



**01197/11/SK
WP 187**

Stanovisko 15/2011 k definícii súhlasu

Prijaté 13. júla 2011

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

Sekretariát poskytuje Riaditeľstvo C (Základné práva a občianstvo Únie) Európskej komisie, Generálne riaditeľstvo pre spravodlivosť, B-1049 Brusel, Belgicko, kancelária č. MO59 06/36.

Webová lokalita: http://ec.europa.eu/justice/data-protection/index_sk.htm

Zhrnutie

Toto stanovisko poskytuje podrobnú analýzu koncepcie súhlasu, ako sa v súčasnosti používa v smernici o ochrane údajov a smernici o súkromí a elektronických komunikáciách. Na základe skúseností členov pracovnej skupiny zriadenej podľa článku 29 sa v stanovisku poskytujú mnohé príklady platného a neplatného súhlasu, so zameraním na jeho kľúčové prvky ako význam výrazov „prejav“, „slobodne poskytnutý“, „konkrétny“, „jednoznačný“, „výslovný“, „vedomý“ atď. V stanovisku sa ďalej vysvetľujú určité hľadiská týkajúce sa pojmu súhlas. Napríklad termín, v ktorom sa musí súhlas získať, ako sa právo namietať líši od súhlasu atď.

Súhlas je jeden z viacerých právnych základov pre spracovanie osobných údajov. Má dôležitú úlohu, ale nevylučuje sa tým možnosť, že v závislosti od kontextu môžu byť z pohľadu kontrolóra údajov aj dotknutej osoby vhodnejšie iné právne základy. Ak sa súhlas správne používa, slúži ako nástroj, ktorý dotknutej osobe poskytuje kontrolu nad spracovaním jej údajov. Ak sa používa nesprávne, kontrola dotknutej osoby sa stáva iluzórnou a súhlas predstavuje nevhodný základ pre spracovanie.

Toto stanovisko sa čiastočne vydáva ako odpoveď na žiadosť Komisie v súvislosti s prebiehajúcim preskúmaním smernice o ochrane údajov. Preto obsahuje odporúčania na zváženie v rámci preskúmania. K týmto odporúčaniam patrí:

- i) vyjasnenie významu pojmu „jednoznačný“ súhlas a vysvetlenie, že iba súhlas založený na výrokoch alebo skutkoch, ktoré sú prejavom súhlasu, predstavuje platný súhlas,
- ii) vyžadovanie, aby kontrolóri údajov zaviedli mechanizmy na preukázanie súhlasu (v rámci všeobecnej povinnosti týkajúcej sa zodpovednosti),
- iii) doplnenie výslovnej požiadavky týkajúcej sa kvality a prístupnosti informácií ako základ pre súhlas a
- iv) niekoľko odporúčaní v súvislosti s maloletými osobami a inými osobami, ktoré nemajú spôsobilosť na právne úkony.

PRACOVNÁ SKUPINA PRE OCHRANU JEDNOTLIVCOV SO ZRETEĽOM NA SPRACOVANIE OSOBNÝCH ÚDAJOV

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

so zreteľom na články 29 a 30 ods. 1 písm. a) a ods. 3 uvedenej smernice,

so zreteľom na jej rokovací poriadok,

PRIJALA TOTO STANOVISKO

I. Úvod

Súhlas dotknutej osoby bol vždy kľúčovým pojmom ochrany údajov, nie je však vždy jasné, kedy je súhlas potrebný a aké podmienky sa musia splniť, aby bol súhlas platný. Môže to viesť k rôznym prístupom a rozdielnym názorom na osvedčený postup v rôznych členských štátoch. Tým sa môže oslabiť pozícia dotknutých osôb. Tento problém sa stal vážnejším, pretože spracovanie osobných údajov je čoraz výraznejším prvkom modernej spoločnosti v prostredí online aj offline a často zahŕňa rôzne členské štáty. Preto sa pracovná skupina zriadená podľa článku 29 rozhodla v rámci svojho pracovného programu na obdobie 2010 – 2011 pozorne preskúmať túto problematiku.

Súhlas je zároveň jednou z tém, ku ktorým si Komisia vyžiadala vstupy v súvislosti s preskúmaním smernice 95/46/ES. V oznámení Komisie „Komplexný prístup k ochrane osobných údajov v Európskej únii“¹ sa uvádza, že: „Komisia preskúma spôsoby ako objasniť a posilniť predpisy týkajúce sa poskytovania súhlasu“. V oznámení sa to vysvetľuje² takto:

„V prípade, že sa vyžaduje vedomý súhlas, súčasné predpisy stanovujú, že súhlas jednotlivca na spracovanie jeho osobných údajov by mal byť „slobodný, konkrétny a vedomý prejav vôle, ktorým jednotlivec dáva najavo svoj súhlas s týmto spracovaním údajov. V členských štátoch sa tieto podmienky v súčasnosti vykladajú rôzne, od všeobecnej požiadavky na písomný súhlas až po akceptovanie implicitného súhlasu.“

„Navyše, v online prostredí je vzhľadom na neprehľadnosť pravidiel ochrany osobných údajov pre jednotlivcov omnoho náročnejšie uvedomovať si svoje práva a poskytnúť vedomý súhlas. Ešte viac to komplikuje skutočnosť, že v niektorých prípadoch nie je dokonca ani jasné, ako by mal slobodný, konkrétny a vedomý prejav vôle vyzeráť – ako príklad možno uviesť behaviorálnu reklamu, pri ktorej niektoré subjekty považujú už samotné nastavenia internetového prehliadača za poskytnutie súhlasu používateľa, zatiaľ čo iné subjekty sa s takýmto názorom nestotožňujú.“

¹ KOM (2010) 609 v konečnom znení zo 4.11.2010.

² Prvá správa Komisie o vykonávaní smernice o ochrane údajov (95/46/ES) (KOM(2003)265 v konečnom znení, spomenutá už na strane 17: „Najmä pojem „jednoznačný súhlas“ (článok 7 písm. a)) v porovnaní s pojmom „výslovný súhlas“ v článku 8 potrebuje ďalšie vysvetlenie a jednotnejší výklad. Je nevyhnutné, aby hospodárske subjekty vedeli, čo tvorí platný súhlas, najmä v scenároch online.“

„Mali by sa preto objasniť podmienky týkajúce sa poskytovania súhlasu dotknutej osoby, aby bolo v súlade s článkom 8 Charty základných práv EÚ možné vždy zaručiť, že jednotlivec poskytol vedomý súhlas na spracovanie svojich údajov a že si je plne vedomý poskytnutia tohto súhlasu, ako aj účelu spracovania týchto údajov. Jasnosť kľúčových koncepcií môže tiež prospieť rozvoju samoregulačných iniciatív na vypracovanie praktických riešení, ktoré sú v súlade s právnymi predpismi EÚ.“

S cieľom vyhovieť žiadosti Komisie o vstupy a vykonať svoj pracovný program na obdobie 2010 – 2011 sa pracovná skupina zriadená podľa článku 29 zaviazala, že pripraví stanovisko. Cieľom stanoviska je vyjasniť určité veci, aby sa zabezpečil spoločný pohľad na existujúci právny rámec. Tento krok zároveň nadväzuje na logiku skorších stanovísk k iným kľúčovým ustanoveniam smernice³. Potenciálne zmeny existujúceho rámca budú trvať určitý čas, takže vyjasnenie súčasného pojmu „súhlas“ a jeho základných prvkov má svoje prednosti a výhody. Vyjasnením existujúcich ustanovení sa takisto lepšie poukáže na oblasti, ktoré je potrebné zlepšiť. Takže pracovná skupina zriadená podľa článku 29 sa v tomto stanovisku pokúsi na základe analýzy formulovať politické odporúčania s cieľom pomôcť Komisii a zákonodarcom pri ich úvahách o zmenách uplatniteľného právneho rámca ochrany údajov.

Toto je základný obsah stanoviska: po poskytnutí prehľadu legislatívnej histórie a úlohy súhlasu v rámci právnych predpisov o ochrane údajov skúmame rôzne prvky a požiadavky, na základe ktorých je súhlas platný podľa uplatniteľných právnych predpisov vrátane určitých relevantných častí smernice o súkromí a elektronických komunikáciách 2002/58/ES. Analýzu dopĺňajú praktické príklady na základe skúseností v jednotlivých členských štátoch. Prehľad, analýza a príklady podporujú odporúčania, uvedené v záverečnej časti tohto stanoviska, v ktorých sa uvádza, že nato, aby bolo možné požiadať a získať platný súhlas podľa tejto smernice, sa musia zaviesť určité prvky. Zároveň poskytuje politické odporúčania pre zákonodarcov, ktoré by mali zvážiť v rámci preskúmania smernice 95/46/ES.

II. Všeobecné poznámky a politické otázky

II.1. Stručná história

Kým v niektorých vnútroštátnych právnych predpisoch o ochrane údajov / súkromia, prijatých v sedemdesiatych rokoch, sa súhlas stanovil ako jeden z právnych základov spracovania osobných údajov⁴, neodzrkadlilo sa to v dohovore Rady Európy 108⁵. Neexistujú žiadne zjavné dôvody, prečo by súhlas nemohol v dohovore zohrávať významnejšiu úlohu⁶.

³ Ako stanovisko 8/2010 k uplatniteľným právnym predpisom, prijaté 16.12.2010 (WP 179) a stanovisko 1/2010 k pojmom „prevádzkovateľ“ a „spracovateľ“, prijaté 16.02.2010 (WP 169).

⁴ Pozri napríklad článok 31 francúzskeho zákona č. 78-17 zo 6. januára 1978 „relative a l'informatique, aux fichiers et aux libertés“.

⁵ Dohovor Rady Európy o ochrane osôb pri automatickom spracúvaní osobných údajov (ďalej len „dohovor 108“). Účinnosť nadobudol 1. októbra 1985.

⁶ V dohovore 108 sa zaviedli pojmy „zákonné spracovanie“ a „legitímny účel“ (článok 5), no na rozdiel od smernice 95/46/ES neposkytol zoznam kritérií pre legitímne spracovanie údajov. Súhlas dotknutej osoby zohrával určitú úlohu iba v kontexte vzájomnej pomoci (článok 15). Požiadavka „súhlasu“ sa však neskôr zopakovala vo viacerých odporúčaniach Výboru ministrov.

Na úrovni EÚ sa spoľahnutie sa na súhlas ako kritérium legitimácie operácií spracovania osobných údajov stanovilo od samého začiatku legislatívneho procesu, ktorého záverom bolo prijatie smernice 95/46/ES. V článku 12 návrhu Komisie⁷ v roku 1990 sa stanovili vlastnosti, ktoré súhlas musel mať, aby legitimoval operácie spracovania údajov: musel byť „*explicitne poskytnutý*“ a „*konkrétny*“. V článku 17 o citlivých údajoch sa vyžadovalo, aby bol súhlas „*výslovný a písomný*“. V zmenenom a doplnenom návrhu Komisie⁸ v roku 1992 sa zaviedlo znenie blízke definícii „súhlasu dotknutej osoby“ v súčasnom článku 2 písm. g), ktorým sa nahradil pôvodný článok 12. Uvádzalo sa v ňom, že súhlas musí byť „*poskytnutý na základe slobodného rozhodnutia a konkrétny*“. Odkaz na „*výslovne poskytnutý*“ sa nahradil súhlasom ako „*výslovným vyjadrením jej želaní (dotknutej osoby)*“. V dôvodovej správe sprevádzajúcej zmenený a doplnený návrh z roku 1992⁹ sa uvádzalo, že súhlas môže byť poskytnutý ústne alebo písomne. Pokiaľ ide o citlivé údaje, zachovala sa požiadavka, aby bol súhlas „*písomný*“. V roku 1992 sa zmeneným a doplneným návrhom Komisie reštrukturalizoval predchádzajúci návrh a zaviedol článok 7 o právnych základoch pre spracovanie. V článku 7 písm. a) sa uvádzalo, že spracovanie sa môže vykonať vtedy, ak „*dotknutá osoba poskytla súhlas*“; pôvodný zoznam obsahoval, ako aj dnes, päť dodatočných právnych základov (popri súhlase), ktoré sa môžu použiť na legitimáciu spracovania údajov.

V spoločnej pozícii Rady¹⁰ v roku 1995 sa zaviedla konečná (dnešná) definícia súhlasu. Definoval sa ako „*akýkoľvek slobodne poskytnutý, konkrétny a vedomý prejav vôle, ktorým dotknutá osoba prejaví svoj súhlas s tým, aby sa osobné údaje, ktoré sa jej týkajú, spracúvali*“. Najväčšia zmena v pozícii Komisie z roku 1992 sa týkala vypustenia slova „*výslovný*“, ktoré predchádzalo slovu „*prejav*“. Zároveň sa do článku 7 písm. a) doplnilo slovo „*jednoznačný*“, takže znie takto: „*ak dotknutá osoba poskytla svoj súhlas jednoznačne*“. Požiadavka písomného súhlasu v prípade citlivých údajov sa nahradila „*výslovným súhlasom*“.

V dôvodoch Rady¹¹ sa tieto zmeny osobitne nevysvetlili. Na strane 4 sa však uvádza, že „*... sa vykonalo niekoľko zmien a doplnení ... s cieľom ... zaviesť opatrenie pružnosti, ktoré zaručuje ekvivalentnú ochranu ... ale nevedie k zníženiu úrovne ochrany; umožňujú uplatňovanie všeobecných zásad účinne a nebyrokraticky a dodržiavajú krok so širokou škálou spôsobov ... spracovania údajov.*“

Úloha súhlasu sa výslovne uznala v Charte základných práv Európskej únie v súvislosti s ochranou osobných údajov. V článku 8 ods. 2 sa uvádza, že osobné údaje sa môžu spracovať „*na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom*“. Súhlas sa preto uznáva ako základný aspekt základného práva na ochranu osobných údajov. Súhlas zároveň podľa charty nie je jediným právnym základom, ktorý umožňuje spracovanie osobných údajov; v charte sa výslovne uznáva, že sa zákonom môžu stanoviť iné legitímne základy, ako je to v prípade smernice 95/46/ES.

⁷ Návrh smernice o ochrane jednotlivcov v súvislosti so spracovaním osobných údajov, KOM (90), 314 v konečnom znení, SYN 287 a 288, Brusel 13. septembra 1990.

⁸ Zmenený a doplnený návrh smernice Rady o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, KOM (92) 422 V KONEČNOM ZNENÍ – SYN 287, Brusel 15. októbra 1992.

⁹ Pozri stranu 11 zmeneného a doplneného návrhu smernice Rady o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, KOM (92) 422 V KONEČNOM ZNENÍ – SYN 287, Brusel 15. októbra 1992.

¹⁰ Spoločná pozícia Rady k návrhu smernice Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, (00/287) KOD, prijatá 15/03/95.

¹¹ Pozri stranu 4 spoločnej pozície.

V krátkosti, legislatívna história, najmä v EÚ, dokazuje, že súhlas zohrával významnú úlohu v rámci koncepcií ochrany údajov a súkromia. Zároveň dokazuje, že súhlas sa neposudzoval za jediný právny základ pre legitimáciu operácií spracovania údajov. Z legislatívnej histórie smernice 95/46/ES vyplýva relatívny konsenzus, pokiaľ ide o podmienky platného súhlasu, ktorý musí byť najmä: *slobodne poskytnutý, konkrétny a vedomý*. Vyplýva z nej však aj určitá neistota v súvislosti so spôsobmi vyjadrenia súhlasu – či musí byť výslovný, písomný atď. Nasleduje ďalšia analýza týchto otázok.

II.2. Úloha pojmu: základ zákonnosti

Všeobecný/konkrétny základ:

Súhlas sa používa v smernici ako všeobecný základ zákonnosti (článok 7) aj ako konkrétny základ v niektorých osobitných súvislostiach [článok 8 ods. 2 písm. a), článok 26 ods. 1 písm. a)]. V článku 7 sa súhlas uvádza ako prvý zo šiestich rôznych základov legitimácie spracovania osobných údajov, kým v článku 8 sa stanovuje možnosť použiť súhlas na legitimáciu spracovania osobitných kategórií (citlivých) údajov, ktoré by bolo za iných okolností zakázané. V tomto poslednom prípade je štandard získania súhlasu vyšší, pretože tento súhlas musí prekročiť rámec všeobecného štandardu súhlasu tým, že je „výslovný“.

Smernica ďalej umožňuje interakciu s inými právnymi predpismi, ako sa uvádza v odôvodnení 23: *„členské štáty sú splnomocnené zabezpečiť zavedenie ochrany jednotlivcov prostredníctvom všeobecného zákona na ochranu jednotlivcov, pokiaľ ide o spracovanie osobných údajov, ako aj sektorových zákonov“*. Spôsob fungovania tohto systému v praxi je zložitý: členské štáty prijali vlastný prístup a v niektorých prípadoch to viedlo k rozmanitosti.

Pojem súhlas sa netransponoval vždy doslovne na vnútroštátnej úrovni. Napríklad, súhlas ako všeobecný pojem nie je definovaný vo francúzskych právnych predpisoch o ochrane údajov, ale jeho význam sa presne a konzistentne vysvetľoval v judikatúre orgánu na ochranu údajov (CNIL) vo vzťahu k definícii uvedenej v smernici o ochrane údajov. V Spojenom kráľovstve sa vyvinul v rámci zvykového práva v odkazoch na znenie smernice. Navyše, súhlas sa niekedy výslovne definoval v konkrétnych sektoroch, napríklad v súvislosti s elektronickým súkromím, elektronickou štátnou správou alebo elektronickým zdravotníctvom. Pojem vyvinutý v konkrétnych právnych predpisoch bude preto v interakcii s pojmom vyvinutým vo všeobecných právnych predpisoch o ochrane údajov.

Súhlas je zároveň pojmom, ktorý sa používa v iných oblastiach práva, najmä v zmluvnom práve. V tejto súvislosti sa na zabezpečenie platnosti zmluvy zohľadnia iné kritériá ako tie, ktoré sú uvedené v smernici, napríklad vek, neprimeraný vplyv atď. Medzi rozsahom občianskeho práva a rozsahom smernice nie je protiklad, ale presah: smernica nerieši všeobecné podmienky platnosti súhlasu v kontexte občianskeho práva, ale nevylučuje ich. To znamená, že napríklad na posúdenie platnosti zmluvy v kontexte článku 7 písm. b) smernice sa musia zohľadniť požiadavky občianskeho práva. Okrem uplatnenia všeobecných podmienok platnosti súhlasu podľa občianskeho práva sa súhlas

požadovaný v článku 7 písm. a) musí zároveň vykladať so zreteľom na článok 2 písm. h) smernice.

Interakcia s inými právnymi predpismi je viditeľná nielen na vnútroštátnej, ale aj na európskej úrovni. Podobné chápanie prvkov smernice sa vyvodilo z iných kontextov, ako ukazuje rozsudok Súdneho dvora v oblasti pracovného práva¹²: v ktorom sa vyžadoval súhlas v súvislosti so vzdaním sa sociálneho práva. Súdny dvor vyložil pojem súhlas v kontexte smernice 93/104 o niektorých aspektoch organizácie pracovného času. Uviedol, že „dohoda pracovníka“ si vyžaduje jeho súhlas (nie odborov v mene pracovníka) a pojem „dohoda“ (...) chápal ako slobodne poskytnutý vedomý súhlas. Zároveň tvrdil, že pracovník, ktorý podpíše pracovnú zmluvu s odkazom na kolektívnu dohodu, ktorou sa schvaľuje predĺženie pracovného času, nespĺňa požiadavky, aby bol súhlas slobodne a výslovne poskytnutý, s plným vedomím všetkých faktov. Výklad pojmu súhlas je v konkrétnom kontexte veľmi blízky zneniu smernice 95/46/ES.

Súhlas nie je jediným základom zákonnosti

V smernici sa súhlas jasne uvádza ako základ zákonnosti. Niektoré členské štáty ho však vnímajú ako uprednostnený základ, niekedy takmer na úrovni ústavnej zásady, spojený s postavením ochrany údajov ako základného práva. Iné členské štáty ho môžu vnímať ako jednu zo šiestich možností, ako operatívnu požiadavku, ktorá nie je dôležitejšia ako iné možnosti. Vysvetlenie vzťahu medzi súhlasom a inými základmi zákonnosti – napríklad v súvislosti so zmluvami, úlohami vo verejnom záujme alebo v legitímnom záujme kontrolóra a právom namietat' – pomôže zvýrazniť úlohu súhlasu v konkrétnych prípadoch.

Poradie, v ktorom sa vymenúvajú právne základy v článku 7 je relevantné, ale neznamená, že súhlas je vždy najvhodnejší základ pre legitimáciu spracovania osobných údajov. Článok 7 začína so súhlasom, pokračuje so zoznamom ďalších základov vrátane zmlúv a právnych povinností a postupne sa dostáva k rovnováhe záujmov. Treba poznamenať, že päť ďalších základov po súhlase si vyžaduje skúšku „nevyhnutnosti“, ktorou sa prísne obmedzuje kontext, v ktorom sa môžu uplatniť. To neznamená, že požiadavka súhlasu ponecháva väčší manévrovací priestor ako iné základy uvedené v článku 7.

Získanie súhlasu navyše neneguje povinnosti kontrolóra podľa článku 6, pokiaľ ide o spravodlivosť, nevyhnutnosť a primeranosť, ako aj kvalitu údajov. Napríklad, aj keď spracovanie osobných údajov vychádza zo súhlasu používateľa, tento súhlas by neoprávňoval na zber údajov, ktoré sú nad rámec nevyhnutný na konkrétny účel.

Získanie súhlasu neoprávňuje ani na obchádzanie iných ustanovení, ako je článok 8 ods. 5. Iba za veľmi obmedzených okolností môže súhlas oprávňovať činnosti spracovania údajov, ktoré by boli inak zakázané, najmä vo vzťahu k spracovaniu určitých citlivých údajov (článok 8) alebo povoľovať použitie osobných údajov na ďalšie spracovanie, či už v rámci pôvodného účelu, alebo nie. V zásade by sa súhlas nemal vnímať ako výnimka z iných zásad ochrany údajov, ale ako záruka. Je v prvom rade základom zákonnosti a neruší uplatňovanie iných zásad.

¹² Rozsudok Súdneho dvora (veľká komora) z 5. októbra 2004, Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele v spojených veciach C-397/01 až C-403/01.

Výber najvhodnejšieho právneho základu nie je vždy zrejмый, najmä ak sa rozhoduje medzi ustanoveniami článku 7 písm. a) a písm. b). Podľa článku 7 písm. b) musí byť spracovanie nevyhnutné na vykonanie zmluvy, alebo s cieľom vykonať opatrenia na požiadanie dotknutej osoby pred uzatvorením zmluvy, a na nič viac. Kontrolór údajov, ktorý použije článok 7 písm. b) ako právny základ v kontexte uzatvorenia zmluvy, ho nemôže rozšíriť s cieľom zdôvodniť spracovanie údajov nad rámec nevyhnutného: bude musieť opraviť toto ďalšie spracovanie nad rámec konkrétnym súhlasom, na ktorý sa budú vzťahovať požiadavky článku 7 písm. a). Z toho vyplýva potreba podrobnosti v súvislosti so zmluvami. V praxi to znamená, že môže byť nevyhnutné získať súhlas ako dodatočnú podmienku pre určitú časť spracovania. Buď je spracovanie nevyhnutné pre výkon zmluvy, alebo sa musí získať (slobodný) súhlas.

Pri niektorých transakciách by sa mohli súčasne uplatňovať viaceré právne základy. Inými slovami, každé spracovanie údajov musí byť vždy v súlade s jedným alebo viacerými právnymi základmi. Týmto sa nevylučuje súbežné použitie rôznych základov za predpokladu, že sa použijú v správnej súvislosti. Určitý zber a ďalšie spracovanie údajov môže byť nevyhnutné podľa zmluvy s dotknutou osobou – článok 7 písm. b); iné spracovanie môže byť nevyhnutné v dôsledku zákonnej povinnosti – článok 7 písm. c); zber dodatočných informácií si môže vyžadovať samostatný súhlas – článok 7 písm. a); no a ďalšie spracovanie by mohlo byť legitímne na základe rovnováhy záujmov – článok 7 písm. f).

Príklad: kúpa auta

Kontrolór údajov môže byť oprávnený spracovať osobné údaje na rôzne účely a na základe rôznych základov:

- údaje nevyhnutné pri kúpe auta: článok 7 písm. b),
- s cieľom spracovať doklady od auta: článok 7 písm. c),
- na účely služieb manažmentu klientov (napríklad aby sa auto mohlo dať opraviť v iných prepojených spoločnostiach v rámci EÚ): článok 7 písm. f),
- s cieľom presunu údajov tretím stranám na účely ich vlastných marketingových činností: článok 7 písm. a).

II.3. Súvisiace pojmy

Kontrola

Pojem súhlas je tradične spojený s myšlienkou, že dotknutá osoba by mala kontrolovať použitie jej údajov. Z pohľadu základných práv je kontrola vykonávaná prostredníctvom súhlasu dôležitým pojmom. Zároveň a z toho istého pohľadu by rozhodnutie jednotlivca akceptovať operáciu spracovania údajov malo podliehať prísnyim požiadavkám, najmä so zreteľom na skutočnosť, že poskytnutím súhlasu sa jednotlivec môže zrieknuť základného práva.

Aj keď súhlas plní úlohu pri zabezpečení kontroly pre dotknuté osoby, nie je jediným spôsobom, ktorým je možné túto kontrolu zabezpečiť. V smernici sa stanovujú iné prostriedky kontroly, najmä právo namietat', ale toto je odlišný nástroj, ktorý sa má

vykonávať v inej fáze spracovania, t. j. keď sa už spracovanie začalo a na inom právnom základe.

Súhlas súvisí s pojmom informačné sebaurčenie. Autonómnosť dotknutej osoby je základnou podmienkou a dôsledkom súhlasu: dáva dotknutej osobe vplyv na spracovanie údajov. Ako sa však vysvetľuje v nasledujúcej kapitole, táto zásada má obmedzenia a existujú prípady, keď dotknutá osoba vlastne nemá možnosť prijať skutočné rozhodnutie. Kontrolór údajov môže mať v úmysle použiť súhlas dotknutej osoby ako prostriedok prenosu jeho zodpovednosti na jednotlivca. Napríklad, poskytnutie súhlasu so zverejnením osobných údajov na internete alebo s ich prenosom pochybnému subjektu v tretej krajine môže dotknutá osoba utrpieť ujmu a kontrolór môže argumentovať, že dotknutá osoba poskytla svoj súhlas. Preto je dôležité pripomenúť, že plne platný súhlas nezabavuje kontrolóra údajov jeho povinností a neopravňuje na spracovanie, ktoré by inak bolo nespravodlivé podľa článku 6 smernice.

Pojem kontrola je spojený aj so skutočnosťou, že dotknutá osoba by mala mať možnosť svoj súhlas zrušiť. Zrušenie súhlasu nie je retroaktívne, ale malo by v zásade zabrániť ďalšiemu spracovaniu údajov jednotlivca kontrolórom. Spôsob, akým táto možnosť funguje v praxi, rozoberieme v ďalších častiach tohto textu (kapitola III).

Transparentnosť

Druhý rozmer súhlasu sa týka informácií: transparentnosti voči dotknutej osobe. Transparentnosť je podmienkou pre existenciu kontroly a platnosť súhlasu. Transparentnosť ako taká nie je dostatočná na oprávnenie spracovania osobných údajov, ale podstatnou podmienkou na zabezpečenie platnosti súhlasu.

Súhlas je platný, iba ak je vedomý. Z toho vyplýva, že vo chvíli, keď sa vyžaduje súhlas sa musia poskytnúť všetky potrebné informácie a že by sa mali týkať podstatných hľadísk spracovania, ktoré má súhlas oprávniť. Bežne by sa týkali prvkov informácií uvedených v článku 10 smernice, ale bude to závisieť aj od toho, kedy, aj od okolností, v ktorých sa súhlas vyžaduje.

Bez ohľadu na to, či sa súhlas poskytne alebo nie, transparentnosť spracovania údajov je zároveň podmienkou spravodlivosti, ktorá má vlastnú hodnotu aj po chvíli poskytnutia počiatočných informácií.

Činnosť / časový rozvrh: spôsoby prejavovania súhlasu

Tento tretí rozmer sa týka spôsobu, akým sa vykonáva kontrola: akými spôsobmi je možné súhlas vyjadriť a kedy by sa mal vyžiadať s cieľom zabezpečiť, aby išlo o skutočný súhlas? Tieto otázky majú rozhodujúci vplyv na spôsob, akým sa súhlas vykonáva a vykladá.

Aj keď časový rozvrh pre vyžiadanie súhlasu sa v smernici neuvádza, jasne vyplýva z jazyka rôznych ustanovení, v ktorých sa uvádza, že ako všeobecné pravidlo sa súhlas musí poskytnúť pred začiatkom spracovania¹³. Získanie súhlasu pred začiatkom spracovania údajov je základnou podmienkou legítimácie spracovania údajov. Tento

¹³ Ako príklad, v nemeckej verzii smernice (a v nemeckom federálnom zákone o ochrane údajov) sa používa pojem „Einwilligung“. Tento pojem sa v nemeckom občianskom zákonníku definuje ako „predchádzajúci súhlas“.

bod sa ďalej rozpracúva v kapitole III.B v súvislosti so smernicou o súkromí a elektronických komunikáciách.

Súhlas považovaný za schválenie jednotlivcom, pokiaľ ide o spracovanie údajov, ktoré sa ho týkajú, sa môže vyjadriť rôznymi spôsobmi: v článku 2 písm. h) sa uvádza akékoľvek „vyjadrenie“; musí byť jednoznačné (článok 7 písm. a) a výslovné, pokiaľ ide o citlivé údaje (v článku 8). Treba však nevyhnutne zdôrazniť skutočnosť, že súhlas sa líši od práva namietat' stanoveného v článku 14. Zatiaľ čo v článku 7 písm. a) kontrolór nemôže spracovať údaje, kým nezíska súhlas dotknutej osoby, v článku 7 písm. f) kontrolór údaje môže spracovať na základe podmienok a záruk, pokiaľ dotknutá osoba nenamietala. Ako sa uvádza v pracovnom dokumente 114 pracovnej skupiny: „význam súhlasu, ktorý predstavuje pozitívny akt, vylučuje *de facto* akýkoľvek systém, v ktorom by dotknutá osoba mala právo namietat' proti prenosu až potom, keď sa uskutočnil“¹⁴.

Z týchto dôvodov by sa právo namietat' uvedené v článku 14 smernice nemalo zamieňať so súhlasom. Súhlas je právny základ spracovania osobných údajov podľa článku 7 písm. a), 8 ods. 2 písm. a), 26 ods. 1 alebo v súlade s rôznymi ustanoveniami smernice 2002/58/ES.

II.4. Vhodné použitie súhlasu ako právneho základu

Existuje potreba zdôrazniť, že súhlas nie je vždy prvoradým alebo najvhodnejším prostriedkom legítimácie spracovania osobných údajov.

Súhlas je niekedy slabým základom pre zdôvodnenie spracovania osobných údajov a stráca svoju hodnotu, ak sa rozšíri, alebo okliešti so zámerom prispôbiť ho situáciám, v ktorých sa jeho použitie nikdy neplánovalo. Použitie súhlasu „v správnom kontexte“ je rozhodujúce. Ak sa použije v okolnostiach, v ktorých nie je vhodný, pretože nie je pravdepodobná prítomnosť prvkov, ktoré tvoria platný súhlas, viedlo by to k veľkej zraniteľnosti a v praxi by to *oslabilo* pozíciu dotknutých osôb.

Tento prístup už podporila pracovná skupina a európsky dozorný úradník pre ochranu údajov vo svojich príspevkoch k diskusiám o novom rámci ochrany údajov. Konkrétne uviedli, že „*nie je vždy jasné, čo tvorí skutočný, jednoznačný súhlas. Niektorí kontrolóri údajov využívajú túto nejasnosť tak, že sa spoliehajú na spôsoby, ktoré nie sú na poskytovanie skutočného, jednoznačného súhlasu vhodné*“¹⁵ v rozpore s podmienkami článku 6 smernice. V rovnakom zmysle pracovná skupina zriadená podľa článku 29 poznamenala, že „*zložitosť postupov zberu údajov, obchodných modelov, predajných vzťahov a technologických aplikácií v mnohých prípadoch predbieha schopnosť alebo ochotu jednotlivca prijať rozhodnutia kontrolovať použitie a zdieľanie informácií prostredníctvom aktívneho výberu*“¹⁶.

¹⁴ WP 114 – Pracovný dokument pracovnej skupiny zriadenej podľa článku 29 o jednotnej interpretácii článku 26 ods. 1 smernice 95/46/ES z 24. októbra 1995.

¹⁵ Stanovisko európskeho dozorného úradníka pre ochranu údajov zo 14. januára 2011 k oznámeniu Komisie „Komplexný prístup k ochrane osobných údajov v Európskej únii“.

¹⁶ „Budúcnosť súkromia: Spoločný príspevok ku konzultáciám Európskej komisie o právnom rámci pre základné právo na ochranu osobných údajov“, 1. decembra 2009, WP 168.

Z tohto dôvodu je dôležité vysvetliť obmedzenia súhlasu a zabezpečiť, aby sa za súhlas považoval iba taký súhlas, ktorý je vytvorený v súlade so zákonom.¹⁷

III. Analýza ustanovení

V tejto analýze sa zameriame na smernicu 95/46/ES v kapitole III.A. Niektoré významné časti smernice o súkromí a elektronických komunikáciách 2002/58/ES budeme analyzovať v kapitole III.B. Treba poznamenať, že smernice sa navzájom nevyklúčujú. Všeobecné podmienky platnosti súhlasu, stanovené v smernici 95/46/ES sa uplatňujú vo svete offline aj online. V smernici 2002/58/ES sa tieto podmienky špecifikujú pre niektoré výslovne identifikované služby poskytované online, vždy vo svetle všeobecných podmienok smernice o ochrane údajov.

III.A Smernica 95/46/ES

Pojem „súhlas dotknutej osoby“ je definovaný v článku 2 písm. h) a následne sa používa v článkoch 7, 8 a 26. Úloha súhlasu sa spomína aj v odôvodneniach 30 a 45. Tieto ustanovenia a všetky relevantné podrobnosti sa budú analyzovať osobitne a v tejto kapitole.

III.A.1. Článok 2 písm. h)

Podľa článku 2 písm. h) „súhlas dotknutej osoby“ znamená „akýkoľvek slobodne daný, konkrétny a vedomý prejav vôle, ktorým dotknutá osoba prejaví svoj súhlas s tým, aby sa osobné údaje, ktoré sa jej týkajú, spracúvali“. Táto definícia obsahuje rôzne kľúčové prvky, o ktorých budem diskutovať v ďalších častiach textu.

„... akýkoľvek ... prejav vôle ..., ktorým dotknutá osoba prejaví ...“

Pokiaľ ide o formu súhlasu, v zásade neexistujú žiadne obmedzenia. Na to, aby bol súhlas platný podľa smernice, by mal byť prejavom vôle. Aj keď to môže byť „akákoľvek“ forma prejavu, malo by byť jasné, čo presne môže patriť do definície prejavu.

Forma prejavu (t. j. spôsob prejavu vôle) v smernici nie je vymedzená. Z dôvodov pružnosti sa z konečného znenia vypustil „písomný“ súhlas. Malo by sa zdôrazniť, že v smernici sa uvádza „akýkoľvek“ prejav vôle. Týmto sa otvára možnosť širokého chápania rozsahu takéhoto prejavu. Minimálne vyjadrenie prejavu by mohol byť akýkoľvek druh signálu, dostatočne jasný na to, aby sa ním mohla prejavovať vôľa dotknutej osoby, ktorý by bol zrozumiteľný pre kontrolóra údajov. Slová „prejav“ a „prejavenie“ poukazujú v smere skutočne potrebného činu (v protiklade so situáciou, v ktorej by sa súhlas mohol vyvodit' z nečinnosti).

Súhlas by mal zahŕňať akýkoľvek prejav vôle, ktorým dotknutá osoba *prejaví* svoj súhlas: mohol by zahŕňať vlastnoručný podpis pripojený na spodku formulára ale aj ústne vyhlásenia o prejavení súhlasu alebo správanie, z ktorého možno logicky vyvodit' súhlas. Preto okrem klasického príkladu podpisu by sa definícia mohla vzťahovať aj na vloženie vizitky do sklenenej nádoby. To isté platí, ak jednotlivец pošle svoje meno a

¹⁷ Stanovisko európskeho dozorného úradníka pre ochranu údajov zo 14. januára 2011, op.cit.

adresu organizácii s cieľom získať od nej informácie. V tomto prípade by sa jeho čin mal chápať ako skutok, ktorý splnomocňuje na spracovanie takýchto údajov, ak je potrebný na spracovanie a na odpoveď na žiadosť.

Pracovná skupina vo svojom Stanovisku k používaniu miestnych údajov s cieľom poskytovať služby s pridanou hodnotou (WP 115) posúdila, ako by sa jednotlivci mali dostať do pozície, v ktorej môžu prejavíť súhlas so službami, ktoré automaticky vyžadujú ich polohu (napríklad možnosť zavolať na konkrétne číslo s cieľom získať informácie o predpovedi počasia podľa polohy jednotlivca). V tomto prípade sa uznalo, že ak používatelia vopred dostali úplné informácie o spracovaní ich polohových údajov, zavolaním na príslušné číslo by prejavili súhlas s tým, že služba zistí ich polohu.

Príklad: Reklama prostredníctvom technológie bluetooth

V súčasnosti sa rozvíja reklamný nástroj, ktorý funguje tak, že okoloidúcim ľuďom posielajú správy s výzvou na aktiváciu spojenia bluetooth, aby mohli prijať reklamné správy. Správy sa posielajú ľuďom, ktorí majú aktivované zariadenie bluetooth na mobile. Samotná aktivácia funkcie bluetooth nepredstavuje platný súhlas (t. j. používateľ by si funkciu bluetooth mohol aktivovať na iné účely). Na druhej strane, ak je niekto oboznámený so službou a so svojím mobilom sa priblíži k takémuto zariadeniu na niekoľko centimetrov, bežne povedané, je to prejavom vôle: na základe toho vidno, ktorí ľudia majú skutočne záujem prijať reklamu. Iba títo ľudia by sa mali považovať za ľudí, ktorí dali svoj súhlas, a iba oni by mali dostať správy na svoj telefón.

Je otázne, či absencia akéhokoľvek správania – alebo ešte lepšie: pasívne správanie – by sa dalo tiež vykladať ako prejav (vôle) za veľmi špecifických okolností (t. j. v úplne jednoznačnom kontexte). Pojem „prejav“ (vôle) je široký, ale zdá sa, že z neho vyplýva potreba skutku. Ďalšie prvky definície súhlasu a dodatočná požiadavka v článku 7 písm. a), aby bol súhlas jednoznačný, podporujú tento výklad. Zdá sa, že požiadavka, aby dotknutá osoba „prejavila“ svoj súhlas, naznačuje, že jednoduchá nečinnosť je nedostatočná a že sa vyžaduje určitý druh činu, ktorým sa prejaví súhlas, aj keď je možné posúdiť rôzne druhy skutkov ako skutky „v kontexte“.

V praxi v absencii aktívneho správania sa dotknutej osoby bude pre kontrolóra údajov problematické overiť, či mlčanie malo znamenať prijatie alebo súhlas. Kontrolór údajov napríklad nemusel mať istotu potrebnú na to, aby predpokladal súhlas v tomto prípade: predstavme si situáciu, v ktorej na list poslaný zákazníkom, v ktorom sú informovaní o plánovanom prenose ich údajov, pokiaľ nevznesú námietku do 2 týždňov, na tento list odpovie iba 10 % zákazníkov. V tomto prípade by sme mohli spochybniť, že tých 90 % zákazníkov, ktorí neodpovedali, skutočne súhlasilo s prenosom. V takýchto prípadoch kontrolór údajov nemá jasný prejav úmyslu dotknutých osôb. Okrem toho nebude mať ani dôkaz, a preto nebude môcť preukázať, že získal súhlas. V praxi nejednoznačnosť pasívnej odpovede sťažuje plnenie požiadaviek smernice.

„... slobodne poskytnutý ...“

Súhlas môže byť platný iba vtedy, ak si dotknutá osoba skutočne môže vybrať a neexistuje riziko podvodu, zastrasovania, nátlaku alebo významných negatívnych následkov, ak dotknutá osoba nebude súhlasiť. Keby následky prejavu súhlasu

ohrozovali slobodu výberu jednotlivcov, súhlas by nebol slobodný. V samotnej smernici sa v článku 8 ods. 2 písm. a) stanovuje, že v niektorých prípadoch, o ktorých rozhodnú členské štáty, nebude možné súhlasom dotknutej osoby zrušiť zákaz spracovania osobitných kategórií osobných údajov.

Príklad uvedených skutočností poskytuje prípad, v ktorom je dotknutá osoba vystavená vplyvu kontrolóra údajov, napríklad v pracovnom pomere. V tomto prípade, aj keď nie nevyhnutne vždy, môže byť dotknutá osoba v situácii závislosti od kontrolóra údajov – pre povahu vzťahu alebo na základe osobitných okolností – a môže sa obávať, že by sa s ňou mohlo zaobchádzať inak, ak neposkytne súhlas so spracovaním údajov.

Pracovná skupina vo viacerých stanoviskách preskúmala obmedzenia súhlasu v situáciách, v ktorých sa nemôže slobodne poskytnúť. Bolo to tak najmä v jej stanoviskách o elektronických zdravotných záznamoch (WP 131), o spracovaní údajov v súvislosti so zamestnaním (WP 48) a o spracovaní údajov Svetovou antidopingovou agentúrou (WP 162).

V stanovisku WP 131 pracovná skupina uvádza, že „slobodný súhlas znamená dobrovoľné rozhodnutie osoby, ktorá má všetky svoje práva, prijaté bez akéhokoľvek druhu donútenia, či už sociálneho, finančného, psychologického alebo iného. Akýkoľvek súhlas pod hrozbou neošetrenia alebo nižšej kvality ošetrovania lekárskeho prípadu nemožno považovať za „slobodný“ ... V prípade, keď zdravotnícky odborník musí spracovať osobné údaje v systéme EZZ v dôsledku nutných a neodvratných dôsledkov zdravotného stavu, je zavádzajúce, ak sa snaží legalizovať toto spracovanie prostredníctvom súhlasu. Spoliehanie sa na súhlas by sa malo obmedziť na prípady, keď individuálna dotknutá osoba má naozaj slobodnú voľbu a môže následne zrušiť súhlas bez ujmy.“¹⁸

Ak po zrušení súhlasu spracovanie údajov pokračuje na základe iného právneho základu, mohli by sa vzniesť pochybnosti v súvislosti s pôvodným použitím súhlasu ako počiatočného právneho základu: ak sa spracovanie mohlo uskutočniť od začiatku na tomto inom základe, predstavenie situácie, v ktorej sa od jednotlivca vyžadoval súhlas so spracovaním, by sa mohlo považovať za zavádzajúce alebo vnútorne nespravodlivé. Bolo by to iné, keby nastala zmena okolností, napríklad keby sa mal počas spracovania objaviť nový právny základ, ako je nový zákon upravujúci príslušnú databázu. Ak sa tento nový základ môže platne uplatňovať na spracovanie údajov, toto spracovanie môže pokračovať. V praxi však takéto okolnosti nie sú časté. V zásade sa súhlas môže považovať za nedostatočný, ak nie je povolené jeho účinné zrušenie.

Pracovná skupina prijala konzistentný postoj k výkladu slobodného súhlasu v súvislosti so zamestnaním¹⁹: „Ak sa súhlas vyžaduje od pracovníka a pritom existuje skutočná alebo potenciálna súvisiaca zaujatosť vyplývajúca z nesúhlasu, súhlas nie je platný z hľadiska splnenia ustanovení článku 7 alebo článku 8, pretože nie je slobodne poskytnutý. Ak pracovník nemá možnosť odmietnuť, potom to nie je súhlas... Ťažkou

¹⁸ V pracovnom dokumente WP 162 o Svetovej antidopingovej agentúre (WADA) sa dospelo k rovnakému záveru: „Na základe sankcií spojených s prípadným odmietnutím účastníkov podrobiť sa povinnostiam podľa kódexu (napr. poskytnutie materiálov o mieste pobytu) dospela pracovná skupina k záveru, že súlad by v žiadnom prípade nebol poskytnutý slobodne“.

¹⁹ WP 48 o spracovaní osobných údajov v kontexte zamestnania. Relevantný je aj pracovný dokument WP 114 – Pracovný dokument pracovnej skupiny zriadenej podľa článku 29 o jednotnej interpretácii článku 26 ods. 1 smernice 95/46/ES z 24. októbra 1995.

oblasťou je situácia, v ktorej je poskytnutie súhlasu podmienkou zamestnania. Pracovník môže teoreticky odmietnuť poskytnúť súhlas, ale následkom môže byť strata pracovnej príležitosti. V takýchto okolnostiach súhlas nie je slobodne poskytnutý, a preto nie je platný. Situácia je ešte jasnejšia v častých prípadoch, keď všetci zamestnávateľia ukladajú rovnakú alebo podobnú podmienku zamestnania.“

Príklad: fotografie na intranete

Súhlas v kontexte zamestnania môže byť platný, ako ukazuje nasledujúci príklad: Spoločnosť sa rozhodne zriadiť intranet, na ktorom budú umiestnené mená a hlavné úlohy zamestnancov. Každého zamestnanca sa opýta, či by chcel mať pri svojom mene aj fotografiu. Jednotlivcov, ktorí chcú mať nahranú fotografiu, vyzve, aby ju poslali na určenú adresu. Po prijatí primeraných informácií by sa skutok jednotlivca spočívajúci v poslaní fotografie považoval za súhlas. Ak spoločnosť má digitálne fotografie každého zamestnanca a každého z nich požiada o súhlas s nahraním tejto fotografie na uvedené účely, potom by sa kliknutie každého zamestnanca na tlačidlo, ktorým prejaví svoj súhlas, tiež považovalo za poskytnutie platného súhlasu. V oboch prípadoch sa v plnom rozsahu rešpektuje vôľa zamestnancov, pokiaľ ide o uvedenie ich fotografie na intranete.

Kontext zamestnania vyžaduje špecifickú diskusiu: v tomto prípade významnú úlohu zohrávajú kultúrne a sociálne hľadiská pracovného pomeru, ako aj spôsob interakcie zásad ochrany údajov s inými právnymi predpismi. V kontexte zamestnania sa osobné údaje môžu spracúvať na rôzne účely:

- o Údaje potrebné na plnenie úloh zamestnancov: uplatnenie článku 7 písm. b) – nevyhnutnosť pre zmluvu
- o Na určenie nároku zamestnancov na získanie ponuky akcií: buď na základe súhlasu – článok 7 písm. a), alebo považované za inherentné v súvislosti s administratívnymi aspektmi zmluvného pracovného pomeru – článok 7 písm. b)
- o Spracovanie čísla sociálneho poistenia na účely sociálneho zabezpečenia: článok 7 písm. c) – zákonná povinnosť, alebo prípadne článok 8 písm. b) – povinnosti v oblasti pracovného práva
- o Spracovanie etnických údajov: v niektorých krajinách by to tiež mohla byť povinnosť vyplývajúca z pracovného práva – článok 8 písm. b), kým v iných krajinách by takéto spracovanie bolo prísne zakázané.

Aj keď môže existovať silný predpoklad, že v takýchto kontextoch je súhlas slabý, nevyklučuje sa tým úplne jeho použitie za predpokladu, že existujú dostatočné záruky, že súhlas je skutočne slobodný.

Situácia podriadenia je často hlavným dôvodom, ktorý bráni tomu, aby bol súhlas slobodný, aj iné kontextuálne prvky však môžu ovplyvniť rozhodnutie dotknutej osoby. Môžu mať napríklad finančný, emočný alebo praktický rozmer. Aj fakt, že zber údajov vykonáva verejný orgán, môže mať určitý vplyv na dotknutú osobu. Môže však byť ťažké stanoviť rozdiel medzi jednoduchým podnetom a niečím, čo má skutočný vplyv na slobodu dotknutej osoby uplatniť si právo voľby. Nasledujúce príklady majú znázorniť rôznu povahu úsilia alebo ceny pre jednotlivcov, ktorá by mohla ovplyvniť ich rozhodnutie.

Príklad – Elektronické zdravotné záznamy

V mnohých členských štátoch existuje trend vytvárať elektronický súhrn zdravotných záznamov pacientov. Takýto súhrn umožní poskytovateľom zdravotnej starostlivosti prístup ku kľúčovým informáciám vždy, keď pacient potrebuje oštenie.

– V prvom scenári je vytvorenie súhrnného záznamu úplne dobrovoľné a pacientovi bude oštenie poskytnuté bez ohľadu na to, či poskytol súhlas na vytvorenie súhrnného záznamu. V tomto prípade je súhlas s vytvorením súhrnného záznamu slobodne poskytnutý, pretože ak pacient súhlas neposkytne alebo zruší, nevyplynú preň z toho žiadne nevýhody.

– V druhom scenári existuje mierny finančný stimul pre voľbu elektronického zdravotného záznamu. Pacienti, ktorí odmietnu vytvorenie elektronického zdravotného záznamu, nebudú mať žiadne nevýhody v zmysle, že sa cena starostlivosti pre nich nezmení. Aj v tomto prípade by sa dalo usúdiť, že majú slobodu súhlasiť alebo nesúhlasiť s novým systémom.

– V treťom scenári pacienti, ktorí odmietnu elektronický zdravotný systém, musia zaplatiť podstatne viac v porovnaní s predošlým tarifným systémom a spracovanie ich spisu trvá podstatne dlhšie. Znamená to jasnú nevýhodu pre tých ktorí súhlas neposkytnú, so zámerom zabezpečiť prechod všetkých občanov na systém elektronického zdravotníctva v plánovanej lehote. Takýto súhlas preto nie je dostatočne slobodný. Z tohto dôvodu by bolo potrebné preskúmať aj existenciu iných legítimných základov pre spracovanie osobných údajov alebo uplatnenie článku 8 ods. 3 smernice 95/46/ES.

Príklad: telesné skenery

V niektorých verejných priestoroch sa rozvíja použitie telesných skenerov, najmä na letiskách pri vstupe do oblasti na nastupovanie. Vzhľadom na to, že vo chvíli skenovania sa spracúvajú údaje pasažierov²⁰, toto spracovanie musí byť v súlade s jedným z právnych základov podľa článku 7. Prechod cez telesné skenery sa niekedy prezentuje ako možnosť pre pasažierov, z čoho vyplýva, že spracovanie by mohlo byť zdôvodnené ich súhlasom. Odmietnutie prechodu cez telesné skenery by však mohlo vzbudiť podozrenie alebo vyvolať dodatočné kontroly, napríklad telesnú prehliadku. Mnohí cestujúci poskytnú svoj súhlas so skenovaním, pretože sa tak vyhnú potenciálnym problémom alebo meškaniu, keďže ich prioritou je nastúpiť na svoj let načas. Takýto súhlas nie je dostatočne slobodný. Keďže sa musí preukázať, že spracovanie je nevyhnutné (z dôvodov verejnej bezpečnosti), legítimný základ by sme nemali hľadať v článku 7 písm. a), ale v akte zákonodarcu – článok 7 písm. c) alebo písm. e) – z ktorého vyplýva povinnosť pasažierov spolupracovať. Základ pre kontrolu telesným skenerom by tak mal byť právny predpis: v tomto právnom predpise by sa však stále mohla stanoviť možnosť výberu medzi skenovaním a osobnou prehliadkou, táto možnosť by sa však jednotlivcovi ponúkla z dopĺňajúcej perspektívy ako súčasť dodatočných opatrení.

²⁰

Pozri list z 11. februára 2009 predsedu pracovnej skupiny zriadenej podľa článku 29 páňovi Danielovi CALLEJA CRESPO, riaditeľovi GR TREN o telesných skeneroch, v odpovedi na konzultácie Komisie o „vplyve použitia telesných skenerov v oblasti leteckej bezpečnosti na ľudské práva, súkromie, osobnú dôstojnosť, zdravie a ochranu údajov“. Dostupný na adrese: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm.

Charakter kontrolóra údajov môže byť tiež rozhodujúci pre výber právneho základu pre spracovanie osobných údajov. Týka sa to najmä kontrolórov údajov vo verejnom sektore, v ktorom je spracovanie údajov obvykle spojené s plnením zákonnej povinnosti, ako sa uvádza v článku 7 písm. c), alebo plnením úlohy vykonávanej vo verejnom záujme, ako sa uvádza v článku 7 písm. e). Z toho vyplýva, že použitie súhlasu príslušného jednotlivca na legitimáciu spracovania údajov nie je vhodný právny základ. Je to zrejmé najmä v prípade spracovania osobných údajov verejnými orgánmi s právomocami vydávať nariadenia – napríklad orgánmi presadzovania práva konajúcimi v oblasti právomocí ich úloh na poli policajných a justičných činností. Policajné orgány sa nemôžu spoliehať na súhlas jednotlivca v prípade opatrení, ktoré neboli stanovené, alebo by inak neboli zákonom povolené.

Napriek tomu treba uznať, že aj keď štáty môžu mať zákonnú povinnosť spracovať osobné údaje, jednotlivec nemá vždy povinnosť spolupracovať. Môžu nastať prípady, keď sa dotknutým osobám poskytujú „služby s pridanou hodnotou“, pri ktorých sa môžu rozhodnúť, či ich budú využívať alebo nie. Vo väčšine prípadov je však spracovanie v skutočnosti povinné. Často nie je ľahké zistiť, či sa verejné orgány pri spracovaní osobných údajov oprávnené spoliehajú na súhlas jednotlivca. Spracovanie osobných údajov vo verejnom sektore preto často zahŕňa hybridné systémy, čo môže viesť k neistote a zneužitiu, ak sa nesprávne zdôvodňuje súhlasom.

Aj keď súhlas môže byť vo výnimočných prípadoch platným základom pre štáty na spracovanie osobných údajov, mala by sa vykonať starostlivá kontrola od prípadu k prípadu s cieľom posúdiť, či je súhlas skutočne dostatočne slobodný. Ako znázorňujú nasledovné príklady, ak je kontrolórom údajov verejný orgán, bude právny základ pre legitimáciu spracovania bude skôr než súhlas predstavovať súlad so zákonnou povinnosťou podľa článku 7 písm. c) alebo plnenie úlohy vo verejnom záujme podľa článku 7 písm. e).

Príklad: elektronická štátna správa

V členských štátoch sa vyvíjajú nové občianske preukazy s elektronickými funkciami zabudovanými do čipu. Nemusí byť povinné aktivovať elektronické služby karty. Ale bez aktivácie by sa používateľovi mohol odmietnuť prístup k určitým administratívnym službám, ku ktorým by bolo veľmi ťažké získať prístup iným spôsobom (prenos určitých služieb online, skrátenie pracovného času). Súhlas sa nemôže považovať za legitímny základ pre oprávnenie spracovania. V tomto prípade by príslušným základom mal byť zákon o organizácii vývoja elektronických služieb spolu so všetkými primeranými zárukami.

Príklad: osobné záznamy o cestujúcich

Diskutovalo sa o otázke, či sa súhlas pasažierov môže platne použiť na legitimáciu prenosu rezervačných údajov („osobných záznamov cestujúcich“) európskymi leteckými spoločnosťami orgánom USA. Pracovná skupina sa nazdáva, že súhlas pasažierov nemôže byť poskytnutý slobodne, pretože letecké spoločnosti majú povinnosť poslať údaje pred odletom, a preto cestujúci nemajú v skutočnosti možnosť výberu, ak chcú letieť.²¹

²¹ Pozri stanovisko 6/2002 pracovnej skupiny zriadenej podľa článku 29 k prenosu evidentných informácií o cestujúcich a iných údajov z aerolínií do Spojených štátov.

Právnym základom tu nie je súhlas cestujúceho, ale skôr v súlade s článkom 7 písm. c) povinnosti stanovené v medzinárodnej dohode medzi EÚ a USA o spracovaní a prenose osobných záznamov o cestujúcich (PNR).

Príklad: celoštátne sčítanie obyvateľstva

Počas celoštátneho sčítania obyvateľstva sa od obyvateľov vyžaduje, aby odpovedali na rôzne otázky o ich osobnej a pracovnej situácii. Odpovedať na tieto otázky je povinné. Okrem toho sčítanie obyvateľstva zahŕňa aj otázku, pri ktorej je odpoveď jasne označená ako voliteľná a táto otázka sa týka dopravných prostriedkov, ktoré jednotliviec používa. Aj keď istotne neexistuje slobodný súhlas pre hlavnú časť sčítania obyvateľstva, existuje možnosť slobodného výberu, pokiaľ ide o odpoveď na túto poslednú nepovinnú otázku. Nemal by sa tým však zahmlievať fakt, že hlavným zámerom štátu pri vydaní tohto dotazníka je získať odpovede. Súhlas v tomto kontexte vo všeobecnosti nepredstavuje platný základ.

„... *konkrétny* ...“

Súhlas je platný, iba ak je konkrétny. Inými slovami nevyplnený súhlas bez uvedenia presného účelu spracovania nie je prijateľný.

Aby bol súhlas konkrétny, musí byť zrozumiteľný: mal by jasne a presne odkazovať na rozsah a následky spracovania údajov. Nemôže sa uplatniť na otvorený súbor činností spracovania. Inými slovami to znamená, že kontext, v ktorom sa súhlas uplatňuje, je obmedzený.

Súhlas sa musí poskytnúť vo vzťahu k rôznym aspektom spracovania, ktoré sa musia jasne identifikovať. Musí obsahovať najmä informácie o tom, aké údaje sa spracúvajú a na aké účely. Toto chápanie by malo byť založené na primeraných očakávaniach strán. „Konkrétny súhlas“ je preto neoddeliteľne spojený so skutočnosťou, že súhlas musí byť vedomý. Existuje požiadavka členitosti súhlasu, pokiaľ ide o rôzne prvky, ktoré tvoria spracovanie údajov: nemôže sa chápať tak, že sa vzťahuje na „všetky legítimne účely“, ktoré sleduje kontrolór údajov. Súhlas by mal odkazovať na spracovanie, ktoré je opodstatnené a nevyhnutné vo vzťahu k účelu.

V zásade by malo stačiť, aby kontrolóri údajov získali súhlas iba raz pre rôzne operácie, ak sú v rámci primeraných očakávaní dotknutej osoby.

Súdny dvor Európskych spoločenstiev vydal predbežné rozhodnutie²² týkajúce sa článku 12 ods. 2 smernice o súkromí a elektronických komunikáciách, pokiaľ ide o potrebu obnoveného súhlasu abonentov, ktorí už raz poskytli svoj súhlas so zverejnením ich osobných údajov v jednom adresári, pred prenosom ich osobných údajov na zverejnenie službami iného adresára. Súdny dvor konštatoval, že keď bol abonent správne informovaný o možnosti postúpenia jeho osobných údajov podniku, ktorý je treťou osobou a abonent už súhlasil so zverejnením týchto údajov v takomto adresári, pre prenos tých istých údajov nie je potrebný obnovený súhlas abonenta, *ak je zaručené, že*

²² Rozsudok Súdneho dvora z 5. mája 2011, Deutsche Telekom AG (vec C-543/09). Táto vec začala žiadosťou, ktorú predložil nemecký Spolkový správny súd v súvislosti s telekomunikačnými adresármi a najmä výkladom článku 25 ods. 2 smernice o univerzálnej službe (2002/22/ES) a článkom 12 ods. 2 smernice o elektronickom súkromí (2002/58/ES). Je jasne spojený so špeciálnou úlohou adresárov v smernici o univerzálnej službe.

príslušné údaje sa nepoužijú na iné účely, než na ktoré sa zbierali s cieľom ich prvého zverejnenia (odsek 65).

Špecifický súhlas však môže byť potrebný, ak kontrolór má v úmysle údaje spracovať na iné účely. Súhlas by sa napríklad mohol poskytnúť pre informácie o nových produktoch určené jednotlivcovi a o osobitných propagačných akciách, pretože by sa mohlo usúdiť, že to patrí do rámca primeraných očakávaní dotknutej osoby. Mal by sa však vyžadovať samostatný a doplňujúci súhlas, ktorý umožní odoslanie údajov jednotlivca tretím stranám. Potreba rozdelenia získania súhlasu by sa mala posúdiť od prípadu k prípadu, v závislosti od účelov alebo príjemcov údajov.

Malo by sa pripomenúť, že spracovanie by mohlo mať viacero rôznych právnych základov: niektoré údaje by sa mohli spracovať, pretože sú nevyhnutné v rámci zmluvy s dotknutou osobou, napríklad na plnenie funkcie produktu a riadenie služby a konkrétny súhlas sa môže vyžadovať na spracovanie nad rámec toho, čo je nevyhnutné pre plnenie zmluvy, napríklad na prístup k platobným funkciám (bodové hodnotenie kreditného rizika) dotknutej osoby.

Pracovná skupina vysvetlila toto hľadisko súhlasu v pracovnom dokumente WP 131 o elektronických zdravotných záznamoch (EZZ): „špecifický“ súhlas sa musí týkať jasne definovanej, konkrétnej situácie, v ktorej sa počíta so spracovaním zdravotných údajov. „Všeobecný súhlas“ dotknutej osoby, napríklad so zberom jej zdravotných údajov pre EZZ a s následnými prenosmi týchto minulých a budúcich zdravotných údajov zdravotníckym odborníkom zapojeným do liečby, by preto nepredstavoval súhlas v zmysle článku 2 písm. h) smernice.

Rovnaká argumentácia sa uvádza v stanovisku WP 115 k používaniu miestnych údajov s cieľom poskytovať služby s pridanou hodnotou: *„Toto vymedzenie pojmu výslovne vylučuje, aby sa súhlas dal v rámci prijatia všeobecných podmienok poskytovania ponúkanej elektronickej komunikačnej služby. ... Súhlas sa však môže v závislosti od druhu ponúkanej služby týkať konkrétnej operácie alebo môže predstavovať dohodu o priebežnom určovaní polohy.“*

V rozhodnutí Súdneho dvora, uvedenom v kapitole II „Úloha súhlasu“, aj keď sa výraz „konkrétny“ výslovne nepoužíva, z argumentácie takisto vyplýva potreba, aby bol súhlas konkrétny, keďže sa v ňom uvádza, že *„nepostačuje, že pracovná zmluva dotknutého zamestnanca odkazuje na kolektívnu zmluvu, ktorá umožňuje takéto prekročenie.“*

Príklad: sociálne siete

Prístup k službám sociálnych sietí je často podmienený súhlasom s rôznymi druhmi spracovania osobných údajov.

Od používateľa sa môže vyžadovať, aby súhlasil s prijímaním behaviorálnej reklamy, ak sa chce zaregistrovať v službe sociálnej siete, bez ďalšej špecifikácie alebo iných možností. Vzhľadom na význam, aký získali niektoré sociálne siete, niektoré kategórie používateľov (ako tínedžeri) prejavujú súhlas s prijímaním behaviorálnej reklamy, aby sa vyhli riziku, že budú čiastočne vylúčení zo sociálnych interakcií. Používateľovi by sa mala ponúknuť pozícia, v ktorej môže poskytnúť slobodný a konkrétny súhlas s prijímaním behaviorálnej reklamy, nezávisle od jeho prístupu k službe sociálnej siete. Mohlo by sa použiť dialógové okno, v ktorom sa používateľovi ponúkne takáto možnosť.

Služba sociálnych sietí ponúka možnosť používať externé aplikácie. Používateľovi sa v praxi často zabráni v používaní aplikácie, ak nesúhlasí s prenosom jeho údajov vývojárovi aplikácie na širokú škálu účelov vrátane behaviorálnej reklamy a opätovného predaja tretím stranám. Vzhľadom na to, že aplikácia môže fungovať bez toho, aby sa akékoľvek údaje prenášali vývojárovi aplikácie, pracovná skupina uprednostňuje rozdelenie získania súhlasu používateľa, t. j. získanie samostatného súhlasu používateľa s prenosom jeho údajov vývojárovi na tieto rôzne účely. Mohli by sa používať rôzne mechanizmy ako dialógové okná s cieľom ponúknuť používateľovi možnosť vybrať si použitie údajov, s ktorým súhlasí (prenos vývojárovi, služby s pridanou hodnotou, behaviorálna reklama, prenos tretím stranám atď.).

Konkrétnosť súhlasu tiež znamená, že ak účely, na ktoré kontrolór údaje spracúva, sa v určitej chvíli zmenia, táto zmena sa musí oznámiť používateľovi a musí sa mu ponúknuť pozícia, v ktorej používateľ môže prejaviť súhlas s novým spracovaním údajov. Poskytnuté informácie sa musia vzťahovať najmä na následky odmietnutia navrhovaných zmien.

„... vedomý ...“

Posledný prvok definície súhlasu – nie však najmenšia požiadavka, ako ďalej uvidíme – je jeho vedomý charakter.

V článkoch 10 a 11 smernice sa stanovila povinnosť poskytnúť dotknutým osobám informácie. Povinnosť informovať je preto špecifická, ale v mnohých prípadoch je evidentne spojená so súhlasom. Kým súhlas nenasleduje vždy po poskytnutí informácií (môže sa použiť ďalší základ z článku 7), pred poskytnutím súhlasu vždy musia existovať informácie.

V praxi to znamená, že „súhlas dotknutej osoby (musí byť) na základe zhodnotenia a pochopenia skutočností a dôsledkov tohto kroku. Príslušnej osobe sa musia jasným a zrozumiteľným spôsobom poskytnúť presné a úplné informácie o všetkých príslušných záležitostiach, najmä o tých, ktoré sú uvedené v článkoch 10 a 11 smernice, napríklad charakter spracovaných údajov, účely spracovania, príjemcovia možných prenosov a práva dotknutej osoby. Patrí sem aj informovanosť o dôsledkoch neposkytnutia súhlasu s príslušným spracovaním“²³.

Súhlas sa v mnohých prípadoch získa vo chvíli zberu osobných údajov na začiatku spracovania. V tomto prípade sa informácie, ktoré sa majú poskytnúť, zhodujú s tým, čo je uvedené v článku 10 smernice. Súhlas sa však môže vyžiadať aj „následne“, keď sa zmení účel spracovania. V tomto prípade budú informácie, ktoré sa majú poskytnúť, zamerané na to, čo je potrebné v konkrétnej súvislosti vo vzťahu k príslušnému účelu.

²³ WP 131 – Pracovný dokument o spracovaní osobných údajov týkajúcich sa zdravotného stavu v elektronických zdravotných záznamoch.

Vedomý súhlas je osobitne rozhodujúci v kontexte prenosu osobných údajov do tretích krajín: „vyžaduje, aby dotknutá osoba bola riadne informovaná o osobitnom riziku, že jej údaje sa majú preniesť do krajiny, v ktorej neexistuje primeraná ochrana“²⁴.

S cieľom zabezpečiť primerané informácie možno identifikovať dva druhy požiadaviek:

- Kvalita informácií – spôsob, akým sa informácie poskytujú (jednoducho, bez žargónu, zrozumiteľne, zreteľne), je rozhodujúci pre posúdenie skutočnosti, či je súhlas „vedomý“. Spôsob, akým by sa tieto informácie mali poskytovať, závisí od kontextu: bežný/priemerný používateľ by im mal rozumieť.
- Prístupnosť a viditeľnosť informácií – informácie sa musia poskytnúť priamo jednotlivcom. Nestačí, aby boli informácie „dostupné“ kdekoľvek. Súdny dvor na tomto bode trval vo svojom rozsudku z roku 2004²⁵, v ktorom uviedol pracovnú zmluvu obsahujúcu podmienky, ktoré neboli uvedené v nej, ale na ktoré sa v nej iba odkazovalo. Informácie musia byť jasne viditeľné (typ a veľkosť písma), nápadné a zrozumiteľné. Vo chvíli vyžiadania súhlasu sa môžu na poskytnutie konkrétnych informácií použiť dialógové okná. Ako sme uviedli vo vzťahu ku „konkrétnej súhlasu“, obzvlášť užitočné sú informačné nástroje online v súvislosti so službami sociálnych sietí na poskytnutie dostatočného rozdelenia a jasnosti nastavení ochrany súkromia. V tomto prípade môžu byť užitočným nástrojom aj vrstvené upozornenia, pretože prispievajú k poskytnutiu správnych informácií ľahko prístupným spôsobom.

Kým plyní čas, môžu vzniknúť pochybnosti, či súhlas pôvodne založený na platných, dostatočných informáciách, je ešte stále platný. Z rôznych dôvodov ľudia často menia svoje názory, pretože ich počiatočné rozhodnutia neboli dobré, alebo pre zmenu okolností, napríklad, keď dieťa dospeje²⁶. Z tohto dôvodu by v rámci osvedčeného postupu kontrolóri údajov mali vyvíjať úsilie, aby po určitom čase revidovali voľby jednotlivca, napríklad tak, že ho budú informovať o jeho aktuálnej voľbe a poskytnú mu možnosť túto voľbu potvrdiť alebo odvolať²⁷. Príslušné obdobie by samozrejme záviselo od kontextu a okolností prípadu.

Príklad: mapovanie trestnej činnosti

Niektoré policajné zložky uvažujú o zverejnení máp alebo uvoľnení iných údajov o tom, kde sa odohrali konkrétne druhy trestnej činnosti. Záruky zabudované do tohto procesu obvykle spočívajú v tom, že sa nezverejňujú žiadne osobné údaje obetí trestného činu, pretože trestná činnosť sa spája iba s pomerne širokými zemepisnými regiónmi. Niektoré policajné zložky však chcú trestný čin presnejšie zamerať, ak s tým súhlasí obeť. V takomto prípade je možné presnejšie spojiť dotknutú osobu s miestom, na ktorom bol trestný čin spáchaný. Obeti sa však konkrétne neoznami, že identifikovateľné informácie o nej sa zverejnia otvorene na internete a ako sa tieto informácie môžu použiť. Preto súhlas v tomto prípade nie je platný, pretože obeť nemusí úplne rozumieť rozsahu, v akom sa zverejňujú informácie o nich.

²⁴ WP 12 – Pracovný dokument Prenos osobných údajov do tretích krajín: uplatňovanie článkov 25 a 26 smernice EÚ o ochrane údajov. Pozri aj WP 114 – Pracovný dokument pracovnej skupiny zriadenej podľa článku 29 o jednotnej interpretácii článku 26 ods. 1 smernice 95/46/ES z 24. októbra 1995.

²⁵ Pozri poznámku pod čiarou 12 (kapitola II.2)

²⁶ Pracovný dokument 1/2008 o ochrane osobných údajov detí, WP 147, 18. februára 2008.

²⁷ Pracovná skupina zriadená podľa článku 29 poskytla podobné odporúčanie vo svojom stanovisku 171 k behaviorálnej reklame online, prijatom 22.06.2010.

Čím zložitejšie je spracovanie údajov, tým viac možno očakávať od kontrolóra údajov. Čím ťažšie je pre priemerného obyvateľa dohliadať na všetky prvky spracovania údajov a pochopiť ich, tým väčšie by malo byť úsilie kontrolóra údajov preukázať, že získal súhlas na základe konkrétnych, zrozumiteľných informácií.

Súhlas podľa definície v článku 2 písm. h) by sa mal vykladať spolu s ďalšími požiadavkami uvedenými v ďalších častiach textu smernice. V článku 7 sa pridáva slovo „jednoznačný“ k prvkom definície a v článku 8 sa pridáva slovo „výslovný“, ak sa spracovanie týka spracovania osobitných kategórií údajov.

III.A.2. Článok 7 písm. a)

Podľa článku 7 písm. a) smernice jednoznačný súhlas dotknutej osoby tvorí právny základ pre spracovanie osobných údajov. Preto, aby bol platný, okrem splnenia kritérií stanovených v článku 2 písm. h), súhlas musí byť aj jednoznačný.

Aby bol súhlas jednoznačný, postup vyžiadania a získania súhlasu nesmie zanechať *žiadne pochybnosti* o úmysle dotknutej osoby udeliť súhlas. Inými slovami, prejav súhlasu dotknutej osoby nesmie nechať priestor na nejednoznačnosť, pokiaľ ide o jej úmysel. Ak existujú dôvodné pochybnosti o úmysle jednotlivca, existuje nejednoznačnosť.

Ako sa ďalej opisuje, táto požiadavka zaväzuje kontrolórov údajov, aby vytvorili účinné postupy poskytovania súhlasu jednotlivcami, teda aby buď vyžadovali jasný výslovný súhlas, alebo aby sa spoliehali na určité druhy postupov, z ktorých je možné vyvodiť jasný súhlas jednotlivcov. Kontrolór údajov musí mať dostatočnú istotu, že osoba, ktorá poskytuje súhlas, je skutočne dotknutou osobou. Toto je zvlášť dôležité pri získavaní súhlasu telefonicky alebo online.

Súvisiaci problém sa týka dôkazu súhlasu. Kontrolóri údajov, ktorí sa spoliehajú na súhlas môžu mať záujem alebo potrebu preukázať, že súhlas získali napríklad v kontexte sporu s dotknutou osobou. V niektorých prípadoch skutočne môžu byť vyzvaní, aby predložili takýto dôkaz v rámci opatrení presadzovania práva. Preto a v zmysle osvedčeného postupu by kontrolóri údajov mali vytvoriť a uchovávať dôkaz, ktorý potvrdzuje, že súhlas bol skutočne poskytnutý, t. j. súhlas by mal byť overiteľný.

Rozoberme teraz nasledujúce metódy poskytnutia súhlasu a posúdme, či zabezpečujú jednoznačný súhlas.

Výslovné výroky prejavu súhlasu, ako podpísaná dohoda alebo písomné vyhlásenia o vôli prejaviť súhlas, sú postupy alebo mechanizmy vhodné na získanie jednoznačného súhlasu. Zároveň v zásade poskytujú kontrolórovi údajov dôkaz o získaní súhlasu.

Príklad: súhlas s prijímaním propagačných informácií klasickou poštou

Hotel požiada jednotlivcov, aby uviedli svoju poštovú adresu vo formulári, ak si želajú dostávať propagačné informácie klasickou poštou. Ak jednotlivец po poskytnutí poštovej adresy podpíše tento formulár, čím vyjadrí svoj súhlas, ide o jednoznačný súhlas. V tomto prípade je súhlas výslovný aj písomný. Tento postup zaručuje kontrolórovi údajov primeraný dôkaz o získaní súhlasu od všetkých zákazníkov, pokiaľ si kontrolór údajov uchová všetky podpísané formuláre.

Avšak nie všetky formy súhlasu, ktoré sa môžu zdať výslovné, skutočne predstavujú súhlas. Tento problém sa riešil v nedávnej veci Súdneho dvora (Volker und Markus Schecke / Land Hessen), ktorá sa týkala uverejňovania názvov príjemcov pomoci z rôznych fondov EÚ²⁸ a súm, ktoré prijali jednotliví príjemcovia. Generálny advokát analyzoval, či boli splnené podmienky jednoznačného súhlasu v prípade, keď jednotlivci podpísali vyhlásenie: „Som si vedomý, že na základe článku 44 písm. a) nariadenia ... č. 1290/2005 sa vyžaduje zverejnenie informácií o príjemcoch [finančných prostriedkov z] EPZF a EPFRV a sumách, ktoré prijali jednotliví príjemcovia.“ Generálny advokát dospel k záveru: „Potvrdenie predchádzajúceho oznámenia, že dôjde k určitému druhu zverejnenia, nie je totožné s udelením „jednoznačného“ súhlasu s konkrétnym druhom podrobného zverejnenia. Nemožno ho ani označiť za „slobodný a výslovný prejav vôle“ žalobcov v súlade s definíciou súhlasu dotknutej osoby v článku 2 písm. h).“ Preto generálna prokurátorka dospela k záveru, že žalobcovia neudelili súhlas so spracovaním (t. j. zverejnením) svojich osobných údajov v zmysle článku 7 písm. a) smernice 95/46/ES.²⁹

Výslovný súhlas sa môže udeliť aj v prostredí online. Tak ako vo svete offline, existujú veľmi vhodné prostriedky na získanie jednoznačného súhlasu, ako znázorňuje nasledujúci príklad.

Príklad: súhlas online so zaregistrovaním do vernostného programu

Na webovej stránke hotela sa nachádza rezervačný formulár, ktorý jednotlivcom umožňuje vopred si rezervovať izby elektronicky. Formulár online, v ktorom jednotlivci uvádzajú želané dátumy a informácie o platbe, obsahuje aj viditeľné políčko, ktoré majú vyznačiť jednotlivci, ktorí si želajú, aby sa ich údaje na účely registrácie do vernostného programu. Vyznačenie políčka po prijatí príslušných informácií by predstavovalo výslovný, jednoznačný súhlas, pretože akt vyznačenia políčka je dostatočne jasný a nezanecháva žiadne pochybnosti o vôle jednotlivca zaregistrovať sa do vernostného programu.

Výslovný súhlas sa môže udeliť aj ústne, vyhláseniami určenými na prejav súhlasu. Výslovný ústny súhlas by sa poskytol v nasledovnej situácii.

Príklad: ústny súhlas s prijímaním propagačných informácií

Pri platení na recepcii hotela sa recepčná opýta klientov, či by chceli poskytnúť svoju adresu, aby im hotel mohol posielat' propagačné informácie. Jednotlivci, ktorí odpovedia poskytnutím svojej poštovej adresy po tom, čo si vypočuli výzvu recepčnej a príslušné informácie, by poskytli výslovný súhlas. Akt poskytnutia ich adresy môže predstavovať jednoznačný prejav vôle jednotlivca. Kontrolór údajov sa však môže rozhodnúť, že zavedie mechanizmy na spoľahlivejšie preukázanie udelenia súhlasu.

²⁸ Európsky poľnohospodársky záručný fond (EPZF) a Európsky poľnohospodársky fond pre rozvoj vidieka (EPFRV).

²⁹ Stanovisko generálneho advokáta Sharpstona, poskytnuté 17. júna 2010, Volker und Markus Schecke GbR, v spojených veciach C-92/09 a C-93/09. Malo by sa poznamenať, že Súdny dvor vo svojom rozsudku z 9. novembra 2010 rozhodol, že spracovanie údajov nebolo na základe súhlasu: „63. Dotknutá právna úprava Únie, ktorá sa obmedzuje na stanovenie toho, že prijímatelia pomoci sú vopred informovaní o uverejnení ich údajov, teda nevyžaduje súhlas dotknutých prijímateľov ako základ pre spracúvanie osobných údajov, ktoré zavádza.“

Za určitých okolností sa jednoznačný súhlas môže *vyvodiť* z určitých aktov, najmä v prípade, ak takéto akty vedú k jednoznačnému záveru, že súhlas bol poskytnutý. Závisí to však od poskytnutia príslušných informácií o spracovaní údajov, ktoré jednotlivcovi umožňujú prijať rozhodnutie (od toho, kto je kontrolór údajov, aké sú účely spracovania atď.).

Príklad: súhlas s vytvorením fotografie

Pri vybavovaní na recepcii hotela recepcná informuje hostí, že sa v jednej z kaviarní hotela popoludní uskutoční fotenie. Vybrané fotografie sa použijú v marketingových materiáloch, najmä v podobe papierových brožúr o hoteli. Ak by sa hoteloví hostia chceli zúčastniť na tomto foteaní, sú pozvaní do kaviarne v určenom čase. Tí, ktorí sa nechcú fotiť, majú k dispozícii inú kaviareň.

Hoteloví hostia, ktorí sa po tom, ako boli informovaní, rozhodnú ísť do kaviarne počas fotografovania sa môžu posúdiť ako hostia, ktorí súhlasili s tým, že ich budú fotografovať. Ich súhlas možno odvodiť z ich aktu navštívenia kaviarne, v ktorej sa fotografuje v určenom čase. Tým, že prišli do tejto kaviarne, prejavili vôľu jednotlivca, čo sa v zásade môže považovať za jednoznačné, pokiaľ neexistujú väčšie pochybnosti o tom, že jednotlivec, ktorý navštívil kaviareň, sa fotografovať nechcel. Hotel však môže považovať za rozvážne uchovať si listinný dôkaz o získanom súhlase pre prípad, že niekto v blízkej budúcnosti platnosť takéhoto súhlasu napadne.

Ako sme už uviedli, rovnaké požiadavky vrátane jednoznačného súhlasu sa vzťahujú na svet offline aj na svet online. Pracovná skupina však poznamenáva, že riziko nejednoznačného súhlasu je pravdepodobne vyššie vo svete online, čo si vyžaduje osobitnú pozornosť. Nasledujúci príklad znázorňuje prípad, v ktorom súhlas odvodený z určitého aktu (účasti na hre online) nespĺňa požiadavky na platný súhlas.

Príklad: hra online

Poskytovateľ hier online vyžaduje, aby hráči uviedli svoj vek, meno a adresu na účely účasti na hre online (rozdelenie hráčov podľa veku a adresy). Na webovej lokalite je oznámenie prístupné prostredníctvom odkazu (aj keď prístup k tomuto oznamu nie je nevyhnutný pre účasť na hre), v ktorom sa uvádza, že používaním webovej lokality (a tým aj poskytnutím informácií) hráči prejavujú súhlas so spracovaním ich údajov na účely poskytovania marketingových informácií poskytovateľom hier online a tretím stranám.

Prístup k hre a účasť na nej sa nerovná udeleniu jednoznačného súhlasu s ďalším spracovaním ich osobných údajov na účely iné, ako je účasť na hre. Účasť na hre neimplikuje úmysel jednotlivcov prejsť súhlas so spracovaním iných údajov, ako sú tie, ktoré sú potrebné pre hru. Tento druh správania nepredstavuje jednoznačný prejav želania jednotlivca, aby sa jeho údaje použili na marketingové účely.

Príklad: predvolené nastavenia ochrany súkromia

Predvolené nastavenia sociálnej siete, ku ktorým používatelia nemusia nevyhnutne pristúpiť, aby mohli sieť používať, aktivujú celú kategóriu „priatelia priateľov“, čím umožňujú všetkým „priateľom priateľov“ vidieť všetky osobné informácie každého používateľa. Používatelia, ktorí si neželajú, aby si ich informácie mohli prezerať „priatelia priateľov“, musia kliknúť na tlačidlo. Ak budú pasívni, alebo sa nepodujú na akt kliknutia na tlačidlo, kontrolór usudzuje, že prejavili súhlas so sprístupnením ich údajov. Je však veľmi otázne, či *nekliknutie* na tlačidlo znamená, že jednotlivci všeobecne *súhlasia* s tým, aby boli ich informácie sprístupnené pre všetkých priateľov priateľov. Pre neistotu, pokiaľ ide o to, či nečinnosť má byť prejavom súhlasu, sa nekliknutie nemusí považovať za jednoznačný súhlas.

Uvedený príklad znázorňuje prípad, v ktorom je jednotlivec pasívny (napríklad nečinnosť alebo „mlčanie“). Jednoznačný súhlas sa dobre nehodí do postupov získania súhlasu na základe nečinnosti alebo mlčania jednotlivcov: z mlčania alebo nečinnosti zúčastnenej strany vyplýva nejednoznačnosť (dotknutá osoba mohla mať v úmysle prejsť súhlas alebo jednoducho nevykonať akt). Nasledujúci príklad ďalej vysvetľuje túto situáciu.

Existuje nejednoznačnosť v situácii, keď sa usudzuje, že jednotlivci poskytli súhlas, keď neodpovedali na list, v ktorom boli informovaní, že neodpovedanie znamená ich súhlas. V takejto situácii správanie jednotlivca (alebo skôr nečinnosť) vyvoláva pochybnosti o tom, či jednotlivec mal v úmysle prejsť súhlas. Fakt, že jednotlivec nevykoná žiadny pozitívny akt, neumožňuje vyvodiť záver, že poskytol svoj súhlas. Preto nespĺňa požiadavku jednoznačného súhlasu. Okrem toho, ako sa vysvetľuje ďalej, pre kontrolóra údajov bude zároveň veľmi ťažké poskytnúť dôkaz o tom, že jednotlivec udelil súhlas.

Pracovná skupina konštatovala nevhodnosť súhlasu na základe mlčania jednotlivcov v kontexte posielania priamej reklamy e-mailami. „*Implikovaný súhlas s prijímaním takýchto mailov nie je zlučiteľný s definíciou súhlasu uvedenou v smernici 95/46/ES Podobne ani vopred vyznačené políčka, napríklad na webových lokalitách, nie sú zlučiteľné s definíciou smernice*“³⁰. Tento názor potvrdzuje nasledujúci príklad:

Príklad: neplatný súhlas s ďalším použitím údajov zákazníka

Predajca kníh online pošle e-mail svojim zákazníkom s vernostným programom, v ktorom ich informuje, že ich údaje prenesie reklamnej spoločnosti, ktorá ich plánuje použiť na marketingové účely. Používatelia dostanú dva týždne na to, aby odpovedali na e-mail. Sú informovaní o tom, že keď neodpovedia, posúdi sa to ako súhlas s prenosom. Tento druh mechanizmu, v ktorom sa súhlas odvodzuje od absencie reakcie jednotlivcov, neposkytuje platný, jednoznačný súhlas. Nie je možné bez akýchkoľvek pochybností sa uistiť, že jednotlivci súhlasili s prenosom, na základe toho, že neodpovedali.

³⁰

Stanovisko 5/2004 k nevyžiadaným oznámeniam na marketingové účely podľa článku 13 smernice 2002/58/ES, prijaté 27. februára 2004 (WP 90).

Z uvedených skutočností vyplýva, že v dôsledku požiadavky, aby bol súhlas *jednoznačný*, sa od kontrolórov údajov *de facto* vyžaduje, aby mali zavedené postupy a mechanizmy, ktoré nezanechávajú žiadne pochybnosti o tom, či bol súhlas poskytnutý, buď na základe výslovného aktu vykonaného jednotlivcom, alebo prostredníctvom súhlasu, ktorý možno jasne vyvodit' z aktu vykonaného jednotlivcom.

Ako sme uviedli, v zmysle osvedčeného postupu by kontrolóri údajov mali zvažovať zavedenie príslušných opatrení a postupov, ktorými preukážu poskytnutie súhlasu. Čím zložitejšie je prostredie, v ktorom pôsobia, tým viac opatrení bude potrebných na zabezpečenie overiteľnosti súhlasu. Tieto informácie by sa na požiadanie mali poskytnúť orgánu na ochranu údajov.

III.A.3. Článok 8 ods. 2 písm. a)

V článku 8 smernice sa stanovuje osobitná ochrana pre „*osobitné kategórie údajov*“, ktoré sa na základe ich povahy považujú za veľmi citlivé. Spracovanie takýchto údajov je zakázané, pokiaľ sa neuplatňuje aspoň jedna z viacerých stanovených výnimiek. V článku 8 ods. 2 písm. a) sa stanovuje, že zákaz sa neuplatňuje, ak dotknutá osoba udelí svoj *výslovný súhlas* so spracovaním.

Z právneho hľadiska sa „výslovný súhlas“ chápe rovnako ako vyjadrený súhlas. Zahŕňa všetky situácie, v ktorých sa jednotlivcom predkladá návrh, aby súhlasili alebo nesúhlasili s konkrétnym použitím alebo sprístupnením ich osobných údajov a oni aktívne odpovedajú na otázku, ústne alebo písomne. Výslovný alebo vyjadrený súhlas sa obvykle udeľuje písomne ručným podpisom. Výslovný súhlas sa udeľuje napríklad vtedy, keď dotknuté osoby podpisujú formulár súhlasu, v ktorom sa jasne uvádza, prečo má kontrolór údajov v úmysle zbierať a ďalej spracúvať osobné údaje.

Aj keď výslovný súhlas je tradične písomný, či už na papieri alebo elektronický, ako sa vysvetľuje v kapitole III.A.2, nemusí mať vždy nevyhnutne túto formu, môže sa poskytnúť ústne. Potvrďuje to skutočnosť, že požiadavka, navrhnutá v článku 8, aby bol súhlas písomný, sa v konečnom znení smernice vypustila. Ako sa však v tej istej kapitole vysvetľuje, môže byť ťažké dokázať ústny súhlas, a preto sa v praxi kontrolórom údajov radí, aby uprednostnili písomný súhlas z dôkazových dôvodov.

Požiadavka výslovného súhlasu znamená, že súhlas, ktorý je vyvodený, za normálnych okolností nespĺňa požiadavku článku 8 ods. 2. V tomto ohľade sa oplatí pripomenúť stanovisko pracovnej skupiny zriadenej podľa článku 29 k elektronickým zdravotným záznamom³¹, v ktorom sa uvádza, že „*Na rozdiel od ustanovení článku 7 smernice musí byť súhlas v prípade citlivých osobných údajov, a teda v EZZ výslovný. Riešenia zahrňujúce výnimky nespĺnia požiadavku „výslovného“ súhlasu.....*“.

Príklad: zdravotné záznamy na výskum

Situácia, v ktorej pacienta klinika informuje, že jeho zdravotné záznamy prenesie výskumníkovi, pokiaľ nevznesie námietku (telefonicky na určité číslo), nespĺní požiadavku výslovného súhlasu.

³¹ WP 131 – Pracovný dokument o spracovaní osobných údajov týkajúcich sa zdravotného stavu v elektronických zdravotných záznamoch (EZZ).

Ako sa uvádza v kapitole II.A.2, jednotlivci môžu výslovný súhlas udeliť ústne a písomne tým, že vykonajú potvrdzujúci akt, ktorým vyjadria svoju vôľu prijať formu spracovania údajov. V prostredí online sa môže výslovný súhlas udeliť pomocou elektronického alebo digitálneho podpisu. Môže sa však udeliť aj pomocou tlačidiel, na ktoré sa dá kliknúť, v závislosti od kontextu, odoslaním potvrdzujúcich e-mailov, kliknutím na ikony atď.³². Schválenie postupov, ktoré zahŕňajú potvrdzujúci akt jednotlivca, sa výslovne uznáva v odôvodnení 17 smernice o súkromí a elektronických komunikáciách, v ktorom sa uvádza, že „Súhlas môže byť vyjadrený akýmkoľvek vhodným spôsobom umožňujúcim vyjadrenie špecifického želania, ktoré nastane na základe slobodného a vecného rozhodnutia užívateľa vrátane označenia poľa na webovej stránke internetu“.

Súhlas nemusí byť zaznamenateľný na to, aby bol platný. Je však v záujme kontrolóra údajov, aby si uchoval dôkaz. Je zrejmé, že dôkazová sila konkrétneho mechanizmu môže byť rôzna, môže poskytovať silnejší alebo slabší dôkaz súhlasu. Súhlas získaný pomocou tlačidla, na ktoré sa dá kliknúť, s identitou jednotlivca podporenou iba e-mailovou adresou bude mať oveľa menšiu dôkazovú hodnotu ako podobný proces podporený napríklad mechanizmami zaznamenateľného súhlasu³³. Potreba silného dôkazu bude takisto závisieť od druhu zbieraných údajov a sledovaného účelu: elektronický podpis nebude potrebný na udelenie súhlasu s prijímaním obchodných ponúk, ale môže byť potrebný na udelenie súhlasu so spracovaním určitých druhov finančných údajov online. Výslovný súhlas udelený v prostredí online musí byť zaznamenateľný, aby bol prístupný pre použitie na následný odkaz.³⁴

Vzhľadom na uvedené skutočnosti registračné formuláre online, ktoré majú vyplniť jednotlivci svojimi identifikačnými informáciami a svojím súhlasom so spracovaním údajov, sa budú považovať za formuláre, ktoré spĺňajú požiadavku výslovného súhlasu za predpokladu, že sú splnené všetky ostatné požiadavky. Napríklad, na otvorenie osobných zdravotných záznamov online môžu pacienti udeliť svoj súhlas tým, že poskytnú svoje kontaktné údaje a vyznačia konkrétne políčko, čím prejavia svoj súhlas. Použitím silnejších metód autentifikácie, napríklad použitím digitálnych podpisov, sa samozrejme dosiahne rovnaký výsledok a zabezpečí silnejší dôkaz³⁵.

V niektorých prípadoch členské štáty môžu rozhodnúť, že určitá operácia spracovania údajov sa musí legitimovať na základe súhlasu a špecifikovať druh súhlasu. Napríklad,

³² Tento výklad je v súlade s právnymi predpismi EÚ, najmä o elektronickom obchode a širšom použití digitálnych podpisov, v ktorých sa od členských štátov vyžaduje, aby zmenili a doplnili svoje formálne právne predpisy, ktoré obsahujú formálne požiadavky, podľa ktorých dokumenty musia byť „písomné“ a „vlastnoručné“, aby boli ekvivalentne akceptované aj ich elektronické verzie, ak sú splnené určité podmienky.

³³ V tomto ohľade pozri napríklad grécke a nemecké zákony týkajúce sa požiadaviek poskytnutia súhlasu elektronicky, v ktorých sa vyžaduje, aby sa súhlas zaznamenal bezpečným spôsobom, možnosť prístupu používateľa alebo abonenta kedykoľvek a aby bol kedykoľvek odvolateľný (článok 5 ods. 3 gréckeho zákona 3471/2006 o ochrane osobných údajov v sektore elektronických komunikácií, článok 13 ods. 2 nemeckého zákona o teleslužbách, článok 94 nemeckého zákona o telekomunikáciách a článok 28 ods. 3 písm. a) nemeckého spolkového zákona o ochrane údajov).

³⁴ Do rozsahu tohto stanoviska nepatrí analýza technických podmienok, ktoré musia spĺňať elektronické dokumenty a digitálne podpisy, aby sa im priznala ekvivalentná dôkazná hodnota ako ich vlastnoručne písaným náprotivkom. Táto problematika prekračuje rámec právnych predpisov o ochrane údajov a upravuje sa na úrovni EÚ.

³⁵ Je to preto, že pri použití určitých druhov digitálnych podpisov (rozšírené elektronické podpisy založené na kvalifikovanom osvedčení vytvorené zariadením na bezpečné vytváranie podpisov) sa automaticky predpokladá, že majú rovnakú právnu hodnotu ako písomné dôkazy.

členské štáty môžu rozhodnúť, že pre žiadosť o zdravotný preukaz obsahujúci prístup k zdravotnej histórii sa jednotlivci, ktorí sa zaregistrujú online, musia podpísať špecifickým digitálnym podpisom. Touto možnosťou sa zabezpečí, aby bol súhlas výslovný a zároveň sa kontrolórovi údajov poskytne väčšia istota, že bude schopný súhlas jednotlivcov dokázať.

III.A.4. Článok 26 ods. 1

V článku 26 ods. 1 písm. a) sa stanovuje jednoznačný súhlas dotknutej osoby ako výnimka zo zákazu prenosu údajov do neprimeraných tretích krajín. Úvahy, uvedené vyššie, týkajúce sa článku 7 písm. a) sa uplatňujú aj v tomto prípade. To znamená, že okrem požiadaviek platného súhlasu podľa článku 2 písm. g) musí byť súhlas aj jednoznačný.

Pracovná skupina zriadená podľa článku 29 venovala veľké úsilie poskytnúť usmernenia týkajúce sa uplatňovania článkov 25 a 26 smernice vrátane výnimky súhlasu. V tomto kontexte sa oplatí pripomenúť dokument pracovnej skupiny WP 12³⁶ o význame jednoznačného súhlasu: *„Keďže súhlas musí byť jednoznačný, akékoľvek pochybnosti o skutočnosti, že bol súhlas udelený, by tiež spôsobili, že výnimka by sa nemohla uplatniť. Toto môže pravdepodobne znamenať, že v mnohých situáciách, v ktorých je súhlas implikovaný (napríklad preto, že jednotlivec bol upozornený na prenos a nenamietal), by sa takýto súhlas nekvalifikoval pre túto výnimku“*.

Vzhľadom na uvedené skutočnosti, je pravdepodobnejšie, že sa jednoznačný súhlas získa vtedy, keď jednotlivci vykonajú potvrdzujúci akt, ktorým prejavia svoj súhlas s prenosom, napríklad podpísaním formulára súhlasu alebo vykonaním iných aktov, ktoré jednoznačne podporujú záver, že bol súhlas poskytnutý.

V pracovnom dokumente WP 114³⁷ v súvislosti s použitím súhlasu na prenos údajov pracovná skupina uviedla, že *„Súhlas zrejme nemôže kontrolórom údajov zabezpečiť primeraný dlhodobý rámec v prípadoch opakovaných alebo dokonca štruktúrovaných prenosov na dané spracovanie. V skutočnosti, najmä ak je prenos neoddeliteľnou súčasťou hlavného spracovania (napríklad centralizácia svetovej databázy ľudských zdrojov, ktorá musí mať vstupy z neustálych a systematických prenosov údajov, aby mohla fungovať), by sa kontrolóri údajov mohli ocitnúť v neriešiteľných situáciách, ak by sa čo i len jedna dotknutá osoba následne rozhodla zrušiť svoj súhlas. Presne povedané, údaje týkajúce sa osoby, ktorá zaručila svoj súhlas, by sa nemohli ďalej prenášať, preto by bol prenos ďalej čiastočne založený na súhlase dotknutej osoby, ale muselo by sa nájsť alternatívne riešenie (zmluva, záväzné firemné pravidlá atď.) pre údaje týkajúce sa subjektov, ktoré zrušili svoj súhlas. Spoliehanie sa na súhlas sa preto môže ukázať ako „falošné dobré riešenie“, jednoduché na prvý pohľad, no v skutočnosti zložité a ťažkopádne.“*

³⁶ WP 12 – Pracovný dokument Prenos osobných údajov do tretích krajín: uplatňovanie článkov 25 a 26 smernice EÚ o ochrane údajov, prijatý 24. júla 1998.

³⁷ Pracovný dokument o jednotnej interpretácii článku 26 ods. 1 smernice 95/46/ES z 24. októbra 1995, prijatý 25.11.2005.

III.A.5. Súhlas udelený jednotlivcami bez úplnej spôsobilosti na právne úkony

Podľa smernice 95/46/ES neexistujú osobitné pravidlá pre získanie súhlasu jednotlivcov bez úplnej spôsobilosti na právne úkony vrátane detí. Je dôležité zohľadniť túto skutočnosť v kontexte preskúmania smernice o ochrane údajov. Okrem uvedených otázok súhlas týchto osôb prináša so sebou svoje vlastné, osobitné problémy.

Pokiaľ ide o deti, podmienky udelenia platného súhlasu sa líšia od jedného členského štátu k druhému členskému štátu. Pracovná skupina zriadená podľa článku 29 pri viacerých príležitostiach uvažovala o otázke súhlasu detí a skúmala prax v členských štátoch³⁸.

Predchádzajúca práca ukázala, že keď je potrebný súhlas detí, právne požiadavky môžu vyžadovať získanie súhlasu dieťaťa a zástupcu, alebo iba súhlas dieťaťa, ak je už dospelý. Veková hranica pri prvom alebo druhom pravidle je rôzna. Neexistujú harmonizované postupy na overenie veku dieťaťa.

Neexistencia všeobecných pravidiel v tejto veci vedie k fragmentovanému prístupu a nerešpektuje potrebu osobitnej ochrany detí v špecifických okolnostiach, pre ich zraniteľnosť a preto, že spôsobuje právnu neistotu, najmä pokiaľ ide o spôsob, akým sa získava súhlas detí.

Pracovná skupina sa nazdáva, že táto absencia harmonizácie má následky súvisiace s právnou istotou. Harmonizácia podmienok umožnenia fyzickým osobám bez úplnej spôsobilosti na právne úkony uplatniť si svoje práva na úrovni EÚ, najmä so zreteľom na vekovú hranicu, by istotne priniesla dodatočné záruky. Pracovná skupina si však uvedomuje, že to môže prekračovať rozsah ochrany údajov, pretože sa to týka všeobecnejších otázok občianskeho práva. Pracovná skupina upriamuje pozornosť Komisie na výzvy, ktoré sa objavili v tejto oblasti.

Pracovná skupina zriadená podľa článku 29 ďalej verí, že záujmy detí a iných jednotlivcov bez úplnej spôsobilosti na právne úkony by boli lepšie chránené, keby smernica obsahovala dodatočné ustanovenia, ktoré by so osobitne týkali zberu a ďalšieho spracovania ich údajov. Tieto ustanovenia by mohli stanovovať okolnosti, za ktorých sa vyžaduje súhlas zástupcu spolu so súhlasom jednotlivca bez úplnej spôsobilosti na právne úkony alebo namiesto neho a mohli by stanoviť okolnosti, za ktorých by nemalo byť možné použiť súhlas ako základ pre legitimáciu spracovania osobných údajov. Mali by tiež stanoviť požiadavku používať mechanizmy overenia veku online. Existujú rôzne mechanizmy a rôzne hranice. Napríklad, overenie veku, namiesto toho, aby podliehalo jednému pravidlu, by mohlo byť založené na prístupe posuvnej stupnice, pričom mechanizmus, ktorý by sa mal použiť, by závisel od okolností, ako je druh spracovania (účely), či je osobitne riskantný, druh zberaných údajov, použitie údajov (či sú údaje určené na sprístupnenie) atď.

³⁸ WP 147 – Pracovný dokument 1/2008 o ochrane osobných údajov detí (Všeobecné usmernenia a osobitný prípad škôl); WP 160 Stanovisko č. 2/2009 k ochrane osobných údajov detí (Všeobecné usmernenia a osobitný prípad škôl).

III.B. Smernica 2002/58/ES

Nedávno zmenená a doplnená smernica o súkromí a elektronických komunikáciách (smernica 2002/58/ES)³⁹ je *lex specialis* voči smernici 95/46/ES, keďže ponúka režim špecifický pre sektor, pokiaľ ide o súkromie a elektronické komunikácie. Väčšina jej ustanovení sa uplatňuje iba na poskytovateľov verejne dostupných služieb elektronickej komunikácie (napríklad na poskytovateľov telefonической služby, internetu atď.).

Niektoré ustanovenia smernice o súkromí a elektronických komunikáciách sa spoliehajú na súhlas ako právny základ, na ktorý sa poskytovatelia verejne dostupných služieb elektronickej komunikácie môžu spoľahnúť pri spracovaní údajov⁴⁰. Je to tak napríklad v prípade použitia prevádzkových alebo lokalizačných údajov.

Pracovná skupina zriadená podľa článku 29 sa nazdáva, že je užitočné vyjadriť sa k vybraným aspektom súvisiacim s použitím súhlasu podľa smernice o súkromí a elektronických komunikáciách, ktoré majú osobitný význam. S týmto cieľom sa budeme zaoberať týmito piatimi otázkami:

- a) Vzťah medzi definíciou a celkovým významom súhlasu medzi smernicou 95/46/ES a smernicou o súkromí a elektronických komunikáciách. Táto otázka vychádza z článku 2 ods. 2 písm. f) smernice o súkromí a elektronických komunikáciách.
- b) Otázka, či na porušenie dôvernosti komunikácie (napríklad na monitorovanie alebo zasahovanie do telefonической komunikácie) je potrebné získať súhlas jednej alebo oboch komunikujúcich strán. Táto otázka vychádza z článku 6 ods. 3 a článku 5 ods. 1.
- c) Otázka týkajúca sa načasovania, teda kedy sa musí súhlas získať. Táto otázka sa rieši v rôznych ustanoveniach smernice o súkromí a elektronických komunikáciách vrátane článku 5 ods. 3, článku 6 a článku 13.
- d) Rozsah uplatňovania práva namietat' a jeho odlíšenie od súhlasu. Toto odlíšenie sa môže analyzovať podľa článku 13 smernice o súkromí a elektronických komunikáciách.
- e) Možnosť zrušiť súhlas, výslovne stanovená v článku 6 ods. 3 a článku 9 ods. 3 a 4 smernice o súkromí a elektronických komunikáciách.

III.B.1. Článok 2 písm. f) – Súhlas a vzťah so smernicou 95/46/ES

„súhlas používateľa alebo predplatiteľa“

V článku 2 smernice o súkromí a elektronických komunikáciách sa výslovne uvádza, že definície smernice 95/46/ES sa uplatňujú v súvislosti so smernicou 2002/58/ES. V

³⁹ Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa, 18.12.2009.

⁴⁰ Prevádzkové údaje sú údaje spracované na účely prenosu komunikácie v elektronickej komunikačnej sieti alebo na účely fakturácie tejto komunikácie vrátane údajov týkajúcich sa smerovania, trvania alebo času komunikácie.

článku 2 písm. f) sa uvádza, že „súhlas užívateľa alebo účastníka zodpovedá súhlasu dotknutej osoby v súlade so smernicou 95/46/ES“.

To znamená, že vždy, keď sa vyžaduje súhlas podľa smernice o súkromí a elektronických komunikáciách sú kritériá určenia platnosti súhlasu rovnaké ako tie, ktoré sú stanovené v smernici 95/46/ES, a to konkrétne definícia v článku 2 písm. g) a špecifickosť uvedená v článku 7 písm. a). Názor, že súhlas v smernici o súkromí a elektronických službách sa musí chápať na základe odkazu na článok 2 písm. g) a článok 7 písm. a) spoločne, je potvrdený v odôvodnení 17⁴¹.

III.B.2. Článok 5.1. – Či je súhlas potrebný od jednej alebo oboch strán

„... súhlas zainteresovaných užívateľov ...“

Článok 5 ods. 1 smernice o súkromí a elektronických komunikáciách ochraňuje dôvernosť komunikácií tým, že zakazuje akýkoľvek druh zachytávania alebo sledovania komunikácie bez súhlasu všetkých zainteresovaných používateľov.

V tomto prípade sa podľa článku 5 ods. 1 vyžaduje súhlas „všetkých zainteresovaných používateľov“, inými slovami, dvoch strán komunikácie. Súhlas jednej zo strán nestačí.

V súvislosti s prípravou svojho stanoviska 2/2006⁴² pracovná skupina zriadená podľa článku 29 preskúmala viaceré služby, ktoré zahŕňajú sledovanie obsahu e-mailov a v niektorých prípadoch sledovanie otvárania e-mailu. Pracovná skupina vyjadrila obavy, že pri týchto službách nebola informovaná jedna z komunikujúcich strán. Aby boli tieto služby v súlade s článkom 5 ods. 1 je nevyhnutný súhlas oboch komunikujúcich strán.

III.B.3 Článok 6 ods. 3, články 9, 13 a článok 5 ods. 3 – Čas, kedy sa vyžaduje súhlas

„... na základe jasných a komplexných informácií, ...“

Rôzne ustanovenia smernice o súkromí a elektronických komunikáciách obsahujú buď výslovné alebo implicitné výroky, ktorými sa naznačuje, že súhlas sa musí poskytnúť pred spracovaním. Je to v súlade so smernicou 95/46/ES.

Článok 6 ods. 3 smernice o súkromí a elektronických komunikáciách obsahuje výslovný odkaz na predchádzajúci súhlas príslušného predplatiteľa alebo používateľa a stanovuje povinnosť poskytnúť informácie a získať predchádzajúci súhlas pred spracovaním prevádzkových údajov na účely marketingu služieb elektronickej komunikácie alebo služieb s pridanou hodnotou. Pre určité druhy služieb sa súhlas môže od predplatiteľa získať vo chvíli registrácie. V iných prípadoch môže byť prípustné získať súhlas priamo od používateľa. Podobný prístup sa využíva podľa článku 9 v súvislosti so spracovaním lokalizačných údajov iných ako prevádzkové údaje. Poskytovateľ služby musí

⁴¹ To znamená: „Na účely tejto smernice...by mal mať rovnaký význam ako súhlas dotknutej osoby definovaný a ďalej špecifikovaný v smernici 95/46/ES“

⁴² Stanovisko 2/2006, ktoré sa zaoberá problematikou ochrany súkromia v kontexte poskytovania služieb spočívajúcich v skríningu elektronickej pošty, prijaté 21.02.2006 (WP 118).

informovať užívateľov alebo účastníkov – *predtým, než získa ich súhlas* – o druhu miestnych dát iných, než sú prevádzkové dáta, ktoré *bude* spracúvať. V článku 13 sa stanovuje požiadavka získať predchádzajúci súhlas od predplatiteľov na použitie automatických volacích systémov bez ľudského zasahovania, faxu alebo e-mailu na účely priameho marketingu.

Článok 5 ods. 3 obsahuje špecifické pravidlo týkajúce sa uchovania informácií alebo získania prístupu k informáciám na termináli používateľa, aj na účely sledovania činností používateľa online. Aj keď sa v článku 5 ods. 3 nepoužíva slovo predchádzajúci, je to jasný a zreteľný záver vyplývajúci zo znenia ustanovenia.

Má to zmysel, aby sa súhlas získal *pred* začiatkom spracovania údajov. Inak by spracovanie vykonané počas obdobia od chvíle začiatku spracovania do chvíle získania súhlasu bolo nezákonné pre absenciu právneho základu. Ďalej, v takýchto prípadoch, keď sa jednotlivец rozhodol nesúhlasiť, celé spracovanie údajov, ktoré sa už uskutočnilo, by bolo nezákonné z toho istého dôvodu.

Z uvedených skutočností vyplýva, že vždy, keď sa *vyžaduje* súhlas, musí predchádzať začiatku spracovania údajov. Možnosť začať spracovanie bez získania predchádzajúceho súhlasu je zákonná iba vtedy, ak skôr smernica o ochrane údajov alebo smernica o súkromí a elektronických komunikáciách ako požiadavka súhlasu poskytujú alternatívny základ a odkazujú na právo namietat' alebo odmietnuť spracovanie. Tieto mechanizmy sa jasne odlišujú od súhlasu. V týchto prípadoch sa spracovanie už mohlo začať a jednotlivец má právo namietat', alebo ho odmietnuť.

Príklad možno nájsť v článku 5 ods. 3 predchádzajúcej smernice o súkromí a elektronických komunikáciách, v ktorom sa uvádza (s dôrazom): „*používanie elektronických komunikačných sietí na ukladanie informácií alebo na získavanie prístupu k informáciám uloženým v koncovom zariadení účastníka alebo užívateľa povolené len pod podmienkou, že príslušný účastník alebo užívateľ má k dispozícii jasné a jednoznačné informácie v súlade so smernicou 95/46/ES, medzi iným aj o účele spracovania a kontrolór údajov mu dá možnosť odmietnuť také spracovanie údajov.*“ Malo by sa to porovnať s novým znením článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, zmenenej a doplnenej smernicou 2009/136/ES⁴³, v ktorom sa uvádza, že „*(...) aby sa ukladanie informácií alebo získavanie prístupu k informáciám, ktoré už boli uložené, v koncovom zariadení účastníka alebo užívateľa povolilo len pod podmienkou, že dotknutý účastník alebo užívateľ dal na to vopred súhlas (...)*“. Následky tejto zmeny znenia článku 5 ods. 3 sa vysvetlila pracovná skupina zriadená podľa článku 29 vo svojom stanovisku 2/2010 k behaviorálnej reklame online⁴⁴. Rozdiel medzi odmietnutím a súhlasom sa takisto ďalej rozoberá v ďalšej kapitole.

⁴³ Smernica Európskeho parlamentu a Rady 2009/136/ES z 25. novembra 2009, ktorou sa mení a dopĺňa smernica 2002/22/ES o univerzálnej službe a právach užívateľov týkajúcich sa elektronických komunikačných sietí a služieb, smernica 2002/58/ES týkajúca sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií a nariadenie (ES) č. 2006/2004 o spolupráci medzi národnými orgánmi zodpovednými za vynucovanie právnych predpisov na ochranu spotrebiteľa, Text s významom pre EHP, Ú. v. L 337, 18/12/2009 P. 0011 - 0036

⁴⁴ Stanovisko z 22. júna 2010, WP 171: otázka, či súhlas užívateľa môže byť vyjadrený použitím „vhodných nastavení prehliadača alebo inej aplikácie“ [odôvodnenie 66 smernice 2009/136/ES], sa výslovne rieši v bode 4.1.1 pracovného dokumentu WP 171.

V mnohých prípadoch, v ktorých smernica o súkromí a elektronických komunikáciách alebo smernica o ochrane údajov poskytuje možnosť odmietnuť spracovanie osobných údajov, je to preto, že právny základ pre počiatočné spracovanie údajov je založený na právnych dôvodoch *iných* ako súhlas, napríklad na existujúcej zmluve. Ďalej sa to vysvetľuje v nasledujúcej časti, ktorá obsahuje poznámky k článku 13 smernice o súkromí a elektronických komunikáciách.

III.B.4. Článok 13 ods. 2 – 3 – právo namietat' a jeho odlišenie od súhlasu

„...zákazníkom bola jasne a jednoznačne poskytnutá možnosť bezplatne a jednoduchým spôsobom protestovať...“

V článku 13 smernice o súkromí a elektronických komunikáciách sa stanovuje použitie súhlasu na zákonné odoslanie elektronických komunikácií na účely priamej reklamy. A to na základe štandardnej zásady a osobitného ustanovenia.

Pokiaľ ide o použitie automatických telefónnych prístrojov, faxov a e-mailov, vyžaduje sa predchádzajúci súhlas dotknutej osoby.

Ak adresát komerčnej komunikácie je existujúci klient a komunikácia je zameraná na propagáciu vlastných produktov alebo služieb poskytovateľa alebo podobných produktov alebo služieb, požiadavkou nie je súhlas, ale zabezpečenie, aby jednotlivcom *„bola poskytnutá možnosť namietat'“* podľa článku 13 ods. 2. V odôvodnení 41 sa vysvetľuje dôvod, prečo zákonodarcu, v tomto prípade nevyžadoval súhlas: *„V súvislosti s existujúcimi zákazníckymi vzťahmi je primerané umožniť používanie elektronických kontaktných informácií na ponuku podobných výrobkov alebo služieb“*. Takže v zásade zmluvný vzťah medzi jednotlivcom a poskytovateľom služieb je právnym základom, ktorý umožňuje prvý kontakt e-mailom. Jednotlivci by však mali mať príležitosť namietat' proti ďalším kontaktom. Ako už pracovná skupina uviedla: *„Táto možnosť by sa mala naďalej bezplatne ponúkať pri každej následnej priamej reklamnej správe, s výnimkou nákladov na prenos takého odmietnutia“*.⁴⁵

Potreba súhlasu by sa mala odlíšiť od tohto práva namietat'. Ako sa vysvetľuje v kapitole III.A.2, súhlas založený na nečinnosti jednotlivcov, napríklad pomocou vopred vyznačených políčok, nespĺňa požiadavky platného súhlasu podľa smernice 95/46/ES. Rovnaký záver platí aj pre nastavenia prehliadačov, ktoré by bolo vopred nastavené tak, aby akceptovali zacielenie užívateľa (pomocou *„cookies“*). Vyjasňuje sa to v novom znení článku 5 ods. 3 citovanom v kapitole III.B.3. V týchto dvoch prípadoch nie sú splnené najmä požiadavky jednoznačného prejavu vôle. Je nevyhnutné, aby dotknutá osoba dostala príležitosť prijať rozhodnutie a vyjadriť ho, napríklad tak, že sama vyznačí políčko, so zreteľom na účel spracovania údajov.

Vo svojom stanovisku k behaviorálnej reklame pracovná skupina dospela k záveru, že *„sa vybavenosť prehliadačov nastaveniami chrániacimi súkromie javí ako kardinálne dôležitá. Inými slovami, mali by byť vybavené nastavením „neprijímania a zákazu prenosu „cookies“ pochádzajúcich od tretích subjektov“. Na doplnenie tohto*

⁴⁵ Stanovisko 5/2004 k nevyžiadaným oznámeniam na marketingové účely podľa článku 13 smernice 2002/58/ES, prijaté 27.02.2004.

nastavenia a jeho zefektívnenie by mali prehliadače od užívateľov požadovať, aby využili sprievodcu na ochranu súkromia („privacy wizard“) pri prvej inštalácii alebo pri aktualizácii prehliadača, a tiež by mali zabezpečiť jednoduchý spôsob nastavovania počas používania“⁴⁶.

III.B.5. Článok 6 ods. 3 a článok 9 ods. 3 a 4. – možnosť zrušiť súhlas

„... možnosť kedykoľvek zrušiť súhlas ...“

Možnosť zrušiť súhlas, ktorá je implicitná v smernici 95/46/ES, prebrali viaceré ustanovenia smernice o súkromí a elektronických komunikáciách. Výslovne sa to uviedlo v stanovisku pracovnej skupiny k používaniu miestnych údajov s cieľom poskytovať služby s pridanou hodnotou⁴⁷:

„Podľa článku 9 smernice 2002/58/ES môžu osoby, ktoré dali súhlas na spracúvanie miestnych údajov iných ako prevádzkové údaje, kedykoľvek tento súhlas odvolať a musia mať možnosť jednoduchým spôsobom a bezplatne dočasne odmietnuť spracúvanie týchto údajov. Pracovná skupina považuje tieto práva – ktoré sa môžu považovať za implementáciu práva protestovať proti spracúvaniu miestnych údajov – vzhľadom na citlivú povahu miestnych údajov za podstatné. Pracovná skupina verí, že predpokladom uplatňovania týchto práv je, aby boli osoby informované nielen pri objednávaní služby, ale aj počas jej využívania. Pracovná skupina zastáva názor, že keď si služba vyžaduje priebežné spracúvanie miestnych údajov, poskytovateľ služby by mal príslušnej osobe pravidelne pripomínať, že bola, bude alebo môže byť určená poloha jej koncového zariadenia. To umožní tejto osobe uplatniť právo na odvolanie súhlasu podľa článku 9 smernice 2002/58/ES, ak by si to želala.“

Ako sa uvádza vyššie, vyplýva z toho, že zrušenie sa vykonáva pre budúce spracovanie údajov, nie pre spracovanie údajov, ktoré sa uskutočnilo v minulosti, v období, počas ktorého sa údaje zbierali legitímne. Rozhodnutia alebo procesy predtým prijaté na základe týchto informácií preto nie je možné jednoducho anulovať. Ak však neexistuje žiadny iný právny základ zdôvodňujúci ďalšie uloženie údajov, kontrolór údajov by ich mal vymazať.

IV. Závery

V tomto stanovisku sa skúma právny rámec týkajúci sa použitia súhlasu podľa smernice 95/46/ES a smernice 2002/58/ES. Cieľ je dvojaký: Po prvé vysvetliť existujúce právne požiadavky a znázorniť, ako fungujú v praxi. Zároveň pritom ponúka úvahy o tom, či existujúci rámec je stále vhodný vzhľadom na mnohé nové spôsoby spracovania osobných údajov, alebo môžu byť nutné jeho zmeny.

IV.1. Vysvetlenie kľúčových aspektov súčasného rámca

V článku 2 písm. h) smernice 95/46/ES sa súhlas definuje ako „akýkoľvek slobodne poskytnutý, konkrétny a vedomý prejav vôle, ktorým dotknutá osoba prejaví svoj súhlas s tým, aby sa osobné údaje, ktoré sa jej týkajú, spracúvali“. V článku 7 smernice, v

⁴⁶ Stanovisko z 22.06. 2010, WP 171, op.cit.

⁴⁷ Stanovisko 5/2005 k používaniu miestnych údajov s cieľom poskytovať služby s pridanou hodnotou, prijaté 25.11.2005 (WP 115).

ktorom sa stanovuje právny základ pre spracovanie osobných údajov, sa určuje *jednoznačný* súhlas ako jeden z právnych základov. V článku 8 sa vyžaduje *výslovný* súhlas ako právny základ pre spracovanie citlivých údajov. V článku 26 ods. 1 smernice 95/46/ES a vo viacerých ustanoveniach smernice o súkromí a elektronických komunikáciách sa vyžaduje súhlas na vykonávanie špecifických činností spracovania údajov v ich rámci uplatňovania. Body vypracované v tomto stanovisku sú zamerané na vysvetlenie rôznych prvkov tohto právneho rámca v úsilí zjednodušiť jeho uplatňovanie zainteresovanými stranami vo všeobecnosti.

Prvky/pripomienky všeobecného charakteru

- Súhlas je jedným zo šiestich právnych základov pre spracovanie osobných údajov (jedným z piatich pre citlivé údaje); je významným základom, pretože poskytuje určitú kontrolu dotknutej osobe, pokiaľ ide o spracovanie jej údajov. Význam súhlasu ako aktu, ktorý umožňuje autonómiu a sebaurčenie jednotlivca spočíva v jeho použití v správnom kontexte a s nevyhnutnými prvkami.
- Vo všeobecnosti, právny rámec smernice 95/46/ES sa uplatňuje vždy, keď je potrebný súhlas, nezávisle od toho, či je to v prostredí offline alebo online. Napríklad, rovnaké pravidlá sa uplatňujú, keď predajca tehál a malty vyžaduje registráciu pre systém vernostných preukazov pomocou papierového formulára, ako aj v prípade, keby to vyžadoval na svojej webovej stránke. V smernici o súkromí a elektronických komunikáciách sa navyše špecifikujú určité operácie spracovania údajov, ktoré podliehajú súhlasu: väčšinou sa týkajú spracovania údajov v spojení s poskytovaním verejne dostupných služieb elektronickej komunikácie. Požiadavky platnosti súhlasu v rámci smernice 2002/58/ES sú rovnaké, ako v rámci smernice 95/46/ES.
- Situácie, v ktorých kontrolóri údajov používajú súhlas ako právny základ pre spracovanie osobných údajov, by sa nemali zamieňať so situáciami, v ktorých kontrolór zakladá spracovanie na iných právnych základoch, z ktorých vyplýva individuálne právo namietat'. Môže to byť napríklad prípad, keď sa spracovanie zakladá na „legitímnych záujmoch“ kontrolóra údajov podľa článku 7 písm. f) smernice 95/46/ES, jednotlivec však má právo namietat' podľa článku 14 písm. a) smernice 95/46/ES. Iným príkladom je situácia, keď kontrolór údajov posiela e-mailové komunikácie existujúcim zákazníkom s cieľom propagovať vlastné produkty alebo služby kontrolóra údajov alebo podobné produkty a služby, jednotlivci však majú právo namietat' podľa článku 13 ods. 2 smernice 2002/58/ES. V oboch prípadoch má dotknutá osoba právo namietat' proti spracovaniu, nie je to však to isté ako súhlas.
- Spol'ahnutie sa na súhlas so spracovaním osobných údajov neznamená kontrolóra údajov jeho povinnosti splniť iné požiadavky právneho rámca pre ochranu údajov, napríklad, povinnosť dodržať zásadu proporcionality podľa článku 6 ods. 1 písm. c), bezpečnosti spracovania podľa článku 17 atď.
- Platný súhlas predpokladá možnosť jednotlivcov udeliť súhlas. Pravidlá týkajúce sa možnosti a schopnosti udeliť súhlas nie sú harmonizované, a preto sa v jednotlivých členských štátoch môžu líšiť.

- Jednotlivci, ktorí udelili svoj súhlas, by mali mať možnosť tento súhlas zrušiť a zabrániť tak ďalšiemu spracovaniu ich údajov. Potvrdzuje to aj smernica o súkromí a elektronických komunikáciách v prípade špecifických operácií spracovania údajov na základe súhlasu, ako je spracovanie lokalizačných údajov iných ako prevádzkových údajov.
- Súhlas sa musí udeliť pred začiatkom spracovania osobných údajov, ale môže sa vyžadovať aj v priebehu spracovania, ak vznikne nový účel. Toto sa zdôrazňuje vo viacerých ustanoveniach smernice 2002/58/ES, buď pomocou požiadavky „predchádzajúceho súhlasu“ (napríklad v článku 6 ods. 3) alebo prostredníctvom znenia ustanovení (napríklad v článku 5 ods. 3).

Špecifické prvky právneho rámca týkajúce sa súhlasu

- Aby bol súhlas platný, musí byť *slobodne poskytnutý*. To znamená, že nesmie existovať riziko podvodu, zastrašovania alebo významných negatívnych následkov pre dotknutú osobu, ak nebude súhlasiť. Operácie spracovania údajov v zamestnaneckom prostredí, pri ktorých existuje prvok podriadenia, ako aj v kontexte služieb štátnej správy, napríklad zdravotníckych, si môžu vyžadovať starostlivé posúdenie skutočnosti, či jednotlivci majú slobodu udeliť svoj súhlas.
- Súhlas musí byť *konkrétny*. Nevyplnený súhlas bez určenia presných účelov nespĺňa túto požiadavku. Preto sa na rozdiel od vloženia informácií do všeobecných podmienok zmluvy vyžaduje, aby sa použili samostatné doložky o súhlase, oddelené od všeobecných podmienok.
- Súhlas musí byť *vedomý*. V článkoch 10 a 11 smernice sa uvádza zoznam druhov informácií, ktoré sa musia nevyhnutne poskytnúť jednotlivcom. V každom prípade poskytnuté informácie musia byť dostatočné na to, aby zaručili, že jednotlivci budú môcť dobre informovaní prijať rozhodnutia o spracovaní ich osobných údajov. Potreba, aby bol súhlas „vedomý“ sa premieta do dvoch dodatočných požiadaviek. Po prvé, spôsob, akým sa informácie poskytujú, musí zabezpečiť použitie primeraného jazyka, aby dotknuté osoby rozumeli, s čím súhlasia a na aké účely. Je to v závislosti od kontextu. Použitie príliš zložitého právneho alebo technického žargónu by nespĺnilo zákonné požiadavky. Po druhé, informácie poskytnuté používateľom by mali byť jasné a dostatočne zreteľné, aby ich používatelia nemohli prehliadnuť. Informácie sa musia poskytnúť priamo jednotlivcom. Nestačí, aby boli jednoducho niekde dostupné.
- Pokiaľ ide o to, ako sa musí súhlas poskytnúť, v článku 8 ods. 2 písm. a) sa vyžaduje *výslovný* súhlas na spracovanie citlivých údajov, čo znamená aktívna odpoveď, ústna alebo písomná, ktorou jednotlivec vyjadruje svoju vôľu udeliť súhlas so spracovaním jeho údajov na určité účely. Preto výslovný súhlas nie je možné získať vopred vyznačenými políčkami. Dotknutá osoba musí vykonať určitý pozitívny akt prejavu súhlasu a musí mať slobodu odmietnuť súhlas.
- V prípade údajov iných, ako sú citlivé údaje, sa v článku 7 písm. a) vyžaduje, aby bol súhlas *jednoznačný*. „Jednoznačný“ súhlas vyžaduje použitie mechanizmov na získanie súhlasu, ktoré nezanechávajú žiadne pochybnosti o úmysle jednotlivca súhlas poskytnúť. V praxi táto požiadavka umožňuje kontrolórom údajov použiť rôzne druhy mechanizmov na získanie súhlasu, od vyhlásení o prejave súhlasu

(výslovný súhlas), po mechanizmy, ktoré sú postavené na aktoch, ktorých cieľom je prejav súhlasu.

- Súhlas založený na nečinnosti alebo mlčaní jednotlivca by za bežných okolností nepredstavoval platný súhlas, najmä v kontexte online. Táto otázka vzniká najmä v súvislosti s použitím prednastavení, ktoré musí dotknutá osoba zmeniť, ak chce odmietnuť spracovanie. Napríklad, je to tak pri použití vopred vyznačených políček alebo nastavení internetového prehliadača, ktoré sú vopred nastavené na zber údajov.

IV.2 Posúdenie súčasného rámca a možná potreba zmien

Celkové posúdenie

Pracovná skupina sa nazdáva, že súčasný rámec na ochranu údajov obsahuje dobre premyslený súbor pravidiel, ktoré stanovujú podmienky platnosti súhlasu s cieľom legitimovať operácie spracovania údajov. Platí to v prostredí offline, aj v prostredí online. Konkrétnejšie:

Rámec úspešne dosahuje rovnováhu množstva oblastí záujmu. Na jednej strane zabezpečuje, že iba skutočný, vedomý súhlas sa posudzuje ako platný súhlas. V tomto smere je relevantný a uspokojujúci článok 2 písm. h), v ktorom sa výslovne vyžaduje, aby bol súhlas slobodne poskytnutý, konkrétny a vedomý. Na druhej strane táto požiadavka nepredstavuje zvieracu kazajku, ale skôr poskytuje dostatočnú pružnosť a vyhýba sa technologicky špecifickým pravidlám. Znázorňuje to ten istý článok 2 písm. h), v ktorom sa súhlas definuje ako akýkoľvek prejav vôle jednotlivca. Poskytuje tak dostatočný manévrovací priestor pre spôsoby, akými sa takýto prejav môže poskytnúť. Články 7 a 8, v ktorých sa vyžaduje jednoznačný a potom výslovný súhlas, dobre riešia potrebu rovnováhy medzi týmito dvoma oblasťami záujmu, poskytujú pružnosť a vyhýbajú sa celkovo strnulým štruktúram a zároveň zaručujú ochranu.

Výsledkom je rámec, ktorý, ak sa správne uplatňuje a vykonáva, je schopný držať krok so širokou škálou operácií spracovania údajov, ktoré sú často výsledkom technologického vývoja.

V praxi však pre nedostatočnú jednotnosť v jednotlivých členských štátoch nie je vždy ľahké určiť, kedy je potrebný súhlas a konkrétnejšie požiadavky platného súhlasu spolu so spôsobom ich správneho uplatnenia. Vykonávanie na národnej úrovni prinieslo rôzne prístupy. Konkrétnejšie nedostatky sa zistili počas diskusií v rámci pracovnej skupiny zriadenej podľa článku 29, ktoré viedli k tomuto stanovisku a opisujú sa v ďalšom texte.

Možné zmeny

- Pojem jednoznačný súhlas je užitočný pre vytvorenie systému, ktorý nie je celkovo strnulý, ale poskytuje silnú ochranu. Hoci má potenciál viesť k primeranému systému, žiaľ, jeho význam sa často nepochopí, alebo jednoducho ignoruje. Aj keď vyššie uvedené súvislosti a príklady by mali prispieť k posilneniu právnej istoty a ochrany práv jednotlivcov, keď sa používa súhlas ako právny základ, zdá sa, že uvedená situácia vyžaduje určité zmeny a doplnenia.
- Konkrétnejšie sa pracovná skupina zriadená podľa článku 29 nazdáva, že samotné slovo („jednoznačný“) by potrebovalo ďalšie vysvetlenie ako súčasť revízie všeobecného rámca ochrany údajov. Vyjasnenie by sa malo zamerať na zdôraznenie

skutočnosti, že jednoznačný súhlas vyžaduje použitie mechanizmov, ktoré nezanechávajú žiadne pochybnosti o úmysle dotknutej osoby prejavíť súhlas. Zároveň by sa malo ujasniť, že použitie vopred nastavených možností, ktoré musí dotknutá osoba zmeniť, ak chce spracovanie odmietnuť (súhlas založený na mlčaní), samo osebe nepredstavuje jednoznačný súhlas. Platí to osobitne v prostredí online.

- Popri vysvetlení opísanom vyššie pracovná skupina zriadená podľa článku 29 odporúča:
 - i. *Po prvé*, zahrnúť do definície súhlasu v článku 2 písm. h) slovo „jednoznačný“ (alebo ekvivalentné) s cieľom posilniť koncepciu, že iba súhlas založený na výrokoch alebo skutkoch, ktoré sú prejavom súhlasu, predstavuje platný súhlas. Zväčšila by sa tak jasnosť a pojem súhlas podľa článku 2 písm. h) by sa zosúladiť s požiadavkami platného súhlasu podľa článku 7. Význam slova „jednoznačný“ by sa navyše mohlo ďalej vysvetliť v odôvodnení budúceho právneho rámca.
 - ii. *Po druhé*, v kontexte všeobecnej povinnosti zodpovednosti by kontrolóri mali byť v pozícii preukázať, že súhlas získali. Skutočne, ak sa dôkazné bremeno posilní tak, že sa od kontrolórov údajov bude vyžadovať, aby preukázali, že skutočne získali súhlas dotknutej osoby, budú musieť zaviesť štandardné postupy a mechanizmy získania a dokázania jednoznačného súhlasu. Druh mechanizmov bude závisieť od kontextu a mal by zohľadniť skutočnosti a okolnosti spracovania, najmä jeho riziká.
- Pracovná skupina zriadená podľa článku 29 nie je presvedčená, že právny rámec by mal vyžadovať výslovný súhlas ako všeobecné pravidlo pre všetky druhy operácií spracovania vrátane tých, na ktoré sa v súčasnosti vzťahuje článok 7 smernice. Nazdáva sa, že jednoznačný súhlas, ktorý zahŕňa výslovný súhlas, ale aj súhlas, ktorý je výsledkom jednoznačných *aktov*, by mal zostať požadovanou normou. Táto voľba poskytuje väčšiu pružnosť kontrolórom údajov, pokiaľ ide o získanie súhlasu a celkový postup môže byť rýchlejší a priaznivejší pre používateľov.
- Viaceré aspekty právneho rámca, ktoré sa vzťahujú na súhlas, sú odvodené od znenia, právnej histórie alebo sa vyvinuli prostredníctvom judikatúry a stanovísk pracovnej skupiny zriadenej podľa článku 29. Zabezpečila by sa väčšia právna istota, keby sa tieto aspekty výslovne vložili do nového legislatívneho rámca ochrany údajov. Mohli by sa zohľadniť tieto body:
 - i. Začlenenie výslovného ustanovenia, ktorým sa stanovuje právo jednotlivcov zrušiť svoj súhlas.
 - ii. Posilnenie koncepcie, že súhlas sa musí poskytnúť pred začiatkom spracovania alebo pred akýmkoľvek ďalším použitím údajov na účely, na ktoré sa nevzťahoval počiatočný súhlas, ak neexistuje iný právny základ pre spracovanie.
 - iii. Začlenenie výslovných požiadaviek týkajúcich sa kvality (povinnosť poskytnúť informácie o spracovaní údajov spôsobom, ktorý je ľahko zrozumiteľný, jasným a jednoduchým jazykom) a dostupnosti informácií (povinnosť zabezpečiť, aby informácie boli zreteľné,

nápadné a priamo prístupné). Je to nevyhnutné preto, aby boli jednotlivci informovaní pri prijímaní rozhodnutí.

- Nakoniec, v súvislosti s jednotlivcami bez spôsobilosti na právne úkony, by sa mohli stanoviť ustanovenia zabezpečujúce posilnenú ochranu vrátane:
 - i. Vysvetlení okolností, za ktorých sa vyžaduje súhlas rodičov alebo zástupcov jednotlivca bez spôsobilosti na právne úkony vrátane vekovej hranice, do ktorej by bol takýto súhlas povinný.
 - ii. Stanovenia povinnosti používať mechanizmy na overenie veku, ktoré môžu byť rôzne v závislosti od okolností, napríklad veku detí, druhu spracovania, podľa toho, či je situácia zvlášť riziková a či si kontrolór údajov informácie uloží, alebo ich poskytne tretím stranám;
 - iii. Požiadavky, aby informácie boli prispôbené deťom tak, aby bolo pre ne jednoduchšie porozumieť tomu, čo to znamená, keď sa zbierajú ich údaje a tým aj poskytuje súhlas;
 - iv. Osobitných záruk na identifikáciu činností spracovania údajov, ako je behaviorálna reklama, pri ktorých by súhlas nemal byť možným základom pre legitimáciu spracovania osobných údajov.

Pracovná skupina zriadená podľa článku 29 sa znova vráti k otázke súhlasu. Konkrétne, vnútroštátne orgány na ochranu údajov, ako aj pracovná skupina, môžu v neskoršej fáze rozhodnúť, že vypracujú usmernenia na ďalší rozvoj tohto stanoviska, v ktorých poskytnú dodatočné praktické príklady spojené s použitím súhlasu.

V Bruseli 13. júla 2011

Za pracovnú skupinu

*Predseda
Jacob KOHNSTAMM*