



**01197/11/CS
WP 187**

Stanovisko č. 15/2011 k definici souhlasu

přijaté dne 13. července 2011

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán pro otázky ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát zajišťuje ředitelství C (základní práva a občanství Unie) Generálního ředitelství pro spravedlnost Evropské komise, B-1049 Brusel, Belgie, kancelář č. MO-59 02/013.

Internetové stránky: http://ec.europa.eu/justice/policies/privacy/index_cs.htm

Shrnutí

Toto stanovisko podává důkladnou analýzu pojmu souhlas, který se v současnosti používá ve směrnici o ochraně údajů a směrnici o soukromí a elektronických komunikacích. Na základě zkušeností členů pracovní skupiny zřízené podle článku 29 je ve stanovisku uvedena řada příkladů platného a neplatného souhlasu s důrazem na význam klíčových složek souhlasu, jako jsou pojmy „projev vůle“, „svobodný“, „výslovný (*specific*)“, „nezpochybnitelný“, „výslovný (*explicit*)“, „vědomý“ atd. Stanovisko také objasňuje některé aspekty, které s pojmem souhlas souvisejí. Jde například o to, kdy je nutné získat souhlas, jak se právo na námitku liší od souhlasu atd.

Souhlas je jedním z několika právních důvodů zpracování osobních údajů. Hraje sice důležitou úlohu, ale to neznamená, že jiné právní důvody nemohou být v některých případech vhodnější z hlediska správce i z hlediska subjektů údajů. Pokud se správně používá, je souhlas nástrojem, který dává subjektu údajů kontrolu nad zpracováním jeho údajů. Jestliže se však používá nesprávně, kontrola subjektu údajů se stává iluzorní a souhlas pak nepředstavuje vhodný základ pro zpracování.

Toto stanovisko bylo zčásti vydáno v reakci na žádost, kterou podala Komise v souvislosti s probíhajícím přezkumem směrnice o ochraně údajů. Proto obsahuje doporučení, která by se měla v rámci tohoto přezkumu zvážit. Tato doporučení zahrnují:

- i) upřesnění významu „nezpochybnitelného“ souhlasu a vysvětlení, že platným souhlasem je pouze souhlas založený na prohlášeních nebo úkonech, kterými se dává svolení;
- ii) uložení povinnosti správcům údajů, aby zavedli mechanismy pro prokazování souhlasu (v rámci obecné odpovědnosti);
- iii) doplnění výslovného požadavku týkajícího se kvality a přístupnosti informací, které tvoří základ souhlasu;
- iv) řadu návrhů, které se týkají nezletilých a dalších osob bez způsobilosti k právům a právním úkonům.

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na článek 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice,

s ohledem na svůj jednací řád,

PŘIJALA TOTO STANOVISKO:

I. Úvod

Souhlas subjektu údajů byl vždy klíčovým pojmem v oblasti ochrany údajů. Přitom však není vždy jasné, kde je souhlas zapotřebí a jaké podmínky musí být splněny, aby byl souhlas platný. To může vést k různým přístupům a rozdílným názorům na správnou praxi v různých členských státech. Důsledkem pak může být oslabení pozice subjektů údajů. Závažnost tohoto problému se zvýšila, protože zpracování osobních údajů je nyní čím dále výraznějším prvkem moderní společnosti jak na internetu, tak v jiných kontextech a často se týká několika různých členských států. Z toho důvodu se pracovní skupina zřízená podle článku 29 v rámci svého pracovního programu na období 2010–2011 rozhodla tímto tématem důkladně zabývat.

Souhlas je také jedním z témat, u kterých Komise požádala o příspěvky v souvislosti s přezkumem směrnice 95/46/ES. Ve sdělení Komise „Komplexní přístup k ochraně osobních údajů v Evropské unii“¹ je uvedeno: „Komise posoudí způsoby, jak zpřesnit a posílit pravidla pro udělování souhlasu.“ Tato záležitost je ve sdělení vysvětlena² takto:

„Je-li požadován informovaný souhlas, podle stávajících pravidel by souhlas jednotlivce se zpracováním jeho osobních údajů měl být „svobodný, výslovný a vědomý projev vůle“, kterým subjekt údajů dává své svolení k tomu, aby tyto osobní údaje byly zpracovány. Tyto podmínky jsou ale v členských státech vykládány různě, od obecného požadavku na udělení písemného souhlasu až po akceptování implicitního souhlasu.

V online prostředí lze kromě toho (vzhledem k neprůhlednosti pravidel pro ochranu soukromí) často obtížněji dosáhnout, aby si osoby byly vědomy svých práv a poskytly informovaný souhlas. K tomu přispívá i skutečnost, že v některých případech ani není zřejmé, jak by svobodný, výslovný a vědomý souhlas se zpracováním údajů měl vypadat. Například u behaviorálně cílené reklamy lze podle některých názorů za poskytnutí souhlasu uživatele považovat nastavení prohlížeče, podle jiných však nikoli.

¹ KOM(2010) 609 v konečném znění ze dne 4. listopadu 2010.

² Již ve své první zprávě o provádění směrnice o ochraně údajů (95/46/ES) (KOM(2003) 265 v konečném znění) Komise na straně 17 uvedla: „Zejména pojem „nezpochybnitelný souhlas“ (čl. 7 písm. a)) – ve srovnání s pojmem „výslovný souhlas“ podle článku 8 – je nutné dále zpřesnit a jednotněji vykládat. Je nutné, aby hospodářské subjekty věděly, co představuje platný souhlas, zvláště pak v online situacích.“

Měly by tedy být objasněny podmínky pro udělení souhlasu subjektem údajů, aby dle článku 8 Listiny základních práv EU bylo možno vždy zaručit informovaný souhlas a zajistit, že si daná osoba bude plně vědoma, že souhlas poskytuje a k jakému zpracování údajů. Pokud budou klíčové pojmy jasné, přispěje to rovněž k rozvoji samoregulačních iniciativ zaměřených na nalezení praktických řešení v souladu s právem EU.“

Pracovní skupina zřízená podle článku 29 se tedy zavázala vypracovat stanovisko, aby vyhověla žádosti Komise o příspěvky a aby splnila svůj pracovní program na období 2010–2011. Cílem stanoviska je vyjasnit dané záležitosti a dosáhnout tak jednotného porozumění stávajícímu právnímu rámci. Současně tento krok odpovídá logice dřívějších stanovisek k jiným klíčovým ustanovením směrnice³. Případné změny stávajícího rámce zaberou určitý čas, a proto je užitečné a výhodné objasnit v současnosti používaný pojem „souhlas“ a jeho hlavní složky. Díky objasnění stávajících ustanovení se také lépe ukáže, které oblasti je zapotřebí zlepšit. Na základě provedené analýzy se tedy stanovisko pokusí podat doporučení pro politiku s cílem pomoci Komisi a tvůrcům politiky při zvažování změn použitelného právního rámce pro ochranu údajů.

Stanovisko má tento základní obsah: Nejprve je podán přehled o legislativní historii a úloze souhlasu v právních předpisech o ochraně údajů. Poté zkoumáme různé aspekty a požadavky, které musí být splněny, aby byl souhlas platný podle použitelného práva, včetně některých příslušných částí směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích). Pro názornost doprovázejí analýzu praktické příklady založené na zkušenostech z jednotlivých členských států. O tuto práci se opírají doporučení podaná v závěrečné části stanoviska, podle nichž musí být splněny určité předpoklady, aby bylo možné v souladu se směrnicí žádat o souhlas a aby byl obdrženy souhlas platný. Podána jsou rovněž doporučení pro politiku, která by měli tvůrci politiky zvážit v rámci přezkumu směrnice 95/46/ES.

II. Obecné poznámky a otázky politiky

II.1 Stručná historie

Přestože některé vnitrostátní právní předpisy o ochraně údajů či soukromí přijaté v sedmdesátých letech předpokládaly, že souhlas bude jedním z právních důvodů zpracování osobních údajů⁴, tento přístup se neodrazil v úmluvě č. 108 Rady Evropy⁵. Přitom neexistují žádné zjevné důvody, proč souhlas v úmluvě nehraje důležitější úlohu.⁶

³ Například stanoviska č. 8/2010 k použitelnému právu (WP 179), které bylo přijato dne 16. prosince 2010, a stanoviska č. 1/2010 k pojmům „správce“ a „zpracovatel“ (WP 169), které bylo přijato dne 16. února 2010.

⁴ Viz například článek 31 francouzského právního předpisu Loi n 78-17 „relative a l'informatique, aux fichiers et aux libertés“ ze dne 6. ledna 1978.

⁵ Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (označovaná jako „úmluva č. 108“), která vstoupila v platnost dne 1. října 1985.

⁶ Úmluva č. 108 zavedla pojmy „zpracování v souladu se zákony“ a „oprávněný účel“ (článek 5), ale na rozdíl od směrnice 95/46/ES neobsahuje seznam kritérií pro oprávněné zpracování údajů. Souhlas subjektu údajů se v úmluvě objevuje pouze v souvislosti se vzájemnou pomocí (článek 15). Požadavek na „souhlas“ byl však později opakovaně zmíněn v různých doporučeních Výboru ministrů.

Na úrovni EU se již od samého počátku legislativního procesu, který vyústil v přijetí směrnice 95/46/ES, předpokládalo, že souhlas bude používán jako kritérium pro legitimizaci zpracování osobních údajů. V článku 12 návrhu Komise⁷ z roku 1990 jsou uvedeny vlastnosti, které souhlas musí mít, má-li legitimizovat zpracování údajů: musí být „výslovně vyjádřený“ a „výslovný“ (*specific*). Článek 17, který se týká citlivých údajů, vyžaduje, aby byl souhlas „výslovný (*express*) a písemný“. Pozměněný návrh Komise z roku 1992⁸ nahradil původní článek 12 zněním, které se podobá definici „souhlasu subjektu údajů“ v čl. 2 písm. h) nyní platné směrnice. V tomto návrhu je uvedeno, že souhlas musí být „svobodný a výslovný (*specific*)“. Formulace „výslovně vyjádřený“ byla nahrazena definicí souhlasu jako „výslovného (*express*) projevu vůle (subjektu údajů)“. V důvodové zprávě k pozměněnému návrhu z roku 1992⁹ se konstatuje, že souhlas je možné dát buď ústně, nebo písemně. Na citlivé údaje se i nadále vztahoval požadavek na „písemný“ souhlas. Pozměněný návrh Komise z roku 1992 změnil strukturu předchozího návrhu a zavedl článek 7, který se týká právních důvodů zpracování. V čl. 7 písm. a) tohoto návrhu je uvedeno, že zpracování může být provedeno, pokud „s tím subjekt údajů souhlasí“. Stejně jako platná směrnice návrh obsahuje seznam pěti dalších právních důvodů (vedle souhlasu), jimiž lze zpracování údajů legitimizovat.

Konečnou (nyní platnou) definici souhlasu zavedl v roce 1995 společný postoj Rady¹⁰. Souhlas byl definován jako „*jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování*“. Hlavní změnou oproti návrhu Komise z roku 1992 bylo vypuštění slova „výslovný (*express*)“, které původně předcházelo slovu „projev“. Současně bylo v čl. 7 písm. a) doplněno slovo „nezpochybnitelně“, takže toto písmeno nyní zní takto: „*subjekt údajů nezpochybnitelně udělil souhlas*“. Požadavek na písemný souhlas u citlivých údajů byl nahrazen požadavkem na „výslovný (*explicit*) souhlas“.

V odůvodnění Rady¹¹ nebyly tyto změny konkrétně vysvětleny. Na straně 4 je nicméně uvedeno: „... byla ... provedena řada změn s cílem ... zavést určitou míru flexibility, která zaručuje rovnocennou ochranu ... ale nijak nesnižuje úroveň ochrany; tyto změny umožňují uplatňovat obecné zásady efektivním a nebyrokratickým způsobem v souladu se širokou škálou způsobů, kterými jsou ... údaje zpracovávány.“

Úloha souhlasu v souvislosti s ochranou osobních údajů je výslovně uznána v Listině základních práv Evropské unie. V čl. 8 odst. 2 je uvedeno, že osobní údaje mohou být zpracovány „na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem“. Souhlas se tedy uznává za podstatný aspekt základního práva na ochranu osobních údajů. Zároveň však souhlas není podle Listiny jediným právním důvodem umožňujícím zpracování osobních údajů; stejně jako směrnice 95/46/ES Listina výslovně uznává, že zákonem mohou být stanoveny i jiné oprávněné důvody.

⁷ Návrh směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, KOM(90) 314 v konečném znění, SYN 287 a 288, v Bruselu dne 13. září 1990.

⁸ Pozměněný návrh směrnice Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, KOM(92) 422 v konečném znění, SYN 287, v Bruselu dne 15. října 1992.

⁹ Viz strana 11 pozměněného návrhu směrnice Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, KOM(92) 422 v konečném znění, SYN 287, v Bruselu dne 15. října 1992.

¹⁰ Společný postoj Rady o návrhu směrnice Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, (00/287) COD, přijatý dne 15. března 1995.

¹¹ Viz strana 4 společného postoje.

Souhrnně řečeno ukazuje legislativní historie, zejména v EU, že v pojetí ochrany údajů a soukromí hraje souhlas důležitou úlohu. Současně z ní ale vyplývá, že se souhlas nepokládá za jediný právní důvod opravňující ke zpracování osobních údajů. Legislativní historie směrnice 95/46/ES svědčí o existenci relativní shody na podmínkách platnosti souhlasu, totiž že souhlas musí být *svobodný, výslovný (specific) a vědomý*. Zároveň však poukazuje na určitou nejistotu ohledně způsobů, kterými může být souhlas vyjádřen, – zda musí být výslovný (*explicit*), písemný atd. Tyto otázky jsou dále analyzovány níže.

II.2 Úloha souhlasu: důvod zákonnosti

Obecný/zvláštní důvod

Ve směrnici se souhlas uplatňuje jednak jako obecný důvod zákonnosti (článek 7) a jednak jako zvláštní důvod v některých konkrétních souvislostech (čl. 8 odst. 2 písm. a), čl. 26 odst. 1 písm. a)). V článku 7 je souhlas uveden jako první z celkem šesti různých důvodů opravňujících ke zpracování osobních údajů a v článku 8 je stanovena možnost použít souhlas k legitimizaci zpracování zvláštních kategorií údajů (citlivých údajů), které by jinak bylo zakázáno. Ve druhém z uvedených případů podléhá získání souhlasu přísnějším kritériím; souhlas totiž musí jít nad rámec obecných kritérií v tom smyslu, že musí být „výslovný (*explicit*)“.

Kromě toho směrnice umožňuje interakci s jinými právními předpisy, jak je uvedeno ve 23. bodě odůvodnění: „*členské státy jsou oprávněny zajistit zavádění ochrany osob jak obecným právním předpisem o ochraně osob v souvislosti se zpracováním osobních údajů, tak právními předpisy z jednotlivých oblastí*“. Fungování tohoto systému v praxi je složité – členské státy uplatňují své vlastní přístupy a to v některých případech vede k nejednotnosti.

Pojem souhlas nebyl ve vnitrostátních právních předpisech vždy proveden doslovně. Například ve francouzských právních předpisech o ochraně údajů není souhlas jako obecný pojem definován, ale jeho význam je přesně a konzistentně vysvětlován v judikatuře orgánu pro ochranu údajů (CNIL), a to ve vztahu k definici obsažené ve směrnici o ochraně údajů. Ve Spojeném království se tento pojem vyvinul v rámci zvykového práva s odkazem na znění směrnice. Souhlas byl navíc v některých případech výslovně definován pro určitá odvětví, například v souvislosti se soukromím v elektronických komunikacích, s elektronickou správou nebo s elektronickým zdravotnictvím. Pojem vypracovaný ve zvláštních právních předpisech tedy bude interagovat s pojmem vypracovaným v obecných právních předpisech o ochraně údajů.

Pojem souhlas se používá také v jiných oblastech práva, zejména ve smluvním právu. V tomto kontextu se pro zajištění platnosti smlouvy berou v potaz jiná kritéria než ta, která jsou uvedena ve směrnici, například věk, nepatřičné ovlivňování atd. Oblast působnosti občanského práva a oblast působnosti směrnice nejsou v rozporu, ale překrývají se: směrnice se nezabývá obecnými podmínkami platnosti souhlasu v kontextu občanského práva, ale ani je nevylučuje. To například znamená, že pro posouzení platnosti smlouvy v souvislosti s čl. 7 písm. b) směrnice bude nutné vzít v potaz požadavky občanského práva. Vedle použití obecných podmínek platnosti

souhlasu podle občanského práva je souhlas vyžadovaný čl. 7 písm. a) nutné vykládat také s ohledem na čl. 2 písm. h) směrnice.

Tato interakce s jinými právními předpisy se neprojevuje jen na vnitrostátní úrovni, ale i na úrovni evropské. Obdobný výklad určitých prvků směrnice vyplývá i z jiných oblastí, jak ukazuje rozsudek Soudního dvora v oblasti pracovního práva¹² – v tomto případě byl souhlas vyžadován v souvislosti se vzdáním se sociálního práva. Soudní dvůr vykládal pojem souhlas v kontextu směrnice 93/104 o některých aspektech úpravy pracovní doby. Při tom konstatoval, že „souhlas pracovníka“ vyžaduje souhlas daného pracovníka (nikoli tedy souhlas odborů daný jeho jménem), a vyložil „souhlas“ (...) jako svobodně vyjádřený vědomý souhlas. Soud měl také za to, že tím, že pracovník podepsal pracovní smlouvu odkazující na kolektivní smlouvu, která připouští překročení pracovní doby, nebyl splněn požadavek, že souhlas musí být vyjádřen svobodně, výslovně a s úplnou znalostí věci. Tento výklad souhlasu ve zvláštním kontextu je velmi blízký znění směrnice 95/46/ES.

Souhlas není jediným důvodem zákonnosti

Ve směrnici je souhlas jasně uveden jako důvod zákonnosti. Některé členské státy jej však v souvislosti se statusem ochrany údajů jako základního práva pokládají za upřednostňovaný důvod, který se v některých případech blíží ústavní zásadě. Jiné členské státy jej mohou považovat jen za jednu ze šesti možností – za provozní požadavek, který není důležitější než ostatní možnosti. Vysvětlení vztahu mezi souhlasem a ostatními důvody zákonnosti – např. v souvislosti se smlouvami, úkoly ve veřejném zájmu či oprávněnými zájmy správce a s právem na námitku – pomůže upozornit na úlohu souhlasu ve zvláštních případech.

Pořadí, v jakém jsou právní důvody v článku 7 uvedeny, má význam, ale nevyplývá z něj, že souhlas je vždy nejvhodnějším důvodem opravňujícím ke zpracování osobních údajů. Článek 7 začíná u souhlasu a pak vypočítává ostatní důvody, včetně smluv a právních povinností, přičemž postupně směřuje k rovnováze zájmů. Je třeba podotknout, že ostatních pět důvodů, které následují po souhlasu, musí splňovat kritérium „nezbytnosti“, jež přísně omezuje možnosti jejich použití. To ale neznamená, že požadavek na souhlas ponechává větší manévrovací prostor než ostatní důvody uvedené v článku 7.

Získání souhlasu navíc nezbavuje správce povinností podle článku 6, které se týkají korektnosti, nezbytnosti a přiměřenosti, jakož i kvality údajů. Například, i když je zpracování osobních údajů založeno na souhlasu uživatele, neopravňuje to ke shromažďování údajů, které by přesahovalo míru s ohledem na konkrétní účel.

Získání souhlasu rovněž neumožňuje obcházet jiná ustanovení, jako je čl. 8 odst. 5. Pouze za velmi úzce vymezených okolností může souhlas opravňovat ke zpracování údajů, které by bylo jinak zakázáno, zejména ve vztahu ke zpracování některých citlivých údajů (článek 8), nebo umožňovat použití osobních údajů k dalšímu

¹² Rozsudek Soudního dvora (velkého senátu) ze dne 5. října 2004 ve spojených věcech C-397/01 až C-403/01 (Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele).

zpracování bez ohledu na to, zda je slučitelné s původním účelem. V zásadě by souhlas neměl být chápán jako výjimka z ostatních zásad ochrany údajů, nýbrž jako ochranné opatření. Jedná se především o důvod zákonnosti, který nezbavuje povinnosti uplatňovat ostatní zásady.

Přitom není vždy evidentní, co by se mělo zvolit jako nejvhodnější právní důvod, zejména pokud jde o volbu mezi čl. 7 písm. a) a čl. 7 písm. b). Podle čl. 7 písm. b) musí být zpracování nezbytné pro splnění smlouvy nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů a nesmí jít za tento rámec. Správce údajů, který v souvislosti s uzavřením smlouvy používá jako právní důvod čl. 7 písm. b), nemůže jeho výklad rozšířit tak, aby jím odůvodnil zpracování údajů jdoucí nad rámec toho, co je nezbytné – případné další zpracování bude muset legitimizovat zvláštním souhlasem, na který se budou vztahovat požadavky čl. 7 písm. a). To ukazuje na nutnost rozčlenění smluvních podmínek. V praxi to znamená, že může být nutné, aby byl souhlas dodatečnou podmínkou pro určitou část zpracování. Buď je zpracování nezbytné pro splnění smlouvy, nebo musí být získán (svobodný) souhlas.

U některých transakcí se může uplatnit současně několik právních důvodů. Jinými slovy, každé zpracování údajů musí být vždy v souladu s jedním nebo více právními důvody. Současné použití několika důvodů tedy není vyloučeno, pokud jsou použity ve správném kontextu. Určité shromáždění a další zpracování údajů může být nezbytné v rámci smlouvy se subjektem údajů (čl. 7 písm. b)), jiné zpracování může být nutné v důsledku právní povinnosti (čl. 7 písm. c)), shromáždění dodatečných informací může vyžadovat samostatný souhlas (čl. 7 písm. a)) a ještě další zpracování může být rovněž oprávněné na základě rovnováhy zájmů (čl. 7 písm. f)).

Příklad: koupě automobilu

Správce údajů může být oprávněn zpracovávat osobní údaje pro různé účely a na základě různých důvodů:

- údaje nezbytné pro koupi automobilu – čl. 7 písm. b),
- pro zpracování dokladů k automobilu – čl. 7 písm. c),
- pro služby poskytované v rámci správy klientů (např. aby mohl být prováděn servis automobilu různými přidruženými podniky v EU) – čl. 7 písm. f),
- pro předání údajů třetím stranám pro účely jejich marketingových činností – čl. 7 písm. a).

II.3 Související pojmy

Kontrola

Pojem souhlas tradičně souvisí s myšlenkou, že by subjekt údajů měl mít kontrolu nad tím, jak se jeho údaje používají. Kontrola vykonávaná prostřednictvím souhlasu je důležitý koncept z pohledu základních práv. Z tohoto hlediska by se na rozhodnutí fyzické osoby souhlasit se zpracováním údajů měly zároveň vztahovat přísné požadavky – zejména s ohledem na to, že se osoba tímto rozhodnutím může vzdávat základního práva.

Pokud jde o poskytnutí kontroly subjektům údajů, má souhlas svůj význam, ale není jediným způsobem, jak toho dosáhnout. Směrnice obsahuje i další prostředky kontroly, zvláště právo na námitku. To je ovšem jiný nástroj, který se používá v jiné fázi zpracování, tj. poté, co zpracování začalo, a na základě jiného právního důvodu.

Souhlas souvisí s pojmem informační sebeurčení. Autonomie subjektu údajů je jak předpokladem, tak důsledkem souhlasu: díky ní má totiž subjekt údajů vliv na zpracování údajů. Avšak jak vyplývá ze zkoumání v následující kapitole, tento princip má své limity a existují případy, kdy subjekt údajů nemá možnost se skutečně rozhodnout. Správce údajů může chtít prostřednictvím souhlasu subjektu údajů přenést svou odpovědnost na tuto fyzickou osobu. Pokud například osoba souhlasí se zveřejněním osobních údajů na internetu nebo s jejich předáním pochybnému subjektu ve třetí zemi, může jí vzniknout škoda a správce pak může tvrdit, že se stalo jen to, s čím subjekt údajů souhlasil. Proto je důležité připomenout, že ani zcela platný souhlas nezbavuje správce údajů jeho povinností a neopravňuje ke zpracování, které by bylo jinak nekorektní podle článku 6 směrnice.

Pojem kontroly souvisí také s tím, že subjekt údajů by měl mít možnost vzít svůj souhlas zpět. Zpětvzetí nemá zpětný účinek, ale mělo by v zásadě zamezit jakémukoli dalšímu zpracování údajů dané fyzické osoby správcem. Způsob, jak to funguje v praxi, je podrobněji prozkoumán níže (v kapitole III).

Transparentnost

Druhý aspekt souhlasu souvisí s informováním, tedy s transparentností vůči subjektu údajů. Transparentnost je podmínkou kontroly a také podmínkou platnosti souhlasu. Sama o sobě sice transparentnost nepostačuje k legitimizaci zpracování osobních údajů, ale je zásadní podmínkou z hlediska zajištění platnosti souhlasu.

Aby byl souhlas platný, musí být vědomý. Z toho vyplývá, že všechny nezbytné informace musí být poskytnuty v okamžiku, kdy se o souhlas žádá, a že by se měly týkat podstatných aspektů zpracování, které má souhlas legitimizovat. Sem budou obvykle patřit druhy informací vyjmenované v článku 10 směrnice. Bude to ovšem záviset také na tom, kdy a za jakých okolností se o souhlas žádá.

Bez ohledu na to, zda by udělen souhlas, je transparentnost zpracování údajů rovněž podmínkou korektnosti, která má hodnotu sama o sobě i poté, co byly prvotní informace poskytnuty.

Činnost/načasování: způsoby vyjádření souhlasu

Tento třetí aspekt souvisí se způsobem, jakým je kontrola vykonávána. Jakými způsoby může být souhlas vyjádřen a kdy by se o něj mělo požádat, aby bylo zajištěno, že půjde o skutečný souhlas? Tyto otázky mají rozhodující vliv na to, jak je souhlas udělován a vykládán.

Ačkoli ve směrnici není výslovně uvedeno, kdy se má žádat o souhlas, ze znění jednotlivých ustanovení jasně vyplývá, že souhlas musí být v zásadě udělen před tím,

než zpracování začne.¹³ Získání souhlasu před tím, než zpracování údajů začne, je zásadní podmínkou oprávněnosti tohoto zpracování. Tento bod je dále rozveden v kapitole III.B, která se zabývá směrnicí o soukromí a elektronických komunikacích.

Souhlas, chápaný jako povolení fyzické osoby ke zpracování údajů, které se jí týkají, může být vyjádřen různými způsoby: v čl. 2 písm. h) je uveden jakýkoli „projev vůle“; souhlas musí být nezpochybnitelný (čl. 7 písm. a)) a v případě citlivých údajů výslovný (*explicit*) (podle článku 8). Je ovšem velmi důležité zdůraznit, že souhlas se liší od práva na námitku, stanoveného v článku 14. Zatímco na základě čl. 7 písm. a) může správce údaje zpracovávat teprve poté, co obdrží souhlas subjektu údajů, na základě čl. 7 písm. f) může správce údaje zpracovávat za předpokladu, že jsou splněny příslušné podmínky a že byla přijata ochranná opatření, pokud subjekt údajů nevznesl námitku. Jak pracovní skupina uvedla ve svém pracovním dokumentu č. 114: „*Význam souhlasu, který je kladným aktem, vylučuje de facto každý systém, ve kterém by měl subjekt údajů právo vznést námitku vůči předání až poté, co k němu došlo*“¹⁴.

Z těchto důvodů by právo na námitku podle článku 14 směrnice nemělo být zaměňováno za souhlas. Souhlas je právním důvodem zpracování osobních údajů podle čl. 7 písm. a), čl. 8 odst. 2 písm. a) a čl. 26 odst. 1 nebo podle různých ustanovení směrnice 2002/58/ES.

II.4 Správné použití souhlasu jako právního základu

Je zapotřebí zdůraznit, že souhlas není vždy hlavním či nejvhodnějším prostředkem, jak legitimizovat zpracování osobních údajů.

Někdy je souhlas slabým základem pro odůvodnění zpracování osobních údajů a svou hodnotu ztrácí v případech, kdy je vykládán příliš široce nebo úzce, aby vyhovoval situacím, pro které nikdy nebyl určen. Zásadně důležité je, aby byl souhlas používán „ve správném kontextu“. Pokud by se používal v situacích, pro které se nehodí, protože složky, které tvoří platný souhlas, v nich pravděpodobně nebudou přítomny, vedlo by to k velké zranitelnosti a v praxi by se postavení subjektů údajů *oslabilo*.

Pracovní skupina a evropský inspektor ochrany údajů již tento přístup podpořili ve svých příspěvcích do diskuzí o novém rámci ochrany údajů. Zejména bylo konstatováno: „*Není však vždy jasné, co je skutečný, nezpochybnitelný souhlas. Někteří správci údajů této nejistoty zneužívají tím, že se spoléhají na metody, které nejsou vhodné pro získání skutečného, nezpochybnitelného souhlasu*“¹⁵, což je v rozporu s podmínkami podle článku 6 směrnice. Ve stejném duchu pracovní skupina zřízená podle článku 29 uvedla, že „*složitost postupů shromažďování údajů, obchodních modelů, dodavatelských vztahů a technologických aplikací v mnoha případech předbíhá*

¹³ Pro ilustraci lze uvést, že v německém znění směrnice (a v německém spolkovém zákoně o ochraně údajů) se používá pojem „Einwilligung“. Tento pojem je v německém občanském zákoníku definován jako „předchozí svolení“.

¹⁴ WP 114 – pracovní dokument pracovní skupiny zřízené podle článku 29 o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995.

¹⁵ Stanovisko evropského inspektora ochrany údajů ze dne 14. ledna 2011 ke sdělení Komise – „Komplexní přístup k ochraně osobních údajů v Evropské unii“.

*schopnost či ochotu fyzických osob přijímat na základě aktivní volby rozhodnutí o kontrole používání a sdílení informací*¹⁶.

Proto je důležité objasnit meze souhlasu a zajistit, aby se za souhlas považoval pouze souhlas vyložený v souladu s právními předpisy.¹⁷

III. Analýza ustanovení

V kapitole III.A se tato analýza zaměřuje na směrnici 95/46/ES. V kapitole III.B jsou analyzovány některé relevantní části směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích). K tomu je třeba poznamenat, že tyto směrnice se navzájem nevylučují. Obecné podmínky platnosti souhlasu stanovené ve směrnici 95/46/ES se vztahují jak na offline, tak na online prostředí. Směrnice 2002/58/ES tyto podmínky upřesňuje pro některé výslovně uvedené online služby, a to vždy s ohledem na obecné podmínky směrnice o ochraně údajů.

III.A Směrnice 95/46/ES

Pojem „souhlas subjektu údajů“ je definován v čl. 2 písm. h) a následně se používá v člancích 7, 8 a 26. Úloha souhlasu je rovněž zmíněna v 30. a 45. bodě odůvodnění. Tato ustanovení a všechny důležité podrobnosti jsou v této kapitole zvláště posouzeny.

III.A.1 čl. 2 písm. h)

Podle čl. 2 písm. h) se „souhlasem subjektu údajů“ rozumí *„jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování“*. Tato definice obsahuje několik klíčových složek, kterými se zabýváme níže.

„... jakýkoli... projev vůle... kterým... dává své svolení...“

Forma, kterou může souhlas mít, není v zásadě nijak omezena. Aby však byl souhlas podle směrnice platný, musí jít o projev (vůle). Přestože se může jednat o „jakoukoli“ formu projevu, mělo by být jasné, co přesně do definice projevu (vůle) může spadat.

Forma projevu (tj. způsob, jakým je vůle projevena) není ve směrnici vymezena. Z důvodu zachování flexibility se do konečného znění směrnice nedostal „písemný“ souhlas. Je třeba zdůraznit, že ve směrnici je uveden „jakýkoli“ projev vůle. Tím se otevírá možnost širokého výkladu tohoto projevu. Minimální podobou projevu vůle může být signál jakéhokoli druhu, který je dostatečně jasný na to, aby jím subjekt údajů mohl projevit svou vůli a aby mu správce údajů mohl porozumět. Formulace „projev vůle“ a „dává své svolení“ naznačují, že je skutečně nutný nějaký úkon (na rozdíl od situace, kdy je souhlas možné odvodit z nečinnosti).

Souhlas by měl zahrnovat jakýkoli projev vůle, kterým subjekt údajů *dává* své svolení – může zahrnovat například vlastnoruční podpis připojený na konci papírového formuláře,

¹⁶ „Budoucnost soukromí. Společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů“ ze dne 1. prosince 2009, WP 168.

¹⁷ Již citované stanovisko evropského inspektora ochrany údajů ze dne 14. ledna 2011.

ale také ústní prohlášení, kterým se dává svolení, nebo určité chování, ze kterého lze souhlas přiměřeně odvodit. Vedle klasického příkladu, kterým je podpis, tak do této definice může spadat například vhození vizitky do skleněné mísy. Totéž platí, pokud fyzická osoba zašle své jméno a adresu organizaci s cílem získat od této organizace informace. V tomto případě je její jednání třeba chápat tak, že představuje souhlas se zpracováním takovýchto údajů, v míře, která je nezbytná pro zpracování a vyřízení žádosti.

Pracovní skupina ve svém stanovisku k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou (WP 115) posoudila, jak by mělo být fyzickým osobám umožněno vyjádřit souhlas se službami, které vyžadují jejich automatickou lokalizaci (např. možnost zatelefonovat na určité číslo a získat informace o povětrnostních podmínkách na místě, kde se volající nachází). V tomto případě bylo konstatováno, že pokud jsou uživatelé v plném rozsahu předem informováni o zpracování jejich lokalizačních údajů, bude zavolání na dotčené číslo představovat souhlas s lokalizací.

Příklad: reklamní panely s technologií Bluetooth

V současnosti se rozvíjí nový reklamní nástroj v podobě panelů, které vysílají zprávy žádající o navázání spojení Bluetooth s cílem posílat reklamy lidem procházejícím v blízkosti panelu. Zprávy jsou zaslány lidem, kteří mají v mobilním telefonu zapnutou funkci Bluetooth. Samotné zapnutí funkce Bluetooth nepředstavuje platný souhlas (tj. funkce Bluetooth mohla být zapnuta za jiným účelem). Na druhé straně, pokud je někdo o službě informován a přiblíží svůj mobilní telefon na vzdálenost několika centimetrů od panelu, lze to běžně považovat za projev vůle – tímto způsobem se ukáže, kteří lidé mají skutečně zájem reklamy obdržet. Pouze o těchto lidech by se mělo mít za to, že vyjádřili souhlas, a pouze jim by měly být do telefonů zaslány příslušné zprávy.

Je pochybné, zda by absence chování či – možná lépe řečeno – pasivní chování mohly být ve velmi zvláštních situacích (tj. v naprosto jednoznačných souvislostech) také vykládány jako projev vůle. Pojem „projev vůle“ je široký, ale zdá se, že z něj vyplývá nutnost jednání. Tento výklad podporují i další složky definice souhlasu, jakož i dodatečný požadavek na nezpochybnitelnost souhlasu uvedený v čl. 7 písm. a). Z požadavku, že subjekt údajů musí „dát“ souhlas, zřejmě vyplývá, že pouhá nečinnost nepostačuje a pro vyjádření souhlasu je nutné nějaké jednání, i když možné jsou různé druhy jednání – to je třeba posoudit „v kontextu“ dané situace.

Bez aktivního jednání subjektu údajů bude pro správce údajů v praxi obtížné ověřit, zda mlčení znamenalo souhlas či svolení. Správce údajů nemusí mít jistotu nutnou k tomu, aby mohl předpokládat souhlas, například v takovémto případě: dejme tomu, že zákazníkům byl zaslán dopis, ve kterém byli informováni o plánovaném předání jejich údajů, ke kterému dojde, pokud do dvou týdnů nevznesou námitku. Na dopis odpovědělo jen 10 % zákazníků. V tomto případě je pochybné, že 90 % zákazníků, kteří neodpověděli, s předáním skutečně souhlasí. V takovýchto situacích nemá správce údajů žádnou jasnou informaci o úmyslu subjektů údajů. Kromě toho nebude mít k dispozici žádné důkazy, takže nebude moci prokázat, že souhlas obdržel. Nejednoznačnost pasivní odpovědi povede v praxi k tomu, že bude obtížné splnit požadavky směrnice.

„... svobodný...“

Souhlas může být platný jen tehdy, když má subjekt údajů skutečnou možnost volby a neexistuje žádné riziko klamání, zastrašování, nátlaku či podstatných záporných důsledků, jestliže souhlas neudělí. Pokud by důsledky udělení souhlasu ohrožovaly svobodu volby jednotlivců, souhlas by nebyl svobodný. Sama směrnice v čl. 8 odst. 2 písm. a) předpokládá, že v některých případech, které určí členské státy, nelze zákaz zpracování zvláštních kategorií osobních údajů zrušit udělením souhlasu subjektu údajů.

Tak je tomu například v případě, kdy je subjekt údajů pod vlivem správce údajů, kupříkladu v pracovním poměru. V tomto případě subjekt údajů může (i když vždy nemusí) být v situaci, kdy je závislý na správci údajů – vzhledem k povaze jejich vztahu nebo ke zvláštním okolnostem – a může se obávat, že nebude-li se zpracováním údajů souhlasit, může s ním být odlišně zacházeno.

Pracovní skupina v několika svých stanoviscích zkoumala meze souhlasu v situacích, kdy nemůže být udělen svobodně. Jde především o stanoviska o elektronických zdravotních záznamech (WP 131), o zpracování údajů v pracovním poměru (WP 48) a o zpracování údajů Světovou antidopingovou agenturou (WP 162).

V dokumentu WP 131 pracovní skupina uvedla: „*svobodným*“ *souhlasem se rozumí dobrovolné rozhodnutí osoby, která je při plném vědomí, přijaté bez jakéhokoli nátlaku společenského, finančního, psychického či jiného druhu. Za „svobodný“ nelze považovat žádný souhlas daný v situaci zdravotní péče pod hrozbou odepření léčby nebo horší kvality léčby... .. jestliže zdravotník musí zpracovat osobní údaje v systému EHR, protože je to nutný a nevyhnutelný důsledek situace zdravotní péče, je zavádějící, když se toto zpracování snaží legitimizovat získáním souhlasu. Opírat se o souhlas by mělo být možné pouze v případech, kdy má jednotlivý subjekt údajů skutečnou svobodu volby a má možnost svůj souhlas následně odvolat, aniž by ho to poškodilo.*¹⁸

Pokud zpracování údajů pokračuje i po zpětvzetí souhlasu na základě jiného právního důvodu, lze původní použití souhlasu jako právního důvodu zpochybnit: jestliže zpracování mohlo být od začátku prováděno na základě tohoto jiného důvodu, pak lze situaci, v níž je osoba žádána o souhlas se zpracováním, považovat za zavádějící či svou podstatou nekorektní. Jinak by tomu bylo v případě, že došlo ke změně okolností, například kdyby se v průběhu zpracování objevil nový právní základ, například nový právní předpis upravující dotčenou databázi. Jestliže pro dané zpracování údajů lze platně použít tento nový důvod, může zpracování pokračovat. V praxi ovšem takovéto okolnosti příliš často nenastávají. V zásadě lze souhlas pokládat za nedostatečný, pokud jej není možné účinně vzít zpět.

Pracovní skupina zaujímá konzistentní postoj k výkladu svobodného souhlasu v kontextu pracovního poměru¹⁹: „*pokud se od pracovníka vyžaduje souhlas a neudělení souhlasu má za následek skutečnou nebo potenciální relevantní újmu, není souhlas platný podle článku 7 ani článku 8, protože není svobodný. Jestliže pracovník nemůže*

¹⁸ Stejný závěr je vyvozen v dokumentu WP 162 k agentuře WADA: „*Vzhledem k sankcím a důsledkům spojeným s případným odmítnutím účastníků podrobit se závazkům stanoveným v kodexu (například nedodání informací o místě pobytu) se pracovní skupina nemůže domnívat, že by byl souhlas skutečně svobodný.*“

¹⁹ Stanovisko ke zpracování osobních údajů v pracovním poměru (WP 48). V této souvislosti má význam také pracovní dokument pracovní skupiny zřízené podle článku 29 o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995 (WP 114).

odmítnout, nejedná se o souhlas. ... Obtížná situace nastává, pokud je udělení souhlasu podmínkou přijetí do zaměstnání. Pracovník sice teoreticky může odmítnout udělit souhlas, ale důsledkem může být ztráta pracovní příležitosti. Za takovýchto okolností souhlas není svobodný, a tedy není platný. Situace je ještě jednoznačnější v případě (který často nastává), že všichni zaměstnavatelé uplatňují stejnou nebo podobnou podmínku přijetí do zaměstnání.“

Příklad: fotografie na intranetu

Souhlas daný v kontextu pracovního poměru může být platný, jak ukazuje tento příklad: společnost se rozhodne zřídit intranet, na kterém budou uvedena jména a hlavní úkoly zaměstnanců. Každému zaměstnanci je položen dotaz, zda si přeje, aby byla vedle jména umístěna jeho fotografie. Ti, kdo si uvedení fotografie přejí, jsou vyzváni, aby svou fotografii zaslali na uvedenou adresu. Poté, co fyzická osoba obdrží přiměřené informace, bude se její úkon spočívající v zaslání fotografie považovat za souhlas. Jestliže má společnost k dispozici digitální fotografie všech zaměstnanců a každého z nich požádá o souhlas, aby je mohla pro uvedené účely umístit na intranet, bude se kliknutí zaměstnance na tlačítko vyjadřující souhlas rovněž považovat za udělení platného souhlasu. V obou případech je plně respektována možnost volby zaměstnanců ohledně umístění jejich fotografií na intranet.

Kontext pracovního poměru vyžaduje zvláštní posouzení: hrají zde úlohu kulturní a sociální aspekty pracovního poměru, stejně jako způsob, jakým na sebe působí zásady ochrany údajů a jiné právní předpisy. Osobní údaje mohou být v rámci pracovního poměru zpracovávány za různými účely:

- údaje nezbytné pro plnění úkolů zaměstnance: použití čl. 7 písm. b – nezbytnost pro splnění smlouvy;
- pro stanovení nároku zaměstnanců na získání akciových opcí – zpracování může být buď založeno na souhlasu podle čl. 7 písm. a), nebo se může považovat za nutnou součást administrativních aspektů smluvního vztahu mezi zaměstnancem a zaměstnavatelem – čl. 7 písm. b);
- zpracování čísla sociálního pojištění pro účely sociálního zabezpečení: čl. 7 písm. c) – právní povinnost – případně čl. 8 odst. 2 písm. b) – povinnosti v oblasti pracovního práva;
- zpracování údajů o etnickém původu: to může být v některých zemích také povinnost podle pracovního práva – čl. 8 odst. 2 písm. b) –, kdežto v jiných zemích je to přísně zakázáno.

I když může existovat silný předpoklad, že souhlas je v takovýchto souvislostech slabým důvodem, jeho použití není zcela vyloučeno, pokud je dostatečně zaručeno, že je souhlas skutečně svobodný.

Hlavním důvodem, který brání tomu, aby byl souhlas svobodný, je často vztah podřízenosti, ale rozhodnutí subjektu údajů mohou ovlivnit i jiné okolnosti vyplývající z kontextu. Tyto okolnosti mohou mít například finanční, emocionální nebo praktický rozměr. Také skutečnost, že údaje shromažďuje orgán veřejné moci, může mít na subjekt údajů určitý vliv. Přitom však může být obtížné rozlišit mezi něčím, co pouze

motivuje, a něčím, co má skutečný vliv na svobodu volby subjektu údajů. Na níže uvedených příkladech se snažíme ukázat různou povahu úsilí nebo nákladů, které se týkají fyzických osob a mohou ovlivnit jejich rozhodnutí.

Příklad: elektronické zdravotní záznamy

V mnoha členských státech existuje snaha vytvářet elektronické souhrny zdravotních záznamů pacientů. Díky tomu budou mít poskytovatelé zdravotní péče přístup ke klíčovým informacím bez ohledu na to, kde pacient potřebuje léčbu.

- V prvním scénáři je vytvoření souhrnného záznamu naprosto dobrovolné a pacient dostane péči bez ohledu na to, zda s vytvořením souhrnného záznamu souhlasil. V tomto případě je souhlas s vytvořením souhrnného záznamu svobodný, protože pacient, který souhlas neudělí nebo vezme zpět, nebude nijak znevýhodněn.

- V druhém scénáři je volba elektronického zdravotního záznamu podpořena mírnou finanční motivací. Pacienti, kteří elektronický zdravotní záznam odmítnou, nejsou znevýhodněni v tom smyslu, že se pro ně náklady nezmění. I v tomto případě je možné mít za to, že se pacienti mohou svobodně rozhodnout, zda budou s novým systémem souhlasit.

- Ve třetím scénáři musí pacienti, kteří systém elektronických zdravotních záznamů odmítnou, hradit podstatné dodatečné náklady v porovnání s předchozím systémem sazeb a zpracování jejich dokumentace je podstatně pomalejší. To znamená jasnou nevýhodu pro ty, kdo nesouhlasí, jejímž účelem je přivést ve stanoveném termínu do systému elektronických zdravotních záznamů všechny občany. Souhlas tudíž není dostatečně svobodný. Proto je třeba posoudit také existenci jiných legitimních důvodů pro zpracování osobních údajů či zvážít použití čl. 8 odst. 3 směrnice 95/46/ES.

Příklad: tělesné skenery

V současnosti se rozšiřuje používání tělesných skenerů v některých veřejných prostorech, zejména na letištích před vstupem do odletové haly. Vzhledem k tomu, že v okamžiku skenování jsou zpracovávány údaje cestujících²⁰, musí být toto zpracování v souladu s jedním z právních důvodů uvedených v článku 7. Někdy je prohlídka tělesným skenerem cestujícím prezentována jako možnost, z čehož by vyplývalo, že zpracování údajů lze odůvodnit jejich souhlasem. Pokud však osoba odmítne projít skenerem, může to vést ke vzniku podezření nebo k použití dodatečných kontrolních opatření, jako je provedení osobní prohlídky. Mnoho cestujících bude se skenováním souhlasit, protože se tím vyhnou možným problémům či zdržením v situaci, kdy jejich hlavní prioritou je dostat se včas na palubu letadla. Takový souhlas není dostatečně svobodný. Jelikož musí být prokázáno, že je zpracování nezbytné (z důvodu veřejné bezpečnosti), jako oprávněný důvod by neměl být použit čl. 7 písm. a), nýbrž akt zákonodárce, který cestujícím ukládá povinnost spolupracovat – čl. 7 písm. c) nebo e). Základem pro prohlídky tělesným skenerem by tedy měly být právní předpisy: tyto předpisy přesto mohou umožňovat volbu mezi použitím skeneru a osobní prohlídkou, ale tato volba by byla osobám nabízena pouze doplňkově jako součást dodatečných opatření.

²⁰ Viz dopis ze dne 11. února 2009 předsedy pracovní skupiny zřízené podle článku 29 panu Danielu CALLEJA CRESPOVI, řediteli v GR TREN, o tělesných skenerech, zaslaný v reakci na konzultaci Komise o „dopadu používání tělesných skenerů v oblasti bezpečnosti letectví na lidská práva, soukromí, osobní důstojnost, zdraví a ochranu údajů“. K dispozici na adrese: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm.

Pro volbu právního důvodu zpracování osobních údajů může být rozhodující také povaha správce údajů. To platí především pro správce údajů ve veřejném sektoru, kde zpracování údajů obvykle souvisí s plněním právní povinnosti, jak je uvedeno v čl. 7 písm. c), nebo s výkonem úkolu ve veřejném zájmu, jak je uvedeno v čl. 7 písm. e). Použití souhlasu dotčené fyzické osoby k legitimizaci zpracování údajů tedy není vhodným právním základem. To je zvláště zřejmé v případě, že osobní údaje zpracovávají orgány veřejné moci, které mají autoritativní pravomoci – například donucovací orgány plnící své úkoly v rámci policejní nebo justiční činnosti. Policejní orgány nemohou u opatření, která nejsou stanovena v právních předpisech nebo která by právní předpisy jinak nepovolovaly, vycházet ze souhlasu fyzické osoby.

Je ovšem třeba uznat, že i když státy mohou mít zákonnou povinnost zpracovávat osobní údaje, fyzická osoba nemá vždy povinnost spolupracovat. Mohou totiž existovat případy, kdy jsou subjektům údajů poskytovány „služby s přidanou hodnotou“, které podle svého rozhodnutí mohou, ale nemusí využívat. Ve většině případů je však zpracování povinné. Často není zcela snadné určit, zda je zpracování osobních údajů orgány veřejné moci oprávněně založeno na souhlasu fyzické osoby. Zpracování osobních údajů ve veřejném sektoru proto často zahrnuje hybridní režimy, které mohou vést k nejistotě a zneužívání, pokud jsou nesprávně odůvodňovány souhlasem.

Souhlas sice výjimečně může být platným důvodem zpracování osobních údajů státem, ale v každém jednotlivém případě je třeba pečlivou kontrolou posoudit, zda je souhlas opravdu dostatečně svobodný. Jak ukazují následující příklady, je-li správcem údajů orgán veřejné moci, nebude právním důvodem legitimizujícím zpracování souhlas, nýbrž splnění právní povinnosti podle čl. 7 písm. c) nebo vykonání úkolu ve veřejném zájmu podle čl. 7 písm. e).

Příklad: elektronická správa (eGovernment)

V členských státech jsou vyvíjeny nové průkazy totožnosti, které jsou vybaveny čipem s elektronickými funkcemi. Aktivace elektronických služeb, které karta poskytuje, nemusí být povinná. Ale bez této aktivace může být uživateli zabráněno v přístupu k některým správním službám, ke kterým pak může být velmi obtížné získat přístup jinak (převod některých služeb na internet, omezení úředních hodin). Nelze tedy tvrdit, že legitimním důvodem zpracování je souhlas. V tomto případě by příslušným důvodem měl být právní předpis, na jehož základě je zavádění elektronických služeb organizováno, spolu se všemi vhodnými ochrannými opatřeními.

Příklad: údaje PNR

Byla projednávána otázka, zda lze souhlas cestujících platně použít k legitimizaci předání údajů o rezervacích („údajů jmenné evidence cestujících, PNR“) evropskými leteckými společnostmi orgánům Spojených států. Pracovní skupina se domnívá, že souhlas cestujících nemůže být udělen svobodně, protože letecké společnosti jsou povinny posílat údaje před odletem, a cestující proto nemají žádnou skutečnou volbu, jestliže chtějí letět.²¹ Právním základem zde není souhlas cestujících, nýbrž, v souladu s čl. 7 písm. c), povinnost stanovená v mezinárodní dohodě mezi EU a USA o zpracovávání a předávání údajů jmenné evidence cestujících (PNR).

²¹ Viz stanovisko pracovní skupiny zřízené podle článku 29 č. 6/2002 o předávání informací o cestujících a jiných údajů leteckými společnostmi Spojeným státům americkým.

Příklad: sčítání lidu

V průběhu celostátního sčítání lidu je obyvatelstvo požádáno, aby zodpovědělo různé otázky o své osobní a pracovní situaci. Zodpovězení těchto otázek je povinné. Kromě toho sčítání zahrnuje také otázku týkající se dopravních prostředků, jež daná osoba používá, u které je jasně uvedeno, že její zodpovězení je dobrovolné. Ačkoli hlavní částí sčítání se zjevně netýká svobodný souhlas, existuje svobodná volba, zda zodpovědět tuto poslední dobrovolnou otázku. To by ovšem nemělo zakrývat skutečnost, že hlavním účelem, který stát vydáním dotazníku sleduje, je získat odpovědi. V tomto kontextu tedy souhlas obecně nepředstavuje platný důvod.

„... *výslovný... (specific)*“

Aby byl souhlas platný, musí být výslovný (*specific*). Jinými slovy není přípustný obecný souhlas udělený bez toho, aby byl uveden přesný účel zpracování.

Má-li být souhlas výslovný (*specific*), musí být srozumitelný, tj. měl by se jasně a přesně vztahovat k rozsahu a důsledkům zpracování údajů. Nemůže se týkat otevřeného souboru různých zpracování. Jinak řečeno to znamená, že souhlas platí jen v omezeném kontextu.

Souhlas musí být udělen ve vztahu k různým aspektům zpracování, které musí být jasně určeny. Sem patří zejména otázka, které údaje se zpracovávají a za jakými účely. Příslušný výklad by měl být založen na přiměřených očekáváních stran. „Výslovný (*specific*) souhlas“ je tedy neoddělitelně spojen se skutečností, že souhlas musí být vědomý. Přitom platí požadavek na rozčlenění souhlasu s ohledem na různé složky, ze kterých se zpracování údajů skládá: není možné pojímat souhlas tak, že se vztahuje na „všechny legitimní účely“, které správce údajů sleduje. Souhlas by se měl týkat zpracování, které je přiměřené a vzhledem k účelu nezbytné.

V zásadě by mělo postačovat, aby správce údajů pro různá zpracování získal souhlas jen jednou, pokud tato zpracování odpovídají přiměřeným očekáváním subjektu údajů.

V nedávné době Soudní dvůr rozhodl o předběžné otázce²² týkající se čl. 12 odst. 2 směrnice o soukromí a elektronických komunikacích a konkrétně toho, zda je nutné, aby účastníci, kteří již souhlasili se zveřejněním svých osobních údajů v jednom seznamu, znovu souhlasili s předáním svých osobních údajů za účelem jejich zveřejnění v jiných seznamech. Soudní dvůr uvedl, že pokud byl účastník náležitě informován o možnosti poskytnutí jeho osobních údajů třetímu podniku a tento účastník již souhlasil se zveřejněním uvedených údajů v takovém účastnickém seznamu, poskytnutí těchto údajů nepodléhá opětovnému souhlasu účastníka, „pokud je zaručeno, že dotčené osobní údaje nebudou použity k jiným účelům než těm, pro které byly shromážděny za účelem jejich prvního zveřejnění“ (bod 65).

²² Rozsudek Soudního dvora ze dne 5. května 2011, Deutsche Telekom AG (věc C-543/09). Tento případ začal žádostí německého Spolkového správního soudu, která se týkala telekomunikačních seznamů a zejména výkladu čl. 25 odst. 2 směrnice o univerzální službě (2002/22/ES) a čl. 12 odst. 2 směrnice o soukromí a elektronických komunikacích (2002/58/ES). Daná otázka zjevně souvisí se zvláštní úlohou účastnických seznamů ve směrnici o univerzální službě.

Samostatný souhlas však může být nutný v případě, že správce zamýšlí údaje zpracovávat pro jiné účely. Může být například udělen souhlas, který se bude vztahovat jak na informování fyzické osoby o nových produktech, tak na zvláštní propagační akce, protože lze předpokládat, že to odpovídá přiměřeným očekáváním subjektu údajů. Avšak v případě zaslání údajů dané osoby třetím stranám by měl být subjekt údajů požádán o dodatečný samostatný souhlas. Potřeba strukturovaného přístupu při získávání souhlasu by se měla posuzovat případ od případu v závislosti na účelech, pro které se údaje poskytují, či na jejich příjemcích.

Je třeba připomenout, že zpracování může být založeno na několika různých právních důvodech: některé údaje mohou být zpracovávány, protože jsou nezbytné v rámci smlouvy se subjektem údajů, například pro dodání produktu a řízení služeb, a zvláštní souhlas může být nutný pro zpracování jdoucí nad rámec toho, co je nezbytné pro splnění smlouvy, například za účelem posouzení platební schopnosti (úvěrového ohodnocení) subjektu údajů.

V dokumentu WP 131 o elektronických zdravotních záznamech (EHR) vysvětlila pracovní skupina tento aspekt takto: „výslovný“ souhlas se musí týkat jasně definované konkrétní situace, v níž se počítá se zpracováním lékařských údajů. „Obecné svolení“ subjektu údajů – např. ke sběru jeho lékařských údajů pro EHR a k případnému budoucímu předávání těchto lékařských údajů zdravotníkům podílejícím se na léčbě – by tedy nepředstavovalo souhlas ve smyslu čl. 2 písm. h) směrnice.

Stejná argumentace je použita v dokumentu WP 115, tj. ve stanovisku k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou: „*definice výslovně vylučuje, aby byl dáván souhlas jako součást přijetí všeobecných podmínek nabízené služby elektronických komunikací. ... V závislosti na typu nabízené služby se však může souhlas vztahovat na určité činnosti nebo může představovat dohodu o průběžné lokalizaci.*“

V rozhodnutí Soudního dvora uvedeném v kapitole II v části nazvané „Úloha souhlasu“ sice není slovo „výslovný“ (*specific*) přímo uvedeno, ale z použité argumentace rovněž vyplývá, že souhlas musí být výslovný, protože se v ní uvádí: „*nepostačuje, aby pracovní smlouva dotčené osoby odkazovala na kolektivní smlouvu, která takové překročení umožňuje.*“

Příklad: sociální sítě

Přístup ke službám sociálních sítí je často podmíněn souhlasem s různými druhy zpracování osobních údajů.

Od uživatele, který se chce zaregistrovat ve službě sociální sítě, může být vyžadováno, aby souhlasil s přijímáním behaviorálně cílené reklamy, a to bez dalšího upřesnění či uvedení alternativních možností. Vzhledem k tomu, jakého významu některé sociální sítě nabyly, budou uživatelé určitých kategorií (například dospívající) s přijímáním behaviorálně cílené reklamy souhlasit, aby se vyhnuli riziku, že budou částečně vyloučeni ze sociálních interakcí. Uživateli by mělo být umožněno, aby udělil svobodný a výslovný (*specific*) souhlas s přijímáním behaviorálně cílené reklamy, nezávisle na jeho přístupu ke službě sociální sítě. Tato možnost může být uživateli nabídnuta například prostřednictvím vyskakovacího okna.

Služba sociální sítě nabízí možnost používat externí aplikace. V praxi uživatel určitou aplikaci často nemůže používat, pokud nesouhlasí s předáváním svých údajů vývojáři této aplikace pro různé účely, včetně behaviorálně cílené reklamy a dalšího prodeje údajů třetím stranám. Vzhledem k tomu, že aplikace může fungovat, aniž by bylo nutné předávat jakékoli údaje jejímu vývojáři, pracovní skupina doporučuje strukturovaný přístup k získávání souhlasu uživatele, tj. získávat zvláštní souhlas uživatele s předáváním jeho údajů vývojáři pro uvedené různé účely. Pomocí různých mechanismů, například vyskakovacích oken, lze uživateli nabídnout možnost zvolit použití údajů, se kterým souhlasí (předání vývojáři, služby s přidanou hodnotou, behaviorálně cílená reklama, předání třetím stranám atd.).

Výslovnost (*specificity*) souhlasu také znamená, že pokud se v určitém okamžiku změní účely, pro které správce údaje zpracovává, uživatel o tom musí být informován a musí mu být umožněno, aby k novému zpracování údajů udělil souhlas. Poskytnuté informace se musí týkat zejména důsledků odmítnutí navrhovaných změn.

„... vědomý...“

Poslední složkou definice souhlasu – ale nikoli posledním požadavkem, jak je vysvětleno dále – je jeho vědomá povaha.

V člancích 10 a 11 směrnice je stanovena povinnost informovat subjekty údajů. Povinnost informovat je tudíž samostatná, ale v mnoha případech zjevně souvisí se souhlasem. Ačkoli po poskytnutí informací vždy nenásleduje souhlas (je možné použít jiný důvod podle článku 7), souhlasu musí vždy předcházet poskytnutí informací.

V praxi to znamená, že „*souhlas subjektu údajů (musí být) založený na uvědomění si a pochopení relevantních skutečností a důsledků určitého jednání.*“ *Dotčené osobě musejí být jasným a srozumitelným způsobem poskytnuty přesné a úplné informace o všech podstatných otázkách, zvláště těch uvedených v člancích 10 a 11 směrnice, jako jsou povaha zpracovávaných údajů, účely zpracování, příjemci, jimž budou údaje případně předány, a práva subjektu údajů. To zahrnuje také vědomí důsledků nesouhlasu s daným zpracováním údajů.*²³

Souhlas bude často získáván v okamžiku shromažďování osobních údajů, kdy zpracování začíná. V tomto případě je třeba poskytnout informace odpovídající výčtu v článku 10 směrnice. O souhlas je ovšem také možné požádat následně, když se změní účel zpracování. V tomto případě se poskytované informace budou muset zaměřit na to, co je nutné v příslušném kontextu, ve vztahu k danému účelu.

Vědomý (informovaný) souhlas má zvláště rozhodující význam v souvislosti s předáváním osobních údajů do třetích zemí: „*vyžaduje, aby byl subjekt údajů náležitě informován o konkrétním riziku, že se jeho údaje mají předat do země, ve které neexistuje dostatečná ochrana*“²⁴.

²³ WP 131 – pracovní dokument o zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (EHR).

²⁴ WP 12 – pracovní dokument Předávání osobních údajů do třetích zemí: uplatnění článků 25 a 26 směrnice EU o ochraně údajů. Viz též WP 114 – pracovní dokument pracovní skupiny zřízené podle článku 29 o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995.

V souvislosti se zajištěním náležitosti informování lze určit dva druhy požadavků:

- Kvalita informací – způsob, jakým se informace poskytují, (obyčejný text, bez použití žargonu, srozumitelně, výrazně) má zásadní význam pro posouzení, zda je souhlas „vědomý“. Způsob, jakým by se měly informace poskytovat, závisí na kontextu – obvyklý/průměrný uživatel by měl být schopen informacím porozumět.
- Přístupnost a viditelnost informací – informace musí být poskytovány přímo fyzickým osobám. Nestačí, aby byly informace někde „k dispozici“. Na tom trval také Soudní dvůr ve svém rozsudku z roku 2004²⁵, jenž se týká pracovní smlouvy zahrnující podmínky, které v ní nebyly výslovně uvedeny, ale bylo na ně jen odkázáno. Informace musí být jasně viditelné (typ a velikost písma), výrazné a komplexní. K poskytnutí zvláštních informací v okamžiku, kdy se žádá o souhlas, mohou být použita dialogová okna. Jak je v souvislosti s „výslovným souhlasem“ uvedeno výše, ve vztahu ke službám sociálních sítí je zvláště vhodné použít online informační nástroje, aby se dosáhlo dostatečné strukturovanosti a jasnosti ohledně nastavení soukromí. Užitečným nástrojem zde mohou být také několikvrstvá upozornění, protože ta přispívají k přístupnému poskytování správných informací.

S postupem času se mohou vyskytnout pochybnosti, zda je souhlas, který byl původně založen na platných a dostatečných informacích, platný i nadále. Lidé z řady různých důvodů často mění své názory, protože jejich původní rozhodnutí nebyla dobrá nebo protože se změnila okolnosti, například když se dítě stalo vyspělejší²⁶. Z toho důvodu by se správci údajů v rámci správné praxe měli snažit rozhodnutí osob vždy po určité době přezkoumat, například tak, že je informují o jejich stávajícím rozhodnutí a nabídnou jim možnost toto rozhodnutí potvrdit, nebo vzít zpět.²⁷ Délka této doby by samozřejmě závisela na kontextu a na okolnostech daného případu.

Příklad: mapování trestné činnosti

Některé policejní složky uvažují o tom, že budou zveřejňovat mapy nebo jiné údaje, z nichž bude vyplývat, kde byly spáchány určité druhy trestných činů. Díky ochranným opatřením, která jsou součástí tohoto procesu, se obvykle nezveřejňují žádné osobní údaje o obětech trestných činů, protože trestná činnost je uváděna jen ve vztahu k poměrně velkým zeměpisným oblastem. Některé policejní složky však chtějí trestné činy identifikovat přesněji, pokud s tím bude oběť trestného činu souhlasit. V takovém případě by bylo možné subjekt údajů přesněji spojit s místem, kde byl spáchán trestný čin. Oběti trestného činu ovšem není konkrétně sděleno, že o ní budou na internetu zveřejněny identifikovatelné informace a jak mohou být tyto informace použity. Souhlas proto v tomto případě není platný, protože oběti nemusí zcela rozumět tomu, v jakém rozsahu se informace o nich zveřejňují.

²⁵ Viz poznámka pod čarou 12 (kapitola II.2).

²⁶ Pracovní dokument č. 1/2008 o ochraně osobních údajů dětí, WP 147, 18. února 2008.

²⁷ Pracovní skupina zřízená podle článku 29 podala obdobné doporučení v dokumentu WP 171, tedy ve stanovisku k internetové reklamě zaměřené na chování, přijatém dne 22. června 2010.

Čím složitější je zpracování údajů, tím větší nároky jsou kladeny na správce údajů. Čím obtížnější je pro průměrného občana dohlížet na všechny složky zpracování údajů a porozumět jim, tím větší úsilí by měl správce údajů vynaložit, aby prokázal, že byl souhlas získán na základě konkrétních a srozumitelných informací.

Definice souhlasu uvedená v čl. 2 písm. h) by měla být vykládána spolu s dalšími požadavky stanovenými v ostatních částech směrnice. Článek 7 doplňuje složky definice o slovo „nezpochybnitelně“ a článek 8 doplňuje slovo „výslovný“ (*explicit*) pro případy, kdy se zpracování týká zvláštních kategorií údajů.

III.A.2 Čl. 7 písm. a)

Podle čl. 7 písm. a) směrnice představuje nezpochybnitelný souhlas subjektu údajů právní základ zpracování osobních údajů. Aby byl tedy souhlas platný, musí nejen splňovat kritéria uvedená v čl. 2 písm. h), ale musí být také *nezpochybnitelný*.

Má-li být souhlas nezpochybnitelný, nesmí postup, kterým se o něj žádá a kterým se uděluje, vzbuzovat *žádné pochybnosti* ohledně úmyslu subjektu údajů udělit souhlas. Jinými slovy nesmí projev vůle, kterým subjekt údajů dává své svolení, obsahovat žádné prvky nejednoznačnosti ohledně jeho záměru. Existuje-li důvodná pochybnost o úmyslu dané osoby, je souhlas zpochybnitelný.

Jak je podrobněji vysvětleno dále, na základě tohoto požadavku musí správci údajů vytvářet důkladné postupy pro udělování souhlasu fyzickými osobami; to znamená, že musí buď žádat o jasný výslovný souhlas, nebo používat určité typy postupů, které zajišťují jasný implicitní souhlas fyzických osob. Správce údajů si musí být také dostatečně jist, že osoba udělující souhlas je skutečně subjektem údajů. To je zvláště důležité v případě udělování souhlasu po telefonu nebo na internetu.

Související otázka se týká důkazů o souhlasu. Správci údajů, kteří používají souhlas, mohou mít úmysl nebo potřebu prokázat, že byl souhlas získán – například v souvislosti se sporem se subjektem údajů. V některých případech od nich mohou být takové důkazy také požadovány v rámci donucovacích opatření. V důsledku toho by měli správci údajů v rámci správné praxe pořizovat a uchovávat důkazy o tom, že byl souhlas skutečně udělen. To znamená, že souhlas by měl být ověřitelný.

Nyní provedeme analýzu několika metod udělování souhlasu a posoudíme, zda vedou k nezpochybnitelnému souhlasu.

Postupy či mechanismy, jež se k zajištění nezpochybnitelného souhlasu dobře hodí, jsou výslovná prohlášení, kterými se dává svolení, například podepsané dohody nebo písemná vyjádření souhlasu. Ty pro správce údajů v zásadě představují současně důkaz o tom, že byl souhlas získán.

Příklad: souhlas se zasláním propagačních informací běžnou poštou

Hotel žádá fyzické osoby, aby na papírovém formuláři uvedly svou poštovní adresu, pokud si přejí dostávat běžnou poštou propagační informace. Jestliže osoba poštovní adresu uvede a následně dá své svolení podepsáním formuláře, bude to představovat nezpochybnitelný souhlas. V tomto případě bude souhlas jak výslovný, tak písemný.

Pokud správce údajů všechny podepsané formuláře uchovává, bude mít díky tomuto postupu dostatečný důkaz, že od všech zákazníků obdržel souhlas.

Ne všechny formu souhlasu, které se zdají být výslovné, však souhlas skutečně zajistí. Tato otázka byla předmětem věci, kterou nedávno posuzoval Soudní dvůr (Volker und Markus Schecke v. Land Hessen) a která se týkala zveřejnění jmen příjemců podpory z různých fondů EU²⁸ a částek, které jednotliví příjemci obdrželi. Generální advokátka analyzovala otázku, zda byly podmínky nezpochybnitelného souhlasu splněny v případě, kdy osoby podepsaly prohlášení v tomto znění: „Jsem si vědom, že článek 44a nařízení (ES) č. 1290/2005 vyžaduje zveřejňování informací o příjemcích prostředků z EZZF a EZFRV a o částkách získaných jednotlivými příjemci.“ Generální advokátka dospěla k tomuto závěru: „Potvrzení toho, že bylo dopředu oznámeno, že dojde k nějakému zveřejnění, není totéž jako dát „nezpochybnitelný“ souhlas s konkrétním druhem podrobného zveřejnění. Stejně tak nelze takové potvrzení správně popsat ani jako „svobodný [zvláštní] projev“ žadatelovy vůle v souladu s definicí souhlasu subjektu údajů v čl. 2 písm. h). Generální advokátka proto vyvodila závěr, že žadatelé neudělili souhlas se zpracováním (tj. zveřejněním) svých osobních údajů ve smyslu čl. 7 písm. a) směrnice 95/46/ES.“²⁹

Výslovný souhlas je možné udělit také v online prostředí. Stejně jako v offline prostředí existují i zde velice vhodné nástroje pro udělení nezpochybnitelného souhlasu, jak je patrné z níže uvedeného příkladu.

Příklad: online souhlas s účastí ve věrnostním programu

Internetová stránka hotelu obsahuje rezervační formulář, který fyzickým osobám umožňuje elektronicky si předem zarezervovat hotelové pokoje. Tento online formulář, do kterého osoby zadávají požadované datum a platební údaje, zahrnuje také viditelné políčko, které mohou zaškrtnout ti, kdo si přejí, aby byly jejich údaje použity pro účely registrace do věrnostního programu. Zaškrtnutí tohoto políčka po obdržení příslušných informací by představovalo výslovný, nezpochybnitelný souhlas, protože zaškrtnutí políčka je dostatečně jednoznačný úkon, který neoponechává žádný prostor pro pochybnost ohledně přání dané osoby zapojit se do věrnostního programu.

Výslovný souhlas může být udělen také ústně, formou prohlášení, kterým se dává svolení. Výslovný ústní souhlas by byl udělen v následující situaci:

Příklad: ústní souhlas se zasíláním propagačních informací

Zaměstnanec na hotelové recepci se ptá hostů, kteří se odhlašují a platí, zda by nechtěli hotelu poskytnout svou adresu, aby jim mohly být zasílány propagační informace. Osoby, které v reakci na žádost tohoto zaměstnance a po vyslechnutí příslušných informací svou poštovní adresu uvedou, udělí výslovný souhlas.

²⁸ Evropský zemědělský záruční fond (EZZF) a Evropský zemědělský fond pro rozvoj venkova (EZFRV).

²⁹ Stanovisko generální advokátky Sharpston ze dne 17. června 2010, Volker und Markus Schecke GbR, spojené věci C-92/09 a C-93/09. Je třeba uvést, že Soudní dvůr ve svém rozsudku ze dne 9. listopadu 2010 rozhodl, že zpracování údajů nebylo založeno na souhlasu: "63. Dotčená právní úprava Unie, která se omezuje na stanovení toho, že příjemci podpor budou informováni před zveřejněním údajů, jež se jich týkají, se tedy nesnaží založit zpracování osobních údajů, které zavádí, na souhlasu dotčených příjemců."

Poskytnutí adresy je úkon, který může představovat jednoznačný projev vůle dané osoby. Správce údajů se však může rozhodnout, že zavede mechanismy, které spolehlivěji prokazují, že byl souhlas udělen.

V některých situacích může být nezpochybnitelný souhlas *odvozen* z určitého jednání. Zejména tomu tak bude v případě, že toto jednání vede k nepochybnému závěru, že je souhlas udělen. Předpokladem ovšem je, aby byly poskytnuty příslušné informace o zpracování údajů, které fyzické osobě umožní přijmout rozhodnutí (kdo je správcem údajů, pro jaké účely se zpracování provádí atd.).

Příklad: souhlas s fotografováním

Zaměstnanec na hotelové recepci informuje hosty, kteří se přihlašují, že v jedné z hotelových jídelen bude v daný den odpoledne probíhat fotografování. Vybrané snímky budou použity pro marketingové materiály, konkrétně pro tištěné hotelové brožury. Hoteloví hosté, kteří se chtějí nechat vyfotografovat, se mohou v příslušnou dobu do jídelny dostavit. Pro hosty, kteří se fotografovat nechtějí, je k dispozici jiná jídelna.

O hotelových hostech, kteří se – poté, co byli informováni, – rozhodnou do jídelny v době fotografování dostavit, lze mít za to, že udělili souhlas s tím, aby byli vyfotografováni. Jejich souhlas je odvozen z jejich jednání, tj. z toho, že v příslušné době přišli do jídelny, kde fotografování probíhá. Příchod do jídelny představuje projev vůle dané osoby, který lze v zásadě považovat za nezpochybnitelný, pokud lze stěží zpochybnit, že se osoba jdoucí do jídelny chce nechat vyfotografovat. Hotel však může pokládat za obezřetné pořídit si písemné doklady o získaném souhlasu pro případ, že by byla platnost tohoto souhlasu v blízké budoucnosti napadena.

Jak již bylo uvedeno, stejné požadavky, včetně požadavku na nezpochybnitelný souhlas, se vztahují jak na offline, tak na online prostředí. Pracovní skupina ovšem konstatuje, že riziko zpochybnitelného souhlasu bude pravděpodobně vyšší v online prostředí. Tomu je třeba věnovat zvláštní pozornost. V následujícím příkladu je popsána situace, kdy souhlas odvozený z určitého jednání (účasti v online hře) nesplňuje požadavky na platný souhlas.

Příklad: online hra

Provozovatel online hry požaduje, aby hráči uvedli svůj věk, jméno a adresu pro účely účasti ve hře (rozdělení hráčů podle věku a místa bydliště). Internetová stránka obsahuje oznámení, které se zobrazí po kliknutí na odkaz (i když jeho zobrazení není podmínkou hraní) a ve kterém je uvedeno, že používáním internetové stránky (a tedy poskytnutím informací) hráči souhlasí se zpracováním svých údajů pro účely doručování marketingových informací od provozovatele online hry a třetích stran.

Přístup uživatelů na stránku a účast ve hře však neznamenají udělení nezpochybnitelného souhlasu s dalším zpracováním jejich osobních informací pro jiné účely, než je účast ve hře. Z účasti ve hře nevyplývá záměr dané osoby souhlasit se zpracováním jdoucím nad rámec toho, co je nezbytné pro hraní. Tento druh chování nepředstavuje nezpochybnitelný projev vůle fyzické osoby, tj. přání, aby byly její údaje použity pro marketingové účely.

Příklad: výchozí nastavení soukromí

Ve výchozím nastavení sociální sítě, které si uživatelé nezbytně nemusí prohlédnout, aby mohli síť používat, je aktivována celá kategorie „přátelé přátel“, takže všechny osobní informace každého uživatele jsou viditelné pro všechny „přátelé přátel“. Uživatelé, kteří nechtějí, aby si jejich informace mohli zobrazit „přátelé přátel“, musí kliknout na určité tlačítko. Pokud zůstanou pasivní čili neprovedou úkon spočívající v kliknutí na tlačítko, správce údajů má za to, že souhlasili s tím, aby jejich údaje bylo možné zobrazit. Je však velice sporné, zda *nekliknutí* na tlačítko znamená, že osoby obecně *souhlasí* s tím, aby si jejich informace mohli prohlížet všichni přátelé přátel. Jelikož je nejisté, zda má nečinnost vyjadřovat souhlas, nekliknutí na tlačítko nelze považovat za nezpochybnitelný souhlas.

Výše uvedený příklad popisuje situaci, kdy osoba zůstane pasivní, (tj. nečinnost nebo „mlčení“). Postupy pro získání souhlasu založené na nečinnosti nebo mlčení fyzických osob se k zajištění nezpochybnitelného souhlasu příliš nehodí: mlčení nebo nečinnost jsou totiž ze své podstaty nejednoznačné (subjekt údajů jimi mohl chtít vyjádřit souhlas, ale také jen nemusel chtít provést daný úkon). To je dále vysvětleno na níže uvedeném příkladu.

Situace, kdy se předpokládá, že osoby udělily souhlas, jestliže neodpověděly na dopis, v němž je uvedeno, že pokud neodpoví, znamená to souhlas, je spojena s nejednoznačností, a tedy zpochybnitelností. V tomto druhu situací vede chování (či spíše nečinnost) fyzické osoby k vážným pochybnostem o tom, zda skutečně chtěla dát svolení. Skutečnost, že osoba neprovedla žádný aktivní krok, nedovoluje učinit závěr, že udělila souhlas. Požadavek na nezpochybnitelný souhlas tak nebude splněn. Kromě toho, jak je podrobněji ukázáno níže, bude pro správce údajů také velmi obtížné prokázat, že určitá osoba souhlasila.

Souhlas založený na mlčení fyzických osob pracovní skupina označila za nevhodný v souvislosti se zasláním materiálů přímého marketingu elektronickou poštou. „*Implicitní souhlas s přijímáním takovýchto zpráv není slučitelný s definicí souhlasu ve směrnici 95/46/ES... Obdobně nejsou s definicí podle směrnice slučitelná ani předem zaškrtnutá zaškrťovací políčka, například na internetových stránkách.*“³⁰ Uvedené stanovisko potvrzuje tento příklad:

Příklad: neplatný souhlas k dalšímu použití údajů zákazníků

Online prodejce knih zašle svým zákazníkům zaregistrovaným ve věrnostním programu e-mail, ve kterém jim sdělí, že jejich údaje budou předány reklamní společnosti, jež je zamýšlí použít pro marketingové účely. Uživatelé dostanou dva týdny na to, aby na e-mail odpověděli, a je jim sděleno, že pokud neodpoví, bude se to považovat za souhlas s předáním. Mechanismus tohoto druhu, kdy se souhlas odvozuje z chybějící reakce fyzických osob, nevede k získání platného, nezpochybnitelného souhlasu. Na základě neexistence odpovědi totiž nelze nepochybně určit, že osoby s předáním souhlasily.

³⁰ Stanovisko č. 5/2004 k nevyžádaným sdělením pro marketingové účely podle článku 13 směrnice 2002/58/ES, přijaté dne 27. února 2004 (WP 90).

Z uvedených argumentů vyplývá, že požadavek, aby byl souhlas *nezpochybnitelný*, správce údajů ve svém důsledku *fakticky* vybízí k tomu, aby používali postupy a mechanismy, které vylučují pochybnost o tom, že byl souhlas udělen – buď proto, že je souhlas založen na jednoznačném jednání fyzické osoby, nebo proto, že jej lze z jednání fyzické osoby jasně odvodit.

Jak je zmíněno výše, správci údajů by v rámci správné praxe měli zvážit zavedení příslušných opatření a postupů umožňujících prokázat, že byl souhlas udělen. Čím je prostředí, ve kterém působí, složitější, tím více opatření bude k zajištění ověřitelnosti souhlasu zapotřebí. Příslušné informace by měly být na vyžádání k dispozici orgánu pro ochranu údajů.

III.A.3 Čl. 8 odst. 2 písm. a)

Článek 8 směrnice stanoví zvláštní ochranu pro „*zvláštní kategorie údajů*“, které se kvůli své povaze považují za velice citlivé. Zpracování takovýchto údajů je zakázáno, jestliže nelze použít alespoň jednu z několika stanovených výjimek. Čl. 8 odst. 2 písm. a) stanoví, že se zákaz nepoužije, pokud subjekt údajů udělí *výslovný (explicit) souhlas* k takovému zpracování.

Z právního hlediska má anglický výraz „*explicit consent*“ stejný význam jako *express consent*, tedy výslovný souhlas. Vztahuje se na všechny situace, kdy je fyzickým osobám položena otázka, zda souhlasí, nebo nesouhlasí s určitým použitím nebo sdělením svých osobních informací, a ony na ni aktivně odpoví – ať ústně, či písemně. Výslovný souhlas se obvykle uděluje písemně s vlastnoručním podpisem. Výslovný souhlas bude například udělen, pokud subjekty údajů podepíší formulář souhlasu, ve kterém je jasně uvedeno, proč chce správce údajů osobní údaje shromažďovat a dále zpracovávat.

Přestože je výslovný souhlas tradičně udělován písemně – ať na papíře nebo elektronicky –, jak je popsáno výše v kapitole III.A.2, nejedná se o nutnou podmínku, a může tedy být udělen i ústně. To potvrzuje také skutečnost, že původně navržený požadavek na písemný souhlas v článku 8 byl v konečném znění směrnice vypuštěn. Jak je ovšem v uvedené kapitole vysvětleno, ústní souhlas může být obtížně prokazatelný, a v praxi se proto správcům údajů doporučuje, aby z důkazních důvodů používali písemný souhlas.

Požadavek na výslovný (*explicit*) souhlas znamená, že odvozený souhlas obvykle nebude v souladu s čl. 8 odst. 2. V této souvislosti je vhodné připomenout stanovisko pracovní skupiny zřízené podle článku 29 k elektronickým zdravotním záznamům³¹, ve kterém je uvedeno: „*Na rozdíl od ustanovení článku 7 směrnice musí být souhlas v případě citlivých osobních údajů, a tedy i v případě EHR, výslovný (explicitní).*“ *Řešení založená na předpokládaném souhlasu (opt-out) požadavek na „výslovný“ souhlas splňovat nebudou.*“

³¹ WP 131 – pracovní dokument o zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (EHR).

Příklad: lékařské údaje určené pro výzkum

Jestliže klinika informuje pacienta, že jeho zdravotní dokumentace bude předána výzkumnému pracovníkovi, pokud proti tomu (zatelefonováním na určité číslo) nevznese námitku, požadavek na výslovný (*explicit*) souhlas nebude splněn.

Jak je uvedeno výše v kapitole II.A.2, fyzické osoby mohou udělit výslovný (*explicit*) souhlas – jak ústně, tak písemně – tím, že potvrzujícím úkonem vyjádří svou vůli souhlasit s určitou formou zpracování údajů. V online prostředí může být výslovný souhlas udělen pomocí elektronického či digitálního podpisu. Může však být udělen také kliknutím na kontextové tlačítko, zasláním potvrzujícího e-mailu, kliknutím na ikonu apod.³² Možnost používat postupy, které zahrnují potvrzující úkon fyzické osoby, má výslovnou oporu v 17. bodě odůvodnění směrnice o soukromí a elektronických komunikacích, kde se uvádí: „*Souhlas může být udělen jakýmkoli vhodným způsobem, který umožňuje vyjádřit svobodně poskytnutý, zvláštní a informovaný projev vůle uživatele, včetně označení zaškrtnutím políčka při návštěvě webové stránky na internetu.*“

Souhlas může být platný, i když jej nelze zaznamenat, avšak uchovávání důkazů je v zájmu správce údajů. Je zřejmé, že síla důkazů, které zajišťuje určitý mechanismus, může být různá, takže souhlas může být lépe nebo hůře doložen. Souhlas získaný prostřednictvím kliknutí na tlačítko v případě, kdy je totožnost fyzické osoby prokázána pouze prostřednictvím e-mailové adresy, bude mít mnohem nižší důkazní hodnotu než obdobný postup, který se opírá například o mechanismy udělování souhlasu umožňujícími jeho záznam.³³ Nezbytnost silných důkazů bude též záviset na tom, jaký druh údajů se shromažďuje a jaký účel se sleduje: elektronický podpis tak nebude zapotřebí v případě souhlasu se zasláním obchodních nabídek, ale může být nezbytný pro souhlas s online zpracováním některých druhů finančních údajů. Výslovný (*explicit*) souhlas udělený v online prostředí musí být možné zaznamenat, aby byl přístupný pro účely následného odkazování.³⁴

Vzhledem k uvedeným skutečnostem se má za to, že online registrační formuláře, do kterých fyzické osoby vyplňují své identifikační údaje spolu se svolením ke zpracování údajů, splňují požadavek na výslovný souhlas, pokud jsou splněny i všechny ostatní požadavky. Například pacienti, kteří si chtějí založit individuální online zdravotní dokumentaci, mohou udělit souhlas tak, že uvedou své kontaktní údaje a dají svolení zaškrtnutím zvláštního políčka. Použitím silnějších autentizačních metod – například

³² Tento výklad je v souladu s právními předpisy EU, zejména předpisy o elektronickém obchodu a o širším používání digitálních podpisů, podle nichž musí členské státy změnit své právní předpisy upravující formální požadavky na dokumenty, pokud jde o pojmy „písemný“ a „vlastnoruční“, tak, aby při splnění určitých podmínek byly rovnocenně přijímány i odpovídající elektronické dokumenty.

³³ V této souvislosti viz například řecké a německé právní předpisy týkající se požadavků na udělování souhlasu elektronickými prostředky, které vyžadují, aby byl souhlas zaznamenán zabezpečeným způsobem, aby k němu měl uživatel nebo účastník kdykoli přístup a aby jej bylo možné kdykoli vzít zpět (čl. 5 odst. 3 řeckého zákona č. 3471/2006 o ochraně osobních údajů v odvětví elektronických komunikací, čl. 13 odst. 2 německého zákona o teleslužbách, článek 94 německého zákona o telekomunikacích a čl. 28 odst. 3a německého spolkového zákona o ochraně údajů).

³⁴ Analýza technických podmínek, které musí elektronické dokumenty a digitální podpisy splňovat, aby jim byla přiznána rovnocenná důkazní hodnota jako papírovým dokumentům a vlastnoručním podpisům, nespadá do působnosti tohoto stanoviska. Jde o záležitost jdoucí nad rámec právních předpisů o ochraně údajů, která je upravena na úrovni EU.

digitálních podpisů – bude samozřejmě dosaženo stejného výsledku a současně se získají silnější důkazy.³⁵

V některých případech mohou členské státy rozhodnout, že určité zpracování údajů musí být legitimizováno na základě souhlasu, a stanovit typ tohoto souhlasu. Pro účely žádosti o zdravotní průkaz, který umožňuje přístup k anamnéze, mohou členské státy například stanovit, že se osoby, které se registrují online, musí podepsat určitým typem elektronického podpisu. Tímto způsobem bude zajištěno, aby byl souhlas výslovný, a správce údajů také bude mít větší jistotu, že bude schopen souhlas fyzických osob doložit.

III.A.4 Čl. 26 odst. 1

Čl. 26 odst. 1 písm. a) stanoví výjimku ze zákazu předávání údajů do třetích zemí bez odpovídající úrovně ochrany na základě nezpochybnitelného souhlasu subjektu údajů. V tomto případě rovněž platí úvahy uvedené výše v souvislosti s čl. 7 písm. a). To znamená, že musí být nejen splněny požadavky čl. 2 písm. h) na platný souhlas, ale souhlas musí být také nezpochybnitelný.

Pracovní skupina zřízená podle článku 29 věnovala mnoho úsilí vypracování pokynů k uplatňování článků 25 a 26 směrnice, včetně výjimky založené na souhlasu. V této souvislosti je vhodné připomenout dokument pracovní skupiny WP 12³⁶, který se týká významu pojmu nezpochybnitelný souhlas: „*Jelikož souhlas musí být nezpochybnitelný, jakákoli pochybnost ohledně skutečnosti, že byl udělen souhlas, povede také k tomu, že bude výjimka nepoužitelná. Znamená to pravděpodobně, že mnohé situace, které souhlas obsahují (například protože jednotlivec byl o předání informován a nevněsł námitku), by se pro tuto výjimku nekvalifikovaly.*“

Vzhledem k výše uvedenému bude nezpochybnitelný souhlas pravděpodobněji získán v situaci, kdy osoby provedou nějaký potvrzující úkon, kterým dají své svolení s předáním, například podepíší formulář souhlasu nebo provedou jiné úkony, které nepochybně vedou k závěru, že byl souhlas udělen.

V dokumentu WP 114³⁷, který se týká použití souhlasu pro účely předávání údajů, pracovní skupina uvedla: „*souhlas pravděpodobně nezajistí odpovídající dlouhodobý rámec pro správce údajů v případech opakovaného, nebo dokonce strukturálního předávání k dotyčnému zpracování. Ve skutečnosti, zejména je-li předání nedílnou součástí hlavního zpracování (např. centralizace světové databáze lidských zdrojů, do které musí být neustále a systematicky předávány údaje, aby byla provozuschopná), by se správci údajů mohli nalézat v neřešitelných situacích, kdyby se pouze jeden subjekt údajů následně rozhodl odvolat svůj souhlas. Striktně řečeno, údaje, které se týkají osoby, jež odvolala svůj souhlas, by již nemohly být předávány; v opačném případě by předání bylo nadále částečně založeno na souhlasu subjektu údajů, ale pro údaje, které*

³⁵ Důvodem je skutečnost, že u některých druhů digitálních podpisů (zaručených elektronických podpisů, které jsou založeny na kvalifikovaném osvědčení (kvalifikovaném certifikátu) a jsou vytvářeny prostředky pro bezpečné vytváření podpisů) se automaticky předpokládá, že mají jako doklad stejnou právní platnost jako vlastnoruční podpisy.

³⁶ WP 12 – pracovní dokument Předávání osobních údajů do třetích zemí: uplatnění článků 25 a 26 směrnice EU o ochraně údajů, přijatý dne 24. července 1998.

³⁷ Pracovní dokument o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995, přijatý dne 25. listopadu 2005.

se týkají subjektů, jež odvolaly svůj souhlas, by se muselo nalézt alternativní řešení (smlouva, závazná podniková pravidla atd.). Spoléhání se na souhlas se tedy může ukázat jako „falešné dobré řešení“, které je na první pohled jednoduché, ale ve skutečnosti složité a nešikovné.“

III.A.5 Souhlas udělený osobami bez plné způsobilosti k právům a právním úkonům

Směrnice 95/46/ES neobsahuje žádná zvláštní pravidla pro získávání souhlasu fyzických osob, které nemají plnou způsobilost k právům a právním úkonům, včetně dětí. Je důležité, aby tato skutečnost byla vzata v potaz v rámci přezkumu směrnice o ochraně údajů. Se souhlasem těchto osob jsou vedle již uvedených otázek spojeny vlastní, specifické problémy.

Co se týče dětí, jsou podmínky udělení platného souhlasu v různých členských státech různé. Pracovní skupina zřízená podle článku 29 otázku souhlasu dětí při několika příležitostech posuzovala a zkoumala příslušné postupy v jednotlivých státech.³⁸

Z již provedené práce vyplývá, že když se žádá o souhlas dětí, mohou právní požadavky ukládat, aby byl získán souhlas jak dítěte, tak jeho zákonného zástupce, nebo jen souhlas dítěte, pokud je dítě již dostatečně vyspělé. Jedno, nebo druhé pravidlo se použije podle věku dítěte, avšak věková hranice není jednotná. Neexistují ani žádné harmonizované postupy pro ověření věku dítěte.

V důsledku neexistence obecných pravidel v této oblasti se používá roztržštěný přístup a není respektována nutnost zvláštní ochrany dětí v určitých situacích vzhledem k jejich zranitelnosti a vzhledem k tomu, že tato situace způsobuje právní nejistotu, zejména pokud jde o způsob získávání souhlasu dětí.

Pracovní skupina se domnívá, že chybějící harmonizace má důsledky z hlediska právní jistoty. Harmonizace podmínek, za kterých je osobám bez právní způsobilosti umožněno uplatňovat jejich práva, na úrovni EU – zejména s ohledem na věkovou hranici – by nepochybně znamenala posílení záruk. Pracovní skupina si je ovšem vědoma, že tato záležitost může jít nad rámec problematiky ochrany údajů, protože se týká širších občanskoprávních otázek. Pracovní skupina upozorňuje Komisi na úkoly, které v této oblasti existují.

Kromě toho se pracovní skupina zřízená podle článku 29 domnívá, že by zájmy dětí a dalších osob, které nemají plnou způsobilost k právům a právním úkonům, byly lépe chráněny, kdyby směrnice obsahovala další ustanovení konkrétně upravující shromažďování a další zpracování jejich údajů. V těchto ustanoveních by mohlo být stanoveno, za jakých okolností je nutný souhlas zákonného zástupce spolu se souhlasem osoby bez právní způsobilosti nebo místo jejího souhlasu a také za jakých okolností by nemělo být možné souhlas jako právní důvod legitimizující zpracování osobních údajů použít. Současně by mohla obsahovat povinnost používat online mechanismy pro ověřování věku. V této oblasti existují různé mechanismy a různé hranice. Ověřování věku by se například nemuselo řídit jediným pravidlem, ale mohlo by vycházet

³⁸ WP 147 – pracovní dokument č. 1/2008 o ochraně osobních údajů dětí (obecné pokyny a zvláštní případ škol), WP 160 – stanovisko č. 2/2009 k ochraně osobních údajů dětí (obecné pokyny a zvláštní případ škol).

z flexibilního přístupu, kdy by se o použití určitého mechanismu rozhodovalo podle okolností, jako je druh zpracování (účely), zda je zpracování zvláště rizikové, druh shromažďovaných údajů, použití údajů (zda mají být údaje někomu sděleny) atd.

III.B Směrnice 2002/58/ES

Nedávno pozměněná³⁹ směrnice o soukromí a elektronických komunikacích (směrnice 2002/58/ES) je ve vztahu ke směrnici 95/46/ES zvláštním právním předpisem (*lex specialis*), protože zavádí zvláštní odvětvový režim týkající se soukromí a elektronických komunikací. Většina jejích ustanovení se vztahuje na poskytovatele veřejně dostupných služeb elektronických komunikací (např. poskytovatele telefonie, poskytovatele přístupu na internet atd.).

Některá ustanovení směrnice o soukromí a elektronických komunikacích uvádějí souhlas jako právní základ, ze kterého mohou poskytovatelé veřejně dostupných služeb elektronických komunikací vycházet pro účely zpracování údajů⁴⁰. Je tomu tak například v případě použití provozních nebo lokalizačních údajů.

Pracovní skupina zřízená podle článku 29 považuje za užitečné okomentovat vybrané zvláště významné aspekty související s použitím souhlasu podle směrnice o soukromí a elektronických komunikacích. Za tímto účelem je dále věnována pozornost těmto pěti otázkám:

- a) vztah mezi směrnicí 95/46/ES a směrnicí o soukromí a elektronických komunikacích, pokud jde o definici a celkový význam souhlasu. Tento vztah je založen na čl. 2 písm. f) směrnice o soukromí a elektronických komunikacích;
- b) otázka, zda je pro porušení důvěrného charakteru sdělení (například sledování nebo zachycování telefonní komunikace) nezbytné získat souhlas jednoho nebo obou účastníků komunikace. Tuto záležitost upravuje čl. 6 odst. 3 a čl. 5 odst. 1;
- c) otázka doby, kdy musí být souhlas získán. Ta je upravena v různých ustanoveních směrnice o soukromí a elektronických komunikacích, včetně čl. 5 odst. 3, článku 6 a článku 13;
- d) oblast uplatnění práva na námitku a jeho odlišení od souhlasu. Rozdíl mezi nimi lze analyzovat podle článku 13 směrnice o soukromí a elektronických komunikacích.
- e) možnost vzít souhlas zpět, která je výslovně uvedena v čl. 6 odst. 3 a čl. 9 odst. 1 a 2 směrnice o soukromí a elektronických komunikacích.

³⁹ Směrnicí Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele, 18.12.2009.

⁴⁰ Provozními údaji se rozumí údaje zpracovávané pro účely přenosu sdělení v síti elektronických komunikací nebo pro účtování tohoto sdělení, včetně údajů týkajících se směrování, délky trvání nebo času sdělení.

III.B.1 Čl. 2 písm. f) – souhlas a vztah se směrnicí 95/46/ES

„souhlas uživatele nebo účastníka“

V článku 2 směrnice o soukromí a elektronických komunikacích je výslovně uvedeno, že se definice ve směrnici 95/46/ES použijí i pro účely směrnice 2002/58/ES. V čl. 2 písm. f) se tedy uvádí: *„souhlas uživatele či účastníka odpovídá souhlasu subjektu údajů podle směrnice 95/46/ES“*.

To znamená, že ve všech případech, kdy směrnice o soukromí a elektronických komunikacích vyžaduje souhlas, jsou kritéria pro posouzení platnosti souhlasu stejná jako kritéria stanovená ve směrnici 95/46/ES, tedy definice uvedená v čl. 2 písm. h) a nezpochybnitelnost uvedená v čl. 7 písm. a). Názor, že je souhlas podle směrnice o soukromí a elektronických komunikacích třeba chápat s odkazem na čl. 2 písm. h) společně s čl. 7 písm. a), potvrzuje 17. bod jejího odůvodnění⁴¹.

III.B.2 Čl. 5 odst. 1 – otázka, zda je nezbytný souhlas jedné strany, nebo obou stran

„... bez souhlasu dotčených uživatelů...“

Čl. 5 odst. 1 směrnice o soukromí a elektronických komunikacích chrání důvěrný charakter sdělení tím, že zakazuje jakýkoli druh zachycování nebo sledování sdělení bez souhlasu všech dotčených uživatelů.

V tomto případě čl. 5 odst. 1 vyžaduje souhlas *„všech dotčených uživatelů“*, jinými slovy obou komunikujících stran. Souhlas jedné z nich tedy nepostačuje.

Pracovní skupina zřízená podle článku 29 se při práci na svém stanovisku č. 2/2006⁴² zabývala několika službami zahrnujícími screening obsahu elektronické pošty a v některých případech také sledování, zda došlo k otevření e-mailu. Pracovní skupina vyslovila znepokojení nad tím, že u takovýchto služeb není jedna z komunikujících stran informována. K tomu, aby tyto služby byly v souladu s čl. 5 odst. 1, je nezbytný souhlas obou komunikujících stran.

III.B.3 Čl. 6 odst. 3, článek 9, článek 13 a čl. 5 odst. 3 – doba, kdy musí být udělen souhlas

„... poté, co mu byly poskytnuty jasné a úplné informace...“

V různých ustanoveních směrnice o soukromí a elektronických komunikacích je výslovně nebo implicitně uvedeno, že souhlas má být udělen před zpracováním. To je v souladu se směrnicí 95/46/ES.

⁴¹ Ve kterém se uvádí: *„pro účely této směrnice by měl mít souhlas... stejný význam jako souhlas subjektu údajů definovaný a dále upřesněný ve směrnici 95/46/ES.“*

⁴² Stanovisko č. 2/2006, které se zabývá problematikou ochrany soukromí v kontextu poskytování služeb spočívajících ve screeningu elektronické pošty, přijaté dne 21. února 2006 (WP 118).

Čl. 6 odst. 3 směrnice o soukromí a elektronických komunikacích výslovně zmiňuje předchozí souhlas dotčeného účastníka nebo uživatele, když stanoví povinnost poskytnout informace a získat předchozí souhlas před zpracováním provozních údajů pro potřeby marketingu služeb elektronických komunikací nebo pro poskytování služeb s přidanou hodnotou. U některých druhů služeb může být souhlas od účastníka získán v okamžiku, kdy se účastníkem v rámci dané služby stává. V jiných případech může být souhlas získán přímo od uživatele. Obdobný přístup je použit v článku 9, který se týká zpracování lokalizačních údajů odlišných od provozních údajů. Poskytovatel služeb musí informovat uživatele nebo účastníky – *před obdržáním jejich souhlasu* – o druhu lokalizačních údajů odlišných od provozních údajů, které *budou* zpracovávány. Článek 13 stanoví povinnost získat předchozí souhlas účastníků s použitím automatických volacích systémů bez zásahu člověka, faxů nebo elektronické pošty pro účely přímého marketingu.

Čl. 5 odst. 3 obsahuje zvláštní pravidlo pro uchovávání informací a získávání přístupu k informacím v koncovém zařízení uživatele, mimo jiné za účelem sledování online aktivit uživatele. V čl. 5 odst. 3 sice není použito slovo „předchozí“ nebo „před“, ale ze znění tohoto ustanovení vyplývá jasný a nepochybný závěr v tomto smyslu.

Získávání souhlasu *před* začátkem zpracování údajů je opravdu smysluplné. Jinak by totiž zpracování provedené v době od začátku zpracování do okamžiku získání souhlasu bylo vzhledem k neexistenci právního důvodu protiprávní. Navíc pokud by se v takovém případě dotčená osoba rozhodla souhlas neudělit, veškeré již proběhlé zpracování údajů by bylo z tohoto důvodu rovněž protiprávní.

Z výše uvedeného vyplývá, že pokud se *vyžaduje* souhlas, musí být vždy udělen před tím, než zpracování údajů začne. Možnost zahájit zpracování bez předchozího získání souhlasu je zákonná pouze v případě, že směrnice o ochraně údajů nebo směrnice o soukromí a elektronických komunikacích nevyžadují souhlas, ale stanoví jiný právní důvod a odkazují na právo vznést námitku nebo odmítnout zpracování. Tyto mechanismy jsou jasně odlišeny od souhlasu. V takovýchto případech již zpracování mohlo začít a příslušná osoba má právo vznést proti němu námitku nebo je odmítnout.

Příkladem tohoto přístupu bylo původní znění čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, kde bylo uvedeno (podtržení doplněno): „*Členské státy zajistí, aby užívání sítí elektronických komunikací k uchovávání informací nebo získávání přístupu k informacím uchovávaným v koncovém zařízení účastníka nebo uživatele bylo povoleno pouze za podmínky, že dotčený účastník či uživatel byl jasně a úplně informován v souladu se směrnicí 95/46/ES, mimo jiné o účelech zpracování, a že je mu správcem údajů nabídnuto právo odmítnout takové zpracování.*“ To je vhodné srovnat s novým zněním čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, pozměněným směrnicí 2009/136/ES⁴³, kde se uvádí: „*Členské státy zajistí, aby uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele povoleno pouze pod podmínkou, že dotčený účastník či uživatel poskytl svůj souhlas (...)*“. Důsledky této změny čl. 5 odst. 3 vysvětlila pracovní skupina zřízená podle článku 29 ve svém

⁴³ Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele (Text s významem pro EHP), Úř. věst. L 337, 18.12.2009, s. 11–36.

stanovisku č. 2/2010 k internetové reklamě zaměřené na chování⁴⁴. Otázka rozdílu mezi odmítnutím a souhlasem je též dále rozvedena v následující kapitole.

V mnoha případech, kdy směrnice o soukromí a elektronických komunikacích nebo směrnice o ochraně údajů stanoví možnost odmítnout zpracování osobních údajů, je důvodem skutečnost, že právním základem původního zpracování údajů byly *jiné* právní důvody než souhlas, například platná smlouva. To je dále vysvětleno v další části tohoto stanoviska, která se zabývá článkem 13 směrnice o soukromí a elektronických komunikacích.

III.B.4 Čl. 13 odst. 2 a 3 – právo nesouhlasit a jeho odlišnost od souhlasu

„...je zákazníkům jasně a zřetelně poskytnuta možnost... nesouhlasit...“

Článek 13 směrnice o soukromí a elektronických komunikacích stanoví, že zákonně zasílat elektronická sdělení pro účely přímého marketingu je možné na základě souhlasu. K tomu tento článek používá obecnou zásadu a zvláštní ustanovení.

Použití automatických volacích přístrojů, faxů a elektronické pošty vyžaduje předchozí souhlas subjektu údajů.

Je-li adresátem obchodního sdělení stávající klient a cílem sdělení je propagace vlastních obdobných výrobků nebo služeb poskytovatele, nepožaduje se získání souhlasu, nýbrž zajištění toho, aby byla osobám „*poskytnuta možnost nesouhlasit*“ podle čl. 13 odst. 2. Argumenty, které zákonodárce v tomto případě vedly k tomu, že souhlas nevyžaduje, jsou vysvětleny v 41. bodě odůvodnění: „*v rámci existujících zákaznických vztahů je rozumné povolit použití kontaktních údajů elektronického styku pro nabízení obdobných výrobků nebo služeb*“. Zde je tedy smluvní vztah mezi fyzickou osobou a poskytovatelem služeb v zásadě právním důvodem, který umožňuje první kontakt elektronickou poštou. Osoby by však měly mít možnost nesouhlasit s dalšími kontakty. Jak již pracovní skupina jednou uvedla: „*Tuto možnost je třeba nabízet opakovaně s každou další zprávou přímého marketingu, a to zdarma, s výjimkou nákladů spojených s přenosem tohoto odmítnutí*“.⁴⁵

Nezbytnost souhlasu by se měla odlišovat od tohoto práva nesouhlasit (vznést námitku). Jak je vysvětleno v kapitole III.A.2 výše, souhlas založený na nečinnosti osob, získaný například prostřednictvím předem zaškrtnutých políček, nesplňuje požadavky na platný souhlas podle směrnice 95/46/ES. Stejný závěr se týká prohlížeče, který by ve výchozím nastavení umožňoval cílení na uživatele (pomocí *cookies*). V novém znění čl. 5 odst. 3, citovaném v kapitole III.B.3 výše, je tato otázka jasně upravena. Uvedené dva příklady nesplňují zejména požadavek na nezpochybnitelný projev vůle. Je velmi důležité, aby subjekt údajů dostal ve vztahu k účelu zpracování údajů možnost rozhodnout se a vyjádřit své rozhodnutí, například tak, že sám zaškrtně políčko.

⁴⁴ Stanovisko ze dne 22. června 2010, WP 171: otázka, zda může být souhlas vyjádřen „vhodným nastavením prohlížeče nebo jiné aplikace“ (66. bod odůvodnění směrnice 2009/136/ES) je výslovně řešena v bodě 4.1.1 dokumentu WP 171.

⁴⁵ Stanovisko č. 5/2004 k nevyžádaným sdělením pro marketingové účely podle článku 13 směrnice 2002/58/ES, přijaté dne 27. února 2004.

Pracovní skupina ve svém stanovisku k reklamě zaměřené na chování dospěla k závěru: „zdá se, že zajištění nastavení na ochranu soukromí u prohlížečů má obrovskou důležitost. Jinými slovy, musí u nich existovat možnost nastavení pro „nepřijetí a nepředávání cookies třetích stran“. Pro doplnění a účinnější provádění tohoto nastavení by prohlížeče měly požadovat, aby uživatelé využili průvodce na ochranu soukromí (privacy wizard), když poprvé instalují nebo aktualizují prohlížeč, a měly by nabízet snadný způsob nastavení jejich volby v průběhu používání.“⁴⁶

III.B.5 Čl. 6 odst. 3, čl. 9 odst. 1 a 2 – možnost vzít souhlas zpět

„... možnost kdykoliv vzít zpět svůj souhlas...“

Možnost vzít souhlas zpět, která je ve směrnici 95/46/ES obsažena implicitně, je upravena v několika ustanoveních směrnice o soukromí a elektronických komunikacích. To je též výslovně uvedeno ve stanovisku pracovní skupiny k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou⁴⁷:

„Podle článku 9 směrnice 2002/58/ES mohou lidé, kteří poskytli souhlas se zpracováním lokalizačních údajů odlišných od provozních údajů, svůj souhlas vzít kdykoli zpět a musí mít možnost jednoduchým způsobem a zdarma dočasně odmítnout zpracování těchto údajů. Pracovní skupina považuje tato práva — která lze považovat za provádění práva vznést námitku proti zpracování lokalizačních údajů — za zásadní, vzhledem k citlivé povaze lokalizačních údajů. Pracovní skupina se domnívá, že základním předpokladem uplatňování těchto práv je, aby byli jednotlivci informováni, a to nejen ve chvíli, když si službu objednávají, ale také když službu využívají. Pokud služba vyžaduje průběžné zpracování lokalizačních údajů, zastává pracovní skupina názor, že poskytovatel služby by měl dotčenému jednotlivci pravidelně připomínat, že jeho koncové zařízení bylo, bude nebo může být lokalizováno. To takové osobě umožní uplatnit právo vzít svůj souhlas zpět podle článku 9 směrnice 2002/58/ES, pokud tak bude chtít učinit.“

Jak je již uvedeno výše, vyplývá z toho, že se zpětvzetí vztahuje na budoucnost, a nikoli na zpracování údajů, které proběhlo v minulosti, v době, kdy byly údaje shromažďovány oprávněně. Rozhodnutí nebo procesy, které z těchto informací v minulosti vycházely, proto nemohou být jednoduše zrušeny. Avšak neexistuje-li jiný právní základ pro další uchovávání údajů, měl by je správce údajů smazat.

IV. Závěry

Toto stanovisko se zabývá právním rámcem pro používání souhlasu podle směrnice 95/46/ES a směrnice 2002/58/ES. Přitom sleduje dvojí cíl: Zprvu se snaží objasnit stávající právní požadavky a ukázat, jak fungují v praxi. Zároveň představuje také určitou reflexi nad tím, zda je stávající rámec i nadále vhodný vzhledem k mnoha novým způsobům zpracování osobních údajů, nebo zda není nutné jej změnit.

⁴⁶ Již citované stanovisko ze dne 22. června 2010, WP 171.

⁴⁷ Stanovisko č. 5/2005 k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou, přijaté dne 25. listopadu 2005 (WP 115).

IV.1 Objasnění hlavních aspektů současného rámce

V čl. 2 písm. h) směrnice 95/46/ES je souhlas definován jako „*jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování*“. V článku 7 směrnice, který stanoví právní základ pro zpracování osobních údajů, je jako jeden z právních důvodů uveden *nezpochybnitelný* souhlas. Článek 8 stanoví *výslovný (explicit)* souhlas jako právní důvod pro zpracování citlivých údajů. Čl. 26 odst. 1 směrnice 95/46/ES a různá ustanovení směrnice o soukromí a elektronických komunikacích ukládají povinnost získat souhlas pro zvláštní druhy zpracování údajů, které spadají do jejich působnosti. Cílem tohoto stanoviska je vyjasnit různé složky tohoto právního rámce, aby jej mohly zúčastněné strany obecně snadněji uplatňovat.

Aspekty a poznámky obecné povahy

- Souhlas je jedním ze šesti právních důvodů pro zpracování osobních údajů (jedním z pěti v případě citlivých údajů); jedná se o důležitý důvod, protože dává subjektu údajů určitou kontrolu nad zpracováním údajů, které se jej týkají. Aby mohl souhlas přispívat k autonomii a sebeurčení fyzické osoby, musí se používat ve správném kontextu a s nezbytnými prvky.
- Obecně platí, že právní rámec směrnice 95/46/ES se použije ve všech případech, kdy se žádá o souhlas, bez ohledu na to, zda je to v offline nebo online prostředí. Pokud například kamenný obchod usiluje o registraci zákazníků do programu věrnostních karet pomocí papírového formuláře, použijí se stejná pravidla, jako kdyby registraci prováděl prostřednictvím svých internetových stránek. Směrnice o soukromí a elektronických komunikacích navíc stanoví určitá zpracování údajů, která podléhají souhlasu – většinou jde o zpracování údajů v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací. Požadavky, které musí být splněny, aby byl souhlas platný podle směrnice 2002/58/ES, jsou stejné jako u směrnice 95/46/ES.
- Situace, kdy správci údajů používají souhlas jako právní důvod zpracování osobních údajů, by neměly být zaměňovány se situacemi, kdy správce při zpracování vychází z jiných právních důvodů, které jsou spojeny s právem fyzické osoby nesouhlasit či vznést námitku. Tak tomu může být například tehdy, když zpracování vychází z „oprávněných zájmů“ správce údajů podle čl. 7 písm. f) směrnice 95/46/ES, ale fyzická osoba má právo vznést námitku podle čl. 14 písm. a) směrnice 95/46/ES. Dalším příkladem je situace, kdy správce údajů rozešle e-mailová sdělení stávajícím klientům za účelem propagace svých vlastních obdobných výrobků nebo služeb; dotčené osoby však mají právo nesouhlasit podle čl. 13 odst. 2 směrnice 2002/58/ES. V obou případech má subjekt údajů právo na námitku proti zpracování, což není totéž jako souhlas.
- Použití souhlasu pro zpracování osobních údajů nezbavuje správce údajů povinnosti plnit ostatní požadavky právního rámce pro ochranu údajů, například dodržovat zásadu přiměřenosti podle čl. 6 odst. 1 písm. c), zajistit bezpečnost zpracování podle článku 17 atd.
- Platný souhlas předpokládá způsobilost fyzické osoby souhlas udělit. Pravidla týkající se způsobilosti k udělení souhlasu nebyla harmonizována, a mohou tedy být v různých členských státech různá.

- Osoby, které udělily souhlas, by měly mít možnost vzít souhlas zpět, a zabránit tak dalšímu zpracování svých údajů. To je potvrzeno také ve směrnici o soukromí a elektronických komunikacích pro zvláštní případy zpracování údajů založeného na souhlasu, jako je zpracování lokalizačních údajů odlišných od provozních údajů.
- Souhlas musí být udělen před tím, než zpracování osobních údajů začne, ale může být nezbytný také v průběhu zpracování, pokud se objeví nový účel. Toto je zdůrazněno v různých ustanoveních směrnice 2002/58/ES – buď prostřednictvím požadavku, aby byl souhlas udělen „předem“ (např. čl. 6 odst. 3) nebo prostřednictvím znění příslušných ustanovení (např. čl. 5 odst. 3).

Konkrétní složky právního rámce související se souhlasem

- Aby byl souhlas platný, musí být *svobodný*. To znamená, že nesmí existovat riziko klamání, zastrašování či podstatných záporných důsledků pro subjekt údajů, pokud souhlas neudělí. U zpracování údajů v kontextu pracovního poměru, kde existuje prvek podřízenosti, jakož i v kontextu veřejných služeb, jako je zdravotnictví, může být nutné pečlivě posoudit, zda mohou osoby udělit souhlas svobodně.
- Souhlas musí být *výslovný (specific)*. Obecný souhlas bez uvedení přesných účelů tuto podmínku nesplňuje. Příslušné informace by tedy neměly být součástí všeobecných smluvních podmínek, ale měla by se používat zvláštní ustanovení o souhlasu, která budou od všeobecných podmínek oddělená.
- Souhlas musí být *vědomý*. V člancích 10 a 11 směrnice jsou vyjmenovány typy informací, které musí být fyzickým osobám nezbytně poskytovány. Poskytované informace musí být v každém případě dostatečné k tomu, aby bylo možné zaručit, že fyzické osoby budou moci přijímat vědomá (informovaná) rozhodnutí o zpracování svých osobních údajů. Nezbytnost „vědomého“ souhlasu vede ke dvěma dodatečným požadavkům. Zaprvé musí způsob, kterým se informace podávají, zajišťovat použití vhodného jazyka, aby subjekty údajů rozuměly tomu, s čím souhlasí a za jakými účely. To závisí na kontextu. Použití nadměrně složitého právního nebo odborného žargonu by požadavky právního předpisu nesplňovalo. Zadruhé by informace poskytované uživatelům měly být jasné a dostatečně výrazné, aby je uživatelé nemohli přehlédnout. Informace musí být poskytovány přímo fyzickým osobám. Nepostačuje, aby byly pouze někde k dispozici.
- Pokud jde o to, jak musí být souhlas udělen, vyžaduje čl. 8 odst. 2 písm. a) pro zpracování citlivých údajů *výslovný (explicit)* souhlas, kterým se rozumí aktivní reakce, ať ústní, nebo písemná, kdy osoba vyjádří svou vůli, aby byly její údaje pro určité účely zpracovávány. Takový výslovný souhlas proto nemůže být získán pomocí předem zaškrtnutého políčka. Subjekt údajů musí učinit nějaký aktivní krok, kterým vyjádří souhlas, a musí mít možnost nesouhlasit.
- U jiných než citlivých údajů vyžaduje čl. 7 písm. a), aby byl souhlas *nezpochybnitelný*. Podmínka „nezpochybnitelnosti“ vyžaduje používání mechanismů pro získání souhlasu, které neponechávají prostor pro pochybnost ohledně úmyslu fyzické osoby souhlas udělit. Z praktického hlediska tento požadavek správcům údajů umožňuje používat různé druhy mechanismů pro získání souhlasu – od prohlášení, kterými se dává svolení, (výslovný souhlas) po mechanismy, v jejichž rámci se svolení dává prostřednictvím určitého jednání.

- Souhlas založený na nečinnosti či mlčení fyzické osoby by obvykle platný souhlas nepředstavoval, zvláště ne v online prostředí. Tato otázka vyvstává zejména v souvislosti s používáním výchozího nastavení, které subjekt údajů musí změnit, pokud chce zpracování odmítnout. Je tomu tak například v případě používání předem zaškrtnutých políček nebo výchozího nastavení internetového prohlížeče, které umožňuje shromažďování údajů.

IV.2 Posouzení stávajícího rámce a případná potřeba změn

Celkové posouzení

Pracovní skupina se domnívá, že současný rámec ochrany údajů obsahuje promyšlený soubor pravidel, který stanoví podmínky pro platný souhlas legitimizující zpracování údajů. Tyto podmínky platí jak v offline, tak v online prostředí. Konkrétněji:

Tento rámec úspěšně vyvažuje celou řadu zájmů. Na jedné straně zajišťuje, aby se za souhlas považoval jen skutečný, vědomý souhlas. V tomto ohledu je důležitý a uspokojivý čl. 2 písm. h), který výslovně vyžaduje, aby byl souhlas svobodný, výslovný (*specific*) a vědomý. Na druhé straně není tento požadavek nadměrně omezující, ale poskytuje dostatečnou flexibilitu a neobsahuje pravidla vázaná na konkrétní technologie. O tom svědčí tentýž čl. 2 písm. h), když souhlas definuje jako jakýkoli projev vůle fyzické osoby. Díky tomu existuje dostatečně široký prostor, pokud jde o způsoby, jakými může být tento projev vůle realizován. Článek 7, který vyžaduje nezpochybnitelný souhlas, a článek 8, který vyžaduje výslovný (*explicit*) souhlas, dobře vystihují potřebu rovnováhy mezi dvěma zájmy, protože zajišťují flexibilitu a nestanoví příliš rigidní struktury a současně zaručují ochranu.

Výsledkem je rámec, který při správném provedení a používání dokáže držet krok s širokou škálou zpracování údajů, která jsou častým důsledkem technického rozvoje.

Vzhledem k nejednotnosti mezi členskými státy však v praxi není vždy snadné určit, kdy je souhlas zapotřebí a především jaké jsou požadavky na platný souhlas a jak mají být konkrétně uplatňovány. Zavedení rámce na úrovni jednotlivých států vedlo k různým přístupům. V průběhu jednání pracovní skupiny zřízené podle článku 29, které vyústilo v přijetí tohoto stanoviska, byly identifikovány některé konkrétnější nedostatky, které jsou popsány níže.

Možné změny

- Pojem nezpochybnitelný souhlas je užitečný pro vytvoření systému, který není nadměrně nepružný, ale současně zajišťuje silnou ochranu. Na základě tohoto pojmu může potenciálně vzniknout přiměřený systém, ale jeho význam je bohužel často nesprávně chápán nebo je jednoduše opomíjen. Vyjádření a příklady uvedené v tomto stanovisku by sice měly přispět k posílení právní jistoty a ochrany práv fyzických osob v situacích, kdy se jako právní základ používá souhlas, avšak popsání situace zřejmě vyžaduje provedení určitých změn.
- Konkrétněji se pracovní skupina zřízená podle článku 29 domnívá, že by v rámci revize obecného rámce ochrany údajů bylo vhodné dále upřesnit samotné slovo „nezpochybnitelný“ (*unambiguous*). Tímto upřesněním by se mělo zdůraznit, že nezpochybnitelný souhlas vyžaduje používání mechanismů, které neponechávají prostor pro pochybnosti ohledně úmyslu subjektu údajů udělit souhlas. Zároveň by mělo být jasně uvedeno, že používání výchozího nastavení, které subjekt údajů musí

změnit, pokud chce zpracování odmítnout, (souhlas založený na mlčení) samo o sobě nevede k získání nezpochybnitelného souhlasu. To platí zvláště v online prostředí.

- Kromě výše popsaného upřesnění pracovní skupina zřízená podle článku 29 navrhuje:
 - i. *zaprvé* doplnit do definice souhlasu v čl. 2 písm. h) slovo „nezpochybnitelný“ (nebo slovo rovnocenného významu), aby bylo jasnější, že platným souhlasem je pouze souhlas založený na prohlášeních nebo úkonech, kterými se dává svolení. Vedle větší jasnosti by tak byl pojem souhlas podle čl. 2 písm. h) rovněž uveden do souladu s požadavky na platný souhlas uvedenými v článku 7. Význam slova „nezpochybnitelný“ by také mohl být dále vysvětlen v některém bodě odůvodnění budoucího právního rámce;
 - ii. *zadruhé* by správci v rámci své obecné odpovědnosti měli být schopni doložit, že byl souhlas získán. Pokud se totiž důkazní břemeno posílí tak, aby byli správci údajů povinni dokládat, že skutečně získali souhlas subjektu údajů, budou nuceni zavést standardní postupy a mechanismy pro získávání a prokazování nezpochybnitelného souhlasu. Druh mechanismu pak bude záviset na kontextu a měl by zohledňovat skutečnosti a okolnosti, které se zpracování týkají, a zejména rizika s ním spojená.
- Pracovní skupina zřízená podle článku 29 není přesvědčena, že by měl právní rámec vyžadovat výslovný (*explicit*) souhlas jako obecné pravidlo pro všechny druhy zpracování údajů, včetně těch, na které se nyní vztahuje článek 7 směrnice. Domnívá se, že by měl i nadále platit požadavek na nezpochybnitelný souhlas, který zahrnuje výslovný (*explicit*) souhlas, ale také souhlas vyplývající z jednoznačného *jednání*. Tato možnost správcům údajů poskytuje větší flexibilitu při získávání souhlasu a celý postup může být rychlejší a vstřícnější k uživatelům.
- Několik aspektů právního rámce, které se týkají souhlasu, je odvozeno ze znění právních předpisů či z legislativní historie nebo vzniklo na základě judikatury a stanovisek pracovní skupiny zřízené podle článku 29. Kdyby se tyto aspekty staly výslovnou součástí nového právního rámce pro ochranu údajů, vedlo by to k větší právní jistotě. V úvahu je možné vzít tyto body:
 - i. doplnění ustanovení, které výslovně stanoví právo fyzických osob na zpětvzetí souhlasu;
 - ii. jasnější stanovení požadavku, že souhlas musí být udělen před tím, než zpracování začne, nebo před dalším využitím údajů pro účely, na které se původní souhlas nevztahoval, pokud neexistuje jiný právní důvod zpracování;
 - iii. doplnění výslovných požadavků na kvalitu informací (povinnost poskytovat informace o zpracování údajů snadno srozumitelným způsobem, jasným a běžným jazykem) a jejich přístupnost (povinnost, aby byly informace zřetelné, výrazné a přímo přístupné). To má zásadní význam pro možnost fyzických osob přijímat informovaná rozhodnutí.

- Konečně by bylo možné zavést ustanovení zajišťující zvýšenou ochranu, pokud jde o osoby, které nemají způsobilost k právům a právním úkonům, obsahující například:
 - i. upřesnění okolností, za kterých se vyžaduje souhlas rodičů nebo zákonných zástupců fyzické osoby bez právní způsobilosti, včetně stanovení věkové hranice, pod kterou by byl tento souhlas povinný;
 - ii. stanovení povinnosti používat mechanismy pro ověřování věku, které by mohly být různé podle okolností, jako je věk dítěte, druh zpracování, případná zvláštní rizikovitost zpracování a otázka, zda si údaje ponechá správce údajů, nebo budou zpřístupňovány třetím stranám;
 - iii. požadavek, aby byly informace přizpůsobovány pro potřeby dětí, pokud by to dětem usnadnilo porozumění, co znamená shromažďování jejich údajů, a tedy i možnost udělit souhlas;
 - iv. zvláštní ochranná opatření, v jejichž rámci by byla stanovena zpracování údajů, například behaviorálně cílená reklama, u nichž by souhlas neměl být možným základem pro legitimizaci zpracování osobních údajů.

Pracovní skupina zřízená podle článku 29 se bude otázkou souhlasu znovu zabývat. Konkrétně se vnitrostátní orgány pro ochranu údajů i pracovní skupina mohou později rozhodnout, že vypracují pokyny pro další rozpracování tohoto stanoviska a poskytnou další praktické příklady související s používáním souhlasu.

V Bruselu dne 13. července 2011

Za pracovní skupinu

předseda
Jacob KOHNSTAMM