

CS

CS

CS



EVROPSKÁ KOMISE

V Bruselu dne 4.11.2010
KOM(2010) 609 v konečném znění

**SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU
HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ**

Komplexní přístup k ochraně osobních údajů v Evropské unii

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ

Komplexní přístup k ochraně osobních údajů v Evropské unii

1. NOVÉ VÝZVY PŘI OCHRANĚ OSOBNÍCH ÚDAJŮ

Směrnice o ochraně údajů z roku 1995¹ se stala milníkem v historii ochrany osobních údajů v Evropské unii. Tato směrnice obsahuje dva nejstarší a stejně důležité cíle procesu evropské integrace: ochranu základních zpráv a svobod jednotlivců, zejména základního práva na ochranu údajů, a dále vytvoření vnitřního trhu, v tomto případě volného pohybu osobních údajů.

Po patnácti letech lze říci, že tento dvojitý cíl a zásady zakotvené ve směrnici stále platí. **Rychlý technologický vývoj a globalizace však hluboce změnily svět kolem nás a přinesly v oblasti ochrany osobních údajů nové výzvy.**

Technologie v současnosti umožňuje jednotlivcům snadno sdílet informace o svém chování a preferencích a v bezprecedentním rozsahu je dát k dispozici prakticky celému světu. Snad nejviditelnějším, avšak nikoli jediným příkladem tohoto fenoménu jsou internetové sociální sítě se stovkami milionů členů po celé Zemi. *Cloud computing*, tj. využívání výpočetních technologií na základě internetu, kdy jsou software, sdílené zdroje a informace uloženy na vzdálených serverech („v mraku“, *cloud* = mrak), by také mohlo vytvářet nové úkoly v oblasti ochrany údajů, protože jednotlivce ukládající svá data na programech spouštěných z cizího hardwaru může zbavit kontroly nad potenciálně citlivými informacemi. Podle nedávné studie se zdá, že orgány pro ochranu údajů, podnikatelská sdružení i sdružení spotřebitelů se shodují, že v souvislosti s online aktivitou vzrůstá riziko ohrožení soukromí i pro ochranu osobních údajů².

Způsoby shromažďování osobních údajů jsou zároveň stále propracovanější a lze je hůře odhalit. Používání sofistikovaných nástrojů například umožňuje hospodářským subjektům sledovat chování jednotlivců, a tak se lépe zaměřit na potenciální zákazníky. Rostoucí využívání postupů pro automatický sběr dat (například elektronický prodej jízdenek či výběr mýtného) nebo geolokačních zařízení umožňuje snadněji zjistit polohu určité osoby jednoduše díky jejímu mobilnímu zařízení. Veřejné orgány také stále více využívají osobních údajů za různým účelem, mimo jiné k vyhledávání osob v případě propuknutí přenosné choroby, pro předcházení terorismu a trestné činnosti a účinnějšímu boji proti nim, pro správu systémů sociálního zabezpečení nebo pro daňové účely, a to v rámci svých aplikací elektronické veřejné správy nebo jinak.

¹ Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, s. 31).

² Viz *Study on the economic benefits of privacy enhancing technologies*, London Economics, červenec 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), s. 14.

V souvislosti s tím vším nevyhnutelně vyvstává otázka, zda se stávající právní předpisy EU pro ochranu údajů stále dokáží s těmito výzvami plně a účinně vyrovnat.

Aby Komise pomohla tuto otázku vyřešit, zahájila v květnu 2009 na konferenci na vysoké úrovni přezkum stávajícího právního rámce. Dále následovala veřejná konzultace probíhající do konce roku 2009³. Byla také provedena řada studií⁴.

Tento přezkum potvrdil, že základní zásady směrnice jsou nadále platné a že by měla být zachována její technologicky neutrální povaha. Bylo však vymezeno několik otázek, jež se jeví jako problematické a představují konkrétní výzvy. Mezi ně patří:

- *Reakce na nové technologie*

Odpovědi jednotlivců i organizací na konzultaci potvrzují, že je nezbytné objasnit a přesně vymežit používání zásad ochrany údajů v souvislosti s novými technologiemi, tak aby mohla být zajištěna účinná ochrana osobních údajů jednotlivce bez ohledu na technologii, jež je ke zpracování jejich údajů použita. Správci údajů jsou si dopadu nových technologií na ochranu údajů plně vědomi. Touto problematikou se částečně zabývala směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích)⁵, jež doplňuje a rozvádí obecnou směrnici o ochraně údajů v oblasti elektronické komunikace⁶.

- *Posílení dimenze vnitřního trhu při ochraně údajů*

Jednou z hlavních obav opakovaně vyjadřovaných zainteresovanými stranami, zejména nadnárodními společnostmi, je nedostatečná harmonizace právních předpisů členských států o ochraně údajů bez ohledu na společný právní rámec EU. Strany zdůraznily potřebu zvýšit právní jistotu, snížit administrativní zátěž a zajistit hospodářským subjektům a dalším správcům údajů stejné podmínky.

³ Viz odpovědi na veřejnou konzultaci Komise na internetové stránce http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. Po celý rok 2010 se vedou cílenější konzultace se zainteresovanými stranami. Místopředsedkyně Komise Viviane Redingová také předsedala setkání na vysoké úrovni s těmito stranami, jež se uskutečnilo 5. října 2010 v Bruselu. Komise dále konzultovala rovněž pracovní skupinu zřízenou podle článku 29 směrnice 95/46/ES, která vypracovala souhrnný příspěvek ke konzultaci z roku 2009 (WP 168) a v červenci 2010 přijala stanovisko ke koncepci odpovědnosti (WP 173).

⁴ Kromě studie s názvem *Study on the economic benefits of privacy enhancing technologies* (pozn. č. 2), viz též *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments* z ledna 2010, k dispozici na internetové stránce (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). Probíhá také studie posouzení dopadů budoucího právního rámce EU pro ochranu osobních údajů.

⁵ Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. L 201, 31.7.2002, s. 37.

⁶ Směrnice o ochraně údajů 95/46/ES stanoví standardy pro ochranu údajů pro všechny legislativní akty EU, a to i pro směrnici o soukromí a elektronických komunikacích 2002/58/ES (ve znění směrnice 2009/136/ES, Úř. věst. L 337, 18.12.2009, s. 11). Směrnice o soukromí a elektronických komunikacích se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích. Převedla zásady stanovené ve směrnici 95/46/ES do zvláštních pravidel pro odvětví telekomunikací. Tato směrnice se použije mimo jiné pro neveřejné komunikační služby.

- *Reakce na globalizaci a zlepšení mezinárodního předávání údajů*

Několik zainteresovaných stran zdůraznilo, že stále běžnější zpracovávání osobních údajů externími dodavateli, často mimo území EU, přináší některé problémy ohledně práva použitelného na zpracování údajů a na určení odpovědnosti. Co se týče mezinárodního předávání údajů, mnoho organizací vyjádřilo názor, že stávající režimy nejsou zcela uspokojivé a je třeba je přezkoumat a racionalizovat s cílem zjednodušit předávání údajů a zmenšit jeho náročnost.

- *Vytvoření silnějšího institucionálního rámce pro účinné prosazování pravidel pro ochranu údajů*

Zúčastněné strany se shodují, že je třeba posílit úlohu orgánů pro ochranu údajů, aby bylo možno pravidla na ochranu údajů lépe prosazovat. Některé organizace rovněž vyzvaly k větší transparentnosti činnosti pracovní skupiny zřízené podle článku 29 (viz oddíl 2.5) a k objasnění jejích úkolů a pravomocí.

- *Zlepšení soudržnosti právního rámce pro ochranu údajů*

Ve veřejné konzultaci všechny zainteresované strany zdůraznily potřebu zastřešujícího nástroje, který by byl použitelný na zpracování údajů ve všech odvětvích a politikách Unie a zajistil integrovaný přístup i komplexní, konzistentní a účinnou ochranu⁷.

Uvedené výzvy vyžadují, aby EU vypracovala komplexní a jednotný přístup zaručující úplné dodržování základního práva jednotlivce na ochranu údajů, a to jak v EU, tak mimo její území. Lisabonská smlouva poskytla EU k splnění tohoto úkolu další nástroje. Listina základních práv EU, jejíž článek 8 uznává zvláštní právo na ochranu osobních údajů, se stala právně závaznou a byl zaveden nový právní základ⁸ umožňující přijímání komplexních a jednotných právních předpisů Unie o ochraně fyzických osob při zpracovávání jejich osobních údajů a o volném pohybu těchto údajů. Tento nový právní základ konkrétně umožňuje EU vytvořit jediný právní nástroj pro regulaci ochrany údajů, mimo jiné v oblasti policejní a justiční spolupráce v trestních věcech. Oblast společné zahraniční a bezpečnostní politiky je jen částečně pokryta článkem 16 SFEU, protože konkrétní pravidla pro zpracování údajů členskými státy musí být stanovena rozhodnutím Rady na jiném právním základě⁹.

S využitím těchto nových právních možností bude Komise přikládat nejvyšší prioritu dodržování základního práva na ochranu údajů v celé Unii a ve všech jejích politikách a zároveň posílí dimenzi vnitřního trhu a usnadní volný pohyb osobních údajů. V této souvislosti je při zabezpečování uvedeného práva nezbytné brát plný ohled na ostatní relevantní základní práva zakotvená v Listině základních práv EU a na ostatní cíle uvedené ve Smlouvách.

Cílem tohoto sdělení je vymezit přístup Komise k modernizaci právního systému EU pro ochranu osobních údajů ve všech oblastech činnosti Unie, zejména s přihlédnutím k výzvám, jež přináší globalizace a nové technologie, aby mohla ve všech takových oblastech být nadále

⁷ Europol a Eurojust ve zvláštních příspěvcích předložených po skončení veřejné konzultace požádaly, aby bylo přihlédnuto ke specifické povaze jejich práce (koordinace vymáhání práva a předcházení trestné činnosti).

⁸ Viz článek 16 Smlouvy o fungování Evropské unie (SFEU).

⁹ Viz čl. 16 odst. 2 poslední odstavec SFEU a článek 39 Smlouvy o EU.

zaručena vysoká úroveň ochrany osob při zpracovávání osobních údajů. To umožní EU, aby při prosazování vysokých standardů pro ochranu údajů zůstala hnací silou.

2. HLAVNÍ CÍLE KOMPLEXNÍHO PŘÍSTUPU K OCHRANĚ ÚDAJŮ

2.1. Posílení práv jednotlivců

2.1.1. Bezpodmínečné zajištění odpovídající ochrany jednotlivcům

Cílem pravidel obsažených ve stávajících nástrojích EU pro ochranu údajů je dle Listiny základních práv EU **chránit základní práva fyzických osob, zejména jejich právo na ochranu osobních údajů**¹⁰.

Pojem „osobní údaje“ je jedním z klíčových pojmů ochrany osob ve stávajících nástrojích EU pro ochranu osobních údajů a aktivuje uplatňování povinností uložených správcům a zpracovatelům údajů¹¹. „Osobními údaji“ se rozumějí veškeré přímé či nepřímé informace o identifikované nebo identifikovatelné osobě. Při určování, zda je osoba identifikovatelná, je třeba přihlídnout „ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby“¹². Výhodou tohoto přístupu, který zákonodárce zvolil úmyslně, je pružnost, protože může být uplatňován v různých situacích ovlivňujících základní práva, včetně těch, které nebylo v okamžiku přijímání směrnice možné předpokládat. Avšak důsledkem takového širokého a pružného přístupu je řada případů, kdy při provádění směrnice není vždy zřejmé, jaký přístup zvolit, zda jedinci požívají práv na ochranu osobních údajů nebo zda by správci údajů měli plnit povinnosti uložené směrnicí¹³.

V některých situacích dochází ke zpracovávání určitých informací, což by vyžadovalo dodatečná opatření podle práva Unie. Taková opatření již v některých případech existují, například uchovávání informací v koncovém zařízení (např. mobilních telefonech) je povoleno pouze pod podmínkou, že k němu dal uživatel souhlas. Tuto otázku může být nutno řešit na úrovni EU v souvislosti např. s kódovanými údaji, lokalizačními údaji, technologiemi pro vytěžování dat (*data mining*) umožňujícími kombinovat údaje z různých zdrojů nebo s případy, kdy je nutno zajistit důvěrnost a integritu systémů informačních technologií¹⁴.

Všechny uvedené otázky je proto třeba pečlivě posoudit.

Komise zvaží, jak zajistit jednotné uplatňování pravidel na ochranu údajů, přičemž přihlédne k dopadu nových technologií na práva osob a jejich svobody a zohlední cíl zajistit volný pohyb osobních údajů na vnitřním trhu.

¹⁰ Viz např. rozsudek Soudního dvora ve věci Bodil Lindqvist, C-101/01, Sb. rozh. 2003, s. I 1297, a ve věci Productores de Música de España (Promusicae) v. Telefónica de España SAU, C-275/06, Sb. rozh. 2008, s. I 271. Viz např. judikaturu Evropského soudu pro lidská práva, např. ve věcech S. a Marper v. Spojené království, 4.12.2008 (stížnosti č. 30562/04 a 30566/04) a Rotaru v. Rumunsko, 4.5.2000, č. 28341/95, § 55, ECHR 2000-V.

¹¹ Pojmy „správce“ údajů a „zpracovatel“ údajů jsou definovány v čl. 2 písm. d) a e) směrnice 95/46/ES.

¹² Viz bod odůvodnění 26 směrnice 95/46/ES.

¹³ Viz např. otázku IP adres zkoumanou ve stanovisku č. 4/2007 k pojmu osobní údaje pracovní skupiny zřízené podle článku 29 (WP 136).

¹⁴ Viz např. rozsudek německého Spolkového ústavního soudu (*Bundesverfassungsgericht*) z 27. února 2008, 1 BvR 370/07.

2.1.2. Zvýšení transparentnosti pro subjekty údajů

Transparentnost je základní podmínkou k zajištění účinné ochrany osobních údajů a k tomu, aby fyzické osoby mohly nad svými údaji vykonávat kontrolu. Je proto zásadní, aby správci údajů fyzické osoby **důkladně a jasně informovali průhledným způsobem**, kdo a jak jejich údaje shromažďuje a zpracovává, za jakým účelem a na jak dlouho i jaká jsou jejich práva, požadují-li přístup ke svým údajům, jejich opravu nebo vymazání. Příslušná ustanovení o informování subjektu údajů¹⁵ nejsou dostačující.

Základním prvkem transparentnosti je požadavek na **snadný přístup k informacím, na srozumitelnost informací a na používání jasného, běžného jazyka**. To je zvláště důležité v online prostředí, kde jsou prohlášení o ochraně soukromí často nejasná, obtížně přístupná, netransparentní¹⁶ a někdy dokonce v částečném rozporu se stávajícími pravidly. Pro ilustraci lze uvést internetovou behaviorálně cílenou reklamu, do níž bývá zapojeno mnoho aktérů a jejíž technologická složitost znesnadňuje jednotlivci, aby byl informován, zda jsou jeho osobní údaje shromažďovány a kdo a za jakým účelem je shromažďuje, a těmto informacím rozuměl.

V této souvislosti si zvláštní ochranu zaslouží **děti**, protože si v souvislosti se zpracováním osobních údajů mohou být méně vědomy rizik, důsledků a ochranných opatření a práv¹⁷.

Komise zváží:

- zavedení **obecné zásady transparentního zpracování** osobních údajů do právního rámce,
- zavedení **zvláštních povinností** pro správce údajů ohledně druhu informací, které mají být poskytovány, a **způsobů** jejich poskytování, včetně ve vztahu k **dětem**,
- vypracování jednoho či více **standardních formulářů EU („prohlášení o ochraně soukromí“)** pro správce údajů.

Je také důležité, aby fyzické osoby byly informovány, jsou-li jejich údaje náhodně nebo neoprávněným způsobem zničeny, ztraceny nebo pozmeněny či zpřístupněny nebo odhaleny neautorizovaným osobám. Revidovaným zněním směrnice o soukromí a elektronických komunikacích bylo zavedeno **povinné oznámení o narušení bezpečnosti osobních údajů**, jež se nicméně týká jen odvětví telekomunikací. Vzhledem k tomu, že rizika narušení bezpečnosti údajů existují i v jiných odvětvích (např. finančnictví), posoudí Komise způsoby, jak rozšířit povinnost oznamovat narušení bezpečnosti osobních údajů na jiná odvětví, a to v souladu s prohlášením Komise k oznámení o narušení bezpečnosti údajů v Evropském parlamentu z roku 2009 v rámci reformy předpisového rámce pro elektronické komunikace¹⁸.

¹⁵ Viz článek 10 a 11 směrnice 95/46/ES.

¹⁶ Průzkum Eurobarometru z roku 2009 ukázal, že zhruba polovina respondentů považuje prohlášení o ochraně soukromí na internetových stránkách za „velmi“ nebo „dostí nejasná“ (viz bleskový průzkum Eurobarometru č.° 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

¹⁷ Viz kvalitativní studie *Safer Internet for Children*, která se zabývala dětmi ve věku 9 až 10 a 12 až 14 let a ukázala, že děti mají tendenci podceňovat rizika plynoucí z používání internetu a zlehčují důsledky svého riskantního chování (k dispozici na internetové stránce http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

¹⁸ „Komise bere na vědomí, že Evropský parlament chce, aby se povinnost oznamovat případy narušení bezpečnosti osobních údajů neomezovala na odvětví elektronických komunikací, ale aby platila i pro subjekty, jako jsou poskytovatelé služeb informační společnosti [...]. Komise proto bez prodlení zahájí vhodné přípravné práce včetně konzultace se zúčastněnými subjekty, aby mohla do konce roku 2011 předložit příslušné návrhy v této oblasti [...]“. Prohlášení je k dispozici na internetové stránce

Tímto posouzením nebudou dotčena ustanovení směrnice o soukromí a elektronických komunikacích, jež musí být převedena do vnitrostátních právních předpisů do 25. května 2011¹⁹. V této záležitosti bude nezbytné zajistit konzistentní a jednotný přístup.

Komise přijme tato opatření:

– posoudí způsoby, jak do obecného právního rámce začlenit **obecné oznámení o narušení bezpečnosti osobních údajů**, včetně adresátů takových oznámení a kritérií vedoucích k vzniku povinnosti takové narušení oznamovat.

2.1.3. Zvýšení kontroly nad vlastními údaji

Dvěma důležitými podmínkami pro zabezpečení toho, aby se fyzické osoby těšily vysoké úrovni ochrany údajů, je **omezení zpracovávání údajů ze strany správce údajů v závislosti na jeho účelu (zásada minimalizace údajů)** a **účinná kontrola** subjektu údajů **nad svými údaji**. V čl. 8 odst. 2 Listiny základních práv EU se stanoví, že „každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu“. Fyzické osoby by měly vždy mít ke svým údajům přístup a měly by mít možnost jejich opravy, vymazání nebo zablokování, ledaže by existovaly oprávněné důvody stanovené právními předpisy, jež by tomu bránily. Tato práva jsou ve stávajícím právním rámci již obsažena. Způsob jejich výkonu ale není harmonizován, a proto je v některých členských státech skutečný výkon těchto práv snazší než v jiných. Mimoto je zvlášť problematický v online prostředí, kde jsou údaje často uchovávány, aniž by o tom dotčená osoba byla informována anebo k tomu poskytla souhlas.

Zvlášť dobrým příkladem jsou internetové sociální sítě, které mohou výrazně ohrožovat možnost fyzické osoby účinně kontrolovat své osobní údaje. Komise obdržela několik dotazů od osob, kterým se nepodařilo získat tyto údaje od poskytovatelů internetových služeb (například své fotografie), a jimž tak bylo zabráněno ve výkonu práva na přístup, opravu a vymazání údajů.

Tato práva by proto měla být vyjádřena explicitněji, objasněna a případně posílena.

Komise proto posoudí, jak:

– posílit **zásadu minimalizace údajů**,

– **zlepšit způsoby faktického výkonu práv na přístup, opravu, vymazání nebo zablokování údajů** (např. zavedením lhůt pro odpověď na žádosti jednotlivců, umožněním výkonu práv elektronicky nebo stanovením, že právo na přístup k údajům by mělo být zajištěno zásadně bezplatně),

– objasnit tzv. „**právo být zapomenut**“, tj. právo fyzických osob, aby jejich údaje nebyly dále zpracovávány a byly vymazány, jestliže jich není již třeba pro legitimní účely. Jedná se například o situace, kdy je ke zpracování nezbytný souhlas dotčené osoby, ale daná osoba souhlas odvolá, nebo kdy doba uchovávání údajů již uplynula;

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//CS>. Viz též bod odůvodnění 59 směrnice 2009/136/ES, kterou se mění

směrnice o soukromí a elektronických komunikacích 2002/58/ES: „Zájem uživatelů být informován se zjevně neomezuje na odvětví elektronických komunikací, a proto by měl být na úrovni Společenství jako priorita zaveden požadavek na výslovné povinné oznamování vztahující se na všechna odvětví.“

¹⁹

Článek 4 směrnice 2009/136/ES.

– doplnit práva subjektů údajů o zajištění „**přenositelnosti údajů**“, tj. poskytnout fyzickým osobám výslovné právo odstranit své údaje (např. fotografie či seznam přátel) z určité aplikace či služby za účelem jejich přesunutí do jiné aplikace či služby v míře, v jaké je to technicky proveditelné, a aniž by tomu správce údajů bránil.

2.1.4. Zvyšování informovanosti

Transparentnost je zásadní, ale je též potřeba zvyšovat informovanost veřejnosti, a zejména mladých lidí, o rizicích souvisejících se zpracováním jejich osobních údajů a o jejich právech. Průzkum Eurobarometru v roce 2008 ukázal, že naprostá většina osob v členských státech EU je názoru, že informovanost o ochraně osobních údajů v jejich vlastní zemi je nízká²⁰. Činnosti v oblasti zvyšování informovanosti by proto měla podporovat celá řada aktérů, tj. orgány členských států, zejména orgány pro ochranu údajů a vzdělávací instituce, jakož i správci údajů a sdružení občanské společnosti. Mezi tyto činnosti by měla patřit nelegislativní opatření (informační kampaně v tisku a elektronických médiích) a sdělování jasných informací na internetových stránkách s jasným uvedením práv subjektu údajů a odpovědnosti správce údajů.

Komise posoudí:

- možnost **spolufinancovat činnosti za účelem zvýšení informovanosti o ochraně údajů** z rozpočtu Unie,
- potřebu a možnost začlenit do právního rámce **povinnost zvyšovat informovanost** v této oblasti.

2.1.5. Zajištění vědomého a svobodného souhlasu

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 zpracovány²¹. 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.

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.

²⁰ Viz bleskový průzkum Eurobarometru č. 225 – *Data Protection in the European Union*: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf.

²¹ Viz čl. 2 písm. h) směrnice 95/46/ES.

2.1.6. Ochrana citlivých údajů

Zpracovávání citlivých údajů, které odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i zpracování údajů týkajících se zdraví a sexuálního života je v současnosti v zásadě již zakázáno, s několika výjimkami za jistých podmínek a při zachování záruk²². S ohledem na vývoj technologií a společnosti je však potřeba opětovně zvážit stávající ustanovení o citlivých údajích, posoudit, zda by měly být doplněny další kategorie údajů a upřesnit podmínky pro jejich zpracovávání. To se týká například genetických údajů, které v současnosti nejsou jako kategorie citlivých údajů výslovně uváděny.

Komise zváží:

- zda by za „**citlivé údaje**“ měly být označeny další kategorie údajů, například **genetické údaje**,
- další zpřesnění a **harmonizaci podmínek** umožňujících zpracování citlivých údajů.

2.1.7. Účinnější soudní přezkum a sankce

Pro prosazování pravidel na ochranu údajů jsou zásadní **účinná ustanovení o přezkumu a sankcích**. Mnoho případů, kdy je jednotlivec dotčen porušením pravidel na ochranu údajů, má také dopad na značný počet jiných osob v podobné situaci.

Komise proto:

- zváží možnost **rozšířit pravomoc obrátit se na vnitrostátní soudy** i na orgány pro ochranu údajů, sdružení občanské společnosti a na **ostatní sdružení zastupující zájmy subjektů údajů**,
- s cílem zlepšit jejich účinnost posoudí potřebu **zpřísnit stávající ustanovení o sankcích**, například výslovným uvedením trestních sankcí v případě závažného porušení ochrany údajů.

2.2. Posílení dimenze vnitřního trhu

2.2.1. Zvýšení právní jistoty a zajištění stejných podmínek pro správce údajů

Ochrana údajů v EU má **silnou dimenzi vnitřního trhu**, tzn. potřebu zajistit volný pohyb osobních údajů mezi členskými státy v rámci vnitřního trhu. Harmonizace vnitrostátních právních předpisů o ochraně údajů podle směrnice proto není pouze minimální harmonizací, ale vede k harmonizaci, která je v zásadě úplná²³.

Směrnice zároveň přiznává členským státům v určitých oblastech rozhodovací prostor a opravňuje je ponechat nebo zavést zvláštní režimy pro konkrétní situace²⁴. Tato situace spolu s tím, že směrnice byla v některých případech členskými státy nesprávně provedena, vedla k **odchykám ve vnitrostátních právních předpisech, jimiž se směrnice začleňuje do právního řádu příslušného státu, což je v rozporu s jedním z jejích hlavních cílů, tj.**

²² Viz článek 8 směrnice 95/46/ES.

²³ Rozsudek Soudního dvora ve věci Bodil Lindqvist, C-101/01, Sb. rozh. 2003, s. I 1297, bod 96 a 97.

²⁴ Ibid., bod 97. Viz též bod odůvodnění 9 směrnice 95/46/ES.

zajištěním volného pohybu osobních údajů v rámci vnitřního trhu. Taková situace nastala v celé řadě sektorů a za různých okolností, např. při zpracovávání osobních údajů v pracovním prostředí nebo pro účely veřejného zdraví. Chybějící harmonizace je skutečně jedním z přetrvávajících hlavních problémů, který zmiňují soukromé zainteresované strany, především hospodářské subjekty, protože jim zvyšuje náklady a administrativní zátěž. Platí to především pro správce údajů usazené v několika členských státech, kteří musí dodržovat příslušné požadavky a postupy v každé z těchto zemí. Rozdíly v provádění směrnice členskými státy kromě toho vytvářejí právní nejistotu nejen pro správce údajů, ale i pro subjekty údajů, čímž by mohly ohrozit stejnou úroveň ochrany, jíž má směrnice dosáhnout a již má zajistit.

Komise posoudí prostředky pro dosažení **další harmonizace pravidel na ochranu údajů na úrovni EU.**

2.2.2. Snížení administrativní zátěže

Zajištění rovných podmínek sníží nutnost plnit různé požadavky v jednotlivých zemích, a tak správcům údajů výrazně ulehčí administrativní zátěž. Dalším konkrétním opatřením ve snižování administrativní zátěže a nákladů pro správce údajů by byl **přezkum a zjednodušení stávající oznamovací povinnosti vůči orgánu dozoru**²⁵. Správci údajů se obecně shodují, že tato obecná povinnost oznamovat veškeré zpracování osobních údajů orgánům pro ochranu údajů je komplikovaná a sama o sobě nemá pro ochranu osobních údajů osob žádný skutečný přínos. Také se jedná o případ, kdy směrnice ponechává určitý rozhodovací prostor členským státům, jež mohou svobodně rozhodovat o možných výjimkách a zjednodušení a předepisovat postupy.

Harmonizovaný a zjednodušený systém by snížil náklady i administrativní zátěž, zejména pro mezinárodní společnosti usazené v několika členských státech.

Komise prozkoumá různé možnosti, jak **zjednodušit a harmonizovat stávající oznamovací povinnost**, včetně možného vypracování **jednotného registračního formuláře pro celou EU.**

2.2.3. Objasnění pravidel pro použitelné právo a odpovědnost členských států

V první zprávě o provádění směrnice o ochraně údajů zveřejněné již v roce 2003²⁶ Komise zdůraznila, že ustanovení o použitelném právu²⁷ byla „v několika případech nedostačující, což může způsobit kolizi práva, jíž se tento článek snaží zabránit“. Situace se od té doby nezlepšila. Je-li dotčeno několik členských států, je tudíž správcům údajů a dozorcím orgánům ochrany údajů často nejasné, který členský stát je odpovědný a jaké právo je použitelné. Platí to zejména v případech, kdy má správce údajů plnit různé požadavky v různých členských státech, když je nadnárodní podnik usazen ve více než jednom členském státě nebo když správce údajů není usazen v EU, ale poskytuje služby rezidentům v EU.

V důsledku globalizace a technického rozvoje je situace čím dál složitější: subjekty údajů stále více působí v několika členských státech a jurisdikcích, kde poskytují nepřetržité služby

²⁵ Viz článek 18 směrnice 95/46/ES.

²⁶ Zpráva Komise – První zpráva o provádění směrnice o ochraně údajů (95/46/ES) (KOM(2003) 265).

²⁷ Viz článek 4 směrnice 95/46/ES.

a asistenci. Internet správcům údajů usazeným mimo Evropský hospodářský prostor²⁸ velmi usnadňuje poskytování služeb na dálku a zpracovávání osobních údajů v online prostředí, a často je proto obtížné určit místo, kde se osobní údaje a používané zařízení právě nacházejí (např. v případě aplikací a služeb využívajících cloud computing).

Komise ale zastává názor, že skutečnost, že zpracování osobních údajů provádí správce údajů usazený v třetí zemi, by neměla zbavovat jednotlivce ochrany, na niž mají právo dle Listiny základních práv EU a právních předpisů EU pro ochranu údajů.

Komise posoudí, jak **přezkoumat a zpřesnit stávající ustanovení o použitelném právu**, včetně hledisek umožňujících určit prvky uspořádaného souboru osobních údajů, aby se zlepšila právní jistota, objasnila odpovědnost členských států za uplatňování pravidel pro ochranu údajů a v neposlední řadě poskytla stejná úroveň ochrany subjektům údajů v EU bez ohledu na místo, kde se nachází správce údajů.

2.2.4. Zvýšení odpovědnosti správců údajů

Zjednodušení administrativy by **nemělo vést k celkovému snížení odpovědnosti správců údajů za zajišťování účinné ochrany údajů**. Komise se naopak domnívá, že jejich povinnosti by měly být v právním rámci jasněji vyjádřeny, i pokud jde o vnitřní kontrolní mechanismy a spolupráci s dozorcími orgány pro ochranu údajů. Dále by se mělo zajistit, aby se taková odpovědnost vztahovala též na správce údajů, kteří jsou vázáni povinnostmi zachovávat profesní tajemství (např. právníci), i na stále častější případy, kdy správci údajů svěří zpracovávání údajů jiným subjektům (např. zpracovatelům).

Komise proto prozkoumá způsoby, jak **zajistit, aby správci údajů zavedli účinné postupy a mechanismy pro zajištění souladu s pravidly pro ochranu údajů**. Přihlédne přitom k probíhající diskusi o možném zavedení zásady „*accountability*“²⁹. Cílem této snahy není zvýšit administrativní zátěž správců údajů, protože případná opatření by se více zaměřovala na vytvoření záruk a mechanismů, které zefektivňují dodržování předpisů na ochranu údajů, a zároveň na omezení a zjednodušení některých administrativních formalit, např. oznámení (viz oddíl 2.2.2).

Významnou úlohu v tomto ohledu i při zajišťování bezpečnosti údajů by mohly hrát podpora používání technologií zvyšujících ochranu soukromí (PETs), jak poukazuje Komise již ve svém sdělení na toto téma z roku 2007, i zásada „ochrany soukromí již od návrhu“³⁰.

Komise posoudí následující prvky pro zvýšení odpovědnosti správců údajů:

- povinné jmenování nezávislého **úředníka pro ochranu údajů** a harmonizaci pravidel týkajících se jeho úkolů a pravomocí³¹ a zvážení vhodného prahu k zamezení nepřiměřené administrativní zátěži, zejména malých podniků a mikropodniků,

²⁸ Do Evropského hospodářského prostoru patří i Norsko, Lichtenštejnsko a Island.

²⁹ Viz zejména stanovisko č. 3/2010 přijaté 13. července pracovní skupinou zřízenou podle článku 29.

³⁰ K PETs viz sdělení Komise Evropskému parlamentu a Radě o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs), KOM(2007) 228. Podle zásady „ochrany soukromí již od návrhu“ (*Privacy by Design*) mají být ochrana soukromí a údajů zapracovány do celého životního cyklu technologií, od fáze raného návrhu, nasazení, používání až po likvidaci. Tato zásada je mimo jiné uvedena ve sdělení Komise „Digitální agenda pro Evropu“, KOM(2010) 245.

³¹ Několik členských států již využilo existující možnosti, aby správce údajů jmenoval úředníka pro ochranu údajů, a tím nezávislým způsobem zajistil splnění evropských a vnitrostátních pravidel pro

- začlenění povinnosti, aby správci údajů prováděli v konkrétních případech **posouzení dopadů na ochranu údajů**, do právního rámce, například při zpracovávání citlivých údajů, nebo přináší-li způsob zpracování jiná zvláštní rizika, zejména při použití určitých technologií, mechanismů nebo postupů, včetně profilování nebo dohledu pomocí videokamer,
- další podporu používání technologií zvyšujících ochranu soukromí a možnost konkrétního provedení koncepce „**ochrany soukromí již od návrhu**“.

2.2.5. Podpora samoregulačních iniciativ a prozkoumání certifikačních režimů EU

Komise nadále zastává názor, že **samoregulační iniciativy** správců údajů mohou **přispět k lepšímu prosazování pravidel pro ochranu údajů**. Stávající ustanovení o samoregulaci ve směrnici o ochraně údajů, zejména možnost vypracovávat kodexy chování³², byla dosud jen málo využívána a soukromé zainteresované strany je nepovažují za uspokojivé.

Komise dále posoudí možnost vytvářet **certifikační režimy na úrovni EU (např. osvědčení o dodržení zásad ochrany soukromí (privacy seals))** pro postupy, technologie, produkty a služby splňující zásady ochrany soukromí³³. Nejenže by to přispělo k orientaci fyzické osoby jako uživatele těchto technologií, produktů a služeb, ale bylo by to důležité ve vztahu k odpovědnosti správců údajů. Volba certifikovaných technologií, produktů či služeb by mohla prokazovat, že správce splnil své povinnosti (viz oddíl 2.2.4). Samozřejmě by bylo zásadní **zabezpečit důvěryhodnost takových osvědčení o dodržení zásad ochrany soukromí** a sledovat, zda jsou v souladu s právními povinnostmi a mezinárodními technickými normami.

Komise přijme tato opatření:

- posoudí, jak **dále podporovat samoregulační iniciativy**, včetně aktivní podpory kodexů chování,
- posoudí proveditelnost vytvoření **certifikačních režimů EU** v oblasti ochrany soukromí a údajů.

2.3. Přezkum pravidel pro ochranu údajů v oblasti policejní a justiční spolupráce v trestních věcech

Směrnice o ochraně údajů se vztahuje na veškeré zpracovávání osobních údajů v členských státech ve veřejném i soukromém sektoru. Nevztahuje se ale na zpracovávání osobních údajů prováděné „pro výkon činností, které nespádají do oblasti působnosti práva Společenství“, například činností v oblasti policejní a justiční spolupráce v trestních věcech³⁴. Lisabonská smlouva však zrušila předchozí pilířovou strukturu EU a zavedla nový ucelený právní základ pro ochranu osobních údajů ve všech politikách Unie³⁵. Vzhledem k této situaci a s ohledem na Listinu základních práv EU Komise ve svých sděleních o Stockholmském programu a Stockholmském akčním plánu³⁶ zdůraznila potřebu zavést „úplný režim ochrany“ a „posílit

ochranu údajů a pomáhat občanům (viz např. *Beaufragter für den Datenschutz* v Německu a *correspondant informatique et libertés* (CIL) ve Francii).

³² Viz článek 27 směrnice 95/46/ES.

³³ K tomuto aspektu viz též sdělení o technologiích zvyšujících ochranu soukromí, pozn. č. 30.

³⁴ Viz čl. 3 odst. 2 první odrážka směrnice 95/46/ES.

³⁵ Viz článek 16 SFEU.

³⁶ Viz KOM(2009) 262, 10.6.2009 a KOM(2010) 171, 20.4.2010.

postoj EU k ochraně osobních údajů jednotlivců v kontextu ostatních politik EU, včetně vymáhání práva a prevence trestných činů“.

Nástrojem EU pro ochranu osobních údajů v oblasti policejní a justiční spolupráce v trestních věcech je **rámcové rozhodnutí 2008/977/SVV**³⁷. Toto rozhodnutí je důležitým krokem vpřed v oblasti, kde existuje velká potřeba stanovit společné standardy pro ochranu údajů. V práci je ale třeba stále pokračovat.

Rámcové rozhodnutí se vztahuje pouze na přeshraniční výměnu osobních údajů v rámci EU, a nikoli na zpracovávání údajů uvnitř členských států. Je velmi obtížné činit tento rozdíl v praxi, což může ztěžovat faktické provádění a používání rámcového rozhodnutí³⁸.

Toto rozhodnutí též obsahuje příliš širokou výjimku ze zásady omezení účelu. Jeho dalším nedostatkem je chybné ustanovení, že různé kategorie údajů by se měly rozlišovat podle stupně jejich přesnosti a spolehlivosti, že údaje založené na faktech by se měly odlišovat od údajů založených na názorech či osobním hodnocení³⁹ a že by se měly rozlišovat různé kategorie subjektů údajů (pachatel, podezřelá osoba, oběť, svědek atd.), přičemž na údaje o osobách, jež nejsou podezřelé, by se měly vztahovat zvláštní záruky⁴⁰.

Rámcové rozhodnutí dále nenahrazuje různé odvětvové legislativní nástroje pro policejní a justiční spolupráci v trestních věcech přijaté na úrovni EU⁴¹, zejména ty, jež upravují fungování Europolu, Eurojustu, Schengenského informačního systému a celního informačního systému⁴², jež buď obsahují zvláštní režimy ochrany údajů anebo obvykle odkazují na nástroje Rady Evropy pro ochranu údajů. Pokud je o činnosti v oblasti policejní a justiční spolupráce, všechny členské státy se přihlásily k doporučení Rady Evropy č. R (87) 15, které stanoví zásady použití úmluvy č. 108 v policejní oblasti. Nejde však o právně závazný nástroj.

Tato situace může přímo ovlivnit možnost osob vykonávat svá práva na ochranu údajů v této oblasti (např. být informován, jaké údaje o nich jsou zpracovávány a vyměňovány, kým a za jakým účelem a jak vykonávat svá práva, např. právo na přístup k svým údajům).

Cíl vytvořit komplexní jednotný systém v EU a vůči třetím zemím **v sobě zahrnuje potřebu zvážit přezkum stávajících pravidel pro ochranu údajů v oblasti policejní a justiční spolupráce v trestních věcech.** Komise zdůrazňuje, že koncepce úplného režimu ochrany údajů nevyklučuje přijmout v obecném rámci zvláštní pravidla pro ochranu údajů v policejní a justiční oblasti, a to s přihlédnutím ke specifické povaze těchto oblastí, jak je uvedeno

³⁷ Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech (Úř. věst. L 350, 30.12.2008, s. 60). Rámcové rozhodnutí předpokládá pouze minimální harmonizaci standardů pro ochranu údajů.

³⁸ V příslušných předpisech Rady Evropy se tento rozdíl nečiní, viz Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku údajů přes hranice (CETS č. 108), dodatkový protokol k této úmluvě o orgánech dozoru a předávání údajů přes hranice (ETS č. 181) a doporučení Výboru ministrů Rady Evropy členským státům č. R (87) 15 upravující používání osobních údajů v policejním sektoru přijaté dne 17. září 1987.

³⁹ Jak vyžaduje zásada 3.2 doporučení č. R (87) 15.

⁴⁰ V rozporu se zásadou 2 v doporučení č. R (87) 15 a jeho hodnotících zprávách.

⁴¹ Viz přehled těchto nástrojů ve sdělení Komise „Přehled o správě informací v prostoru svobody, bezpečnosti a práva“, KOM(2010) 385.

⁴² Pro dohled nad ochranou údajů byly příslušnými nástroji zřízeny společné kontrolní orgány, jejichž pravomoci doplňují obecnou pravomoc evropského inspektora ochrany údajů, tj. vykonávat dozor nad orgány, institucemi a jinými subjekty Unie na základě nařízení (ES) č. 45/2001.

v prohlášení 21 připojeném k Lisabonské smlouvě. Z toho například vyplývá, že může být zapotřebí zvážit míru, v jaké by v určitém případě výkon práv jednotlivce na ochranu údajů mohl ohrozit předcházení, vyšetřování, odhalování nebo stíhání trestných činů či výkon trestní sankce.

Komise zejména:

- zváží **rozšíření používání obecných pravidel pro ochranu údajů na oblast policejní a justiční spolupráce v trestních věcech**, a to i na zpracovávání údajů uvnitř dané země, a v případě potřeby vytvoří harmonizovaná **omezení** některých práv na ochranu údajů fyzických osob, např. práva na přístup nebo zásady transparentnosti,
- posoudí potřebu zavést do nového obecného rámce pro ochranu údajů **zvláštní harmonizovaná ustanovení**, například o ochraně **genetických údajů** při jejich zpracovávání pro účely trestního práva nebo o rozlišování různých kategorií subjektů údajů (svědci, podezřelí atd.) v oblasti policejní a justiční spolupráce v trestních věcech,
- v roce 2011 zahájí **konzultaci** se všemi zainteresovanými stranami, jak co nejlépe **revidovat stávající systémy dohledu v oblasti policejní a justiční spolupráce v trestních věcech**, aby byla zajištěn účinný a důsledný dohled nad ochranou údajů ve všech orgánech, institucích a jiných subjektech Unie,
- posoudí potřebu **sladit** v dlouhodobém horizontu **stávající různá pravidla pro jednotlivé oblasti, jež byla přijata v podobě zvláštních nástrojů na úrovni EU pro policejní a justiční spolupráci v trestních věcech**, s novým obecným právním rámcem pro ochranu údajů.

2.4. Globální rozměr ochrany údajů

2.4.1. Objasnění a zjednodušení pravidel pro mezinárodní předávání údajů

Jedním z prostředků, jak umožnit předávání osobních údajů mimo EU a EHP, je **hodnocení odpovídající úrovně ochrany** (*adequacy assessment*). V současnosti může o tom, zda třetí země poskytuje takovou úroveň ochrany, jakou EU považuje za odpovídající, rozhodnout Komise a členské státy.

Pokud třetí země v tomto hodnocení uspěje, mohou se na základě zjištění Komise osobní údaje volně pohybovat z 27 členských států EU a tří členských zemí EHP do této třetí země, aniž by bylo třeba dodatečných záruk. Přesné požadavky pro uznání odpovídající úrovně ochrany ze strany Komise nyní ale nejsou ve směrnici o ochraně údajů dostatečně podrobně vysvětleny. V rámcovém rozhodnutí kromě toho není možnost, aby Komise vydala takové rozhodnutí, uvedena.

V některých členských státech je odpovídající úroveň ochrany posuzována v prvním stupni správcem údajů, který sám předává osobní údaje do třetí země, a někdy je následně kontrolována orgánem dozoru nad ochranou údajů. Tato situace může vést k různému přístupu při posuzování dostatečnosti úrovně ochrany v třetí zemi nebo mezinárodní organizaci a **představuje riziko, že úroveň ochrany subjektů údajů poskytovaná třetí zemí bude v různých členských státech hodnocena odlišně**. Stávající právní nástroje také neobsahují podrobné harmonizované požadavky na to, jaké transfery údajů mohou být považovány za zákonné, v důsledku čehož se praxe v různých členských státech liší.

Kromě toho u předávání údajů třetím zemím, jež nezajišťují odpovídající úroveň ochrany, současné standardní smluvní doložky Komise pro předávání osobních údajů správcům⁴³ a zpracovatelům⁴⁴ údajů nejsou navrženy pro použití v mimosmluvních vztazích a nemohou být například použity pro předávání údajů mezi orgány veřejné správy.

Do mezinárodních dohod uzavřených EU nebo jejími členskými státy musí být často začleňovány zásady ochrany údajů a zvláštní ustanovení. Výsledkem mohou být různorodá znění s nekonzistentními ustanoveními a právy, u nichž hrozí riziko, že budou ke škodě subjektu údajů vykládána odlišně. V reakci na to Komise oznámila, že bude pro účely vymáhání práva pracovat na základních prvcích dohod o ochraně údajů uzavíraných mezi Evropskou unií a třetími státy⁴⁵.

Další prostředky, které se vyvinuly jako forma samoregulace, např. vnitřní kodexy chování společností – závazná podniková pravidla (*Binding Corporate Rules*)⁴⁶, mohou také být užitečným nástrojem pro zákonné předávání osobních údajů mezi společnostmi v rámci jedné skupiny. Zainteresované strany nicméně navrhy, že tento mechanismus by mohl být ještě zlepšen a jeho používání usnadněno.

Aby byly zde vymezené otázky vyřešeny, je **obecně potřeba zlepšit stávající mechanismy mezinárodního předávání osobních údajů** a zároveň zajistit odpovídající ochranu těchto údajů, jsou-li předávány mimo EU a EHP a tam zpracovávány.

Komise posoudí, jak

- **zlepšit a zjednodušit stávající postupy** pro mezinárodní předávání údajů, včetně právně závazných nástrojů a závazných podnikových pravidel, s cílem zajistit **jednotnější a soudržnější přístup EU** k třetím zemím a mezinárodním organizacím,
- **vyjasnit postup Komise pro hodnocení odpovídající úrovně ochrany** a lépe vymezit **kritéria a požadavky** pro posouzení úrovně ochrany údajů v třetí zemi či mezinárodní organizaci,
- **definovat hlavní prvky ochrany údajů v EU**, jež by mohly být použity pro všechny druhy mezinárodních dohod.

⁴³ Rozhodnutí Komise 2001/497/ES ze dne 15. června 2001 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle směrnice 95/46/ES (Úř. věst. L 181, 4.7.2001, s. 19), rozhodnutí Komise 2002/16/ES ze dne 27. prosince 2001 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice 95/46/ES (Úř. věst. L 6, 10.1.2002, s. 52), rozhodnutí Komise 2004/915/ES ze dne 27. prosince 2004, kterým se mění rozhodnutí 2001/497/ES, pokud jde o zavedení alternativního souboru standardních smluvních doložek pro předávání osobních údajů do třetích zemí (Úř. věst. L 385, 29.12.2004, s. 74).

⁴⁴ Rozhodnutí Komise ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES (Úř. věst. L 39, 12.2.2010, s. 5).

⁴⁵ Stockholmský akční plán (viz pozn. č. 36).

⁴⁶ Závazná podniková pravidla jsou předepsané postupy založené na evropských standardech pro ochranu údajů, které dobrovolně vypracovávají a dodržují nadnárodní organizace, aby zajistily odpovídající záruky pro předávání osobních údajů nebo pro kategorie předávání těchto údajů mezi společnostmi, jež patří do stejné skupiny a jež jsou těmito pravidly vázány. Viz http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

2.4.2. Podpora všeobecných zásad

Zpracovávání údajů se odehrává v globalizovaném světě, a proto vyžaduje vypracování všeobecných zásad pro ochranu osob při zpracovávání osobních údajů.

Právní rámec EU pro ochranu údajů často slouží **třetím zemím jako měřítko pro jejich vlastní regulaci ochrany údajů**. Jeho účinek a dopad uvnitř Unie i mimo ni má proto obrovskou důležitost. **Evropská unie musí proto zůstat hnací silou vývoje a prosazování mezinárodních právních a technických standardů pro ochranu osobních údajů**, a to na základě příslušných nástrojů EU pro ochranu údajů a jiných evropských nástrojů. To je zvlášť důležité v rámci politiky rozšiřování EU.

Pokud jde o mezinárodní technické normy vypracované normalizačními organizacemi, Komise se domnívá, že vzájemný soulad budoucího právního rámce a těchto norem je velmi významná pro zajištění konzistentního používání pravidel na ochranu údajů ze strany správců údajů v praxi.

Komise přijme tato opatření:

- bude nadále podporovat **vypracování přísných právních a technických norem pro ochranu údajů** v třetích zemích a na mezinárodní úrovni,
- bude usilovat o dodržování **zásady reciprocity ochrany** v mezinárodní činnosti Unie, zejména pokud jde o subjekty údajů, jejichž údaje jsou vyvázeny z EU do třetích zemí,
- **za tímto účelem zvýší spolupráci s třetími zeměmi a mezinárodními organizacemi**, například s OECD, Radou Evropy, OSN, a regionálními organizacemi,
- bude **bedlivě sledovat mezinárodní technické normy, které vypracovávají normalizační organizace** jako CEN a ISO s cílem zajistit, aby užitečným způsobem doplňovaly právní předpisy, a zabezpečit účinné využívání hlavních požadavků na ochranu údajů v praxi.

2.5. Silnější institucionální rámec umožňující lepší prosazování pravidel pro ochranu údajů

Provádění a prosazování zásad a pravidel ochrany údajů je klíčovým prvkem při dodržování práv fyzických osob.

V této souvislosti hrají **zásadní úlohu** v prosazování pravidel pro ochranu údajů **orgány pro ochranu údajů**. Tyto orgány jsou nezávislými strážci základních práv a svobod v oblasti ochrany osobních údajů, jimž fyzické osoby důvěřují, že zabezpečí ochranu a zpracování jejich osobních údajů v souladu s právem. Z tohoto důvodu se Komise domnívá, že jejich role by měla být posílena, zejména s ohledem na nedávnou judikaturu ESD o jejich nezávislosti⁴⁷, a že by jim měly být uděleny nezbytné pravomoci a zdroje, aby mohly řádně plnit své úkoly na vnitrostátní úrovni i při spolupráci mezi sebou.

Komise zároveň zastává názor, že **orgány pro ochranu údajů by měly více spolupracovat a lépe koordinovat své činnosti**, zejména při řešení úkolů, jež jsou svojí povahou přeshraniční. Jedná se zejména o případy, kdy mají nadnárodní podniky sídlo v několika členských státech

⁴⁷ Rozsudek ESD ze dne 9. března 2010, Komise v. Německo, věc C-518/07.

a jsou činné v každé z těchto zemí, nebo o případy, kdy je nutný dozor v koordinaci s evropským inspektorem ochrany údajů⁴⁸.

Za těchto okolností může **důležitou roli hrát pracovní skupina zřízená podle článku 29⁴⁹**, jejímž úkolem je kromě poradní funkce⁵⁰ napomáhat jednotnému uplatňování unijních pravidel pro ochranu údajů v jednotlivých státech. Skutečnost, že orgány pro ochranu údajů nadále odlišně používají a vykládají pravidla EU, ačkoli se celá EU potýká stejnými výzvami, však vyžaduje posílení úlohy této pracovní skupiny při koordinaci stanovisek uvedených orgánů, tak aby bylo zajištěno jednotnější uplatňování pravidel v jednotlivých státech, a tedy rovnocenná úroveň ochrany údajů.

Komise posoudí:

- jak v novém právním rámci **posílit, vyjasnit a harmonizovat postavení a pravomoci vnitrostátních orgánů pro ochranu údajů**, včetně provedení koncepce „úplné nezávislosti“⁵¹ v plném rozsahu,
- způsoby **zlepšení spolupráce a koordinace mezi orgány pro ochranu údajů**,
- jak zajistit jednotnější uplatňování pravidel EU pro ochranu údajů na celém vnitřním trhu. **Může se tak stát prostřednictvím zesílení úlohy vnitrostátních orgánů ochrany údajů, zlepšením jejich koordinace v pracovní skupině zřízené podle článku 29 (která by se měla stát transparentnější) anebo vytvořením mechanismu, který pod záštitou Evropské komise zajistí jednotnost na vnitřním trhu.**

3. ZÁVĚR: DALŠÍ POSTUP

Používání a sdílení našich osobních údajů ve společnosti se podobně jako technologie neustále mění. Zákodárci tak mají za úkol vypracovat právní rámec, který obstojí ve zkoušce času. Po dokončení reformy by evropská pravidla pro ochranu údajů měla nadále zaručovat vysokou úroveň ochrany a poskytovat na vnitřním trhu jednotlivcům, veřejné správě a podnikům právní jistotu po několik generací. Bez ohledu na složité okolnosti či důmyslnost technologií musí být jasná platná pravidla a normy, které musí vnitrostátní orgány prosazovat a jež musí podniky vyvíjející technologie a ostatní podniky dodržovat. Fyzické osoby by si také měly být jasně vědomy svých práv.

Komplexní přístup Komise, jenž má řešit problematické otázky a dosáhnout hlavních cílů uvedených v tomto sdělení, bude základem pro další diskuse s ostatními orgány EU a zainteresovanými stranami a v budoucnu se promítne do konkrétních návrhů a opatření legislativní i nelegislativní povahy. Komise proto uvítá reakci na problematiku předloženou v tomto sdělení.

⁴⁸ V současnosti se jedná o rozsáhlé informační systémy, např. SIS II (viz článek 46 nařízení (ES) č. 1987/2006, Úř. věst. L 318, 28.12.2006, s. 4) a VIS (viz článek 43 nařízení (ES) č. 767/2008, Úř. věst. L 218, 13.8.2008, s. 60).

⁴⁹ Pracovní skupina zřízená podle článku 29 je poradním orgánem složeným z jednoho zástupce orgánu pro ochranu údajů z každého členského státu, ze zástupce evropského inspektora ochrany údajů a Komise (bez hlasovacího práva), která zároveň poskytuje sekretariát. Viz http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

⁵⁰ Úkolem pracovní skupiny zřízené podle článku 29 je radit Komisi ohledně úrovně ochrany v EU a třetích zemích a o jakýchkoli dalších opatřeních týkajících se zpracování osobních údajů.

⁵¹ Viz rozsudek ESD ze dne 9. března 2010, Komise v. Německo, věc C-518/07.

Po posouzení dopadů a na základě Listiny základních práv EU **předloží Komise v roce 2011 legislativní návrhy** na revizi právního rámce pro ochranu údajů s cílem posílit postoj EU k ochraně osobních údajů jednotlivců v kontextu ostatních politik EU, včetně vymáhání práva a prevence trestných činů, jejichž specifika je nutno zohlednit. Souběžně budou probíhat nelegislativní opatření jako podpora samoregulace a zkoumání možnosti používat osvědčení o dodržení zásad ochrany soukromí (*privacy seals*).

V druhé fázi Komise **vyhodnotí potřebu přizpůsobit ostatní právní nástroje** novému obecnému rámci pro ochranu údajů. To se týká v první řadě nařízení (ES) č. 45/2001, jež bude muset být tomuto novému právnímu rámci přizpůsobeno. Později bude třeba též pečlivě posoudit jeho dopad na ostatní odvětvové nástroje.

Komise bude nadále bedlivě dohlížet na správné provádění práva Unie v této oblasti, bude tedy **aktivně vystupovat v případě nesprávného provedení nebo používání pravidel EU** pro ochranu údajů. Současný přezkum nástrojů pro ochranu údajů se nijak nedotýká povinnosti členských států provádět stávající právní nástroje pro ochranu osobních údajů a zabezpečit jejich řádné používání⁵².

Vysoká a jednotná úroveň ochrany údajů v rámci EU bude nejlepším způsobem, jak podpořit a prosadit evropské normy pro ochranu údajů globálně.

⁵² To se týká i rámcového rozhodnutí 2008/977/SVV: členské státy musí přijmout opatření nezbytná pro dosažení souladu s tímto rámcovým rozhodnutím do 27. listopadu 2010.