organizačné zmeny a navyše pridáva aj vlastné. Zodpovednosti na rôznych úrovniach – často v dôsledku organizačnej diferenciacie – často vyžadujú a stimulujú rozsiahle používanie IKT. Vývoj a nasadenie produktov a služieb IKT takisto vedie k vzniku nových úloh a zodpovedností, ktoré nie vždy jasne súvisia s existujúcimi alebo rozvíjajúcimi sa zodpovednosťami v zákaznických organizáciách. Preto je dôležité uvedomovať si príslušné rozdiely a ak je to potrebné, vysvetľovať zodpovednosti. Zavádzanie mikrotechnológie – ako RFID čipy v spotrebiteľských produktoch – vyvoláva podobné otázky presúvania zodpovednosti. Na druhej strane existujú nové, závažné otázky súvisiace s používaním distribuovaných výpočtových technológií, najmä „cloud computing“ a „grid computing“⁸.

Ďalším činiteľom, ktorý sa podieľa na komplikácii, je globalizácia. Keď organizačná diferenciacia a vývoj IKT zahŕňajú viacero jurisdikcií, čo sa často stáva v prípade internetu, vždy vznikajú problémy v súvislosti s uplatniteľnými právnymi predpismi, nielen v rámci EÚ alebo EHP, ale aj vo vzťahu k tretím krajinám. Ako príklad môže slúžiť rámec v kontexte boja proti dopingu – Svetová antidopingová agentúra (WADA), založená vo Švajčiarsku, prevádzkuje databázu obsahujúcu informácie o atlétoch (ADAMS), ktorá je riadená z Kanady v spolupráci s vnútroštátnymi antidopingovými organizáciami na celom svete. Pracovná skupina zriadená podľa článku 29 zdôraznila, že rozdelenie zodpovedností a pridelenie kontroly vyvoláva osobitné ťažkosti⁹.

⁸ „Cloud computing“ je druh výpočtovej služby, v rámci ktorej sa poskytujú prispôsobiteľné a pružné IT funkcie ako služba viacerým zákazníkom pomocou internetových technológií. Typické služby ponúkajúce cloud computing poskytujú bežné obchodné programy online, ku ktorým sa pristupuje cez webový prehliadač, zatiaľ čo softvér a údaje sú uložené na serveroch. V tomto zmysle výraz „cloud“, t. j. oblak, nie je ostrovom, ale globálnym prepojením informácií a používateľov z celého sveta. Pokiaľ ide o „grid computing“, pozri ďalej uvedený príklad 19.

⁹ Stanovisko 3/2008 z 1. augusta 2008 k návrhu medzinárodnej normy Svetového antidopingového kódexu pre ochranu súkromia, WP156.

To znamená, že ústredné otázky, ktorými sa zaoberá toto stanovisko, majú vysoký stupeň praktického významu a môžu mať veľké následky.

II.3. Niektoré najväčšie výzvy

Pokiaľ ide o ciele smernice, najdôležitejšie je zabezpečiť, aby bola zodpovednosť za spracovanie údajov jasne vymedzená a mohla sa účinne uplatňovať.

Ak nie je dostatočne jasné, čo sa od koho vyžaduje – napríklad, niekedy nie je nikto zodpovedný alebo existujú viacerí možní prevádzkovatelia – jestvuje zrejmé riziko, že sa vykoná veľmi málo (ak vôbec niečo) a právne ustanovenia zostanú neúčinné. Zároveň je možné, že nejasnosti vo výklade povedú k protichodným tvrdeniam a iným rozporom a v takom prípade budú kladné účinky nižšie oproti očakávaniam alebo by ich mohli nepredvídané záporné následky znížiť respektíve prevážiť.

Vo všetkých týchto prípadoch je rozhodujúcou výzvou zaručiť dostatočnú jasnosť s cieľom umožniť a zabezpečiť účinné uplatňovanie a dodržiavanie v praxi. V prípade pochybností môže riešenie, ktoré s najväčšou pravdepodobnosťou podporí takéto účinky, oprávnenne predstavovať uprednostnenú možnosť.

Tie isté kritériá, ktoré zabezpečujú dostatočnú jasnosť, však môžu viesť aj k väčšej zložitosti a neželaným následkom. Napríklad diferenciácia kontroly v súlade s organizačnými skutočnosťami môže spôsobiť zložitosť uplatniteľných vnútroštátnych právnych predpisov, ak je možné v danej situácii uplatniť rôzne jurisdikcie.

V rámci analýzy je preto potrebné prísne rozlišovať medzi prijateľnými následkami podľa súčasných pravidiel a možnou potrebou úpravy súčasných pravidiel s cieľom zabezpečiť nepretržitú účinnosť a zabrániť nevhodným následkom v dôsledku zmien okolností.

To znamená, že táto analýza má veľký strategický význam a mala by sa uplatňovať pozorne a s plným vedomím možných vzájomných vzťahov medzi rôznymi otázkami.

III. Analýza definícií

III.1. Vymedzenie pojmu prevádzkovateľ

Definícia uvedená v smernici obsahuje tri základné stavebné prvky, ktoré sa na účely tohto stanoviska analyzujú samostatne. Ide o tieto prvky:

- „fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán“,
- „ktorý sám alebo v spojení s inými“
- „určuje účely a prostriedky spracovania osobných údajov“.

Prvý stavebný prvok sa týka osobného hľadiska definície. Tretí prvok obsahuje základné prvky potrebné na odlíšenie prevádzkovateľa od ostatných aktérov, kým druhý prvok rieši možnosť „spoločnej kontroly“. Tieto stavebné prvky sú navzájom veľmi úzko späté. Na účely metodológie dodržiavanej v tomto stanovisku sa však každým z týchto prvkov budeme zaoberať samostatne.

Z praktických dôvodov je vhodné začať s *prvým prvkom* tretieho stavebného prvku – t. j. významom slova „určuje“ – a pokračovať s ostatnými slovami tretieho stavebného prvku a až potom sa zaoberať prvým a druhým stavebným prvkom.

III.1.a) Úvodný prvok: „určuje“

Ako sme už skôr uviedli, pojem prevádzkovateľ plnil v dohovore č. 108 nevýznamnú úlohu. Podľa článku 2 dohovoru sa pojmom „prevádzkovateľ súboru“ rozumie orgán, „ktorý má právomoc ... rozhodovať“. V dohovore sa zdôrazňuje potreba právomoci, ktorá sa určí „podľa vnútroštátnych právnych predpisov“. Z tohto dôvodu sa v dohovore spätne odkazuje na vnútroštátne právne predpisy v oblasti ochrany údajov, ktoré by podľa odôvodnenia mali obsahovať „presné kritériá na určenie zodpovednej osoby“.

Kým prvý návrh Komisie odzrkadľoval toto ustanovenie, zmenený a doplnený návrh Komisie namiesto toho odkazuje na orgán, „ktorý rozhoduje“, čím sa odstránila potreba zavádzať rozhodovaciu právomoc zákonom: zákonné vymedzenie je stále možné, nie je však nevyhnutné. Tento prístup sa potvrdil v spoločnej pozícii Rady a prijatom znení, keďže obidva texty odkazujú na orgán, „ktorý určuje“.

Na základe týchto súvislostí treba v historickom vývoji zdôrazniť dva významné prvky: v prvom rade, že je možné byť prevádzkovateľom bez ohľadu na osobitnú právomoc kontrolovať údaje, ktorá vyplýva zo zákona; v druhom rade, že v procese prijímania smernice 95/46 sa určenie prevádzkovateľa stáva pojmom na úrovni Spoločenstva, pojmom, ktorý má svoj vlastný nezávislý význam v rámci právnych predpisov Spoločenstva, ktorý sa nemení v dôsledku – pravdepodobne rozdielných – ustanovení vnútroštátnych právnych predpisov. Druhý uvedený prvok je nevyhnutný na zabezpečenie účinného uplatňovania smernice a vysokej úrovne ochrany v členských štátoch, čo si vyžaduje jednotný a preto nezávislý výklad takého kľúčového pojmu, ako je „prevádzkovateľ“, ktorý v smernici nadobúda význam, aký mu v dohovore č. 108 ešte nepatrilo.

Z tohto pohľadu sa vývoj ukončuje v smernici, v ktorej sa stanovuje, že aj keď právomoc „určovať“ môže vyplývať z osobitného pridelenia na základe zákona, obvykle by mala vyplývať z analýzy faktických prvkov alebo okolností prípadu: je potrebné preskúmať konkrétne operácie spracovania a pochopiť, kto ich určuje, a to v prvej fáze zodpovedaním týchto otázok: „prečo prebieha tento proces? Kto ho inicioval?“.

Byť prevádzkovateľom je v prvom rade následok faktickej okolnosti, že sa určitý subjekt rozhodol spracovať osobné údaje na svoje vlastné účely. Čisto formálne kritérium by skutočne nebolo dostatočné prinajmenšom z dvoch dôvodov: v niektorých prípadoch formálne ustanovenie prevádzkovateľa – napríklad na základe zákona, v zmluve alebo v oznámení orgánu na ochranu údajov – by bolo jednoducho nedostatočné; v iných prípadoch sa môže stať, že formálne ustanovenie nebude zodpovedať skutočnosti, ak sa úloha prevádzkovateľa formálne zverí orgánu, ktorý v skutočnosti nemá právo „určovať“.

Význam faktického vplyvu dokazuje aj prípad SWIFT¹⁰, keď sa spoločnosť SWIFT formálne považovala za spracovateľa údajov, no *de facto* konala – aspoň do určitej miery

¹⁰ Tento prípad sa týka prenosu údajov orgánom USA s cieľom boja proti financovaniu terorizmu, pričom ide o bankové údaje, ktoré zbiera spoločnosť SWIFT s cieľom uskutočniť finančné transakcie v mene bánk a finančných inštitúcií.

– ako prevádzkovateľ údajov. V tomto prípade sa ujasnilo, že napriek tomu, že zmluvné ustanovenie prevádzkovateľa alebo spracovateľa údajov môže odhaliť významné informácie o právnom postavení poverenej strany, takéto zmluvné ustanovenie nie je rozhodujúce pri určení jej skutočného postavenia, ktoré musí vychádzať z konkrétnych okolností.

Tento faktický prístup podporuje aj skutočnosť, že v smernici sa stanovuje, že prevádzkovateľ je subjekt, ktorý „určuje“, a nie „zákonne určuje“ účel a prostriedky. Účinná identifikácia kontroly je rozhodujúca, aj keď sa ustanovenie javí ako nezákonné alebo ak sa spracovanie údajov vykonáva nezákonným spôsobom. Nie je relevantné, či rozhodnutie spracovať údaje bolo „záonné“ v tom zmysle, že subjekt, ktorý takéto rozhodnutie prijal, mal na to právnu moc, alebo prevádzkovateľ bol formálne ustanovený v súlade s osobitným postupom. Otázka zákonnosti spracovania osobných údajov však zostáva relevantná v inej fáze a posúdi sa s ohľadom na iné články (konkrétne články 6 – 8) smernice. Inými slovami, dôležité je zabezpečiť, aby aj v prípadoch, keď sa údaje spracúvajú nezákonne, bolo možné ľahko nájsť prevádzkovateľa, ktorý zodpovedá za takéto spracovanie.

Poslednou črtou pojmu prevádzkovateľ je jeho nezávislosť, a to v tom zmysle, že hoci pri identifikácii prevádzkovateľa môžu pomôcť externé právne zdroje, výklad pojmu by mal primárne vychádzať z právnych predpisov o ochrane údajov¹¹. Na pojem prevádzkovateľ by nemali mať vplyv ostatné – niekedy kolidujúce alebo prekrývajúce – pojmy z iných oblastí práva, napríklad tvorca alebo držiteľ práv v oblasti práv duševného vlastníctva. Keď je subjekt držiteľom práv duševného vlastníctva, nevylučuje sa možnosť, že sa môže kvalifikovať aj ako „prevádzkovateľ“ a následne podliehať povinnostiam vyplývajúcim z právnych predpisov o ochrane údajov.

Potreba typológie

Pojem prevádzkovateľ je funkčný pojem, ktorého cieľom je pridelit' zodpovednosť tam, kde je aj skutočný vplyv, a preto je založený skôr na faktickej ako na formálnej analýze. Pridelenie kontroly si preto môže niekedy vyžadovať dôkladné a dlhé skúmanie. Potreba zabezpečiť účinnosť však vyžaduje prijatie pragmatického prístupu s cieľom zabezpečiť predvídateľnosť kontroly. Z tohto pohľadu sú potrebné praktické pravidlá a predpoklady, ktoré usmernia a zjednodušia uplatňovanie právnych predpisov o ochrane údajov.

Vzniká potreba výkladu smernice, ktorým sa zabezpečí vo väčšine prípadov jednoduchá a jasná identifikácia „určujúceho orgánu“ pomocou odkazu na tie – právne a/alebo faktické – okolnosti, z ktorých sa obvykle dá vyvodit' faktický vplyv, ak iné prvky nenaznačujú opak.

Tieto okolnosti je možné analyzovať a klasifikovať podľa týchto troch kategórií situácií, ktoré umožňujú systematický prístup k uvedeným otázkam:

1) Kontrola vyplývajúca z explicitnej právnej moci. Ide tu okrem iného o prípad uvedený v druhej časti definície, t. j. keď prevádzkovateľ alebo osobitné kritériá jeho menovania sú stanovené vnútroštátnymi právnymi predpismi alebo právnymi predpismi Spoločenstva. Explicitné menovanie prevádzkovateľa na základe právnych predpisov nie je časté a obvykle nespôsobuje veľké problémy. V niektorých krajinách sa vo

¹¹ Pozri ďalej interferenciu s pojmami existujúcimi v iných oblastiach práva (napríklad pojem držiteľ práv duševného vlastníctva alebo vedeckého výskumu, alebo zodpovednosť podľa občianskeho práva).

vnútroštátnych právnych predpisoch stanovuje, že verejné orgány sú zodpovedné za spracovanie osobných údajov v kontexte plnenia svojich povinností.

Čoraz častejšie sa však stáva, že zákon nemenuje priamo prevádzkovateľa alebo nestanoví kritéria jeho menovania, ale uloží niekomu úlohu alebo povinnosť zbierať a spracovávať určité údaje. Takýto prípad nastáva napríklad vtedy, keď je subjekt poverený určitými verejnými úlohami (napr. v oblasti sociálneho zabezpečenia), ktoré nie je možné splniť bez zberu aspoň niektorých osobných údajov a tento subjekt s cieľom splniť dané úlohy zavedie register. V tomto prípade funkcia prevádzkovateľa vyplýva zo zákona. Vo všeobecnosti môže zákon verejným alebo súkromným subjektom ukladať povinnosť uchovávať alebo poskytovať určité údaje. Tieto subjekty sa potom za obvyklých podmienok považujú za prevádzkovateľa pri akomkoľvek spracovaní osobných údajov v tomto kontexte.

2) Kontrola vyplývajúca z implicitnej právomoci. Ide o prípad, keď moc určovať nie je explicitne stanovená zákonom a nie je ani priamym následkom explicitných právnych ustanovení, no napriek tomu vyplýva zo spoločných právnych ustanovení alebo zaužívanej právnej praxe v rôznych oblastiach (občianske právo, obchodné právo, pracovné právo atď.). V tomto prípade existujúce tradičné úlohy, ktoré obvykle ukladajú určitú zodpovednosť, pomôžu pri identifikácii prevádzkovateľa: napríklad zamestnávateľ vo vzťahu k údajom o svojich zamestnancoch, vydavateľ vo vzťahu k údajom o predplatiteľoch, združenie vo vzťahu k údajom o svojich členoch alebo prispievateľoch.

Vo všetkých takýchto prípadoch sa moc určovať činnosti spracovania môže považovať za prirodzenú súčasť funkčnej úlohy (súkromnej) organizácie, v konečnom dôsledku zahŕňajúcu aj zodpovednosť z hľadiska ochrany údajov. Z právneho hľadiska by to platilo bez ohľadu na to, či by moc určovať bola zákonom udelená uvedeným právnickým osobám, či by ju vykonávali vhodné orgány konajúce v ich mene alebo fyzická osoba s podobnou úlohou [pozri ďalej vysvetlenie prvého prvku v bode c)]. To isté by platilo aj v prípade verejného orgánu s určitými administratívnymi úlohami v krajine, v ktorej by právne predpisy neboli explicitné vo vzťahu k jeho zodpovednosti za ochranu údajov.

Príklad č. 1: Telekomunikační operátori

Zaujímavý príklad právneho poradenstva pre súkromný sektor sa týka úlohy telekomunikačných operátorov: V odôvodnení 47 smernice 95/46/ES sa vysvetľuje, že „*keď sa prenáša správa, ktorá obsahuje osobné údaje prostredníctvom telekomunikácií alebo pomocou elektronickej pošty, ktorej jediným účelom je doručenie takýchto správ, ten, kto spracovanie riadi, pokiaľ ide o osobné údaje, ktoré sú obsiahnuté v správe, je považovaný za osobu, od ktorej správa pochádza, a nie za osobu, ktorá ponúka služby prenosu; (...) tí, ktorí ponúkajú takéto služby sú považovaní za tých, ktorí spracovanie riadia vo vzťahu k spracovaniu dodatočných osobných údajov nevyhnutných pre činnosť služby*“. Poskytovateľ telekomunikačných služieb by sa mal preto v zásade považovať za prevádzkovateľa iba v súvislosti s prenosom a registráciou údajov, a nie s prenášanými údajmi¹². Toto právne usmernenie zo strany zákonodarcu Spoločenstva je v úplnom súlade s funkčným prístupom uplatňovaným v tomto stanovisku.

¹² Orgán na ochranu údajov sa zaoberal kontrolou v prípade, ktorý iniciovala dotknutá osoba, ktorá sa sťažovala na nevyžiadajúcu e-mailovú reklamu. Vo svojej sťažnosti dotknutá osoba požadovala, aby

3) Kontrola vyplývajúca z faktického vplyvu. Ide o prípad, keď sa zodpovednosť prevádzkovateľa prideliť na základe posúdenia faktických okolností. V mnohých prípadoch takéto posúdenie zahŕňa aj posúdenie zmluvných vzťahov medzi rôznymi zúčastnenými stranami. Toto posúdenie umožňuje pripraviť externé závery, ktorými sa jednej alebo viacerým stranám prideliť úloha a zodpovednosť prevádzkovateľa. Tento postup môže byť užitočný najmä v komplikovaných prostrediach, v ktorých sa často využívajú nové informačné technológie a príslušní aktéri majú často sklon považovať sami seba za „sprostredkovateľov“, a nie za zodpovedných prevádzkovateľov.

Môže nastať situácia, že v zmluve nie je zmienka o tom, kto je prevádzkovateľ, ale obsahuje dostatočné prvky na to, aby zodpovednosť prevádzkovateľa mohla byť pridelená strane, ktorá v tejto súvislosti zjavne plní dominantnú úlohu. Môže sa aj stať, že v zmluve je konkrétne uvedené, kto je prevádzkovateľ. Ak nie je dôvod pochybovať, že to presne zodpovedá skutočnosti, nič nebráni tomu, aby sa plnili podmienky zmluvy. Podmienky zmluvy však nie sú rozhodujúce vo všetkých okolnostiach, pretože by to umožnilo stranám jednoducho prideliť zodpovednosť podľa vlastného usúdenia.

Zo samotnej skutočnosti, že niekto určuje, ako sa osobné údaje spracovávajú, môže vyplývať kvalifikácia prevádzkovateľa údajov, aj keď táto kvalifikácia vzniká mimo rozsahu zmluvného vzťahu, alebo ju zmluva explicitne vylučuje. Jasným príkladom bol prípad SWIFT, keď táto spoločnosť prijala rozhodnutie sprístupniť určité osobné údaje, ktoré boli pôvodne v mene finančných inštitúcií spracované na obchodné účely, aj na účel boja proti financovaniu terorizmu po súdnych výzvach vydaných ministerstvom financií USA.

V prípade pochybností môžu byť pri hľadaní prevádzkovateľa užitočné aj iné elementy ako podmienky zmluvy, napríklad stupeň skutočnej kontroly vykonávanej určitou stranou, obraz poskytnutý dotknutým osobám a dôvodné očakávania dotknutých osôb na základe tejto viditeľnosti [pozri aj ďalej vysvetlenie k tretiemu prvku v bode b)]. Táto kategória je osobitne dôležitá, pretože umožňuje určiť a prideliť zodpovednosť aj v prípadoch protizákonného konania, keď sa skutočné činnosti spracovania môžu vykonávať dokonca proti záujmu a vôli niektorých strán.

Predbežný záver

Prvé dve z týchto kategórií umožňujú v zásade bezpečnejšie označenie určujúceho orgánu a v praxi môžu zahŕňať viac ako 80 % súvisiacich situácií. Formálne právne ustanovenie by však malo byť v súlade s pravidlami ochrany údajov tak, že sa zabezpečí, aby mal určený orgán účinnú kontrolu nad operáciami spracovania, inými slovami, aby právne ustanovenie zodpovedalo skutočnosti.

Kategória č. 3 vyžaduje zložitejšiu analýzu a je pri nej viac pravdepodobné, že povedie k rozdielnym výkladom. Pri vyjasnení problému môžu často pomôcť podmienky zmluvy, nie sú však rozhodujúce za každých okolností. Stále rastie počet aktérov, ktorí sa sami nepovažujú za určujúcich činnosti spracovania, a teda za nesúcich zodpovednosť. Záver na základe faktického vplyvu je v takýchto prípadoch jedinou prípustnou možnosťou.

poskytovateľ komunikačnej siete buď potvrdil alebo odmietol, že bol odosielateľom reklamného e-mailu. Orgán na ochranu údajov skonštatoval, že spoločnosť, ktorá iba poskytuje klientovi prístup do komunikačnej siete, t. j. neinicuje prenos údajov, nevyberá adresy, ani neupravuje informácie, ktoré prenos obsahuje, sa nemôže považovať za prevádzkovateľa údajov.

Otázka zákonnosti tohto spracovania sa bude stále posudzovať vzhľadom na iné články (6 – 8).

Ak nie je možné uplatniť žiadnu z vyššie uvedených kategórií, stanovenie prevádzkovateľa by sa malo považovať za „neplatné“. Orgán, ktorý nemá ani právny ani faktický vplyv na určovanie spôsobu spracovania osobných údajov, sa skutočne nemôže považovať za prevádzkovateľa.

Z formálneho hľadiska existuje úvaha, ktorá podopiera tento prístup – definícia prevádzkovateľa údajov by sa mala považovať za povinné právne ustanovenie, od ktorého strany sa jednoducho nemôžu odchýliť. Zo strategického hľadiska by takéto stanovenie bolo proti účinnému uplatňovaniu právnych predpisov o ochrane údajov a zrušilo by zodpovednosť vyplývajúcu zo spracovania údajov.

III.1.b) Tretí prvok: „účely a prostriedky spracovania“

Tretí prvok predstavuje podstatnú časť kritéria: čo by mala strana určovať, aby sa mohla kvalifikovať ako prevádzkovateľ.

Toto ustanovenie prešlo viacerými vývojovými trendmi. V dohovore č. 108 sa uvádzal účel automatizovaných súborov údajov, kategórie osobných údajov a operácie, ktoré sa s nimi vykonávajú. Komisia prevzala tieto podstatné prvky s menšími jazykovými úpravami a pridala právomoc rozhodovať, ktoré tretie strany môžu mať prístup k údajom. V zmenenom a doplnenom návrhu Komisia vykonala krok vpred tým, že sa definícia presunula od „účelov súboru“ k „účelom a cieľu spracovania“, čím sa statická definícia spojená so súborom zmenila na dynamickú definíciu spojenú s činnosťou spracovania. V zmenenom a doplnenom návrhu sa stále uvádzajú štyri prvky (účely/cieľ, osobné údaje, operácie a tretie strany s prístupom k nim), ktorých počet sa znížil na dva („účely a prostriedky“) až v spoločnej pozícii Rady.

Slovníkové definície hovoria, že „účel“ je „predpokladaný výsledok, ktorý plánujete, alebo ktorý riadi vaše plánované činy“ a „prostriedky“ sú „spôsob dosiahnutia výsledku alebo splnenia cieľa“.

Na druhej strane sa v smernici stanovuje, že údaje musia byť zhromaždené na špecifikované, explicitné a zákonné účely a nebudú sa ďalej spracovávať spôsobmi, ktoré nie sú zlučiteľné s týmito účelmi. Z tohto dôvodu je obzvlášť dôležité určiť „účely“ spracovania a „prostriedky“ na ich splnenie.

Dá sa tiež povedať, že určením účelov a prostriedkov sa dostaneme k postupnému určeniu otázok „prečo“ a „ako“ v súvislosti s určitými činnosťami spracovania. Z tohto hľadiska a so zreteľom na spojenie oboch prvkov existuje potreba poskytnúť určité rady o tom, z akej úrovne vplyvu na otázky „prečo“ a „ako“ môže vyplývať kvalifikácia subjektu ako prevádzkovateľa.

Preto pokiaľ ide o posúdenie určenia účelov a prostriedkov s cieľom prisúdenia úlohy prevádzkovateľa údajov, rozhodujúcou otázkou je, s akým stupňom podrobnosti by mal niekto určovať účely a prostriedky, aby sa mohol považovať za prevádzkovateľa. A v súvislosti s tým, aký je manévrovací priestor, ktorý smernica umožňuje spracovateľovi údajov. Tieto definície sa stávajú osobitne významnými, ak sú do spracovania osobných údajov zapojení viacerí aktéri a je potrebné určiť, ktorý z nich je prevádzkovateľ údajov (sám alebo v spojení s inými) a prípadne, ktorí sa považujú za spracovateľov údajov.

Na účely alebo prostriedky by sa mal klásť rôzny dôraz v závislosti od konkrétneho kontextu, v ktorom sa spracovávanie údajov odohráva.

Potrebný je pragmatický prístup, v ktorom sa bude klásť väčší dôraz na voľné uváženie pri určovaní účelov a voľnosť pri prijímaní rozhodnutí. V týchto prípadoch spočíva otázka v tom, prečo sa spracovanie vykonáva a aká je úloha možných prepojených aktérov, ako sú subdodávateľské spoločnosti: spracovala by subdodávateľská spoločnosť údaje, keby ju o to nepožiadala prevádzkovateľ a za akých podmienok? Spracovateľ by mohol ďalej postupovať podľa všeobecných pokynov, ktoré by sa týkali najmä účelov a nepisovali by veľmi podrobne prostriedky.

Príklad č. 2: Poštový marketing

Spoločnosť ABC uzatvorí zmluvy s rôznymi organizáciami, ktoré majú realizovať jej kampane poštového marketingu a viesť mzdové účtovníctvo. Vydá jasné pokyny (aký marketingový materiál sa má posielat', komu sa má posielat' a komu treba platiť, aké sumy, s akou splatnosťou atď.). Aj keď organizácie majú určitú mieru voľného uváženia (vrátane možnosti výberu softvéru), ich úlohy sú pomerne jasne a presne vymedzené a aj keď zásielková spoločnosť môže ponúknuť rady (napríklad neodporúčať, aby sa pošta posielala v auguste), organizácie sú jasne viazané konať podľa pokynov spoločnosti ABC. Navyše, iba jeden subjekt, spoločnosť ABC, má právo používať spracovávané údaje – všetky ostatné subjekty sa musia spoliehať na právny základ spoločnosti ABC, ak sa spochybní ich právne oprávnenie na spracovanie údajov. V tomto prípade je zrejmé, že spoločnosť ABC je prevádzkovateľom údajov a každá samostatná organizácia sa môže považovať za spracovateľa v súvislosti s konkrétnym spracovávaním údajov, ktoré vykonáva v mene spoločnosti ABC.

Pokiaľ ide o určenie prostriedkov, pojem „prostriedky“ očividne zahŕňa veľmi rozdielne prvky, čo dokazuje aj história tejto definície. V pôvodnom návrhu úloha prevádzkovateľa vyplývala z určenia štyroch prvkov (účelov/cieľa, osobných údajov, operácií a tretích strán s prístupom k nim). Nemôžeme sa domnievať, že konečná formulácia ustanovenia, v ktorej sa uvádzajú iba „účely a prostriedky“, je v rozpore so staršou verziou, pretože niet pochyb, že napríklad prevádzkovateľ musí určiť, ktoré údaje sa budú spracovávať na plánované účely. Z tohto dôvodu musíme konečnú definíciu chápať skôr ako skrátenú verziu, ktorá však obsahuje zmysel staršej verzie. Inými slovami, výraz „prostriedky“ neodkazuje iba na technické spôsoby spracovania osobných údajov, ale aj na otázku „ako“ v súvislosti so spracovaním, ktorá zahŕňa ďalšie otázky ako „ktoré údaje sa majú spracovať“, „ktoré tretie strany majú mať prístup k týmto údajom“, „kedy sa majú údaje vymazať“ atď.

Určenie „prostriedkov“ preto zahŕňa technické aj organizačné otázky, v prípade ktorých sa rozhodnutie môže delegovať na spracovateľov (napríklad „aký hardvér alebo softvér sa má použiť?“) a základné prvky, ktoré tradične a neodmysliteľne podliehajú rozhodnutiu prevádzkovateľa, napríklad „aké údaje sa majú spracovávať?“, „ako dlho sa budú spracovávať?“, „kto k nim bude mať prístup?“ atď.

Z uvedeného vyplýva, že kým určovanie účelu spracovania v každom prípade vedie k tomu, že sa subjekt kvalifikuje ako prevádzkovateľ, určenie prostriedkov znamená kontrolu iba vtedy, ak sa týka základných prvkov prostriedkov.

Z tohto pohľadu je dosť možné, že o technických a organizačných prostriedkoch rozhoduje výlučne spracovateľ údajov.

V týchto prípadoch – ak existuje dobré vymedzenie účelov, ale obmedzené alebo žiadne pokyny týkajúce sa technických alebo organizačných prostriedkov – prostriedky by mali predstavovať odôvodnený spôsob dosiahnutia účelu alebo účelov a prevádzkovateľ údajov by mal byť v plnej miere informovaný o použitých prostriedkoch. Ak by mal zmluvný dodávateľ vplyv na účel a vykonával spracovanie (tiež) vo vlastný prospech, napríklad využívaním získaných osobných údajov na vytvorenie služieb s pridanou hodnotou, bol by prevádzkovateľom (alebo pravdepodobne spoločným prevádzkovateľom) ďalšej činnosti spracovania a z tohto dôvodu by podliehal všetkým povinnostiam platných právnych predpisov o ochrane údajov.

Príklad č. 3: Spoločnosť označená ako spracovateľ údajov, konajúca však ako prevádzkovateľ

Spoločnosť MarketinZ poskytuje služby propagačnej reklamy a priameho marketingu rôznym spoločnostiam. Spoločnosť GoodProductZ uzavrie zmluvu so spoločnosťou MarketinZ, podľa ktorej spoločnosť MarketinZ poskytuje obchodnú reklamu pre zákazníkov spoločnosti GoodProductZ a je označená ako spracovateľ údajov. Spoločnosť MarketinZ sa však rozhodne využiť databázu zákazníkov spoločnosti GoodProducts aj na účel propagácie výrobkov iných zákazníkov. Po tomto rozhodnutí pridať ďalší účel k účelu, za ktorým sa osobné údaje pôvodne prenášali, sa zo spoločnosti MarketinZ stáva prevádzkovateľ údajov v súvislosti s touto operáciou spracovania. Otázka zákonnosti tohto spracovania sa ešte posúdi vzhľadom na ostatné články (6 – 8).

V niektorých právnych systémoch sú rozhodnutia prijaté v súvislosti s bezpečnostnými opatreniami zvlášť dôležité, pretože bezpečnostné opatrenia sa explicitne považujú za základnú črtu, ktorú má definovať prevádzkovateľ. Vzniká tak otázka, ktoré rozhodnutia o bezpečnosti môžu mať za následok to, že sa spoločnosť, ktorá je externým dodávateľom spracovania údajov, kvalifikuje ako prevádzkovateľ.

Predbežný záver

Určenie „účelu“ spracovania je vyhradené pre „prevádzkovateľa“. Nech toto rozhodnutie prijme ktokoľvek, stáva sa (*de facto*) prevádzkovateľom. Určenie „prostriedkov“ spracovania môže prevádzkovateľ delegovať na ďalší subjekt, pokiaľ ide o technické alebo organizačné otázky. Podstatné otázky, ktoré sú nevyhnutné pre základnú zákonnosť spracovania, sú vyhradené pre prevádzkovateľa. Osoba alebo subjekt, ktorý rozhoduje, napríklad ako dlho sa údaje budú uchovávať v pamäti, alebo kto bude mať prístup k spracovávaným údajom, koná ako „prevádzkovateľ“ v súvislosti s touto časťou využitia údajov a preto musí plniť všetky povinnosti prevádzkovateľa.

III.1.c) Prvý prvok: „fyzickú alebo právnickú osobu, alebo akýkoľvek iný orgán“

Prvý prvok definície odkazuje na osobné hľadisko: kto môže byť prevádzkovateľom a tak sa považovať v konečnom dôsledku za zodpovedného za povinnosti vyplývajúce z ustanovení smernice. Táto definícia presne odzrkadľuje formuláciu článku 2 dohovoru č. 108 a nebola predmetom osobitnej diskusie v rozhodovacom procese smernice.

Vzťahuje sa na širokú škálu subjektov, ktoré môžu plniť úlohu prevádzkovateľa, od fyzických po právnické osoby vrátane „akéhokolvek iného orgánu“.

Dôležité je, aby výklad tohto prvku zabezpečoval účinné uplatňovanie smernice tak, že bude uprednostňovať v najväčšej možnej miere jasnú a jednoznačnú identifikáciu prevádzkovateľa za všetkých okolností bez ohľadu na to, či sa vykonalo a uverejnilo formálne vymenovanie.

V prvom rade je dôležité nevzdialiť sa od praxe zaužívanej vo verejnom aj súkromnom sektore v rámci iných oblastí práva, napríklad občianskeho, správneho a trestného práva. Vo väčšine prípadov tieto ustanovenia naznačujú, ktorým osobám alebo orgánom by sa mali zodpovednosti prideliť a v zásade pomáhajú identifikovať prevádzkovateľa údajov.

Zo strategického hľadiska (pokiaľ ide o pridelenie zodpovednosti), aby sa dotknutým osobám zabezpečil stabilnejší a spoľahlivejší referenčný subjekt na uplatnenie ich práv v rámci smernice, by sa mala za prevádzkovateľa skôr považovať spoločnosť alebo orgán ako taký než konkrétna osoba v rámci spoločnosti alebo orgánu. Spoločnosť alebo orgán sa bude považovať za konečne zodpovedného za spracovanie údajov a plnenie povinností vyplývajúcich z právnych predpisov o ochrane údajov, ak neexistujú jasné prvky, ktoré poukazujú na to, že by mala byť zodpovedná fyzická osoba. Vo všeobecnosti by mal platiť predpoklad, že spoločnosť alebo verejný orgán je ako taký zodpovedný za činnosti spracovania, ktoré sa uskutočňujú v rámci jeho činností a rizík.

Niekedy spoločnosti a verejné orgány poveria vykonávaním činností spracovania konkrétnu osobu. Ani v takomto prípade, keď je zabezpečením súladu so zásadami ochrany údajov alebo spracovaním osobných údajov poverená konkrétna fyzická osoba, však nie je táto osoba prevádzkovateľom, ale osobou, ktorá koná v mene právneho subjektu (spoločnosti alebo verejného orgánu), ktorý bude vždy zodpovedný v prípade porušenia zásad v rámci svojej funkcie prevádzkovateľa¹³.

Najmä pre veľké a zložité štruktúry je rozhodujúcim aspektom „riadenia ochrany údajov“ zabezpečiť jasnú zodpovednosť fyzickej osoby zastupujúcej spoločnosť a konkrétne funkčné zodpovednosti v rámci štruktúry, napríklad poverením iných osôb, aby konali ako zástupcovia alebo kontaktné miesta pre dotknuté osoby.

Osobitná analýza je potrebná v prípadoch, keď fyzická osoba konajúca v rámci právnickej osoby používa údaje na vlastné účely mimo rozsahu a možnej kontroly činností právnickej osoby. V tomto prípade by bola príslušná fyzická osoba prevádzkovateľom rozhodnutého spracovania a niesla by zodpovednosť za toto použitie osobných údajov. Pôvodný prevádzkovateľ by si však mohol ponechať určitú zodpovednosť v prípade nového spracovania z dôvodu nedostatočných bezpečnostných opatrení.

Ako už bolo uvedené, úloha prevádzkovateľa je rozhodujúca a osobitne významná, pokiaľ ide o určenie zodpovednosti a uloženie sankcií. Aj keď zodpovednosť a sankcie sú rôzne v jednotlivých členských štátoch, keďže sa ukladajú podľa vnútroštátnych právnych predpisov, niet pochýb o potrebe jasne identifikovať fyzickú alebo právnickú

¹³ Podobná argumentácia sa uplatňuje v súvislosti s nariadením (ES) 45/2001, ktorého článok 2 písm. d) odkazuje na „inštitúciu alebo orgán Spoločenstva, generálne riaditeľstvo, útvar alebo inú organizačnú jednotku“. V praxi dozoru sa ujasnilo, že úradníci inštitúcií a orgánov EÚ menovaní za „prevádzkovateľov“ konajú v mene orgánu, pre ktorý pracujú.

osobu zodpovednú za porušenie právnych predpisov o ochrane údajov, pretože táto identifikácia je základným predpokladom pre účinné uplatňovanie smernice.

Identifikácia „prevádzkovateľa“ z pohľadu ochrany údajov bude v praxi prepojená s právnymi predpismi občianskeho, správneho alebo trestného práva, ktorými sa stanovuje pridelenie zodpovednosti alebo sankcií, ktorých predmetom sa môžu stať právnické alebo fyzické osoby¹⁴.

Občianska zodpovednosť by nemala v tejto súvislosti spôsobovať osobitné problémy, pretože sa v zásade vzťahuje rovnako na právnické ako aj fyzické osoby. Trestná a/alebo správna zodpovednosť sa však podľa vnútroštátnych právnych predpisov niekedy môže vzťahovať iba na fyzické osoby. Ak sú udelené trestné alebo správne sankcie za porušenie pravidiel ochrany údajov podľa príslušných vnútroštátnych právnych predpisov, rovnaké právne predpisy obvykle rozhodnú aj o tom, kto je zodpovedný: ak sa trestná alebo správna zodpovednosť právnických osôb neuzná, takúto zodpovednosť môžu prevziať funkcionári právnických osôb v súlade s osobitnými pravidlami vnútroštátneho práva¹⁵.

Európske právo obsahuje užitočné príklady kritérií pridelenia trestnej zodpovednosti¹⁶, najmä ak je spáchaný trestný čin v prospech právnickej osoby. V takomto prípade sa zodpovednosť môže pripísať akejkolvek osobe, „konajúcej buď samostatne alebo ako súčasť orgánu tejto právnickej osoby, ktorá má vedúce postavenie v rámci právnickej osoby založené na:

- a) oprávnení zastupovať túto právnickú osobu;
- b) právomoci prijímať rozhodnutia v mene tejto právnickej osoby;
- c) právomoci vykonávať kontrolu v rámci tejto právnickej osoby.“

Predbežný záver

Keď zhrnieme uvedené úvahy, môžeme vysloviť záver, že za porušenie pravidiel ochrany údajov je vždy zodpovedný prevádzkovateľ, t. j. právnická osoba (spoločnosť alebo verejný orgán) alebo fyzická osoba formálne identifikovaná podľa kritérií smernice. Ak fyzická osoba pracujúca v rámci spoločnosti alebo verejného orgánu používa údaje na svoje vlastné účely mimo činností spoločnosti, táto osoba sa považuje *de facto* za prevádzkovateľa a ako taká je zodpovedná.

¹⁴ Pozri „komparatívnu štúdiu Komisie o situácii v 27 členských krajinách v súvislosti s rozhodným právom pre mimozmluvné záväzky vyplývajúce z porušenia práva na súkromie a práva na ochranu osobnosti“, február 2009, ktorá je dostupná na tejto adrese: http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf.

¹⁵ Nevyklučuje sa, že vnútroštátne právne predpisy môžu stanovovať trestnoprávnu alebo správnu zodpovednosť nielen pre prevádzkovateľa, ale aj pre akúkoľvek osobu porušujúcu právne predpisy o ochrane údajov.

¹⁶ Pozri napríklad smernicu Európskeho parlamentu a Rady 2008/99/EC z 19. novembra 2008 o ochrane životného prostredia prostredníctvom trestného práva, rámcové rozhodnutie Rady z 13. júna 2002 o boji proti terorizmu. Právne nástroje sa zakladajú buď na článku 29, článku 31 písm. e) a článku 34 ods. 2 písm. b) Zmluvy o Európskej únii alebo zodpovedajú právnym základom pre nástroje používané v prvom pilieri, vyplývajúce z judikatúry Súdneho dvora Európskych spoločenstiev vo veciach C-176/03, KOM/Rada, Zb. 2005, s. I-7879 a C-440/05, KOM/Rada, Zb. 2007, s. I-9097. Pozri aj oznámenie KOM(2005) 583 v konečnom znení.

Príklad č. 4: Tajné monitorovanie zamestnancov

Člen predstavenstva spoločnosti sa rozhodne tajne monitorovať zamestnancov spoločnosti napriek tomu, že toto rozhodnutie nie je formálne schválené predstavenstvom. Spoločnosť by sa mala považovať za prevádzkovateľa a mala by čeliť možným sťažnostiam a zodpovednosti v súvislosti so zamestnancami, ktorých osobné údaje boli zneužitú.

Zodpovednosť spoločnosti vyplýva najmä zo skutočnosti, že ako prevádzkovateľ má povinnosť zabezpečiť dodržiavanie pravidiel bezpečnosti a dôvernosti. Zneužitie funkcionárom spoločnosti alebo jej zamestnancom by sa mohlo považovať za výsledok neprimeraných bezpečnostných opatrení. A to bez ohľadu na to, že v neskoršom štádiu možno považovať za zodpovedného aj člena predstavenstva alebo inú fyzickú osobu v spoločnosti z hľadiska občianskeho práva – aj voči spoločnosti – ako aj z trestnoprávneho hľadiska. Takýto prípad by mohol nastať napríklad vtedy, ak by člen predstavenstva využíval zozbierané údaje na vydieranie zamestnancov na účel získania osobných výhod: musel by sa považovať za „prevádzkovateľa“ a bol by zodpovedný v súvislosti s týmto konkrétnym použitím údajov.

III.1.d) Druhý prvok: „sám, alebo v spojení s inými“

V tomto odseku sa na základe predchádzajúcej analýzy typických črt prevádzkovateľa budeme zaoberať prípadmi, keď sa na spracovaní osobných údajov podieľajú viacerí aktéri. Naozaj rastie počet prípadov, v ktorých v úlohe prevádzkovateľa vystupujú rôzni aktéri a práve na takéto situácie sa vzťahuje definícia stanovená v smernici.

Možnosť, že prevádzkovateľ koná „sám alebo v spojení s inými“ sa v dohovore č. 108 neuvádzala a zaviedol ju až Európsky parlament pred prijatím smernice. Komisia vo svojom stanovisku k pozmeňujúcemu a doplňujúcemu návrhu Európskeho parlamentu uvádza možnosť, že „pri jednej operácii spracovania môže spoločne viacero strán určovať účel a prostriedky spracovania, ktoré sa má vykonať“ a preto sa v takomto prípade „každý prevádzkovateľ musí považovať za viazaného povinnosťami uloženými smernicou s cieľom chrániť fyzické osoby, ktorých údaje sa spracúvajú“.

Stanovisko Komisie neodzrkadľovalo úplne zložitú, ktorá dnes v skutočnosti vládne v oblasti spracovania údajov, pretože bolo zamerané iba na prípad, keď všetci prevádzkovatelia rovnakou mierou určujú a sú rovnakou mierou zodpovední za jednu operáciu spracovania. Realita však potvrdzuje, že toto je iba jeden z rôznych existujúcich druhov „spoločnej kontroly“. Z tohto pohľadu sa výraz „v spojení“ musí vykladať vo význame „spolu s“ alebo „nie samostatne“ v rôznych podobách a kombináciách.

V prvom rade je potrebné poznamenať, že pravdepodobnosť viacerých aktérov zapojených do spracovania osobných údajov je prirodzene spätá s rôznymi druhmi činností, ktoré podľa smernice môžu viesť k „spracovaniu“, ktoré sa na konci dňa stáva predmetom „spoločnej kontroly“. Definícia spracovania stanovená v článku 2 písm. b) smernice nevyklučuje možnosť, že rôzni aktéri sú zapojení do rôznych operácií alebo súborov operácií s osobnými údajmi. Tieto operácie môžu prebiehať súčasne alebo v rôznych fázach.

V takomto zložitom prostredí je ešte dôležitejšie, aby bolo možné ľahko pridelit' úlohy a zodpovednosť s cieľom zabezpečiť, aby výsledkom zložitej spoločnej kontroly nebolo neuskutočniteľné rozdelenie zodpovednosti, ktoré by bránilo účinnosti právnych predpisov o ochrane údajov. Pre množstvo možných konfigurácií žiaľ nie je možné vytvorit' vyčerpávajúci „uzavretý“ zoznam alebo kategorizáciu rôznych druhov „spoločnej kontroly“. Napriek tomu je užitočné poskytnúť aj v tomto kontexte určité usmernenie pomocou niektorých kategórií a príkladov spoločnej kontroly a prostredníctvom niektorých faktických prvkov, z ktorých je možné spoločnú kontrolu odvodiť alebo predpokladať.

Všeobecne platí, že posúdenie spoločnej kontroly by malo odzrkadľovať posúdenie „samostatnej“ kontroly uvedené v bode III.1.a) až c). Rovnako pri posudzovaní spoločnej kontroly by sa mal prijať podstatný a funkčný prístup podľa vyššie uvedeného opisu, zameraný na to, či účely a prostriedky určuje viac ako jedna strana.

Príklad č. 5: Inštalácia bezpečnostných kamier

Majiteľ budovy uzatvorí zmluvu s bezpečnostnou službou, v rámci ktorej bezpečnostná služba v mene prevádzkovateľa nainštaluje niekoľko kamier v rôznych častiach budovy. Účely videodohľadu pomocou kamier a spôsob získavania a ukladania obrazových záznamov určuje výlučne majiteľ budovy, ktorý sa preto musí považovať za jediného prevádzkovateľa tejto operácie spracovania.

Aj v tomto kontexte môžu byť pri posúdení spoločnej kontroly užitočné zmluvné podmienky, no mali by sa vždy porovnať s faktickými okolnosťami vzťahu medzi zmluvnými stranami.

Príklad č. 6: Náboroví pracovníci

Spoločnosť Headhunterz Ltd. pomáha spoločnosti Enterprize Inc. pri náboře nových zamestnancov. V zmluve sa jasne uvádza, že „spoločnosť Headhunterz Ltd. koná v mene spoločnosti Enterprize a v rámci spracovania osobných údajov koná ako spracovateľ údajov. Spoločnosť Enterprize je jediným prevádzkovateľom údajov“. Spoločnosť Headhunterz Ltd. je však v nejednoznačnej pozícii: na jednej strane plní úlohu prevádzkovateľa voči uchádzačom o zamestnanie, na druhej strane sa zaväzuje prijať úlohu spracovateľa konajúceho v mene prevádzkovateľov, ako je spoločnosť Enterprize Inc. a ostatné spoločnosti, ktoré pomocou nej hľadajú nových zamestnancov. Navyše, spoločnosť Headhunterz – so svojou preslávenou službou s pridanou hodnotou „global matchz“ – vyhľadáva vhodných kandidátov podľa životopisov, ktoré prichádzajú priamo do spoločnosti Enterprize, ale aj podľa tých, ktoré už má vo svojej rozsiahlej databáze. Týmto si spoločnosť Headhunterz, ktorá je podľa zmluvy platená iba za skutočne podpísané nové zmluvy, rozširuje porovnávanie pracovných ponúk s uchádzačmi o prácu, čím si zvyšuje svoje príjmy. Na základe uvedeného možno povedať, že napriek zmluvnej kvalifikácii sa spoločnosť Headhunterz Ltd. považuje za prevádzkovateľa a spoločne so spoločnosťou Enterprize Inc. kontroluje prinajmenšom tie súbory operácií, ktoré sa týkajú náboru nových zamestnancov pre Enterprize.

Z tohto pohľadu spoločná kontrola vzniká vtedy, keď rôzne strany v súvislosti s konkrétnymi operáciami spracovania určujú účel alebo tie základné prvky prostriedkov, ktoré charakterizujú prevádzkovateľa [pozri bod III.1.a) až c)].

V kontexte spoločnej kontroly však účasť strán na spoločnom určovaní môže mať rôzne podoby a nemusí byť rovnomerne rozdelená. Ak je aktérov viac, môžu mať veľmi úzky vzťah (napríklad spoločné všetky účely a prostriedky spracovania) alebo voľnejší vzťah (napríklad spoločné iba všetky účely alebo prostriedky alebo ich časti). Preto by sa malo uvažovať o širokej škále typov spoločnej kontroly a podľa toho by sa mali posudzovať aj ich právne následky, aby sa umožnila určitá pružnosť s cieľom vystihnúť rastúcu zložitosť súčasnej skutočnosti v oblasti spracovania údajov.

Na základe týchto súvislostí je nevyhnutné riešiť rôzne stupne interakcie alebo vzájomného prepojenia viacerých strán pri spracovaní osobných údajov.

V prvom rade, zo samotnej skutočnosti, že na spracovaní osobných údajov spolupracujú viaceré subjekty (napríklad formou reťazca) nemusí vždy vyplývať, že ide o spoločných prevádzkovateľov, pretože výmena údajov medzi dvomi stranami bez spoločných účelov alebo prostriedkov v spoločnom súbore operácií by sa mala považovať len za presun údajov medzi samostatnými prevádzkovateľmi.

Príklad č. 7: Cestovná agentúra (1)

Cestovná agentúra posielala osobné údaje svojich zákazníkov leteckej spoločnosti a hotelovému reťazcu s cieľom rezervácie miest v rámci cestovného balíka. Letecká spoločnosť a hotel potvrdia požadované voľné miesta a izby. Cestovná agentúra vystaví svojim zákazníkom cestovné dokumenty a poukážky. V tomto prípade sú cestovná agentúra, letecká spoločnosť a hotel traja rôzni prevádzkovatelia údajov a všetci traja podliehajú povinnostiam ochrany údajov v súvislosti s vlastným spracovaním osobných údajov.

Posúdenie sa však môže zmeniť, ak by sa rôzni aktéri rozhodli vytvoriť spoločnú infraštruktúru pre svoje vlastné individuálne účely. Keď pri vytvorení tejto infraštruktúry aktéri určujú základné prvky prostriedkov, ktoré sa majú použiť, kvalifikujú sa ako spoloční prevádzkovatelia údajov – v akomkoľvek prípade v tejto súvislosti – aj keď nemusia sledovať rovnaké účely.

Príklad č. 8: Cestovná agentúra (2)

Cestovná agentúra, hotelový reťazec a letecká spoločnosť sa rozhodnú vytvoriť spoločnú internetovú platformu s cieľom zlepšiť svoju spoluprácu pri manažmente cestovných rezervácií. Dohodnú sa na dôležitých prvkoch prostriedkov, ktoré sa majú použiť, napríklad, aké údaje sa majú ukladať, ako sa budú prideliť a potvrdzovať rezervácie a kto bude mať prístup k uloženým informáciám. Navyše sa rozhodnú spoločne využívať údaje o svojich zákazníkoch s cieľom vykonávať integrované marketingové akcie.

V tomto prípade cestovná agentúra, letecká spoločnosť a hotelový reťazec budú mať spoločnú kontrolu nad spôsobom spracovania osobných údajov vlastných zákazníkov a preto budú spoločnými prevádzkovateľmi v súvislosti s operáciami spracovania týkajúcimi sa spoločnej internetovej rezervačnej platformy. Každý z nich si však zachová výlučnú kontrolu nad ostatnými činnosťami spracovania, napríklad činnosťami súvisiacimi s riadením ľudských zdrojov.

V niektorých prípadoch rôzni aktéri spracúvajú rovnaké osobné údaje po sebe. V týchto prípadoch je pravdepodobné, že na mikroúrovni sa rôzne operácie spracovania v rámci reťazca zdajú byť oddelené, pretože každá operácia môže mať iný účel. Je však potrebné overiť, či by sa tieto operácie spracovania nemali na makroúrovni považovať za „súbor operácií“, ktoré sledujú spoločný účel alebo používajú spoločne definované prostriedky.

Nasledujúce dva príklady objasňujú túto myšlienku pomocou dvoch rôznych možných scenárov.

Príklad č. 9: Prenos údajov o zamestnancoch daňovému orgánu

Spoločnosť XYZ zbiera a spracúva osobné údaje svojich zamestnancov na účel riadenia miezd, úloh, zdravotného poistenia atď. Zákon jej zároveň ukladá povinnosť posielat' všetky údaje o mzdách daňovému orgánu s cieľom posilniť daňovú kontrolu.

V tomto prípade napriek tomu, že spoločnosť XYZ a daňový orgán spracúvajú rovnaké údaje o mzdách, absencia spoločných účelov alebo prostriedky v súvislosti s týmto spracovaním údajov majú za následok kvalifikáciu oboch subjektov ako dvoch samostatných prevádzkovateľov údajov.

Príklad č. 10: Finančné transakcie

Zoberme si pre zmenu prípad banky, ktorá na uskutočňovanie svojich finančných transakcií využíva služby doručovateľa finančných správ. Banka a doručovateľ sa dohodnú na prostriedkoch spracovania finančných údajov. Spracovanie osobných údajov týkajúcich sa finančných transakcií vykonáva v prvej fáze finančná inštitúcia a až v neskoršej fáze doručovateľ finančných informácií. Napriek tomu, že na mikroúrovni každý z týchto dvoch subjektov sleduje vlastný účel, na makroúrovni sú rôzne fázy, účely a prostriedky spracovania úzko prepojené. V tomto prípade je možné banku a doručovateľa správ považovať za spoločných prevádzkovateľov.

Existujú ďalšie prípady, v ktorých rôzni zapojení aktéri spoločne určujú, v niektorých prípadoch v rôznom rozsahu, účely a/alebo prostriedky operácie spracovania.

Existujú prípady, keď každý prevádzkovateľ je zodpovedný iba za časť spracovania, ale informácie sa spájajú a spracúvajú pomocou platformy.

Príklad č. 11: Portály elektronickej štátnej správy

Portály elektronickej štátnej správy konajú ako sprostredkovatelia medzi občanmi a jednotkami štátnej správy: portál prenáša požiadavky občanov a uchováva dokumenty jednotky štátnej správy, kým si ich občania nevyžiadajú. Každá jednotka štátnej správy zostáva prevádzkovateľom údajov spracovaných na jej vlastné účely. Za prevádzkovateľa je však možné považovať aj samotný portál. Portál v skutočnosti spracúva (t. j. zbiera a prenáša príslušnej jednotke) žiadosti občanov ako aj verejné dokumenty (t. j. uchováva ich a riadi prístup k týmto dokumentom, napr. ich stiahnutie občanmi) na ďalšie účely (podpora služieb elektronickej štátnej správy), ako sú účely pôvodného spracovania údajov každou jednotkou štátnej správy. Títo prevádzkovatelia musia okrem iných povinností zabezpečiť, aby bol systém prenosu osobných údajov od používateľa po systém štátnej správy bezpečný, pretože na makroúrovni je tento prenos nevyhnutnou súčasťou súboru operácií spracovania vykonávaných prostredníctvom portálu.

Ďalšou možnou štruktúrou je „prístup na základe pôvodu“, ktorý vzniká vtedy, keď je každý prevádzkovateľ zodpovedný za údaje, ktoré zavádza do systému. Takýto prípad nastáva napríklad pri niektorých celoeurópskych databázach EÚ, v ktorých kontrola – a teda aj povinnosť konať na žiadosť o prístup a opravu – sa prideľuje na základe vnútroštátneho pôvodu osobných údajov.

Ďalší zaujímavý scenár predstavujú sociálne siete online.

Príklad č. 12: Sociálne siete

Poskytovatelia služby sociálnych sietí online poskytujú komunikačné platformy online, ktoré umožňujú jednotlivcom uverejňovať a vymieňať si informácie s inými používateľmi. Títo poskytovatelia služby sú prevádzkovateľmi údajov, pretože určujú účely a prostriedky spracovania týchto informácií. Používatelia takýchto sietí, ktorí uploadujú aj osobné údaje tretích strán, by sa kvalifikovali ako prevádzkovatelia za predpokladu, že ich činnosti nepodliehajú takzvanej „domácej výnimke“¹⁷.

Po analýze prípadov, v ktorých rôzne subjekty spoločne určujú iba časť účelov a prostriedkov, spočíva veľmi jasne vymedzený a bezproblémový prípad v tom, že viaceré subjekty spoločne určujú a používajú všetky účely a prostriedky činností spracovania, na základe čoho vzniká plnoprávna spoločná kontrola.

V tomto prípade je ľahké určiť, kto je zodpovedný a má právomoc zabezpečovať práva dotknutých osôb, ako aj povinnosť plniť požiadavky ochrany údajov. Úloha určiť, ktorý prevádzkovateľ je kompetentný a zodpovedný a za ktoré povinnosti a práva dotknutých osôb, sa však stáva omnoho zložitejšou v tom prípade, ak sledovanie spoločných účelov a použitie spoločných prostriedkov spracovania je medzi rôznymi spoločnými prevádzkovateľmi nerovnomerne rozdelené.

Potreba ujasniť rozdelenie kontroly

V prvom rade je potrebné zdôrazniť, že najmä v prípadoch spoločnej kontroly, neschopnosť priamo plniť všetky povinnosti prevádzkovateľa (zabezpečovať informácie, prístupové právo atď.) nevylučuje možnosť, že sa príslušný subjekt nachádza vo funkcii prevádzkovateľa. Môže sa stať, že v praxi by tieto povinnosti v mene prevádzkovateľa ľahko dokázali splniť iné strany, ktoré majú niekedy bližšie k dotknutej osobe. Prevádzkovateľ však v každom prípade v konečnom dôsledku zostáva zodpovedným za svoje povinnosti a za každé ich porušenie.

Podľa predchádzajúceho textu, ktorý Komisia predložila počas procesu prijímania smernice, by z prístupu k určitým osobným údajom vyplývala funkcia (spoločného) prevádzkovateľa týchto údajov. Táto formulácia sa však nedostala do konečného znenia a skúsenosti dokazujú, že na jednej strane, z prístupu k údajom ako takého nevyplýva kontrola, kým na druhej strane, prístup k údajom nie je nevyhnutnou podmienkou pre funkciu prevádzkovateľa. Z tohto dôvodu v zložitých systémoch s viacerými aktérmi môžu prístup k osobným údajom a práva dotknutých osôb zabezpečovať rôzni aktéri na rôznych stupňoch.

¹⁷ Pokiaľ ide o ďalšie podrobnosti a príklady, pozri stanovisko 5/2009 pracovnej skupiny zriadenej podľa článku 29 k sociálnym sieťam online, prijaté 12. júna 2009 (WP 163).

So zodpovednosťou prevádzkovateľov súvisia aj právne následky, ktoré vyvolávajú najmä otázku, či zo „spoločnej kontroly“ stanovenej smernicou vždy vyplýva spoločná a nerozdielna zodpovednosť. V článku 26 o zodpovednosti sa používa výraz „prevádzkovateľ“ v jednotnom čísle, čo by mohlo naznačovať kladnú odpoveď. Ak sa už spomínalo, v skutočnosti môžu nastať rôzne spôsoby konania „v spojení s“, t. j. „spolu s“. Za určitých okolností to môže viesť k spoločnej a nerozdielnej zodpovednosti, nie je to však pravidlo: v mnohých prípadoch môžu byť rôzni prevádzkovatelia kompetentní – a teda aj zodpovední – za spracovanie osobných údajov v rôznych fázach a stupňoch.

Základom by malo byť zabezpečiť, aby aj v zložitých prostrediach spracovania údajov, v ktorých pri spracovaní osobných údajov plnia určitú úlohu rôzni prevádzkovatelia, boli dodržiavanie pravidiel ochrany údajov a zodpovednosť za možné porušenie týchto pravidiel jasne pridelené s cieľom zabrániť tomu, aby sa znížila ochrana osobných údajov alebo aby vznikol „negatívny konflikt kompetencií“ a právne medzery, keďže niektoré povinnosti alebo práva vyplývajúce zo smernice nie sú zabezpečené žiadnou zo strán.

V týchto prípadoch je viac ako pri iných dôležité, aby sa dotknutým osobám poskytlo jasné informačné oznámenie, v ktorom sa vysvetlia rôzne fázy a aktéri spracovania. Ďalej by sa malo ujasniť, či je každý prevádzkovateľ kompetentný na plnenie všetkých práv dotknutých osôb alebo ktorý prevádzkovateľ je zodpovedný za ktoré právo.

Príklad č. 13: Banky a združené informačné databázy o neplatiacich zákazníkoch

Viacere banky môžu vytvoriť spoločnú „databázu informácií“ – ak to umožňujú vnútroštátne právne predpisy – pričom každá banka prispieva informáciami (údajmi) o neplatiacich zákazníkoch a všetky banky majú prístup k celému objemu informácií. Niektoré právne systémy stanovujú, že všetky žiadosti dotknutých osôb, napríklad o prístup alebo odstránenie, sa predkladajú iba v jednom „vstupnom bode“, teda poskytovateľovi. Poskytovateľ je zodpovedný za nájdenie správneho prevádzkovateľa a zorganizovanie poskytnutia riadnych odpovedí dotknutej osobe. Identita poskytovateľa je zverejnená v registri spracovania údajov. V iných jurisdikciách môžu takéto databázy informácií prevádzkovať samostatné právnické osoby ako prevádzkovateľ, zatiaľ čo žiadosti o prístup vybavujú zúčastnené banky konajúce ako jeho sprostredkovateľ.

Príklad č. 14: Behaviorálna reklama

Behaviorálna reklama využíva informácie zozbierané o správaní jednotlivca pri prehliadaní webu (napr. navštívené stránky alebo vyhľadávané slová) s cieľom vybrať reklamy, ktoré sa tomuto jednotlivcovi neskôr zobrazia. Vydavatelia, ktorí veľmi často prenajímajú reklamné miesta na svojich webových lokalitách a poskytovatelia reklamných sietí, ktorí zaplňajú tieto miesta cielenou reklamou, môžu zbierať a vymieňať si informácie o používateľoch v závislosti od konkrétnych zmluvných podmienok.

Z hľadiska ochrany údajov sa vydavateľ považuje za nezávislého prevádzkovateľa, keďže zbiera osobné údaje od používateľa (profil používateľa, IP adresu, lokalizáciu, jazyk operačného systému atď.) na svoje vlastné účely. Poskytovateľ reklamnej siete je tiež prevádzkovateľ, keďže určuje účely (monitorovanie používateľov na webových lokalitách) alebo základné prostriedky spracovania údajov. V závislosti od podmienok

spolupráce medzi vydavateľom a poskytovateľom reklamnej siete, ak napríklad vydavateľ umožní prenos osobných údajov poskytovateľovi reklamnej siete, napr. aj prostredníctvom presmerovania používateľa na webovú stránku poskytovateľa reklamnej siete, mohli by byť spoločnými prevádzkovateľmi v súvislosti so súborom operácií spracovania, ktoré vedú k behaviorálnej reklame.

Vo všetkých prípadoch spoloční prevádzkovatelia musia zabezpečiť aby im zložitosť a technické podrobnosti systému behaviorálnej reklamy nebránili v nájdení vhodných spôsobov dodržiavania povinností prevádzkovateľov a zabezpečili práva dotknutých osôb. Týka sa to najmä:

- *informácií* pre používateľa o skutočnosti, že jeho údaje sú sprístupnené tretej strane: toto môže účinnejšie vykonať vydavateľ, ktorý je hlavným sprostredkovateľom používateľa,
- a podmienok *prístupu* k osobným údajom: spoločnosť poskytujúca reklamnú sieť musí odpovedať na otázky používateľov o spôsobe vykonávania cieľenej reklamy na základe údajov o používateľoch a musí vyhovieť žiadostiam o opravu a vymazanie.

Navyše, vydavatelia a poskytovatelia reklamnej siete môžu podliehať ďalším povinnostiam vyplývajúcim z občianskeho práva a zákonov na ochranu spotrebiteľa, vrátane práva v oblasti občianskoprávných deliktov a nekalých obchodných praktík.

Predbežný záver

Strany konajúce spoločne disponujú určitou mierou flexibility pri rozdeľovaní a pridelovaní povinností a zodpovedností medzi sebou, pokiaľ zaistia úplné dodržiavanie právnych predpisov. Pravidlá o spôsobe vykonávania spoločnej zodpovednosti by mali v zásade určiť prevádzkovatelia. Aj v tomto prípade by sa však mali zohľadniť faktické okolnosti s cieľom posúdiť, či dohodnuté podmienky zodpovedajú realite príslušného spracovania údajov.

Z tohto hľadiska by sa mala v posúdení spoločnej kontroly zohľadniť na jednej strane nevyhnutnosť zabezpečiť úplné dodržiavanie pravidiel ochrany osobných údajov a na druhej strane skutočnosť, že zvýšenie počtu prevádzkovateľov môže viesť aj k neželanej zložitosti a možnému nedostatku jasnosti pridelenia zodpovednosti. Vzniklo by tak riziko, že celé spracovanie bude pre nedostatočnú transparentnosť nezákonné a porušila by sa zásada spravodlivého spracovania.

Príklad č. 15: Platformy pre spravovanie zdravotných údajov

V členskom štáte verejný orgán zriadi vnútroštátnu ústredňu riadiacu výmenu údajov pacientov medzi poskytovateľmi zdravotnej starostlivosti. Množstvo prevádzkovateľov – desaťtisíce – má za následok, že v takejto neprehľadnej situácii pre dotknuté osoby (pacientov) by mohla byť ohrozená ochrana ich práv. Pre dotknuté osoby by skutočne nebolo jasné, na koho sa majú obrátiť so sťažnosťou, otázkou a žiadosťou o informácie, opravu alebo prístup k osobným údajom. Verejný orgán je navyše zodpovedný za skutočný spôsob spracovania a jeho využívania. Tieto prvky vedú k záveru, že verejný orgán, ktorý zriadil ústredňu, sa bude považovať za spoločného prevádzkovateľa ako aj kontaktnú osobu pre žiadosti dotknutých osôb.

Na základe týchto súvislostí možno tvrdiť, že spoločná a neoddeliteľná zodpovednosť všetkých zúčastnených strán by sa mala považovať ako prostriedok odstránenia neistoty, a preto by sa mala prijímať iba vtedy, ak zúčastnené strany nevytvorili alternatívne, jasné a rovnako účinné pridelenie povinností a zodpovednosti, alebo ak jasne nevyplýva z faktických okolností.

III.2. Vymedzenie pojmu spracovateľ

Pojem spracovateľ nebol stanovený v dohovore č. 108. Úloha spracovateľa sa prvýkrát uznáva v prvom návrhu Komisie, ale bez zavedenia pojmu s cieľom „zabrániť situáciám, v ktorých spracovanie treťou stranou v mene prevádzkovateľa súboru má účinok zníženia úrovne ochrany dotknutej osoby“. Až v zmenenom a doplnenom návrhu Komisie a neskôr v návrhu Európskeho parlamentu sa pojem spracovateľ uvádza explicitne a nezávisle, aby nadobudol súčasnú podobu uvedenú v spoločnej pozícii Rady.

Ako pri definícii pojmu prevádzkovateľ, aj definícia pojmu spracovateľ zahŕňa širokú škálu aktérov, ktorí môžu plniť úlohu spracovateľa („... fyzickú alebo právnickú osobu, štátny orgán, agentúru alebo akýkoľvek iný orgán ...“).

Existencia spracovateľa závisí od rozhodnutia, ktoré prijíma prevádzkovateľ, ktorý sa môže rozhodnúť spracúvať údaje v rámci svojej organizácie, napríklad pomocou zamestnancov oprávnených spracovávať údaje pod jeho priamym dohľadom [pozri *a contrario* článok 2 písm. f)], alebo poveriť všetkými alebo časťou činností spracovania externú organizáciu, t. j. – ako sa navrhuje v odôvodnení zmeneného a doplneného návrhu Komisie – „právne samostatnú osobu konajúcu v jeho mene“.

Preto dve základné podmienky kvalifikácie spracovateľa spočívajú na jednej strane v tom, že musí byť samostatnou právnickou osobou vo vzťahu k prevádzkovateľovi a na druhej strane, musí spracovávať osobné údaje v jeho mene. Táto činnosť spracovania môže byť obmedzená na veľmi konkrétnu úlohu či kontext alebo môže byť všeobecnejšia a rozšírená.

Úloha spracovateľa navyše nevyplýva z povahy subjektu, ktorý spracúva údaje, ale z jeho konkrétnych činností v určitom kontexte. Inak povedané, ten istý subjekt môže konať ako prevádzkovateľ v súvislosti s určitými operáciami spracovania a zároveň ako spracovateľ v súvislosti s inými operáciami a kvalifikácia prevádzkovateľa alebo spracovateľa sa musí posudzovať s ohľadom na konkrétne súbory údajov alebo operácií.

Príklad č. 16: Poskytovatelia služieb webového servera

Poskytovateľ internetového pripojenia, ktorý poskytuje služby webového servera je v zásade spracovateľ osobných údajov zverejňovaných online jeho zákazníkmi, ktorí využívajú tohto poskytovateľa na služby webového servera a údržby svojich stránok. Avšak keď poskytovateľ ďalej spracúva údaje uvedené na webových lokalitách na vlastné účely, potom je prevádzkovateľom údajov vzhľadom na toto konkrétne spracovanie. Táto analýza je iná ako analýza poskytovateľa internetového pripojenia, ktorý poskytuje služby elektronickej pošty alebo prístupu na internet (pozri aj príklad č. 1: telekomunikační operátori).

Najdôležitejším prvkom je ustanovenie, že spracovateľ koná „...v mene prevádzkovateľa...“. Výraz „konať v mene“ znamená slúžiť záujmu niekoho iného a pripomína právny pojem „poverenie“. V prípade právnych predpisov o ochrane údajov

je spracovateľ prizvaný, aby vykonával pokyny, ktoré mu dáva prevádzkovateľ prinajmenšom v súvislosti s účelom spracovania a základnými prvkami prostriedkov.

Z tohto hľadiska o zákonnosti činnosti spracovania údajov vykonávanej spracovateľom rozhoduje mandát od prevádzkovateľa. Spracovateľ, ktorý prekročí svoj mandát a získa významnú úlohu pri určovaní účelov alebo základných prostriedkov spracovania, je (spoločným) prevádzkovateľom, a nie spracovateľom. Otázka zákonnosti tohto spracovania sa stále bude posudzovať v zmysle ďalších článkov (6 – 8). Z poverenia však tiež môže vyplývať určitý stupeň voľnosti uváženia v súvislosti s tým, ako najlepšie slúžiť záujmom prevádzkovateľa, čo spracovateľovi umožňuje vybrať si najvhodnejšie technické a organizačné prostriedky.

Príklad č. 17: Outsourcing poštových služieb

Súkromné orgány poskytujú poštové služby v mene (verejných) agentúr – napríklad posielanie rodinných alebo materských príspevkov v mene národnej agentúry sociálneho zabezpečenia. V takomto prípade orgán na ochranu údajov uviedol, že príslušné súkromné orgány by mali byť menované ako spracovatelia, keďže ich úloha, hoci vykonávaná s určitým stupňom nezávislosti, bola obmedzená iba na časť operácií spracovania potrebných na účely určené prevádzkovateľom údajov.

S cieľom zabezpečiť, aby outsourcing a poverenie nevedli k zníženiu štandardu ochrany údajov, smernica obsahuje dve ustanovenia, ktoré sa konkrétne venujú spracovateľovi a veľmi podrobne vymedzujú jeho povinnosti v súvislosti s dôvernosťou a bezpečnosťou.

– V článku 16 sa stanovuje, že samotný spracovateľ, ako aj akákoľvek osoba konajúca v jeho právomoci, ktorá má prístup k osobným údajom, nesmie tieto údaje spracovať s výnimkou toho, keď koná na základe pokynov prevádzkovateľa.

– V článku 17 sa vo vzťahu k bezpečnosti spracovania stanovuje potreba zmluvy alebo záväzného právneho aktu, ktorým sa upravia vzťahy medzi prevádzkovateľom údajov a spracovateľom údajov. Táto zmluva musí mať písomnú formu na účely dokazovania a musí mať minimálny obsah, v ktorom sa stanoví najmä podmienka, že spracovateľ údajov koná výlučne na základe pokynov prevádzkovateľa a vykonáva technické a organizačné opatrenia na primeranú ochranu osobných údajov. Táto zmluva by mala obsahovať dostatočne podrobný opis mandátu spracovateľa.

V tejto súvislosti treba poznamenať, že v mnohých prípadoch poskytovatelia služieb špecializovaní na určité spracovanie údajov (napríklad výplatu miezd) predložia prevádzkovateľom údajov na podpísanie štandardnej zmluvy o poskytovaní služieb, čím sa *de facto* stanoví určitý štandardný spôsob spracovania osobných údajov¹⁸. Avšak skutočnosť, že zmluvu a jej podrobné obchodné podmienky pripraví poskytovateľ služieb a nie prevádzkovateľ, nie je *sama osebe* dostatočným základom, podľa ktorého je možné dospieť k záveru, že poskytovateľ služieb by sa mal považovať za prevádzkovateľa, keďže prevádzkovateľ slobodne prijal zmluvné podmienky, čím za ne prevzal plnú zodpovednosť.

Rovnako, nerovnováha zmluvných právomocí malého prevádzkovateľa údajov vo vzťahu k veľkým poskytovateľom služieb by sa nemala považovať za odôvodnenie, na

¹⁸ Vypracovanie podmienok zmluvy poskytovateľom služby nemá dosah na skutočnosť, že základné hľadiská spracovania opísané v bode III.1.b) určuje prevádzkovateľ.

základe ktorého môže prevádzkovateľ prijať ustanovenia a podmienky zmlúv, ktoré nie sú v súlade s právnymi predpismi o ochrane údajov.

Príklad č. 18: E-mailové platformy

Pán John Smith hľadá e-mailovú platformu, ktorú by mohol využívať on a jeho piati zamestnanci. Zistí, že vhodná platforma priaznivá pre používateľa – a aj jediná ponúkaná zadarmo – uchováva osobné údaje veľmi dlhý čas a prenáša ich do tretích krajín bez primeraných záruk. Navyše zmluvné podmienky majú charakter „ber, alebo nechaj tak“.

V tomto prípade by si mal pán Smith nájsť iného poskytovateľa alebo – v prípade predpokladaného nesúladu iných poskytovateľov s pravidlami ochrany údajov alebo nedostupnosti vhodných poskytovateľov na trhu – by mal túto záležitosť postúpiť príslušným orgánom, napríklad orgánom na ochranu údajov, ochranu spotrebiteľa a protimonopolnému úradu atď.

Skutočnosť, že smernica vyžaduje písomnú zmluvu na zaistenie bezpečnosti spracovania, neznamená, že nemôžu existovať vzťahy medzi prevádzkovateľmi alebo spracovateľmi bez predchádzajúcich zmlúv. Z tohto pohľadu nie je zmluva ani podstatná, ani rozhodujúca, aj keď môže pomôcť lepšie pochopiť vzťahy medzi stranami¹⁹. Preto sa aj v tomto prípade uplatní funkčný prístup, v ktorom sa analyzujú faktické prvky vzťahov medzi rôznymi subjektmi a spôsob, akým sa určujú účely a prostriedky spracovania. Ak sa zdá, že existuje vzťah medzi prevádzkovateľom a spracovateľom, tieto strany sú povinné uzatvoriť zmluvu podľa príslušných zákonov (porovnaj článok 17 smernice).

Pluralita spracovateľov

Čoraz častejšie sa stáva, že na spracovanie osobných údajov prevádzkovateľ využíva viacerých spracovateľov údajov prostredníctvom outsourcingu. Títo spracovatelia môžu mať priamy vzťah s prevádzkovateľom údajov, alebo môžu byť subdodávatelia, ktorých spracovatelia poverili časťou činností spracovania, ktoré im boli zverené.

Tieto zložité (viacúrovňové alebo rozptýlené) štruktúry spracovania osobných údajov sa príchodom nových technológií rozmáhajú a niektoré vnútroštátne právne predpisy na ne priamo odkazujú. Žiadne ustanovenie smernice nebráni tomu, aby sa so zreteľom na organizačné požiadavky viaceré subjekty mohli označovať za spracovateľov údajov alebo (sub-)spracovateľov, a to aj na základe ďalšieho rozdelenia príslušných úloh. Všetci z nich však musia dodržiavať pokyny, ktoré im dáva prevádzkovateľ údajov v súvislosti s vykonávaním spracovania.

¹⁹ V niektorých prípadoch však existencia písomnej zmluvy môže predstavovať nevyhnutnú podmienku, aby sa daný subjekt v určitých situáciách automaticky kvalifikoval ako spracovateľ. Napríklad v Španielsku správa o telefonických centrách definuje ako spracovateľov všetky telefonické centrá v tretích krajinách, ak dodržiavajú zmluvu. Platí to dokonca aj v prípade, keď zmluvu pripravil spracovateľ a prevádzkovateľ sa jej jednoducho „pridržiava“.

Príklad č. 19: Grid computing

Rozsiahle výskumné infraštruktúry čoraz častejšie využívajú distribučné výpočtové prostriedky, najmä gridy (siete), s cieľom zisku z hľadiska výpočtovej a úložnej kapacity. Gridy sú nainštalované v rôznych výskumných infraštruktúrach zriadených v rôznych krajinách. Európsky grid môže pozostávať napríklad z vnútroštátnych gridov, ktoré má na starosti vnútroštátny orgán. Pre tento európsky grid však nemusí existovať ústredný orgán zodpovedný za jeho fungovanie. Výskumníci využívajúci takýto grid nedokážu obvykle zistiť, kde presne sa ich údaje spracúvajú, a teda, kto je zodpovedný spracovateľ údajov (ešte zložitejší prípad nastáva, ak sa infraštruktúry gridov nachádzajú v tretích krajinách). Ak by infraštruktúra gridov používala údaje neoprávneným spôsobom, táto strana sa môže považovať za prevádzkovateľa údajov, ak nekoná v mene výskumníkov.

Strategickou úlohou v tomto prípade je – pri pluralite aktérov zapojených do procesu – zabezpečiť, aby povinnosti a zodpovednosť vyplývajúca z právnych predpisov o ochrane údajov bola jasne pridelená, a nie rozptýlená v reťazci outsourcingu/subdodávateľstva. Inými slovami, je potrebné zabrániť vytvoreniu reťazca (sub-)spracovateľov, ktorý by obmedzil účinnú kontrolu, alebo jej dokonca bránil, rovnako ako jasnej zodpovednosti za činnosti spracovania, ak zodpovednosti rôznych strán v reťazci nie sú jasne stanovené.

Z tohto hľadiska rovnako, ako bolo uvedené v bode III.1.b) – kým nie je nevyhnutné, aby prevádzkovateľ vymedzil a súhlasil so všetkými podrobnosťami týkajúcimi sa prostriedkov používaných na splnenie plánovaných účelov – stále je však potrebné, aby bol aspoň informovaný o hlavných prvkoch štruktúry spracovania (napríklad o zapojených subjektoch, bezpečnostných opatreniach, zárukách pri spracovaní v tretích krajinách atď.), aby si udržal pozíciu, v ktorej má kontrolu nad údajmi spracúvanými v jeho mene.

Netreba zabúdať, že kým smernica ukladá zodpovednosť prevádzkovateľovi, nebráni tomu, aby sa vo vnútroštátnych predpisoch o ochrane údajov stanovilo, že v určitých prípadoch by sa navyše za zodpovedného mal považovať aj spracovateľ.

Niektoré kritériá môžu byť užitočné pri určení kvalifikácie rôznych zapojených subjektov:

- úroveň predchádzajúcich pokynov vydaných prevádzkovateľom údajov, ktorá rozhoduje o manévrovacích možnostiach spracovateľa údajov,
- spôsob, akým prevádzkovateľ údajov monitoruje výkon služby. Neustály a dôsledný dohľad prevádzkovateľa s cieľom zabezpečiť dôsledné dodržiavanie pokynov a zmluvných podmienok spracovateľom naznačuje, že prevádzkovateľ má stále plnú a výlučnú kontrolu nad operáciami spracovania,
- viditeľnosť/obraz, ktorý prevádzkovateľ poskytuje dotknutej osobe a očakávaní dotknutých osôb na základe tejto viditeľnosti.

Príklad č. 20: Telefonické kontaktné centrá

Prevádzkovateľ údajov využíva na niektoré svoje operácie telefonické kontaktné centrum pomocou outsourcingu a tomuto centru dá pokyn, aby sa pri telefonovaní klientom prevádzkovateľa údajov predstavovalo identitou prevádzkovateľa údajov. V tomto prípade očakávania klientov a spôsob, akým sa im prevádzkovateľ predstavuje prostredníctvom outsourcingovej spoločnosti, vedú k záveru, že outsourcingová spoločnosť koná ako spracovateľ údajov pre (v mene) prevádzkovateľa.

- Odborné znalosti strán: v určitých prípadoch tradičné postavenie a odborné znalosti poskytovateľa služieb plnia rozhodujúcu úlohu, z ktorých môže vyplývať jeho kvalifikácia ako prevádzkovateľa údajov.

Príklad č. 21: Advokáti

Advokát zastupuje svojho klienta na súde a v súvislosti s týmto poslaním spracúva osobné údaje týkajúce sa klientovho prípadu. Právny základ pre využitie potrebných informácií je mandát od klienta. Tento mandát však nie je zameraný na spracovanie údajov, ale na zastupovanie na súde a pre túto činnosť majú takéto profesie tradične vlastný právny základ. Z tohto dôvodu sa takéto profesie považujú za nezávislých „prevádzkovateľov“, keď spracúvajú údaje v priebehu právneho zastupovania svojich klientov.

V inom kontexte môže byť rozhodujúce aj bližšie posúdenie prostriedkov použitých na splnenie účelov.

Príklad č. 22: Webová lokalita „Straty a nálezy“

Webová lokalita „Straty a nálezy“ bola predstavená iba ako spracovateľ, pretože tí, ktorí uverejňujú stratené veci by mali určovať obsah informácií a teda na mikroúrovni aj účel (napríklad nájdenie stratenej brošne, papagája atď.). Orgán na ochranu údajov odmietol tento argument. Webová lokalita bola vytvorená na obchodný účel zarobiť peniaze na umožnení uverejňovania stratených vecí a skutočnosť, že neurčovali, ktoré konkrétne veci sa uverejňujú (na rozdiel od určenia kategórií vecí), nebol rozhodujúci, pretože definícia pojmu „prevádzkovateľ údajov“ explicitne neobsahuje určenie obsahu. Webová lokalita určuje podmienky uverejňovania atď. a je zodpovedná za vhodnosť obsahu.

Aj keď sa mohla objaviť tendencia všeobecne identifikovať outsourcing ako úlohu spracovateľa, v súčasnosti sú situácie a posúdenia často oveľa zložitejšie.

Príklad č. 23: Účtovníci

Kvalifikácia účtovníkov môže byť rôzna v závislosti od kontextu. Ak účtovníci poskytujú služby širokej verejnosti a živnostníkom na základe veľmi všeobecných pokynov („Pripravte mi daňové priznanie“), potom – ako v prípade právnych zástupcov konajúcich za podobných okolností a z podobných dôvodov – je účtovník prevádzkovateľom údajov. Ak však účtovníka zamestnáva firma a on podlieha podrobným pokynom interného účtovníka, napríklad v súvislosti s vykonaním podrobného auditu, potom, ak nie je radovým zamestnancom, vo všeobecnosti bude spracovateľom, a to z dôvodov jasnosti pokynov a následného obmedzeného rozsahu voľného uváženia. To však podlieha dôležitej námietke, a síce v prípade, keď si účtovník myslí, že odhalil priestupok, ktorý je povinný oznámiť, potom v dôsledku profesijných povinností, ktoré sa na neho vzťahujú, koná nezávisle ako prevádzkovateľ.

Niekedy zložitosť operácií spracovania môže viesť k potrebe väčšieho zamerania na manévrovacie možnosti tých, ktorí sú poverení výkonom spracovania osobných údajov, napríklad vtedy, ak zo spracovania vyplýva konkrétne riziko týkajúce sa súkromia. Zavedenie nových prostriedkov spracovania môže viesť k tomu, že sa uprednostňuje označenie prevádzkovateľ údajov miesto spracovateľ údajov. Tieto prípady môžu takisto viesť k objasneniu (a menovaniu prevádzkovateľa), ako je výslovne stanovené v právnych predpisoch.

Príklad č. 24: Spracovanie na historické, vedecké a štatistické účely

Vo vnútroštátnych právnych predpisoch sa môže vzhľadom na spracovanie osobných údajov na historické, vedecké a štatistické účely stanoviť pojem sprostredkovateľskej organizácie na označenie orgánu zodpovedného za transformáciu nekódovaných údajov na kódované údaje tak, aby prevádzkovateľ spracovania na historické, vedecké a štatistické účely nemohol spätne identifikovať dotknuté osoby.

Ak viacerí prevádzkovatelia prvotných operácií spracovania prenášajú údaje jednej tretej strane alebo viacerým tretím stranám na ďalšie spracovanie na historické, vedecké a štatistické účely, tieto údaje najskôr zakóduje sprostredkovateľská organizácia. V tomto prípade sa sprostredkovateľská organizácia môže považovať za prevádzkovateľa podľa konkrétnych vnútroštátnych právnych predpisov a podlieha všetkým povinnostiam, ktoré z tejto kvalifikácie vyplývajú (relevantnosť údajov, informovanie dotknutej osoby, oznamovanie atď.). Je to zdôvodnené skutočnosťou, že keď sa spájajú údaje z rôznych zdrojov, existuje osobitné nebezpečenstvo v súvislosti s ochranou údajov, čo opodstatňuje vlastnú zodpovednosť sprostredkovateľskej organizácie. Následne sa táto organizácia nepovažuje iba za spracovateľa, ale plne za prevádzkovateľa podľa vnútroštátnych právnych predpisov.

Rovnako relevantná je právomoc nezávislého rozhodovania, ktorou disponujú rôzne strany zapojené do spracovania. Prípád klinických testov liekov ukazuje, že vzťah medzi sponzormi a externými subjektmi poverenými výkonom testov závisí od voľného uváženia, ktorým disponujú externé subjekty v súvislosti so spracovaním údajov. Z toho vyplýva, že môže existovať viac ako jeden prevádzkovateľ, ale aj viac ako jeden spracovateľ prípadne osoba zodpovedná za spracovanie.

Príklad č. 25: Klinické testy liekov

Farmaceutická spoločnosť XYZ sponzoruje určité testy liekov a vyberie si kandidátske testovacie centrá na základe posúdenia ich dostupnosti a záujmu. Pripraví testovací protokol, zabezpečí potrebné poradenstvo pre centrá v súvislosti so spracovaním údajov a overuje si súlad centier s protokolom a príslušnými vnútornými postupmi.

Aj keď sponzor nezbiera žiadne údaje priamo, získava údaje pacientov, ktoré zbierajú testovacie centrá a tieto údaje spracúva rôznymi spôsobmi (vyhodnocuje informácie uvedené v zdravotnej dokumentácii, získava údaje o nepriaznivých účinkoch, zaznamenáva tieto údaje v príslušnej databáze, vykonáva štatistické analýzy s cieľom dosiahnuť želané výsledky testov). Testovacie centrum vykonáva testy nezávisle (aj keď v súlade s usmerneniami sponzora), poskytuje informačné oznámenia pacientom a získava ich súhlas aj so spracovaním údajov, ktoré sa ich týkajú, umožňuje spolupracovníkom sponzora prístup k pôvodnej zdravotnej dokumentácii pacientov na účel vykonania monitorovacích činností, ďalej sa stará o bezpečné uchovanie týchto dokumentov a je zaň zodpovedný. Preto sa zdá, že zodpovednosťou sú poverení jednotliví aktéri.

Z uvedeného vyplýva, že v tomto prípade testovacie centrá aj sponzori významnou mierou určujú spôsob spracovania osobných údajov v súvislosti s klinickými testami. Na základe toho sa môžu považovať za spoločných prevádzkovateľov údajov. Vzťah medzi sponzorom a testovacími centrami by sa dal vyložiť inak v prípadoch, keď sponzor určuje účely a základné prvky prostriedkov a výskumníkov zostáva veľmi malý manévrovací priestor.

III.3. Vymedzenie pojmu tretia strana

Pojem „tretia strana“ nebol stanovený v dohovore č. 108, ale zaviedol sa v zmenenom a doplnenom návrhu Komisie a neskôr v pozmeňujúcom a doplňujúcom návrhu Európskeho parlamentu. Podľa odôvodnenia sa znenie pozmeňujúceho a doplňujúceho návrhu zmenilo tak, aby sa ujasnilo, že k tretím stranám nepatria dotknuté osoby, prevádzkovateľ ani žiadna osoba oprávnená spracúvať údaje pod priamym dohľadom prevádzkovateľa alebo v jeho mene ako v prípade spracovateľa. To znamená, že *„osoby pracujúce pre inú organizáciu, aj keď patrí do rovnakej skupiny alebo holdingovej spoločnosti, sú vo všeobecnosti tretie strany“*, zatiaľ čo na druhej strane *„pobočky banky, ktoré spracúvajú účty zákazníkov pod priamym dohľadom svojho ústredia, nie sú tretie strany“*.

V smernici sa pojem „tretia strana“ používa spôsobom, ktorý sa neodlišuje od spôsobu bežného použitia tohto pojmu v občianskom práve, v ktorom je tretia strana obyčajne subjekt, ktorý nie je súčasťou iného subjektu alebo dohody. V kontexte ochrany údajov by sa tento pojem mal vykladať ako pojem označujúci akýkoľvek subjekt, ktorý nemá osobitné oprávnenie na spracovanie osobných údajov, ktoré by mohlo vyplývať napríklad z jeho úlohy prevádzkovateľa, spracovateľa alebo zamestnanca.

V smernici sa tento pojem používa v mnohých ustanoveniach, obvykle s cieľom stanoviť zákazy, obmedzenia a povinnosti v prípadoch, v ktorých by osobné údaje mohli spracovať iné strany, ktoré pôvodne nemali spracúvať určité osobné údaje.

Na základe týchto súvislostí môžeme vysloviť záver, že tretia strana prijímajúca osobné údaje – či už zákonne alebo nezákonne – je v zásade novým prevádzkovateľom za predpokladu, že ostatné podmienky kvalifikácie tejto strany ako prevádzkovateľa a uplatňovanie právnych predpisov o ochrane údajov sú dodržané.

Príklad č. 26: Neoprávnený prístup zamestnanca

Zamestnanec spoločnosti pri plnení svojich úloh zistí osobné údaje, ku ktorým nemá oprávnený prístup. V tomto prípade by sa mal tento zamestnanec považovať za „tretiu stranu“ voči svojmu zamestnávateľovi so všetkými následkami a zodpovednosťou, ktorá z tejto skutočnosti vyplýva v súvislosti so zákonnosťou komunikácie a spracovania údajov.

IV. Záver

Pojem prevádzkovateľ údajov a jeho vzájomný vzťah s pojmom spracovateľ údajov zohrávajú rozhodujúcu úlohu pri uplatňovaní smernice 95/46/ES, pretože určujú, kto má niesť zodpovednosť za dodržiavanie pravidiel ochrany údajov, ako si môžu dotknuté osoby uplatniť svoje práva, ktoré vnútroštátne právne predpisy sú uplatniteľné a ako účinne môžu pracovať orgány na ochranu údajov.

Organizačná diferenciacia vo verejnom a súkromnom sektore, vývoj IKT a globalizácia spracovania údajov, zvyšujú zložitosť spôsobu spracovania osobných údajov a vyžadujú si ujasnenie týchto pojmov s cieľom zabezpečiť účinné uplatňovanie a dodržiavanie pravidiel v praxi.

Pojem prevádzkovateľ je nezávislý v tom zmysle, že by sa mal vykladať najmä podľa právnych predpisov Spoločenstva o ochrane údajov, a funkčný v tom zmysle, že jeho cieľom je prideliť zodpovednosť tam, kde je aj skutočný vplyv, a preto je založený skôr na faktickej ako na formálnej analýze.

Definícia uvedená v smernici obsahuje tri základné stavebné prvky: osobné hľadisko („*fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán*“); možnosť spoločnej kontroly („*ktorý sám, alebo v spojení s inými*“); a základné prvky na odlišenie prevádzkovateľa od ostatných aktérov („*určuje účely a prostriedky spracovania osobných údajov*“).

Analýza týchto stavebných prvkov vedie k týmto základným výsledkom:

- Právomoc „*určovať účely a prostriedky ...*“ môže vyplývať z rôznych právnych a/alebo faktických okolností: explicitnej právnej moci, keď je prevádzkovateľ menovaný na základe právnych predpisov, alebo na základe takýchto predpisov je poverený úlohou alebo povinnosťou zbierať a spracúvať určité údaje; spoločných právnych ustanovení alebo existujúcich tradičných úloh, z ktorých za normálnych podmienok vyplýva určitá zodpovednosť v rámci určitých organizácií (napr. zamestnávateľ vo vzťahu k údajom svojich zamestnancov); faktických okolností a ostatných prvkov (napr. zmluvných vzťahov, skutočnej kontroly strany, viditeľnosti z pohľadu dotknutých osôb atď.).

Ak nie je možné uplatniť žiadnu z týchto kategórií, stanovenie prevádzkovateľa by sa malo považovať za „neplatné“. Orgán, ktorý nemá ani právny ani faktický vplyv na určovanie spôsobu osobných údajov, sa skutočne nemôže považovať za prevádzkovateľa.

Určenie „účelu“ spracovania vyvoláva kvalifikáciu (*de facto*) prevádzkovateľa. Naopak, určenie „prostriedkov“ spracovania môže prevádzkovateľ delegovať na ďalší subjekt, pokiaľ ide o technické alebo organizačné otázky. Podstatné otázky, ktoré sú nevyhnutné pre základnú zákonnosť spracovania však musí určiť prevádzkovateľ, napr. údaje, ktoré sa majú spracovať, dĺžku uchovania, prístup atď.

- *Osobné* hľadisko definície sa vzťahuje na širokú škálu subjektov, ktoré môžu plniť úlohu prevádzkovateľa. Avšak, zo strategického hľadiska pridelenia zodpovednosti by sa mala za prevádzkovateľa skôr považovať spoločnosť alebo orgán ako taký než konkrétna osoba v rámci spoločnosti alebo orgánu. Spoločnosť alebo orgán je v konečnom dôsledku zodpovedný za spracovanie údajov a plnenie povinností vyplývajúcich z právnych predpisov o ochrane údajov, ak neexistujú jasné prvky, ktoré poukazujú na to, že by mala byť zodpovedná fyzická osoba, napríklad vtedy, ak fyzická osoba pracujúca v spoločnosti alebo vo verejnom orgáne používa údaje na vlastné účely mimo činností spoločnosti.
- Možnosť *pluralistickej kontroly* rieši rastúci počet situácií, v ktorých rôzne strany konajú ako prevádzkovatelia. Posúdenie tejto spoločnej kontroly by malo odzrkadľovať posúdenie „samostatnej“ kontroly pomocou podstatného a funkčného prístupu a zameraním sa na to, či viac ako jedna strana určuje účely a základné prvky prostriedkov.

Účasť strán na určovaní účelov a prostriedkov spracovania v kontexte spoločnej kontroly môže mať rôzne podoby a nemusí byť rovnomerne rozdelená. Toto stanovisko poskytuje mnoho príkladov rôznych druhov a stupňov spoločnej kontroly. Rôzne stupne kontroly môžu vyvolať rôzne stupne zodpovednosti a „spoločná a nerozdielna“ zodpovednosť sa určite nemôže predpokladať vo všetkých prípadoch. Okrem toho je dostatočne pravdepodobné, že v zložitých systémoch s viacerými aktérmi môžu prístup k osobným údajom a vykonávanie ďalších práv dotknutých osôb zabezpečovať aj iní aktéri na rôznych úrovniach.

V tomto stanovisku sa analyzuje aj pojem spracovateľ, ktorého existencia závisí od rozhodnutia prevádzkovateľa, ktorý sa môže rozhodnúť spracovať údaje vo svojej vlastnej organizácii alebo poveriť externú organizáciu vykonaním všetkých činností spracovania alebo ich časti. Na kvalifikáciu spracovateľa je potrebné splniť dve základné podmienky, na jednej strane, musí ísť o samostatný právnický subjekt nezávislý od prevádzkovateľa a na druhej strane, tento subjekt musí spracovávať osobné údaje v mene prevádzkovateľa. Táto činnosť spracovania môže byť obmedzená na veľmi konkrétnu úlohu či kontext alebo môže zahŕňať určitý stupeň voľného uváženia v súvislosti so spôsobom najlepšieho plnenia záujmov prevádzkovateľa, ktorý umožňuje spracovateľovi vybrať si najvhodnejšie technické a organizačné prostriedky.

Úloha spracovateľa navyše nevyplýva z povahy aktéra, ktorý spracúva osobné údaje, ale z jeho konkrétnych činností v určitom kontexte a v súvislosti s konkrétnymi súbormi údajov alebo operácií. Niektoré kritériá môžu byť užitočné pri určení kvalifikácie rôznych aktérov zapojených do spracovania: úroveň predchádzajúcich pokynov od

prevádzkovateľa údajov, monitorovanie úrovne služby prevádzkovateľom údajov, viditeľnosť z pohľadu dotknutých osôb, odborné znalosti strán, právomoc nezávislého rozhodovania ponechaná jednotlivým stranám.

Posledná kategória „tretia strana“ je vymedzená ako akýkoľvek aktér, ktorý nemá osobitné oprávnenie na spracovanie osobných údajov, ktoré by mohlo vyplývať napríklad z jeho úlohy prevádzkovateľa, spracovateľa alebo zamestnanca.

* * *

Pracovná skupina si uvedomuje ťažkosti súvisiace s uplatňovaním definícií smernice v zložitom prostredí, v ktorom je možné predpokladať veľké množstvo scenárov, v ktorých prevádzkovatelia a spracovatelia vystupujú samostatne alebo spoločne, s rôznymi stupňami samostatnosti a zodpovednosti.

Pracovná skupina vo svojej analýze zdôrazňuje potrebu prideliť zodpovednosť takým spôsobom, aby sa dostatočne zabezpečilo dodržiavanie pravidiel ochrany údajov v praxi. Nenašla však dôvod domnievať sa, že by v tomto ohľade súčasné rozlíšenie medzi prevádzkovateľom a spracovateľom už nebolo relevantné a nedalo by sa s ním pracovať.

Pracovná skupina preto dúfa, že vysvetlenie, ktoré ponúka v tomto stanovisku doplnené o konkrétne príklady každodennej praxe orgánov na ochranu údajov prispeje k účinnému usmerneniu na ceste k výkladu týchto ústredných definícií smernice.

V Bruseli 16. februára 2010

*Za pracovnú skupinu
predseda
Jacob KOHNSTAMM*