

SK

SK

SK



EURÓPSKA KOMISIA

Brusel, 4.11.2010
KOM(2010) 609 v konečnom znení

**OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE,
HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV**

Komplexný prístup k ochrane osobných údajov v Európskej únii

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV

Komplexný prístup k ochrane osobných údajov v Európskej únii

1. NOVÉ VÝZVY V OBLASTI OCHRANY OSOBNÝCH ÚDAJOV

Smernica o ochrane údajov z roku 1995¹ sa stala medzníkom v histórii ochrany osobných údajov v Európskej únii. V smernici sú zakotvené dve najstaršie a rovnako dôležité ambície európskeho integračného procesu: na jednej strane ochrana základných práv a slobôd jednotlivcov a najmä základného práva na ochranu údajov a na druhej strane dokončenie vnútorného trhu – v tomto prípade v oblasti voľného pohybu osobných údajov.

Aj po pätnástich rokoch je tento dvojnásobný cieľ stále aktuálny a zásady ukotvené v smernici si zachovávajú svoje ráco. **Avšak svet sa okolo nás vďaka rýchlemu technickému rozvoju a globalizácii úplne zmenil a v oblasti ochrany osobných údajov sa objavili nové výzvy.**

Jednotlivcom dnes technika umožňuje zdieľať informácie o svojom správaní a preferenciách a v doteraz nevídanom rozsahu umožňuje ich zverejňovanie a globálnu dostupnosť. Webové stránky zamerané na sociálne siete, ktorých stovky miliónov členov sú roztrúsené po celej zemeguli, patria k tým najzjavnejším, ale nie jediným príkladom tohto javu. „Internetový oblak počítačov“ (tzv. cloud computing) – t. j. používanie funkcií počítača v internetovom prostredí, keď softvér, zdieľané zdroje a informácie sa nachádzajú na vzdialených serveroch („v oblakoch“) – môže tiež predstavovať výzvu pre ochranu údajov, keďže v sebe môže zahŕňať stratu kontroly jednotlivcov nad ich potenciálne citlivými informáciami, keď si svoje údaje ukládajú pomocou programov, ktoré sú umiestnené na hardvéri niekoho iného. Nedávna štúdia potvrdila, že orgány na ochranu údajov, podnikateľské združenia a organizácie zastupujúce spotrebiteľov sa zhodujú v tom, že online činnosti² so sebou prinášajú zvýšené riziká z hľadiska ochrany súkromia a osobných údajov.

Zároveň sú spôsoby zberu osobných údajov čoraz komplikovanejšie a čoraz ťažšie ich možno odhaliť. Používanie sofistikovaných nástrojov napríklad ekonomickým subjektom umožňuje sledovať správanie jednotlivcov a lepšie sa tak zameriavať na potenciálnych zákazníkov. Navyše rastúce využívanie postupov umožňujúcich automatický zber údajov, ako napríklad elektronické vydávanie cestovných lístkov, výber cestného mýta alebo zariadenia na zistenie zemepisnej polohy uľahčujú zistiť polohu jednotlivcov jednoducho preto, že používajú mobilné zariadenia. Aj verejné orgány využívajú osobné údaje čoraz častejšie na rôzne účely, ako napríklad na vystopovanie jednotlivcov v prípade vypuknutia nákazlivej choroby, na účinnejšie predchádzanie terorizmu a trestnej činnosti a boj proti nim, na správu systémov sociálneho zabezpečenia alebo na účely výberu daní, a to v rámci svojho systému elektronickej štátnej správy (e-vlády) atď.

¹ Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 23.11.1995, s. 31).

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

Všetky uvedené príklady nabádajú k otázke, či existujúce právne predpisy EÚ v oblasti ochrany údajov ešte stále dokážu v plnej miere a účinne na tieto výzvy reagovať.

Komisia s cieľom riešiť túto otázku otvorila proces posúdenia súčasného právneho rámca, najprv prostredníctvom konferencie na vysokej úrovni, ktorá sa uskutočnila v máji 2009, a potom prostredníctvom verejnej konzultácie, ktorá prebiehala do konca roka 2009³. V tejto súvislosti sa tiež začalo s realizáciou viacerých štúdií⁴.

Z uvedeného posúdenia vyplýva, že hlavné zásady smernice sú stále platné a ich technicky neutrálny charakter by sa mal zachovať. Zistilo sa však, že viacero otázok je problematických a predstavujú konkrétne výzvy. Ide o:

- *Riešenie vplyvu nových technológií*

Reakcie súkromných osôb, ako aj organizácií na konzultácie potvrdili, že existuje potreba vyjasniť a spresniť uplatňovanie zásad ochrany údajov pri nových technológiách, aby sa zabezpečila skutočne efektívna ochrana osobných údajov jednotlivcov bez ohľadu na technológie, ktoré sa pri spracovaní týchto údajov využívajú a že prevádzkovatelia údajov sú si plne vedomí dôsledkov, ktoré má používanie nových technológií na ochranu údajov. Čiastočne sa týmito otázkam venuje smernica 2002/58/ES⁵ (tzv. smernica o ochrane osobných údajov v elektronickom sektore), ktorá v sektore elektronických komunikácií rozvádza do podrobností a dopĺňa všeobecnú smernicu o ochrane údajov⁶.

- *Rozšírenie ochrany údajov o rozmer vnútorného trhu*

Napriek existencii spoločného právneho rámca EÚ v oblasti ochrany údajov je jednou z hlavných pretrvávajúcich obáv zainteresovaných strán, najmä nadnárodných spoločností, nedostatočná harmonizácia právnych predpisov členských štátov. Zdôrazňuje sa potreba

³ Pozri odpovede na verejné konzultácie Komisie: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. Cielenejšie konzultácie so zainteresovanými stranami sa uskutočňovali počas celého roka 2010. Podpredsedníčka EK Viviane Redingová tiež predsedala stretnutiu zainteresovaných strán na vysokej úrovni, ktoré sa uskutočnilo 5. októbra 2010 v Bruseli. Komisia tiež uskutočnila konzultácie s pracovnou skupinou zriadenou podľa článku 29, ktorej prínos do procesu konzultácií v roku 2009 mal komplexný charakter (pracovný dokument č. 168), a v júli 2010 prijala osobitné stanovisko ku koncepcii zodpovednosti (pracovný dokument č. 173).

⁴ Popri štúdií s názvom *Study on the economic benefits of privacy enhancing technologies* (c. d. v poznámke pod čiarou 2), pozri tiež *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, január 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). V súčasnosti sa realizuje aj štúdia o hodnotení vplyvov budúceho právneho rámca EÚ v oblasti ochrany osobných údajov.

⁵ Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

⁶ Smernica o ochrane údajov 95/46/ES stanovuje normy ochrany údajov pre všetky právne akty EÚ vrátane smernice o ochrane osobných údajov v elektronickom sektore 2002/58/ES (zmenenej a doplnenej smernicou 2009/136/ES – Ú. v. EÚ L 337, 18.12.2009, s. 11). Smernica o ochrane osobných údajov v elektronickom sektore sa vzťahuje na spracovávanie osobných údajov v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach. Zásady stanovené v smernici o ochrane údajov pretavila do konkrétnych pravidiel v sektore elektronických komunikácií. Smernica 95/46/ES sa uplatňuje *inter alia* na neverejné komunikačné služby.

zvýšiť právnu istotu, znížiť administratívnu záťaž a zaistiť rovnaké podmienky pre ekonomické subjekty a ostatných prevádzkovateľov údajov.

- *Riešenie otázok globalizácie a skvalitňovanie medzinárodného prenosu údajov*

Viacere zainteresované strany zdôraznili, že zvýšené využívanie externých zdrojov pri spracovávaní údajov, veľmi často mimo EÚ, spôsobuje nejasnosti ohľadom právnych predpisov uplatniteľných na spracovanie údajov, ako aj ohľadom určenia príslušnej zodpovednosti. Pokiaľ ide o medzinárodný prenos údajov, mnohé organizácie sa domnievajú, že súčasné režimy nie sú dostačujúce a že je potrebné ich preskúmať a zdokonaľiť, aby sa prenos údajov zjednodušil a administratívne odbremenil.

- *Zabezpečenie silnejšieho inštitucionálneho rámca pre efektívne presadzovanie predpisov o ochrane údajov*

Zainteresované strany sa zhodujú v tom, že je potrebné posilniť úlohu orgánov na ochranu údajov, aby sa zaistilo lepšie presadzovanie predpisov o ochrane údajov. Niektoré organizácie tiež požadovali zvýšenie transparentnosti práce pracovnej skupiny zriadenej podľa článku 29 (pozri bod 2.5. *d'alej v texte*) a ozrejenie jej úloh a právomocí.

- *Zvýšenie koherentnosti právneho rámca pre ochranu údajov*

V rámci verejnej konzultácie všetky zainteresované strany zdôraznili potrebu syntetizujúceho nástroja, ktorý by sa uplatňoval pri operáciách spracovania údajov vo všetkých sektoroch a politikách EÚ a ktorý by zabezpečil integrovaný prístup, ako aj bezproblémovú, konzistentnú a efektívnu ochranu⁷.

Uvedené výzvy si **vyžadujú, aby EÚ vypracovala komplexný a koherentný prístup**, ktorý by zabezpečoval **úplné dodržiavanie základného práva jednotlivcov na ochranu údajov, a to tak v rámci EÚ, ako aj mimo nej**. Na dosiahnutie tohto cieľa Lisabonská zmluva Európsku úniu vybavila dodatočnými prostriedkami: Chartou základných práv EÚ s jej článkom 8 uznávajúcim autonómne právo na ochranu osobných údajov, ktorá sa stala právne záväznou, a zaviedol sa nový právny základ⁸, na základe ktorého možno vytvoriť komplexné a koherentné právne predpisy Únie v oblasti ochrany jednotlivcov so zreteľom na spracovanie ich osobných údajov, ako aj v oblasti voľného pohybu takýchto údajov. Nový právny základ konkrétne umožňuje, aby EÚ disponovala jediným právnym nástrojom upravujúcim ochranu údajov, a to okrem iného aj v oblasti policajnej a justičnej spolupráce v trestných veciach. Článok 16 ZFEÚ iba čiastočne pokrýva oblasť spoločnej zahraničnej a bezpečnostnej politiky, keďže osobitné pravidlá pre spracovávanie údajov členskými štátmi sa musia ustanoviť rozhodnutím Rady, ktoré sa opiera o rozdielny právny základ⁹.

Vychádzajúc z týchto nových právnych možností bude Komisia najvyššiu prioritu prisudzovať zaisteniu dodržiavania základného práva na ochranu údajov v celej Únii a vo všetkých jej politikách, pričom zároveň bude rozširovať rozmer vnútorného trhu a uľahčovať voľný pohyb osobných údajov. V tejto súvislosti sa budú musieť v plnej miere zohľadniť

⁷ Vo svojich individuálnych príspevkoch predložených po skončení verejnej konzultácie Eurojust a Eurojust požiadali o zohľadnenie osobitného charakteru ich činnosti, pokiaľ ide o koordináciu presadzovania práva a predchádzania trestnej činnosti.

⁸ Pozri článok 16 Zmluvy o fungovaní Európskej únie (ZFEÚ).

⁹ Pozri posledný odsek článku 16 ods. 2 ZFEÚ a článok 39 Zmluvy o Európskej únii (ZEÚ).

ostatné príslušné základné práva ukotvené v charte a ostatné ciele uvedené v zmluvách, pričom sa súčasne zabezpečí základné právo na ochranu osobných údajov.

Cieľom predkladaného oznámenia je ustanoviť postup Komisie pri modernizácii právneho systému EÚ v oblasti ochrany osobných údajov vo všetkých oblastiach činnosti Únie a zohľadniť pri tom najmä výzvy, ktoré sú dôsledkom globalizácie a nových technológií, aby bola vo všetkých oblastiach činnosti Únie aj naďalej zaručená vysoká úroveň ochrany jednotlivcov so zreteľom na spracovávanie osobných údajov. EÚ sa tým umožní, aby zostala hybnou silou pri podporovaní vysokých štandardov ochrany údajov na celom svete.

2. KĽÚČOVÉ CIELE KOMPLEXNÉHO PRÍSTUPU K OCHRANE ÚDAJOV

2.1. Posilnenie práv jednotlivcov

2.1.1. Zabezpečenie primeranej ochrany jednotlivcov za každých okolností

Cieľom pravidiel v súčasných nástrojoch EÚ v oblasti ochrany údajov je v súlade s Chartou základných práv EÚ¹⁰ **chrániť základné práva fyzických osôb a najmä ich právo na ochranu osobných údajov.**

Pojem „osobné údaje“ jej jedným z kľúčových pojmov pri ochrane jednotlivcov súčasnými nástrojmi EÚ v oblasti ochrany údajov a uvádza do pohybu uplatňovanie záväzkov pripadajúcich prevádzkovateľom údajov a spracovateľom údajov¹¹. Cieľom vymedzenia pojmu „osobné údaje“ je obsiahnuť všetky informácie týkajúce sa priamo alebo nepriamo identifikovanej alebo identifikovateľnej osoby. S cieľom určiť, či je osoba identifikovateľná, by sa mali brať do úvahy všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije prevádzkovateľ, alebo ľubovoľná iná osoba na identifikáciu príslušnej osoby¹². Výhodou tohto premysleného prístupu, ktorý si zákonodarca zvolil, je flexibilita, ktorá mu umožňuje, že sa môže uplatňovať v rôznych situáciách majúcich vplyv na základné práva vrátane tých, ktoré nebolo možné v čase prijatia smernice predvídať. Avšak dôsledkom takéhoto širokého a pružného prístupu je skutočnosť, že v mnohých prípadoch nie pri vykonávaní smernice vždy zrejmé, ktorý prístup je potrebné zvoliť, či jednotlivci požívajú práva na ochranu údajov a či by mal prevádzkovateľ údajov dodržiavať záväzky uložené v uvedenej smernici¹³.

V niektorých situáciách dochádza k spracovávaniu osobitných informácií, ktoré by si vyžadovali dodatočné opatrenia v rámci právnych predpisov Únie. V niektorých prípadoch už takéto opatrenia existujú. Napríklad, ukladanie informácií v koncových zariadeniach (napr. mobilných telefónoch) je dovoľené iba pod podmienkou, že dotknutý jednotlivec dal k tomu svoj súhlas. Možno bude preto potrebné, aby sa riešenia na úrovni EÚ hľadali napríklad

¹⁰ Pozri Európsky súdny dvor, vec C-101/01, „Bodil Lindqvist“, ECR [2003], I-1297, 96, 97, a vec C-275/06, Productores de Música de España (Promusicae) vs. Telefónica de España SAU, ECR [2008] I-271. Pozri tiež judikatúru Európskeho súdu pre ľudské práva, napr. vo veciach: S. a Marper vs. Spojené kráľovstvo, 4.12. 2008 (podania č. 30562/04 a 30566/04) a Rotaru vs. Romania, 4.5. 2000; č. 28341/95, § 55, EŠLP 2000-V.

¹¹ Pozri vymedzenie pojmov „prevádzkovateľ údajov“ „spracovateľ údajov“ v článku 2 písm. d) a e) smernice 95/46/ES.

¹² Pozri odôvodnenie 26 smernice 95/46/ES

¹³ Pozri napríklad vec týkajúcu sa IP adries, ktorá bola preskúmaná v stanovisku pracovnej skupiny zriadenej podľa článku 29 č. 4/2007 k pojmu osobných údajov (pracovný dokument č. 136).

pokiaľ ide o kľúčom kódované údaje, lokalizačné údaje, technológie „hĺbkovej analýzy údajov“ umožňujúce kombináciu údajov z rôznych zdrojov, alebo prípady, v ktorých sa musí zaistiť dôvernosť a integrita systémov informačných technológií¹⁴.

Všetky uvedené otázky si preto vyžadujú dôkladné preskúmanie.

Komisia zväží, **ako zaistiť koherentné uplatňovanie pravidiel ochrany údajov, pričom zohľadní vplyv nových technológií na práva a slobody jednotlivcov, ako aj cieľ zaistiť voľný pohyb osobných údajov v rámci vnútorného trhu.**

2.1.2. Zvýšenie transparentnosti pre dotknuté osoby

Transparentnosť je základnou podmienkou toho, aby jednotlivci mohli svoje vlastné údaje kontrolovať a zabezpečuje efektívnu ochranu osobných údajov. Preto je dôležité, aby jednotlivci boli prevádzkovateľmi údajov **transparentným spôsobom, správne a jasne informovaní** o tom, kto a ako ich údaje zbiera a spracúva, na základe čoho, na ako dlho a aké sú ich práva, ak žiadajú o prístup k svojim údajom, o ich opravu alebo vymazanie. Príslušné ustanovenia o informáciách, ktoré sa poskytujú dotknutej osobe¹⁵ nie sú dostačujúce.

K základným prvkom transparentnosti patria požiadavky, aby boli **predmetné informácie ľahko dostupné a zrozumiteľné a aby sa používal jasný a zrozumiteľný jazyk**. Osobitný význam to má v online prostredí, v ktorom sú oznámenia o ochrane osobných údajov často nejasné, ťažko dostupné, netransparentné¹⁶ a nie vždy v súlade s existujúcimi pravidlami. Takéto nedostatky možno pozorovať napríklad pri online behaviorálnej reklame v prípade ktorej má jednotlivec, v dôsledku znásobovania aktérov zapojených do poskytovania behaviorálnej reklamy ako aj v dôsledku technologickej zložitosti tohto reklamného postupu, ťažkosti rozoznať a pochopiť, či sa osobné údaje zbierajú, kým a za akým účelom.

V tejto súvislosti si osobitnú ochranu zasluhujú **deti**, keďže si môžu byť v menšej miere vedomé rizík, dôsledkov, záruk a práv súvisiacich so spracovávaním osobných údajov¹⁷.

Komisia zväží:

- zavedenie **všeobecnej zásady transparentného spracovávania** osobných údajov do právneho rámca,
- zavedenie **konkrétnych záväzkov** pre prevádzkovateľov údajov, pokiaľ ide o druh poskytovaných informácií a spôsob ich poskytovania, a to aj vo vzťahu k **deťom**,
- vypracovanie jedného alebo viacerých **štandardných formulárov EÚ** („oznámenia o ochrane osobných údajov“), ktoré budú prevádzkovatelia údajov používať.

¹⁴ Pozri napríklad rozsudok nemeckého Spolkového ústavného súdu (Bundesverfassungsgericht) z 27. februára 2008, 1 BvR 370/07.

¹⁵ Pozri článok 10 a článok 11 smernice 95/46/ES.

¹⁶ Prieskum Eurobarometra uskutočnený v roku 2009 ukázal, že asi polovica opýtaných považovala oznámenia o ochrane osobných údajov na webových stránkach za „veľmi“ alebo „úplne nejasné“ (pozri Flash Eurobarometer č. 282: http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

¹⁷ Pozri kvalitatívnu štúdiu Bezpečnejší internet pre deti týkajúcu sa 9-10-ročných a 12-14-ročných detí, ktorá ukázala, že u detí je tendencia podceňovať riziká súvisiace s používaním internetu a minimalizovať dôsledky svojho rizikového správania (dostupné na: http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

Taktiež je dôležité, aby boli jednotlivci informovaní, keď dôjde k náhodnému alebo nezákonnému zničeniu, strate alebo pozmeneniu ich údajov alebo k ich náhodnému alebo nezákonnému sprístupneniu alebo odhaleniu neoprávneným osobám. Nedávna revízia smernice o ochrane osobných údajov v elektronickom sektore zaviedla **povinné oznamovanie porušenia ochrany osobných údajov**, ktorá sa však týka iba sektora telekomunikácií. Vzhľadom na to, že riziko porušenia ochrany osobných údajov existuje aj v iných sektoroch (napr. finančnom), Komisia preskúma spôsoby rozšírenia povinnosti oznamovať porušenia ochrany osobných údajov na iné sektory v súlade s vyhlásením Komisie o oznamovaní prípadov nepovoleného prístupu k údajom, ktoré urobila v Európskom parlamente v roku 2009 v súvislosti s reformou regulačného rámca pre elektronické komunikácie¹⁸. Uvedené preskúmanie nebude mať vplyv na ustanovenia smernice o ochrane osobných údajov v elektronickom sektore, ktoré sa do vnútroštátnych právnych predpisov musia transponovať do 25. mája 2011¹⁹. Bude potrebné zabezpečiť konzistentný a koherentný prístup v tejto otázke.

Komisia:

- preskúma spôsoby zavedenia **všeobecného oznámenia o porušení ochrany osobných údajov** do všeobecného právneho rámca, vrátane adresátov takýchto oznámení a kritérií na základe ktorých bude toto oznamovanie povinné.

2.1.3. Zvýšenie kontroly nad vlastnými údajmi

Medzi dva dôležité predpoklady vysokej úrovne ochrany údajov jednotlivcov patrí **obmedzenie spracovania údajov prevádzkovateľom údajov len na presne stanovené účely (zásada minimalizácie údajov)** a zachovanie **efektívnej kontroly vlastných údajov** dotknutými osobami. V článku 8 ods. 2 charty sa uvádza, že „každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu“. Jednotlivci by mali mať vždy možnosť prístupu k svojim údajom, možnosť tieto údaje opraviť, zmazať alebo blokovat', pokiaľ na základe zákona neexistujú oprávnené dôvody, ktoré by to zamedzovali. V súčasnom právnom rámci tieto práva už existujú. Avšak spôsobom, akým možno tieto práva uplatňovať, nie je jednotný, a preto je skutočné uplatňovanie týchto práv v niektorých členských štátoch jednoduchšie ako v ostatných. Tento aspekt je mimoriadne problematický v online prostredí, kde často dochádza k uchovávaniu údajov bez toho, aby o tom bola dotknutá osoba informovaná a/alebo k tomu dala svoj súhlas.

Názorným príkladom sú v tejto súvislosti online sociálne siete, pri ktorých je efektívna kontrola vlastných údajov dotknutými osobami mimoriadne náročná. Na Komisiu sa obrátilo viacero jednotlivcov, ktorým sa nepodarilo získať od poskytovateľov online služieb svoje

¹⁸ „Komisia berie do úvahy želanie Európskeho parlamentu, že povinnosť oznamovať narušenia osobných údajov by sa nemala týkať len sektora elektronických komunikácií, ale mala by sa vzťahovať aj na subjekty, ako sú napríklad poskytovatelia služieb informačnej spoločnosti. [...]. Komisia preto bezodkladne začne s príslušnými prípravnými prácami vrátane konzultácie so zainteresovanými stranami s cieľom predstaviť vhodným spôsobom návrhy v tejto oblasti do konca roku 2011 [...]“, pozri <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//SK>. Pozri tiež odôvodnenie 59 smernice 2009/136/ES, ktorou sa mení a dopĺňa smernica 2002/58/ES o ochrane osobných údajov v elektronickom sektore: „Tento záujem občanov o informácie sa zjavne neobmedzuje na sektor elektronických komunikácií, a preto by malo byť prioritou zaviesť na úrovni Spoločenstva jednoznačné požiadavky na povinné oznamovanie, uplatniteľné na všetky odvetvia.“

¹⁹ Článok 4 smernice 2009/136/ES.

osobné údaje, ako napríklad svoje fotografie, a ktorým tak bolo zabránené uplatniť svoje právo na prístup k týmto údajom, ich opravu a vymazanie.

Tieto práva by mali byť teda explicitnejšie a jasnejšie formulované a mali by sa prípadne posilniť.

Komisia preto preskúma spôsoby, ako:

- posilniť **zásadu minimalizácie údajov**,
- **zlepšiť spôsoby skutočného uplatňovania práv na prístup k údajom, ich opravu, výmaz alebo blokovanie** (napr. zavedením lehôt na odpovedanie na žiadosti jednotlivcov, umožnením uplatňovania práv elektronickými prostriedkami alebo stanovením, že právo na prístup k údajom by sa malo zo zásady zaistiť bezplatne),
- ozrejmiť tzv. „**právo byť zabudnutý**“, t. j. právo jednotlivcov na ukončenie spracovávania ich údajov a na ich vymazanie, ak sa tieto údaje už viac nepoužívajú na zákonné účely. Ide napríklad o situácie, keď sa spracovanie opiera o súhlas dotknutej osoby a keď táto osoba svoj súhlas stiahne alebo keď už uplynulo obdobie na uchovávanie údajov,
- doplniť práva dotknutých osôb zabezpečením „**prenosnosti údajov**“, t. j. zabezpečiť jednotlivcovi výslovné právo stiahnuť svoje vlastné údaje (napr. svoje fotografie alebo zoznam priateľov) z aplikácie alebo služby tak, aby sa stiahnuté údaje mohli preniesť do inej aplikácie alebo služby, pokiaľ je to technicky možné, a to bez toho, aby tomu prevádzkovateľ údajov bránil.

2.1.4. Zvyšovanie informovanosti

Hoci transparentnosť má kľúčový význam, rovnako potrebné je zvyšovať informovanosť verejnosti, a najmä mladých ľudí, o rizikách súvisiacich so spracovaním osobných údajov a ich právach. Prieskum Eurobarometra z roku 2008 ukázal, že veľká väčšina obyvateľov členských štátov EÚ považuje informovanosť o ochrane osobných údajov v ich krajine za nízku²⁰. Činnosti na zvyšovanie informovanosti by preto mali stimulovať a podporovať najrôznejší aktéri, t. j. orgány členských štátov, najmä orgány na ochranu údajov a vzdelávacie inštitúcie, ako aj prevádzkovatelia údajov a občianske združenia. Tieto činnosti by mali okrem iného prebiehať formou nelegislatívnych opatrení, ako sú informačné kampane v tlačенých a elektronických médiách, ako aj formou poskytovania jasných informácií na webových stránkach, ktoré by jasne formulovali práva dotknutých osôb a zodpovednosť prevádzkovateľov údajov.

Komisia preskúma:

- možnosť **spolufinancovania činností na zvyšovanie informovanosti o ochrane údajov** z rozpočtu Únie,
- potrebu a následnú možnosť zahrnúť do právneho rámca **povinnosť týkajúcu sa zvyšovania informovanosti** v tejto oblasti.

²⁰ Pozri Flash Eurobarometer č. 225 – Ochrana údajov v Európskej únii: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

2.1.5. *Zaistenie vedomého a slobodného súhlasu*

V prípade, že sa vyžaduje vedomý súhlas, súčasné predpisy stanovujú, že súhlas jednotlivca na spracovanie jeho osobných údajov by mal byť slobodný, výslovný a vedomý prejav vôle, ktorým jednotlivec dáva najavo svoj súhlas s týmto spracovaním údajov²¹. V členských štátoch sa tieto podmienky v súčasnosti vykladajú rôzne, od všeobecnej požiadavky na písomný súhlas až po akceptovanie implicitného súhlasu.

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

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

Komisia preskúma spôsoby, ako **objasniť a posilniť predpisy týkajúce sa poskytovania súhlasu**.

2.1.6. *Ochrana citlivých údajov*

Spracovanie citlivých údajov, t. j. údajov, ktoré prezrádzajú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie, členstvo v odborových zväzoch, ako aj spracovanie údajov týkajúcich sa zdravia alebo sexuálneho života je už v súčasnosti spravidla zakázané, až na malý počet výnimiek, pri ktorých sa vyžadujú splnenie určitých podmienok a poskytnutie záruk²². Avšak vzhľadom na technický rozvoj a vývoj v iných spoločenských oblastiach je potrebné prehodnotiť existujúce ustanovenia o citlivých údajoch, preskúmať, či by sa nemali pridať iné kategórie údajov a viac ozrejmiť podmienky na ich spracovávanie. Týka sa to napríklad genetických údajov, ktoré sa v súčasnosti v kategórii citlivých údajov výslovne neuvádzajú.

Komisia zvaží:

- či by sa za „**citlivé údaje**“ nemali považovať aj iné kategórie údajov, napríklad **genetické údaje**,
- ďalšie ozrejenie a **harmonizáciu podmienok**, ktoré umožnia spracovanie kategórií citlivých údajov.

²¹ Porov. článok 2 písm. h) smernice 95/46/ES.

²² Porov. článok 8 smernice 95/46/ES.

2.1.7. Zefektívnenie opravných prostriedkov a postihov

S cieľom zaistiť presadzovanie predpisov o ochrane údajov je dôležité, aby boli k dispozícii **efektívne ustanovenia o opravných prostriedkoch a postihoch**. Mnohé prípady, v ktorých dôjde k porušeniu predpisov o ochrane údajov, môžu mať vplyv aj na značný počet iných jednotlivcov nachádzajúcich sa v podobnej situácii.

Komisia preto:

- zväži možnosť **rozšíriť právomoc podávať žalobu na vnútroštátnych súdoch aj na orgány na ochranu údajov a občianske združenia, ako aj na ostatné združenia zastupujúce záujmy dotknutých osôb**,
- posúdi potrebu **posilniť existujúce ustanovenia o postihoch**, napríklad výslovným zahrnutím trestných postihov v prípade vážneho porušenia ochrany údajov, a to v záujme posilnenia účinnosti týchto postihov.

2.2. Rozšírenie rozmeru vnútorného trhu

2.2.1. Zvýšenie právnej istoty a zabezpečenie rovnakých podmienok pre prevádzkovateľov údajov

Ochrana údajov v EÚ má **výrazný rozmer vnútornému trhu**, t. j. je potrebné zaistiť voľný pohyb osobných údajov medzi členskými štátmi v rámci vnútorného trhu. V dôsledku toho sa harmonizácia vnútroštátnych právnych predpisov o ochrane údajov na základe smernice neobmedzuje na minimum, ale predstavuje skôr úplnú harmonizáciu²³.

Smernica zároveň členským štátom poskytuje manévrovací priestor v určitých oblastiach a oprávňuje ich k zachovaniu alebo zavedeniu osobitných predpisov pre špecifické situácie²⁴. Na základe toho, ako aj v dôsledku skutočnosti, že smernica bola členskými štátmi v niektorých prípadoch nesprávne vykonávaná, vznikli **medzi vnútroštátnymi právnymi predpismi, ktorými sa táto smernica vykonáva, odchýlky, čo odporuje jednému z jej hlavných cieľov, t. j. zaisteniu voľného pohybu osobných údajov v rámci vnútorného trhu**. Týka sa to veľkého počtu sektorov a situácií, napr. spracovania osobných údajov v pracovno-právnom prostredí alebo na účely verejného zdravia. Súkromné zainteresované strany, najmä ekonomické subjekty, upozorňujú, že nedostatočná harmonizácia je skutočne jedným z hlavných a opakujúcich sa problémov, v dôsledku ktorého im vznikajú dodatočné náklady a administratívna záťaž. Je to najmä prípad prevádzkovateľov údajov, ktorí pôsobia vo viacerých členských štátoch a sú povinní dodržiavať požiadavky a postupy každej z týchto krajín. Odlišné vykonávanie uvedenej smernice jednotlivými členskými štátmi navyše vedie k právnej neistote, a to nielen pre prevádzkovateľov údajov, ale aj pre dotknuté osoby, čo ohrozuje rovnakú úroveň ochrany, ktorú má smernica dosiahnuť a zaistiť.

Komisia preskúma prostriedky na dosiahnutie lepšej **harmonizácie predpisov o ochrane údajov na úrovni EÚ**.

2.2.2. Zníženie administratívnej záťaže

Zabezpečením rovnakých podmienok sa zníži potreba splňať rozdielne vnútroštátne požiadavky a výrazne sa tým zníži administratívna záťaž pre prevádzkovateľov. **Revízia**

²³ Európsky súdny dvor, C-101/01, „Bodil Lindqvist“, ECR [2003], I-1297, 96, 97.

²⁴ Tamže, 97. Pozri odôvodnenie 9 smernice 95/46/ES.

a zjednodušenie súčasného systému oznamovania²⁵ bude ďalším konkrétnym prvkom na zmenšenie administratívnej záťaže a zníženie nákladov prevádzkovateľov údajov. Medzi prevádzkovateľmi údajov panuje všeobecná zhoda v tom, že súčasná všeobecná povinnosť oznamovať všetky operácie spracovávania údajov orgánom na ochranu údajov je dosť ťažkopádna, a sama osebe vôbec neprispieva k ochrane osobných údajov jednotlivca. Navyše je to jeden z prípadov, kde smernica členským štátom ponecháva určitý manévrovací priestor slobodne sa rozhodnúť o prípadných výnimkách a zjednodušeníach, ako aj o postupoch, ktoré sa budú uplatňovať.

Harmonizovaným a zjednodušeným systémom by sa znížili náklady, ako aj administratívna záťaž, najmä pre nadnárodné spoločnosti so sídlom vo viacerých členských štátoch.

Komisia preskúma rôzne možnosti **zjednodušenia a harmonizácie súčasného systému oznamovania** vrátane možného vypracovania **jednotného registračného formulára pre celú EÚ**.

2.2.3. Ozrejenie pravidiel týkajúcich sa uplatniteľných právnych predpisov a zodpovednosti členských štátov

Už v roku 2003 sa v prvej správe Komisie o vykonávaní smernice o ochrane údajov²⁶ zdôrazňuje skutočnosť, že ustanovenia uplatniteľných právnych predpisov²⁷ „vo viacerých prípadoch vykazovali nedostatky, výsledkom čoho môžu byť práve tie právne kolízie, ktorým sa tento článok snaží predchádzať“. Situácia sa odvtedy nezlepšila, v dôsledku čoho nie je pre prevádzkovateľov údajov a dozorné orgány na ochranu údajov vždy jasné, ktorý členský štát je zodpovedný a ktoré právne predpisy sa uplatňujú v prípade zapojenia viacerých členských štátov. Ide najmä o prípad, keď prevádzkovateľ údajov musí splňať rôzne požiadavky rôznych členských štátov, keď nadnárodný podnik má sídlo vo viac ako jednom členskom štáte alebo keď prevádzkovateľ údajov nemá sídlo v EÚ, ale poskytuje svoje služby obyvateľom EÚ.

Zložitosť situácie sa zvyšuje aj v dôsledku globalizácie a technického rozvoja: Pri poskytovaní nepretržitých služieb a asistencie prevádzkovateľa údajov čoraz viac prevádzkujú činnosť vo viacerých členských štátoch a jurisdikciách. Vďaka internetu môžu prevádzkovatelia údajov so sídlom mimo Európskeho hospodárskeho priestoru (EHP)²⁸ oveľa ľahšie poskytovať služby na diaľku a spracovávať osobné údaje v online prostredí, pričom je často ťažké zistiť, kde sa osobné údaje a zariadenia používané na ich spracovávanie momentálne nachádzajú (napr. aplikácie a služby v rámci tzv. cloud computing).

Komisia sa však domnieva, že skutočnosť, že spracovávanie osobných údajov sa vykonáva prevádzkovateľom údajov so sídlom v tretej krajine, by nemala jednotlivcov zbavovať ochrany, na ktorú majú podľa Charty základných práv EÚ a právnych predpisov EÚ o ochrane údajov nárok.

²⁵ Pozri článok 18 smernice 95/46/ES.

²⁶ Správa Komisie – Prvá správa o vykonávaní smernice o ochrane osobných údajov (95/46/ES) – KOM(2003) 265.

²⁷ Pozri článok 4 smernice 95/46/ES.

²⁸ Európsky hospodársky priestor zahŕňa Nórsko, Lichtenštajnsko a Island.

Komisia preskúma spôsob, ako **zrevidovať a ozrejmiť existujúce ustanovenia týkajúce sa uplatniteľných právnych predpisov** vrátane súčasných určujúcich kritérií, aby sa zvýšila právna istota, vyjasnila zodpovednosť členských štátov za uplatňovanie predpisov o ochrane údajov a napokon zabezpečil rovnaký stupeň ochrany pre dotknuté osoby z EÚ, a to bez ohľadu na zemepisné umiestnenie prevádzkovateľa údajov.

2.2.4. Zvýšenie zodpovednosti prevádzkovateľov údajov

Administratívne zjednodušenie by nemalo viesť k **celkovému zníženiu zodpovednosti prevádzkovateľov údajov za zaistenie efektívnej ochrany údajov**. Naopak, Komisia je presvedčená, že ich povinnosti je potrebné jasnejšie vymedziť v právnom rámci, a to aj v súvislosti s vnútornými kontrolnými mechanizmami a spoluprácou s dozornými orgánmi na ochranu údajov. Malo by sa okrem toho zaistiť, aby sa takáto zodpovednosť vzťahovala aj na prevádzkovateľov, na ktorých sa vzťahujú povinnosti zachovania služobného tajomstva (napr. právnikov) a aby sa uplatňovala aj v čoraz častejších prípadoch, keď prevádzkovatelia údajov delegujú spracovanie údajov na iné subjekty (napr. spracovávateľov).

Komisia preto preskúma možnosti, ako **zaistiť, aby prevádzkovatelia údajov zaviedli efektívne politiky a mechanizmy na zaistenie dodržiavania predpisov o ochrane údajov**. Komisia pritom zohľadní súčasnú diskusiu o možnom zavedení zásady tzv. *accountability*²⁹. Cieľom týchto krokov by nebolo zvyšovanie administratívnej záťaže prevádzkovateľov údajov, keďže takéto opatrenia by sa skôr zameriavali na vytvorenie záruk a mechanizmov, na základe ktorých by bolo dodržiavanie predpisov v oblasti ochrany údajov efektívnejšie, pričom by sa zároveň dosiahlo obmedzenie a zjednodušenie určitých administratívnych formalít, ako sú napríklad oznámenia (*pozri bod 2.2.2 predtým*).

Podpora využívania technológií na zvyšovanie súkromia (PETs), ako sa už zdôrazňuje v oznámení Komisie o tejto otázke z roku 2007, ako aj zásada „ochrany súkromia už v štádiu návrhu príslušných technológií“ môžu zohrávať v tejto súvislosti významnú úlohu, a to aj pokiaľ ide o zaistenia ochrany údajov³⁰.

²⁹ Pozri najmä stanovisko prijaté pracovnou skupinou zriadenej podľa článku 29 z 13. júla 2010, s. 3.

³⁰ K technológiám na zvyšovanie súkromia pozri: oznámenie Komisie Európskemu parlamentu a Rade o podpore ochrany údajov prostredníctvom technológií na zvyšovanie súkromia (PETs) – KOM(2007) 228. Zásada „ochrany súkromia už v štádiu návrhu príslušných technológií“ znamená, že ochrana súkromia a údajov je pevnou súčasťou celého životného cyklu technológií, od počiatkových fáz ich koncipovania, cez ich zavádzanie a využívanie až po ich definitívne vyradenie a likvidáciu. Táto zásada je *inter alia* uvedená aj v oznámení Komisie „Digitálna agenda pre Európu“ – KOM(2010) 245.

Za účelom zvýšiť zodpovednosť prevádzkovateľov údajov Komisia preskúma tieto prvky:

- zaviesť povinné menovanie nezávislého **úradníka pre ochranu údajov** a harmonizovať predpisy týkajúce sa jeho úloh a právomocí³¹, pričom sa zváži vhodná hranica, najmä pokiaľ ide o malé podniky a mikropodniky, aby sa predišlo neprimeranej administratívnej záťaži,
- do právneho rámca zahrnúť povinnosť prevádzkovateľov údajov vykonávať v osobitných prípadoch **posudzovanie vplyvu na osobné údaje**, napríklad, pri spracovávaní citlivých údajov alebo ak druh spracovania v sebe inak zahŕňa osobitné riziká, najmä pri použití špecifických technológií, mechanizmov alebo postupov vrátane vytvárania profilov a kamerového sledovania,
- ďalej podporovať využívanie technológií na zvyšovanie súkromia a možnosti konkrétneho vykonávania koncepcie „**ochrany súkromia už v štádiu návrhu príslušných technológií**“.

2.2.5. Podporovanie samoregulačných iniciatív a preskúmanie certifikačných schém EÚ

Komisia sa aj naďalej domnieva, že **samoregulačné iniciatívy** prevádzkovateľov údajov môžu **prispieť k lepšiemu presadzovaniu predpisov o ochrane údajov**. Súčasná ustanovenia týkajúce sa samoregulácie, ktoré sú obsiahnuté v smernici o ochrane údajov, menovite rozsah pôsobnosti na vypracovanie kódexov správania³², sa doteraz iba zriedka používali a súkromné zainteresované strany ich nepovažujú za dostačujúce.

Komisia okrem toho preskúma možné vytvorenie **certifikačných schém EÚ (napr. „osvedčenia o zachovaní dôverného charakteru informácií“)** na účely postupov, technológií, produktov a služieb, ktoré spĺňajú požiadavky na ochranu súkromia³³. Tento krok by uľahčil nielen orientáciu jednotlivcov ako používateľov takýchto technológií, produktov a služieb, ale mal by význam aj z hľadiska zodpovednosti prevádzkovateľov údajov: voľbou certifikovaných technológií, produktov a služieb by totiž prevádzkovatelia mohli preukázať, že si splnili svoje záväzky (*pozri bod 2.2.4 predtým*). Bolo by samozrejme dôležité **zaistiť dôveryhodnosť takýchto osvedčení o zachovaní dôverného charakteru informácií** a preskúmať, či zodpovedajú právnym záväzkom a medzinárodným technickým normám.

Komisia:

- preskúma prostriedky, ako **ďalej podporovať samoregulačné iniciatívy** vrátane aktívneho propagovania kódexu správania,
- preskúma uskutočniteľnosť vytvorenia **certifikačných schém EÚ** v oblasti ochrany súkromia a údajov.

³¹ Vo viacerých členských štátoch sa už pre prevádzkovateľa údajov zaviedla aktuálna možnosť vymenovať úradníka pre ochranu údajov, aby nezávisle zaisťoval dodržiavanie predpisov EÚ o ochrane údajov a vnútroštátnych predpisov o ochrane údajov, a jednotlivcom poskytoval pomoc (pozri napr. *Beauftragter für den Datenschutz v Německu a correspondant informatique et libertés (CIL)* vo Francúzsku.

³² Pozri článok 27 smernice 95/46/ES.

³³ K tomuto hľadisku pozri tiež oznámenie o technológiách na zvyšovanie súkromia, c. d. v pozn. pod čiarou 30.

2.3. Revízia predpisov o ochrane údajov v oblasti policajnej a justičnej spolupráce v trestných veciach

Smernica o ochrane údajov sa vzťahuje na všetky činnosti spracovávaní osobných údajov v členských štátoch vo verejnom, ako aj súkromnom sektore. Neuplatňuje sa však na spracovávanie osobných údajov v rámci činnosti, ktorá spadá mimo rozsah pôsobnosti právnych predpisov Spoločenstva, ako sú činnosti v oblasti policajnej a justičnej spolupráce v trestných veciach.³⁴ Lisabonskou zmluvou sa však zrušila predchádzajúca „pilierová štruktúra“ EÚ a vo všetkých politikách Únie sa zaviedol nový a komplexný právny základ ochrany osobných údajov³⁵. Na tomto základe a s ohľadom na Chartu základných práv EÚ sa v oznámeniach Komisie o Štokholmskom programe a Štokholmskom akčnom pláne³⁶ zdôraznila potreba „komplexného systému ochrany“ s cieľom „posilniť pozíciu EÚ v oblasti ochrany osobných údajov jednotlivcov v súvislosti so všetkými politikami EÚ vrátane presadzovania práva a predchádzania trestnej činnosti“.

Nástrojom EÚ na ochranu osobných údajov v oblasti policajnej a justičnej spolupráce v trestných veciach je **rámcové rozhodnutie 2008/977/SVV**³⁷. Toto rámcové rozhodnutie je dôležitým krokom vpred v oblasti, kde sú veľmi potrebné spoločné normy pri ochrane údajov. Je však potrebné sa tejto otázke venovať viac.

Uvedené rámcové rozhodnutie sa uplatňuje iba na cezhraničnú výmenu osobných údajov v rámci EÚ a nie na operácie spracovávaní v rámci samotných členských štátov. V praxi je ťažké tento rozdiel rozpoznať a môže to skomplikovať vlastné vykonávanie a uplatňovanie tohto rámcového rozhodnutia³⁸.

Navyše, **pokiaľ ide o zásadu obmedzenia účelu, toto rámcové rozhodnutie obsahuje priveľmi široko formulovanú výnimku**. Ďalším nedostatkom je absencia ustanovení o potrebe rozlišovať medzi rozdielnymi kategóriami údajov v súlade s ich stupňom presnosti a spoľahlivosti, o potrebe rozlišovať údaje vychádzajúce zo skutočností od údajov vychádzajúcich z názorov alebo osobných hodnotení³⁹, ako aj o potrebe rozlišovať medzi rôznymi kategóriami dotknutých osôb (trestané osoby, podozrivé osoby, obeť, svedkovia atď.), pričom na údaje osôb, ktoré sú mimo podozrenia, by sa mali vzťahovať osobitné záruky⁴⁰.

Okrem toho sa týmto rámcovým rozhodnutím nenahrádzajú najrôznejšie sektorové legislatívne nástroje v oblasti policajnej a justičnej spolupráce v trestných veciach, ktoré

³⁴ Pozri prvú zarážku v článku 3 ods. 2 smernice 95/46/ES.

³⁵ Pozri článok 16 ZFEÚ.

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

³⁷ Rámcové rozhodnutie Rady 2008/977/SVV z 27. novembra 2008 o ochrane osobných údajov spracúvaných v rámci policajnej a justičnej spolupráce v trestných veciach (Ú. v. EÚ L 350, 30.12.2008, s. 60). Toto rámcové rozhodnutie predpokladá harmonizáciu noriem ochrany údajov iba v minimálnej miere.

³⁸ Tento rozdiel nie je prítomný v príslušných nástrojoch Rady Európy, ako sú napríklad: dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (CETS č. 108), jeho dodatkový protokol o dozorných orgánoch a cezhraničných tokoch údajov (ETS č. 181) a odporúčanie výboru ministrov členským štátom č. R (87) 15 prijaté 17. septembra 1987, ktorým sa upravuje využívanie osobných údajov v policajnej oblasti.

³⁹ Ako sa to požaduje v zásade 3.2 odporúčania č. R (87) 15.

⁴⁰ V protiklade so zásadou 2 odporúčania č. R (87) 15 a jeho hodnotiacimi správami.

boli prijaté na úrovni EÚ⁴¹, najmä tie, ktorými sa riadi fungovanie Europolu, Eurojustu, Schengenského informačného systému (SIS) a Colného informačného systému (CIS)⁴². Tieto legislatívne nástroje buď obsahujú osobitné režimy ochrany údajov a/alebo zvyčajne uvádzajú odkaz na nástroje Rady Európe v oblasti ochrany údajov. V prípade činností v oblasti policajnej a justičnej spolupráce všetky členské štáty schválili odporúčanie Rady Európy č. R (87) 15, ktoré vytyčuje zásady dohovoru č. 108 pre policajnú oblasť. Toto odporúčanie však nie je právne záväzným nástrojom.

Tento stav môže priamo ovplyvniť možnosti jednotlivcov uplatňovať svoje práva na ochranu údajov v tejto oblasti (napr. mať vedomosť, ktoré z ich osobných údajov sa spracovávajú a vymieňajú, kým a na aké účely, a ako si uplatňovať svoje práva, ako je napríklad právo na prístup k svojim údajom).

V záujme vytvorenia komplexného a koherentného systému v EÚ a voči tretím krajinám je **potrebné zvážiť revíziu súčasných predpisov o ochrane údajov v oblasti policajnej a justičnej spolupráce v trestných veciach**. Komisia zdôrazňuje, že myšlienka komplexného režimu ochrany údajov nevyklučuje prijať vo všeobecnom rámci osobitné pravidlá o ochrane údajov v policajnej a justičnej oblasti, a to pri zohľadnení osobitnej povahy týchto oblastí, ako sa uvádza vo vyhlásení č. 21 pripojenom k Lisabonskej zmluve. Predpokladá to napríklad potrebu zvážiť rozsah, v ktorom by uplatňovanie niektorých práv jednotlivcom v oblasti ochrany údajov mohlo v konkrétnom prípade ohroziť predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie alebo vykonávanie trestných postihov.

Komisia najmä:

- zváži **rozsah uplatňovania všeobecných predpisov o ochrane údajov na oblasti policajnej a justičnej spolupráce v trestných veciach** vrátane spracovávania údajov na domácej úrovni, pričom tam, kde je to nevyhnutné, zabezpečí harmonizované **obmedzenia** určitých práv jednotlivcov na ochranu údajov, napr. pokiaľ ide o právo na prístup alebo o zásadu transparentnosti,
- preskúma potrebu zaviesť **osobitné a harmonizované ustanovenia** v novom všeobecnom rámci ochrany údajov, napríklad o ochrane údajov so zreteľom na spracovávanie **genetických údajov** na trestnoprávne účely alebo na rozlišovanie medzi rôznymi kategóriami dotknutých osôb (svedkovia, podozrivé osoby atď.) v oblasti policajnej a justičnej spolupráce v trestných veciach,
- začne v roku 2011 **konzultáciu** so všetkými dotknutými zainteresovanými stranami o najlepšom postupe na uskutočnenie **revízie súčasných dozorných systémov v oblasti policajnej a justičnej spolupráce v trestných veciach**, aby sa zaistil efektívny a súvislý dozor ochrany údajov vo všetkých inštitúciách, orgánoch, úradoch a agentúrach Únie,
- posúdi potrebu **zosúladiť** v dlhodobom časovom horizonte nový všeobecný právny rámec ochrany údajov s **existujúcimi sektorovými predpismi, ktoré boli vo forme osobitných nástrojov prijaté na úrovni EÚ v oblasti policajnej a justičnej spolupráce v trestných veciach**.

⁴¹ Pozri prehľad takýchto nástrojov v oznámení Komisie „Prehľad o riadení informácií v oblasti slobody, bezpečnosti a spravodlivosti“ – KOM(2010) 385.

⁴² Na základe príslušných nástrojov sa zriadili spoločné dozorné orgány, aby sa zaistil dohľad nad ochranou údajov mimo všeobecných dozorných právomocí európskeho dozorného úradníka pre ochranu údajov (EDPS) voči inštitúciám, orgánom, úradom a agentúram Únie, ktoré vychádzajú z nariadenia (ES) č. 45/2001.

2.4. Globálny rozmer ochrany údajov

2.4.1. Ozrejenie a zjednodušenie predpisov pri medzinárodnom prenose údajov

Prenos osobných údajov mimo EÚ a EHP je okrem iného podmienený aj tzv. **hodnotením primeranosti**. V súčasnosti je to Komisia a členské štáty, ktoré určujú primeranosť ochrany údajov v tretej krajiny, t.j. či tretia krajina zaistuje takú úroveň ochrany, ktorú EÚ považuje za primeranú.

Ak Komisie usúdi, že úroveň ochrany údajov v tretej krajine je primeraná, osobné údaje sa môžu voľne pohybovať z 27 členských štátov EÚ a troch členských krajín EHP do predmetnej tretej krajiny bez toho, aby boli potrebné dodatočné záruky. Presné požiadavky uznávania primeranosti Komisiou ale v súčasnosti nie sú v smernici o ochrane údajov dostatočne podrobne konkretizované. Okrem toho uvedené rámcové rozhodnutie neobsahuje ustanovenia o prijímaní takéhoto rozhodnutia Komisiou.

V niektorých členských štátoch túto primeranosť v prvom rade hodnotí prevádzkovateľ údajov, ktorý sám prenáša osobné údaje do tretej krajiny, pričom niekedy sa toto hodnotenie uskutočňuje pod *ex-post* dohľadom dozorného orgánu na ochranu údajov. Následkom takéhoto stavu môžu byť rôzne prístupy k hodnoteniu úrovne primeranosti tretích krajín alebo medzinárodných organizácií a **spája sa s ním riziko, že úroveň ochrany údajov dotknutých osôb zabezpečených treťou krajinou posudzujú jednotlivé členské štáty rozdielne**. Navyše súčasné právne nástroje neobsahujú žiadne podrobné a harmonizované požiadavky, na základe ktorých možno stanoviť, že prenos údajov prebehol v súlade s právnymi predpismi. Výsledkom toho je, že v jednotlivých členských štátoch existuje rozdielna prax.

Okrem toho, pokiaľ ide o prenosi údajov do tretích krajín, ktoré nezaistujú primeranú úroveň ochrany, súčasné štandardné zmluvné doložky Komisie, ktoré sa vzťahujú na prenos osobných údajov prevádzkovateľom⁴³ a spracovateľom⁴⁴, nie sú navrhnuté pre mimozmluvné vzťahy a nemožno ich napríklad použiť pri prenosoch údajov medzi orgánmi verejnej správy.

Medzinárodné dohody uzatvorené EÚ alebo jej členskými štátmi navyše často požadujú začlenenie zásad ochrany údajov a osobitné ustanovenia. Výsledkom toho môže byť rozdielne znenie dohôd s nekonzistentnými ustanoveniami a právami, čím sa na škodu dotknutej osoby otvára priestor na rôzne výklady. Komisia v dôsledku toho oznámila, že na účely presadzovania práva bude pracovať na ústredných prvkoch ochrany osobných údajov, ktoré sú obsiahnuté v dohodách medzi Úniou a tretími krajinami⁴⁵.

Došlo k vytvoreniu ďalších prostriedkov ako určitej formy samoregulácie, ako je napríklad vnútropodnikový kódex správania známy pod názvom „Záväzná firemná pravidlá“ (Binding

⁴³ Rozhodnutie Komisie 2001/497/ES z 15. júna 2001 o štandardných zmluvných doložkách na prenos osobných údajov do tretích krajín podľa smernice 95/46/ES (Ú. v. ES L 181, 4.7.2001, s. 19); rozhodnutie Komisie 2002/16/ES z 27. decembra 2001 o štandardných zmluvných doložkách pre prenos osobných údajov spracovateľom z tretích krajín podľa smernice 95/46/ES (Ú. v. ES L 6, 10.1.2002, s. 52); rozhodnutie Komisie 2004/915/ES z 27. decembra 2004, ktorým sa mení a dopĺňa rozhodnutie 2001/497/ES o zavedení alternatívneho súboru o štandardných zmluvných doložkách na prenos osobných údajov do tretích krajín (Ú. v. EÚ L 385, 29.12.2004, s. 74).

⁴⁴ Rozhodnutie Komisie z 5. februára 2010 o štandardných zmluvných doložkách pre prenos osobných údajov spracovateľom usadeným v tretích krajinách podľa smernice Európskeho parlamentu a Rady 95/46/ES (Ú. v. EÚ L 39, 12.2.2010, s. 5).

⁴⁵ Štokholmský akčný plán, c. d. v pozn. pod čiarou 36.

Corporate Rules)⁴⁶, ktoré môžu tiež poslúžiť ako užitočný nástroj, ktorý zabezpečí, že prenos osobných údajov medzi spoločnosťami rovnakej skupiny podnikov prebehne v súlade s právnymi predpismi. Zainteresované strany však navrhli, že tento mechanizmus možno ďalej zlepšiť a uľahčiť jeho vykonávanie.

S cieľom riešiť uvedené otázky existuje **všeobecná potreba zlepšiť súčasné mechanizmy medzinárodného prenosu osobných údajov**, pričom je zároveň potrebné zaistiť primeranú ochranu osobných údajov pri ich prenose a spracovávaní mimo EÚ a EHP.

Komisia má v úmysle preskúmať, ako:

- **zlepšiť a zjednotiť súčasné postupy** pri medzinárodnom prenose údajov vrátane právne záväzných nástrojov a „Záväzných firemných pravidiel“, aby sa zaistil **jednoduchší a koherentnejší prístup EÚ** voči tretím krajinám a medzinárodným organizáciám,
- **ozrejmiť postup Komisie pri zisťovaní primeranosti** a viac konkretizovať **kritériá a požiadavky** týkajúce sa hodnotenia úrovne ochrany údajov v tretích krajinách alebo medzinárodných organizáciách,
- vymedziť **ústredné prvky EÚ pri ochrane údajov**, ktorý by sa mohli uplatňovať pri všetkých druhoch medzinárodných dohôd.

2.4.2. Podpora univerzálnych zásad

Spracovávanie údajov je globálnou záležitosťou a vyžaduje si vypracovanie univerzálnych zásad ochrany jednotlivcov so zreteľom na spracovávanie údajov.

Právny rámec EÚ **tretím krajinám** často slúžil ako **kritérium pri ich vlastnej úprave ochrany údajov**. V rámci Únie a mimo nej mal jeho účinok a vplyv nesmiernu dôležitosť. **Európska únia musí preto zostať hybnou silou rozvoja a podpory medzinárodných právnych a technických noriem v oblasti ochrany osobných údajov**, a to na základe príslušných nástrojov ochrany údajov EÚ a ostatných európskych nástrojov. Osobitný význam to má v rámci politiky EÚ v oblasti rozšírenia.

Pokiaľ ide o medzinárodné technické normy vypracované normalizačnými organizáciami, Komisia je presvedčená, že koherentnosť medzi budúcim právnym rámcom a týmito normami je mimoriadne dôležitá z hľadiska zaistenia konzistentného a praktického vykonávania predpisov o ochrane údajov prevádzkovateľmi údajov.

⁴⁶ „Záväzné firemné pravidlá“ predstavujú kódexy osvedčených postupov, ktoré sa opierajú o európske normy ochrany údajov a ktoré nadnárodné organizácie vypracovali a dobrovoľne dodržiavajú, aby sa zaistili primerané záruky vo vzťahu k prenosom alebo kategóriám prenosov osobných údajov medzi spoločnosťami, ktoré sú súčasťou rovnakej skupiny podnikov a ktoré sú týmito firemnými pravidlami viazané. Pozri: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faqs/international_transfers_faqs.pdf.

Komisia bude:

- naďalej **podporovať rozvíjanie vysokokvalitných právnych a technických noriem ochrany údajov** v tretích krajinách a na medzinárodnej úrovni,
- dbať na dodržiavanie **zásady reciprocitu ochrany** v rámci medzinárodných opatrení Únie, najmä pokiaľ ide o dotknuté osoby, ktorých údaje sú vyvážené z EÚ do tretích krajín,
- **rozširovať za týmto účelom svoju spoluprácu s tretími krajinami a medzinárodnými organizáciami**, ako je OECD, Rada Európy, Organizácia Spojených národov a iné regionálne organizácie,
- **pozorne sledovať vytváranie medzinárodných technických noriem normalizačnými organizáciami**, ako je CEN a ISO, aby sa zaistilo ich vhodné dopĺňanie právnych predpisov a zabezpečilo operatívne a efektívne vykonávanie kľúčových požiadaviek pri ochrane údajov.

2.5. Silnejší inštitucionálny rámec pre efektívnejšie presadzovanie predpisov o ochrane údajov

Kľúčovým prvkom pri zaručení dodržiavania práv jednotlivcov je vykonávanie a presadzovanie zásad a predpisov týkajúcich sa ochrany údajov.

V tejto súvislosti **zohrávajú** pri presadzovaní predpisov o ochrane údajov **podstatnú úlohu orgány na ochranu údajov**. Sú totiž nezávislými strážcami základných práv a slobôd v oblasti ochrany osobných údajov, ktorým jednotlivci dôverujú, že zabezpečia ochranu a spracovanie ich osobných údajov v súlade s právnymi predpismi. Komisia je z tohto dôvodu presvedčená, že ich úloha by sa mala posilniť, a to najmä vzhľadom na nedávnu judikatúru SDEÚ o ich nezávislosti⁴⁷, a mali by mať preto potrebné právomoci a prostriedky na riadne plnenie svojich úloh na vnútroštátnej úrovni, ako aj na úrovni vzájomnej spolupráce.

Komisia sa zároveň domnieva, že **orgány na ochranu údajov by mali posilniť vzájomnú spoluprácu a lepšie koordinovať svoje činnosti**, najmä keď čelia otázkam, ktoré zo svojej povahy majú cezhraničný rozmer. Týka sa to najmä prípadov, keď majú nadnárodné spoločnosti sídlo vo viacerých členských štátoch a svoje činnosti vykonávajú v každom z týchto štátov alebo prípadov, kde sa vyžaduje koordinovaný dohľad európskym dozorným úradníkom pre ochranu údajov⁴⁸.

V tejto súvislosti **môže významnú úlohu zohrávať pracovná skupina zriadená podľa článku 29**⁴⁹, ktorá popri svojej poradnej funkcii⁵⁰ má za úlohu prispieť k jednotnému uplatňovaniu predpisov EÚ o ochrane údajov na vnútroštátnej úrovni. Avšak pokračovanie v rozdielnom uplatňovaní a výklade predpisov EÚ orgánmi na ochranu údajov, hoci výzvy súvisiace s ochranou údajov sú v celej EÚ rovnaké, si žiada posilnenie úlohy tejto pracovnej

⁴⁷ Rozsudok SDEÚ z 9.3.2010, Komisia vs. Nemecko, vec C-518/07.

⁴⁸ V súčasnosti sa to týka rozsiahlych systémov IT, napr. SIS II [porov. článok 46 nariadenia (ES) č. 1987/2006 – Ú. v. EÚ L 318, 28.12.2006, s. 4] a VIS [porov. článok 43 nariadenia (ES) č. 767/2008 – Ú. v. EÚ L 218, 13.8.2008, s. 60].

⁴⁹ Pracovná skupina zriadená podľa článku 29 je poradným orgánom, ktorý sa skladá zo zástupcov orgánov na ochranu údajov jednotlivých členských štátov, európskeho dozorného úradníka pre ochranu údajov a Komisie (bez hlasovacích práv), ktorá tiež poskytuje svoj sekretariát. Pozri: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

⁵⁰ Úlohou pracovnej skupiny zriadenej podľa článku 29 je poskytovanie poradenstva Komisii, pokiaľ ide o úroveň ochrany osobných údajov v EÚ a v tretích krajinách a o hociktoré iné opatrenia súvisiace so spracovávaním osobných údajov.

skupiny pri koordinovaní stanovísk orgánov na ochranu údajov, aby sa zabezpečilo jednotnejšie uplatňovanie týchto predpisov na vnútroštátnej úrovni a tým aj rovnaká úroveň ochrany údajov.

Komisia preskúma:

- spôsob, ako **posilniť, ozrejmiť a zladíť postavenie a právomoci vnútroštátnych orgánov na ochranu údajov** v novom právnom rámci vrátane plného vykonávania koncepcie „úplnej nezávislosti“⁵¹,
- spôsoby, ako **zlepšiť spoluprácu a koordináciu medzi orgánmi na ochranu údajov**,
- spôsob, ako zaistiť konzistentnejšie uplatňovanie predpisov EÚ o ochrane údajov v rámci celého vnútorného trhu. Môže to zahŕňať **posilnenie úlohy vnútroštátnych dozorných úradníkov pre ochranu údajov, lepšiu koordináciu ich práce prostredníctvom pracovnej skupiny zriadenej podľa článku 29 (ktorá by sa malo stať transparentnejším orgánom) a/alebo vytvorenie mechanizmu na zaistenie konzistentnosti v rámci vnútorného trhu na základe autority Európskej komisie.**

3. ZÁVER: ĎALŠÍ POSTUP

Podobne ako technika aj spôsob používania a zdieľania našich osobných údajov sa v našej spoločnosti neustále mení. Pre zákonodarcov z toho plynie výzva vytvoriť taký právny rámec, ktorý obstojí v skúške časom. Po dovŕšení reformného procesu by európske predpisy o ochrane údajov mali naďalej zaručovať vysokú úroveň ochrany a jednotlivcom, orgánom verejnej správy a podnikom činným na vnútornom trhu zároveň zabezpečovať dlhodobú právnu istotu. Bez ohľadu na komplexnosť situácie alebo zložitost' technológie musia existovať jasné uplatniteľné predpisy a normy, ktoré majú vnútroštátne orgány presadzovať a podniky a vývojári technológií dodržiavať. Jednotlivcom by tiež mali byť jasné práva, ktoré požívajú.

Komplexný prístup Komisie na riešenie uvedených otázok a dosiahnutie kľúčových cieľov podčiarknutých v tomto oznámení poslúži ako základ pre ďalšie diskusie s ostatnými európskymi inštitúciami a inými zainteresovanými stranami a neskôr sa premietne do konkrétnych legislatívnych ako aj nelegislatívnych návrhov a opatrení. Komisia za týmto účelom víta spätnú väzbu, pokiaľ ide o otázky vznesené v tomto oznámení.

V nadväznosti na posudzovanie vplyvu a zohľadňujúc Chartu základných práv EÚ Komisia na tomto základe **v roku 2011 predloží návrhy právnych predpisov** zameraných na revíziu právneho rámca ochrany údajov s cieľom posilniť pozíciu EÚ pri ochrane osobných údajov jednotlivca v kontexte všetkých politík EÚ vrátane presadzovania práva a predchádzania trestnej činnosti, pričom zohľadní osobitosti týchto oblastí. Súčasne sa budú presadzovať nelegislatívne opatrenia, ako je stimulovanie samoregulácie a skúmanie uskutočniteľnosť osvedčení EÚ o zachovaní dôverného charakteru informácií.

Druhým krokom Komisie bude **posúdenie potreby prispôbiť iné právne nástroje** novému všeobecnému rámcu ochrany údajov. Predovšetkým sa to týka nariadenia (ES) č. 45/2001, ktorého ustanovenia sa budú musieť prispôbiť novému všeobecnému právnemu

⁵¹ Pozri rozsudok SDEÚ z 9.3.2010, Komisia vs. Nemecko, vec C-518/07.

rámcu. Neskôr bude potrebné podrobne preskúmať dosah tohto rámca aj na ostatné sektorové nástroje.

Presadzovaním **aktívnej politiky týkajúcej sa porušovania práva** v prípadoch nesprávneho vykonávania a uplatňovania predpisov EÚ o ochrane údajov bude Komisia aj naďalej zaisťovať riadne monitorovanie správneho vykonávania právnych predpisov Únie v tejto oblasti. Súčasné posudzovanie nástrojov ochrany údajov nemá žiaden vplyv na záväzok členských štátov vykonávať a zabezpečiť riadne uplatňovanie existujúcich právnych nástrojov v oblasti ochrany osobných údajov⁵².

Vysoká a jednotná úroveň ochrany údajov v EÚ bude najlepšou cestou, ako podporovať a povzbudzovať normy EÚ v oblasti ochrany údajov na celom svete.

⁵² Zahŕňa to tiež rámcové rozhodnutie Rady 2008/977/SVV: je potrebné, aby členské štáty prijali nevyhnutné opatrenia na dosiahnutie súladu s ustanoveniami tohto rámcového rozhodnutia do 27. novembra 2010.