



V Bruselu dne 24.7.2019
COM(2019) 374 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

**Pravidla pro ochranu údajů zprostředkující důvěru v EU i za jejími hranicemi –
vyhodnocení**

Sdělení Komise Evropskému parlamentu a Radě

Pravidla pro ochranu údajů zprostředkující důvěru v EU i za jejími hranicemi – vyhodnocení

I. Úvod

Obecné nařízení o ochraně údajů¹ (dále jen „nařízení“) platí v celé Evropské unii již déle než rok. Je klíčovým prvkem soudržného a modernizovaného prostředí EU v oblasti ochrany údajů, které rovněž zahrnuje směrnici o prosazování práva v souvislosti s ochranou údajů² a nařízení o ochraně údajů pro orgány a instituce EU³. Tento rámec bude uzavřen nařízením o soukromí a elektronických komunikacích, které v současné době prochází legislativním procesem.

Přísná pravidla ochrany údajů jsou nezbytná pro zajištění základního práva na ochranu osobních údajů. Jsou zásadní pro demokratickou společnost⁴ a důležitou součástí hospodářství čím dál tím silněji založeného na datech. EU chce využít množství příležitostí, které digitální transformace v oblasti služeb, pracovních míst a inovací nabízí, a zároveň řešit výzvy, které v této souvislosti vznikají. Krádeže identity, úniky citlivých údajů, diskriminace osob, zakořeněná předpojatost, sdílení ilegálního obsahu a vývoj technologií sledování narušujících soukromí představují jen pár příkladů, o jakých problémech veřejnost čím dál tím častěji debatuje, přičemž je zřejmé, že lidé očekávají, že jejich údaje budou chráněny.

Lidé po celém světě si čím dál tím více váží ochrany a bezpečnosti svých údajů, a jejich ochrana se tak stala vskutku celosvětovým fenoménem. Mnoho zemí přijalo komplexní pravidla ochrany údajů vycházející z podobných zásad jako nařízení nebo na jejich přijetí pracují, díky čemuž se sbližují pravidla ochrany údajů na celém světě. To otevírá nové příležitosti, jak usnadnit pohyb údajů mezi hospodářskými subjekty nebo orgány veřejné správy a zároveň zlepšit úroveň ochrany osobních údajů v EU i po celém světě.

¹ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1): <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

² Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:32016L0680>). Tuto směrnici měly členské státy provést ve vnitrostátním právu do 6. května 2018. O stavu provádění informují zprávy bezpečnostní unie.

³ Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39): <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32018R1725>). Je použitelné od 11. prosince 2018.

⁴ Indický nejvyšší soud v přelomovém rozsudku ze dne 24. srpna 2017 uznal soukromí za základní právo, „zásadní složku lidské důstojnosti“.

Ochrana údajů dosud nikdy nebyla brána tak vážně a má dalekosáhlé důsledky pro různé zúčastněné strany a odvětví. Komise je pevně rozhodnuta vést EU k úspěšnému provádění nového režimu ochrany údajů a podporovat všechny aspekty procesu vedoucí k jeho plné funkčnosti. V tomto sdělení Komise hodnotí výsledky, jichž bylo dosud dosaženo, pokud jde o soudržné uplatňování pravidel pro ochranu údajů napříč EU, fungování nového správního systému, dopad na občany a podniky a o úsilí EU v oblasti propagace celosvětového sbližování režimů ochrany údajů. Navazuje na sdělení Komise o uplatňování nařízení z ledna 2018⁵ a obsažené informace vychází z činnosti odborné skupiny různých zúčastněných stran⁶, především z jejího příspěvku k výročnímu hodnocení, i z diskusí, které se konaly na hodnotící akci zorganizované Komisí dne 13. června 2019⁷. Toto sdělení je rovněž příspěvkem k přezkumu, který má Komise v plánu provést do května 2020⁸.

Legislativní rámec EU pro ochranu údajů představuje základ evropského přístupu k inovacím zaměřeného na člověka. Stává se z něj součást regulačního podkladu v čím dál vyšším počtu oblastí politiky včetně zdravotnictví a výzkumu, umělé inteligence, dopravy, energetiky, hospodářské soutěže a prosazování práva. Komise neustále zdůrazňuje význam řádného uplatňování a prosazování nových pravidel ochrany údajů, jak zdůraznila ve svém sdělení o uplatňování nařízení zveřejněném v lednu 2018 a v pokynech pro využívání osobních údajů ve volebním kontextu vydaných v září 2018⁹. V době, kdy bylo toto sdělení vydáno, bylo dosaženo velkého pokroku při plnění tohoto cíle, ačkoli je nepochybně zapotřebí další práce, aby bylo nařízení plně funkční.

II. Jeden kontinent, jeden zákon: v členských státech byl zaveden rámec pro ochranu údajů

Jedním z klíčových cílů nařízení bylo odstranit problém roztržitého prostředí 28 různých vnitrostátních právních úprav, které existovaly v rámci předcházející směrnice o ochraně údajů¹⁰, a poskytnout jednotlivcům i podnikům napříč EU právní jistotu. Tento cíl byl z velké části splněn.

⁵ Sdělení komise Evropskému parlamentu a Radě s názvem „Posílená ochrana, nové příležitosti – pokyny Komise týkající se přímého uplatňování obecného nařízení o ochraně osobních údajů ke dni 25. května 2018“, COM(2018) 43 final:

<https://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043>.

⁶ Odborná skupina různých zúčastněných stran pro nařízení zřízená Komisí zahrnuje zástupce občanské společnosti, komerční sféry, akademické obce a odborníky z praxe:

<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537&Lang=CS>.

⁷ http://europa.eu/rapid/press-release_IP-19-2956_cs.htm.

⁸ Článek 97 nařízení.

⁹ „Pokyny Komise k uplatňování práva Unie o ochraně údajů ve volebním kontextu“, COM(2018) 638 final: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52018DC0638&qid=1563875255437&from=EN>.

¹⁰ 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

<https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A31995L0046&from=EN&lang3=choose&lang2=choose&lang1=CS>.

Harmonizace právního rámce

Ačkoli je nařízení v členských státech přímo použitelné, ukládalo jim povinnost podniknout řadu právních kroků na vnitrostátní úrovni, zejména zřídit vnitrostátní orgány pro ochranu údajů a přidělit jim pravomoci¹¹, stanovit pravidla pro konkrétní otázky, např. sjednocení ochrany osobních údajů se svobodou projevu a informací, a pozměnit nebo zrušit odvětvové právní předpisy obsahující aspekty ochrany údajů. V době vydání tohoto sdělení své vnitrostátní právní předpisy o ochraně údajů aktualizovaly všechny členské státy kromě tří¹². Práce na přizpůsobení odvětvových právních předpisů na vnitrostátní úrovni stále probíhají. Poté co bylo uplatňování nařízení začleněno do Dohody o Evropském hospodářském prostoru, rozšířilo se do Norska, na Island a do Lichtenštejnska, jež rovněž přijaly vnitrostátní právní předpisy pro ochranu údajů.

Zúčastněné strany nicméně volají po ještě větším stupni harmonizace v určitých oblastech¹³. Nařízení skutečně členským státům umožňuje v určité míře dále specifikovat uplatňování nařízení v určitých oblastech, např. u věkové hranice souhlasu dítěte pro používání internetových služeb¹⁴ nebo zpracování osobních údajů v oblastech, jako je lékařství a veřejné zdraví. V takové situaci se činnost členských států řídí dvěma prvky:

- i) jakýkoli vnitrostátní upřesňující právní předpis musí splňovat požadavky Listiny základních práv¹⁵ (a nepřekračovat hranice stanovené nařízením, které z Listiny vychází);
- ii) nesmí zasahovat do volného pohybu osobních údajů v rámci EU¹⁶.

V některých případech zavedly členské státy další vnitrostátní požadavky nad rámec nařízení, především prostřednictvím řady odvětvových předpisů, což vede k roztržičnosti a vytváří zbytečnou zátěž. Příkladem dodatečného požadavku zavedeného členským státem nad rámec nařízení je povinnost vyplývající z německých právních předpisů určit pověřence pro ochranu osobních údajů ve společnostech s 20 a více zaměstnanci, které jsou trvale zapojeny do automatického zpracování osobních údajů.

Pokračující úsilí o větší harmonizaci

Komise se zapojuje do dvoustranných dialogů s vnitrostátními orgány, během nichž věnuje zvláštní pozornost vnitrostátním opatřením, která se týkají těchto oblastí:

¹¹ Patří mezi ně např. pravomoc ukládat správní pokuty.

¹² Ke dni 23. července 2019 na přijetí své vnitrostátní právní úpravy dosud pracuje Řecko, Portugalsko a Slovinsko.

¹³ Viz zpráva odborné skupiny různých zúčastněných stran pro nařízení, která byla vydána dne 13. června 2019: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=CS>.

¹⁴ 13 let v Belgii, Dánsku, Estonsku, Finsku, Lotyšsku, na Maltě, ve Švédsku a ve Spojeném království, 14 let v Rakousku, Bulharsku, na Kypru, ve Španělsku, v Itálii a v Litvě, 15 let v Česku a ve Francii, 16 let v Německu, Maďarsku, Chorvatsku, Irsku, Lucembursku, Nizozemsku, Polsku, Rumunsku a na Slovensku.

¹⁵ Článek 8.

¹⁶ V souladu s čl. 16 odst. 2 Smlouvy o fungování Evropské unie.

- účinná nezávislost orgánů pro ochranu údajů, a to i prostřednictvím vhodných finančních, lidských a technických zdrojů,
- jak vnitrostátní právní předpisy omezují práva subjektů údajů,
- skutečnost, že vnitrostátní právní předpisy by neměly zavádět požadavky nad rámec nařízení v situacích, kdy neexistuje rezerva pro specifikaci, např. pro další podmínky pro zpracování,
- splnění povinnosti sjednotit právo na ochranu osobních údajů se svobodou projevu a informací s ohledem na to, že tato povinnost by se neměla zneužívat za účelem odrazování od novinářské práce.

Činnost orgánů pro ochranu údajů spolupracujících v prostředí Evropského sboru pro ochranu osobních údajů (dále jen „sbor“) je klíčovým stimulem k soudržnému uplatňování nových pravidel: kroky v oblasti prosazování, které mají dopad na několik členských států, procházejí mechanismem spolupráce a soudržnosti¹⁷ v rámci sboru a pokyny přijaté sborem přispívají k harmonizovanému výkladu nařízení. Zúčastněné strany nicméně očekávají, že orgány pro ochranu údajů v tomto směru podniknou ještě další kroky.

Činnost vnitrostátních soudů a Soudního dvora Evropské unie také napomáhá k vytvoření soudržného výkladu pravidel ochrany údajů. Vnitrostátní soudy v nedávné době vydaly rozsudky, které ruší platnost ustanovení vnitrostátních právních předpisů, které se od nařízení odchylují¹⁸.

III. Jednotlivé prvky nového správního systému do sebe dobře zapadají

Nařízení vytvořilo novou správní strukturu, která se zaměřuje na nezávislé vnitrostátní orgány pro ochranu údajů jakožto subjekty prosazující nařízení a místa prvního kontaktu pro zúčastněné strany. Ačkoli většina orgánů pro ochranu údajů v uplynulém roce získala větší zdroje, mezi členskými státy přetrvávají velké rozdíly¹⁹.

Orgány pro ochranu údajů využívají své nové pravomoci

Nařízení orgánům pro ochranu údajů uděluje větší donucovací pravomoci. Obavy, které před květnem 2018 vyjadřovaly některé zúčastněné strany, se nevyplnily a vnitrostátní orgány pro ochranu údajů své donucovací pravomoci využívají vyváženým způsobem. Zaměřují se spíše na dialog než na sankce, zejména v případě nejmenších subjektů, pro které zpracování osobních údajů nepředstavuje hlavní činnost. Zároveň se nebály své nové pravomoci účinně použít, kdykoli to bylo nutné, a mimo jiné zahajovaly vyšetřování v oblasti sociálních sítí²⁰.

¹⁷ Článek 60 nařízení stanoví spolupráci mezi orgány pro ochranu údajů, aby se v konkrétních případech uplatňoval jediný výklad nařízení. Článek 64 stanoví, že sbor v určitých případech vydává stanoviska, aby se zajistilo soudržné provádění nařízení. Sbor má rovněž pravomoc přijímat závazná rozhodnutí zaměřená na orgány pro ochranu údajů, pokud mezi nimi nedojde ke shodě.

¹⁸ To je případ Německa a Španělska.

¹⁹ https://edpb.europa.eu/sites/edpb/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

²⁰ Irská komise pro ochranu údajů například zahájila 15 formálních vyšetřování v oblasti dodržování nařízení nadnárodními technologickými společnostmi. Viz s. 49 výroční zprávy irské komise pro ochranu údajů za rok 2018:

a udělovaly správní pokuty ve výši od několika tisíc euro až k několika milionům v závislosti na závažnosti porušení pravidel ochrany údajů.

Příklady pokut udělených orgány pro ochranu údajů²¹:

- 5 000 EUR pro kavárnu provozující sportovní sázky v Rakousku za nezákonný dohled pomocí videokamer,
- 220 000 EUR pro společnost z Polska zprostředkující informace za neinformování osob o tom, že jejich údaje se zpracovávají,
- 250 000 EUR pro španělskou fotbalovou ligu LaLiga za nedostatečně transparentní design aplikace pro chytré telefony,
- 50 milionů EUR pro společnost Google ve Francii za podmínky pro získávání souhlasu uživatelů.

Při provádění vyšetřování je nezbytné, aby orgány pro ochranu údajů shromáždily relevantní důkazy, dodržovaly veškeré procedurální kroky podle vnitrostátních právních předpisů a zajistily náležitý postup u mnohdy složitých spisů. To vyžaduje čas a zahrnuje významný objem práce, což vysvětluje skutečnost, proč většina vyšetřování, jež byla zahájena poté, co nařízení nabylo účinnosti, stále probíhá.

S ohledem na tuto skutečnost by úspěch nařízení neměl být posuzován podle počtu udělených pokut, nýbrž podle změn v kultuře a chování všech zúčastněných stran. V této souvislosti mají orgány pro ochranu údajů k dispozici jiné nástroje, např. uvalení dočasného nebo trvalého omezení zpracování včetně zákazu nebo nařízení pozastavení pohybu údajů směrem k příjemci ve třetí zemi²².

Některé orgány pro ochranu údajů vytvořily nové nástroje, např. telefonní poradny a soubory nástrojů pro podniky, zatímco jiné vyvinuly inovativní přístupy, např. regulační pískoviště²³, jež mají podnikům pomoci při jejich úsilí o dodržování nařízení. Přesto se řada zúčastněných stran (především malé a střední podniky v některých členských státech) domnívá, že se jim nedostalo dostatečné podpory a informací²⁴. Komise s cílem tuto situaci napravit nabízí orgánům pro ochranu údajů dotace, aby se jim dařilo oslovovat zúčastněné strany, především jednotlivce a malé a střední podniky²⁵.

<https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018>.

²¹ Několik rozhodnutí o udělení pokut je stále předmětem soudního přezkoumání.

²² Čl. 58 odst. 2 písm. f) a j).

²³ <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/>.

²⁴ Viz zpráva odborné skupiny různých zúčastněných stran pro nařízení: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=CS>.

²⁵ V roce 2018 byla přidělena částka 2 miliony EUR na činnosti v období 2018–2019 devíti orgánům pro ochranu údajů: Belgie, Bulharsko, Dánsko, Maďarsko, Litva, Lotyšsko, Nizozemsko, Slovinsko a Island: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017>;

v roce 2019 bude rozdělena částka 1 milion EUR:

Evropský sbor pro ochranu osobních údajů funguje

Orgány pro ochranu údajů posílily svou činnost v Evropském sboru pro ochranu osobních údajů²⁶. Tato intenzivní činnost sboru umožnila přijetí přibližně 20 pokynů týkajících se klíčových aspektů nařízení²⁷. Oblasti budoucí činnosti sboru jsou představeny ve dvouletém programu²⁸, jak nařízení vyžaduje.

V přeshraničních případech již orgány pro ochranu údajů nejsou pouze vnitrostátními orgány, nýbrž součástí skutečně celoevropského postupu ve všech fázích od vyšetřování až po rozhodnutí. Taková úzká spolupráce se stala každodenní praxí: do konce června 2019 bylo prostřednictvím mechanismů pro spolupráci řešeno 516 přeshraničních případů.

Komise aktivně přispívá k činnosti sboru²⁹ s cílem podpořit literu a ducha nařízení a připomíná obecné zásady právních předpisů EU³⁰.

Na cestě k vytvoření kultury ochrany údajů v EU

Nový správní systém dosud plně nerealizoval svůj potenciál. Je důležité, aby sbor i nadále zefektivňoval své rozhodování a aby vyvinul společnou kulturu ochrany údajů v EU u všech svých členů. Možnosti, jak mohou orgány pro ochranu údajů spojovat své úsilí³¹ v otázkách týkajících se více než jednoho členského státu, např. při provádění společných vyšetřování a donucovacích opatření, mohou k takovému cíli přispět a zároveň zmírnit dopady omezených zdrojů.

Mnoho zúčastněných stran by si přálo ještě vyšší míru spolupráce a jednotný přístup vnitrostátních orgánů pro ochranu údajů³². Rovněž požadují, aby bylo poradenství poskytované orgány pro ochranu údajů soudržnější³³ a aby byly vnitrostátní pokyny a pokyny sboru plně sjednocené. Některé rovněž očekávají další upřesnění klíčových konceptů nařízení, např. přístupu založeného na posouzení rizik, se zvláštním ohledem na obavy především malých a středních podniků.

V této souvislosti je nezbytné, aby mohly zúčastněné strany lépe přispívat k činnosti sboru. Proto Komise vítá systematické veřejné konzultace, které sbor pro své pokyny organizuje.

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019>.

²⁶ Sbor je právníkou osobou a je složen z ředitelů vnitrostátních dozorových úřadů pro ochranu údajů a evropského inspektora ochrany údajů.

²⁷ https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_cs.

²⁸ https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_cs.

²⁹ Jako účastník bez hlasovacího práva.

³⁰ Komise rovněž pomohla bezproblémovému zřízení sboru a podporuje jeho fungování tím, že zajišťuje jeho komunikační systém.

³¹ Článek 62 nařízení.

³² Viz zpráva odborné skupiny různých zúčastněných stran pro nařízení:

<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670&Lang=CS>.

Podniky se například domnívají, že vnitrostátní seznamy těch druhů operací zpracování, jež podle článku 35 nařízení vyžadují posouzení dopadů na ochranu údajů, mohly být lépe harmonizovány.

³³ A to i mezi různými orgány ve federálních státech.

Tato praxe spolu s pořádáním workshopů pro zúčastněné strany na cílená témata v rané fázi posuzování by měla pokračovat a měla by být rozšířena, aby se zajistila transparentnost, inkluzivnost a relevantnost činnosti sboru.

IV. Fyzické osoby využívají svá práva, ale osvěta by měla pokračovat

Dalším klíčovým cílem nařízení bylo posílit práva fyzických osob. Občanskoprávní asociace a spotřebitelské organizace považují nařízení obecně za významný přínos ke spravedlivé digitální společnosti založené na vzájemné důvěře.

Větší povědomí o právech v oblasti ochrany údajů

Lidé v EU mají čím dál tím vyšší povědomí o pravidlech ochrany údajů a o svých právech: 67 % respondentů průzkumu Eurobarometr z května 2019³⁴ o nařízení ví a 57 % ví, že existuje vnitrostátní orgán pro ochranu údajů, na který se mohou obracet s žádostmi o informace nebo s podáním stížnosti. 73 % respondentů slyšelo alespoň o jednom z práv, která nařízení poskytuje. Řada lidí v EU ovšem stále nepodniká aktivní kroky na ochranu svých osobních údajů, když jsou na internetu. 44 % respondentů například nezměnilo výchozí nastavení ochrany soukromí na sociálních sítích.

Lidé uplatňují stále více svá práva

Toto zvýšené povědomí o právech vedlo Evropany k intenzivnějšímu uplatňování těchto práv prostřednictvím spotřebitelských dotazů a tím, že se častěji obrací na orgány pro ochranu údajů s žádostmi o informace nebo stížnosti³⁵. Podniky rovněž hlásí, že v několika odvětvích, např. v bankovníctví a telekomunikacích, se zvýšil počet žádostí o přístup k osobním údajům. Lidé také často odvolávají svůj souhlas a uplatňují právo vznést námitku proti zasílání komerčních sdělení³⁶.

Některé subjekty ovšem hlásily, že lidé pravidlům ochrany údajů špatně rozumějí – např. se domnívají, že každá osoba musí udělit souhlas s veškerým zpracováním nebo že právo na výmaz je absolutní (přičemž hospodářské subjekty musí např. některé osobní údaje kvůli právním závazkům uchovávat)³⁷. Organizace občanské společnosti si stěžují na dlouhé prodlevy v odpovědích některých podniků a orgánů pro ochranu údajů.

Důležitou informací je, že nevládní organizace zahájily několik zástupných žalob poté, co k tomu byly jednotlivci pověřeny, a využily tak nové možnosti vyplývající z nařízení³⁸. Využití zástupných žalob by bylo snazší, pokud by možnost dovolit nevládním organizacím podávat žaloby bez pověření³⁹, kterou nařízení připouští, využilo více členských států.

³⁴ http://europa.eu/rapid/press-release_IP-19-2956_cs.htm.

³⁵ https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.

³⁶ Viz zpráva odborné skupiny různých zúčastněných stran pro nařízení.

³⁷ Viz zpráva odborné skupiny různých zúčastněných stran pro nařízení.

³⁸ Čl. 80 odst. 1 nařízení.

³⁹ Čl. 80 odst. 2 nařízení.

Dialog a osvěta zaměřené na širokou veřejnost proto musí na vnitrostátní i na unijní úrovni pokračovat. Komise za tímto účelem v červenci 2019 zahájila novou internetovou kampaň⁴⁰, jejímž cílem je povzbudit fyzické osoby k tomu, aby četly prohlášení o ochraně soukromí a přizpůsobovaly si nastavení ochrany soukromí.

V. Podniky upravují své postupy

Cílem nařízení je podpořit podniky v digitální ekonomice pomocí nabídky řešení, která budou fungovat i v budoucnu. Podniky obecně vítají zásadu odpovědnosti vyplývající z nařízení, která se odklání od předchozího zatěžujícího přístupu *ex ante* (odstranění oznamovacích požadavků, škálovatelnost povinností a flexibilita záměrné a standardní ochrany údajů umožňující hospodářskou soutěž na základě řešení zohledňujících soukromí). Některé podniky zároveň požadují vyšší míru právní jistoty a další nebo jasnější pokyny od orgánů pro ochranu údajů⁴¹.

Spolehlivá správa údajů

Ačkoli společnosti informují o řadě potíží při přizpůsobování se novým pravidlům⁴², mnoho společností zdůrazňuje, že nařízení bylo rovněž příležitostí, jak na otázku ochrany údajů upozornit správní rady společností, uspořádat si uchovávané údaje, zlepšit bezpečnost, být lépe připraven na incidenty, snížit vystavování zbytečným rizikům a budovat důvěryhodnější vztahy se spotřebiteli a obchodními partnery. Ohledně transparentnosti podniky a organizace občanské společnosti uvádějí, že je třeba dosáhnout křehké rovnováhy mezi tím, aby fyzickým osobám poskytovaly všechny informace požadované podle nařízení a zároveň používaly jasný a jednoduchý jazyk a formu, jimž budou jednotlivci rozumět. Hospodářské subjekty v tomto směru pracují na inovativních řešeních.

Podniky obecně naznačily, že se jim daří uplatňovat nová práva subjektů údajů, ačkoli kvůli vyššímu počtu žádostí a jejich rozsáhlejší povaze⁴³ bylo někdy náročné dodržet termíny nebo ověřit totožnost osoby podávající žádost.

⁴⁰ Navazuje na předchozí kampaň, která byla zaměřena na šíření informačních materiálů pro jednotlivce a podniky; je dostupná na adrese: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_cs.

⁴¹ Viz zpráva odborné skupiny různých zúčastněných stran pro nařízení.

⁴² Jako jeden z hlavních problémů se často zmiňuje aktualizace IT systému, především pokud jde o uplatňování zásad záměrné a standardní ochrany údajů, práva na výmaz zálohovaných údajů atd.

⁴³ Podniky rovněž žádají o pokyny sboru pro nepodložené žádosti nebo nadměrný počet žádostí.

Dopad na inovace

Nařízení nejen umožňuje, ale přímo podporuje vývoj nových technologií, a zároveň respektuje základní právo na ochranu osobních údajů. To je případ oblastí, jako je např. umělá inteligence.

Podniky začaly vyvíjet nabídku nových služeb, které lépe chrání soukromí. Například vyhledávače, které nesledují uživatele nebo nepoužívají reklamu založenou na chování spotřebitelů, v některých členských státech získávají větší podíly na trhu. Jiné společnosti vyvíjejí služby, které vycházejí z nových práv přiznaných fyzickým osobám, např. přenositelnosti osobních údajů. Čím dál vyšší počet podniků podporuje respektování osobních údajů jako konkurenční výhodu a obchodní přínos. Tento vývoj se neodehrává pouze v EU, nýbrž se dotýká i velmi inovativních zahraničních hospodářství⁴⁴.

Specifická situace „nízkorizikových“ mikropodniků a malých podniků

Situace v jednotlivých členských státech se liší, ovšem mezi zúčastněnými stranami, které kladly nejvíce otázek ohledně provádění nařízení, byly mikropodniky a malé podniky⁴⁵, jejichž hlavní oblastí podnikání není zpracování osobních údajů. Přestože to částečně zřejmě vyplývá z nedostatečného povědomí o pravidlech ochrany údajů, jejich obavy někdy také zhoršují kampaně konzultačních společností, které usilují o získání klientů pro své placené poradenství, jakož i šíření nesprávných informací, např. o potřebě systematicky získávat souhlas fyzických osob⁴⁶, a další požadavky ukládané na vnitrostátní úrovni.

Mikropodniky a malé podniky v této souvislosti žádají o pokyny, které budou přizpůsobeny jejich specifické situaci a poskytnou velmi praktické informace. Některé orgány pro ochranu údajů je již na vnitrostátní úrovni vytvořily⁴⁷. Komise s cílem doplnit vnitrostátní iniciativy vydala informační materiál, který má takovým společnostem pomoci dodržovat nová pravidla prostřednictvím řady praktických kroků⁴⁸.

Využívání souboru nástrojů podle nařízení

Nařízení poskytuje nástroje pro prokázání dodržování předpisů, např. standardní smluvní doložky, kodexy chování a nově zavedené certifikační mechanismy.

Standardní smluvní doložky jsou vzorové doložky, které lze dobrovolně zahrnout do smlouvy, např. mezi správcem údajů a zpracovatelem údajů, a které stanoví povinnosti smluvních stran podle nařízení. Nařízení rozšiřuje možnosti využití standardních smluvních

⁴⁴ Například podle zprávy, kterou zveřejnilo izraelské sdružení pro odvětví kybernetické bezpečnosti, bylo částečně díky nabytí účinnosti nařízení dílčí odvětví „ochrana údajů a soukromí“, spadající do odvětví kybernetické bezpečnosti, nejrychleji rostoucím dílčím odvětvím v roce 2018.

⁴⁵ Jak stanoví definice malých a středních podniků dostupná na této adrese: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_cs.

⁴⁶ Nařízení ve skutečnosti nespočítá pouze na souhlas, nýbrž stanoví i několik zákonných důvodů pro zpracování osobních údajů.

⁴⁷ Např. pokyny vypracované francouzským orgánem pro ochranu údajů: <https://www.cnil.fr/fr/la-cnile-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement>.

⁴⁸ <https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-en-n.pdf>.

doložek jak pro mezinárodní předávání, tak předávání v rámci EU⁴⁹. Jejich rozšířené využívání v oblasti mezinárodního předávání naznačuje⁵⁰, že podnikům při úsilí o dodržování pravidel tyto doložky velmi pomáhají a mají zvláštní přínos pro společnosti, které nemají k dispozici zdroje k vyjednání individuálních smluv s každým ze svých zpracovatelů údajů.

Řada odvětví přijetí standardních smluvních doložek rovněž považuje za užitečný způsob, jak podpořit harmonizaci, především pokud je přijímá Komise. Komise bude spolupracovat se zúčastněnými stranami s cílem využít možnosti, které nařízení nabízí, a aktualizovat stávající doložky.

Dodržování kodexů chování je dalším funkčním a praktickým nástrojem, který má toto odvětví k dispozici, aby mohlo prokázat dodržování nařízení⁵¹. Tyto kodexy by měly být vypracovány obchodními asociacemi nebo orgány zastupujícími kategorii správců a zpracovatelů a měly by popisovat, jak lze v konkrétním odvětví uplatňovat pravidla ochrany údajů. Pokud tyto kodexy vyladí závazky oproti rizikům⁵², mohou se také stát velmi užitečným a nákladově účinným způsobem, jak mohou malé a střední podniky plnit své povinnosti.

Také certifikace může být užitečným nástrojem k prokázání dodržování konkrétních požadavků nařízení. Může zvýšit právní jistotu pro podniky a propagovat nařízení po celém světě. Pokyny pro certifikaci a akreditaci⁵³, které před nedávnem Evropský sbor pro ochranu osobních údajů přijal, umožní vypracování certifikačních schémat v EU. Komise bude tento vývoj sledovat a ve vhodných případech využije pravomoc, kterou jí nařízení uděluje, a stanoví požadavky na certifikaci. Komise může rovněž požádat orgány EU pro normalizaci o normalizaci prvků souvisejících s nařízením.

VI. Vzestupné sbližování pokračuje na mezinárodní úrovni

Poptávka po ochraně osobních údajů není omezena pouze na EU. Jak ukázal nedávný celosvětový průzkum zabývající se bezpečností na internetu, nedostatek důvěry se po celém světě prohlubuje, což mění způsob chování lidí na internetu⁵⁴. Zvyšující se počet společností

⁴⁹ Viz článek 28 nařízení. Standardní smluvní doložky přijaté Komisí jsou platné v celé EU. Naproti tomu doložky přijaté podle čl. 28 odst. 8 orgánem pro ochranu údajů jsou závazné pouze pro orgán, který je přijal, a mohou být tedy použity jako standardní smluvní doložky pro operace zpracování, pro které je daný orgán příslušným orgánem podle článků 55 a 56.

⁵⁰ Ve skutečnosti jsou hlavním nástrojem, na který se společnosti při exportu údajů spoléhají.

⁵¹ Evropský sbor pro ochranu osobních údajů přijal pokyny pro kodexy chování dne 4. června 2019. Ty upřesňují postupy a pravidla spojená s předložením, schválením a vydáním kodexů na vnitrostátní i unijní úrovni.

⁵² 98. bod odůvodnění nařízení.

⁵³ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_cs;
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_cs.

⁵⁴ Viz celosvětový průzkum společností CIGI a Ipsos z roku 2019 o bezpečnosti a důvěře na internetu. Podle tohoto výzkumu si 78 % respondentů dělá starosti ohledně svého soukromí na internetu, 49 % uvedlo, že jejich nedůvěra je vedla k tomu, že na internetu sdílejí méně osobních informací, zatímco 43 % uvedlo, že si dávají více záležet na zabezpečení svého zařízení, a 39 % odpovědělo, že kromě jiných preventivních

kvůli těmto obavám rozšiřuje svou vlastní volbu práv stanovených nařízením i na zákazníky mimo EU.

Kromě toho platí, že zároveň s tím, jak se čím dál více zemí po celém světě podobnými problémy zabývá, zavádějí nová pravidla ochrany údajů nebo modernizují ta stávající. Tyto zákony mají často řadu společných prvků, které jsou zahrnuty i v režimu EU na ochranu údajů, např. zastřešující právní předpis spíše než odvětvová pravidla, vynutitelná práva osob a nezávislý dozorový úřad. Tato tendence je skutečně celosvětová a objevuje se od Jižní Korey po Brazílii, od Chile po Thajsko, od Indie po Indonésii. Dalším jasným znamením tohoto sblížování je čím dál globálnější členství v „úmluvě č. 108“⁵⁵ Rady Evropy (tato úmluva byla v nedávné době za významného přispění Komise modernizována⁵⁶).

Podpora bezpečného a volného pohybu údajů nejen pomocí rozhodnutí o odpovídající ochraně

Toto rozvíjející se sblížování nabízí nové příležitosti, jak usnadnit pohyb údajů, a tím i obchod a spolupráci mezi veřejnými orgány, a zároveň zlepšuje úroveň ochrany osobních údajů jednotlivců v EU, pokud dochází k jejich předání do zahraničí.

Díky provádění strategie stanovené ve sdělení z roku 2017 o výměně a ochraně údajů v globalizovaném světě⁵⁷ Komise posílila své zapojení ve třetích zemích a s jinými mezinárodními partnery a dále rozvíjí prvky sblížování mezi systémy soukromí, ze kterých zároveň čerpá. To zahrnovalo i prozkoumání možnosti uznání odpovídající ochrany s vybranými třetími zeměmi⁵⁸. Tato činnost přinesla významné výsledky – zejména vstoupilo v únoru 2019 v platnost vzájemné ujednání o odpovídající ochraně mezi EU a Japonskem, díky němuž vznikl největší prostor volného a bezpečného pohybu údajů na světě. Jednání s Jižní Koreou o odpovídající ochraně jsou v pokročilé fázi a probíhá průzkum s cílem zahájit tato jednání s několika latinskoamerickými zeměmi – např. Chile nebo Brazílií – v závislosti na dokončení probíhajících legislativních postupů. Slibný je i vývoj v některých částech Asie, např. v Indii, Indonésii a na Tchaj-wanu, i v evropském východním a jižním sousedství, což by mohlo otevřít dveře pro budoucí rozhodnutí o odpovídající ochraně.

opatření používají internet selektivněji. Průzkum byl proveden v 25 hospodářstvích: Austrálii, Brazílii, Kanadě, Číně, Egyptě, Francii, Německu, Velké Británii, Hongkongu, Indii, Indonésii, Itálii, Japonsku, Keni, Mexiku, Nigérii, Pákistánu, Polsku, Rusku, Jižní Africe, Korejské republice, Švédsku, Tunisku, Turecku a Spojených státech.

⁵⁵ Úmluva Rady Evropy ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních údajů (ETS č. 108) a dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat, o orgánech dozoru a toku dat přes hranice z roku 2001 (ETS č. 181). Toto je jediný závazný mnohostranný nástroj v oblasti ochrany údajů. Posledními zeměmi, které úmluvu ratifikovaly, jsou Argentina, Mexiko, Kapverdy a Maroko.

⁵⁶ Protokol o změně Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat (ETS č. 108) podle dohody ze 128. zasedání výboru ministrů v Helsinku v Dánsku, 17.–18. května 2018. Konsolidované znění modernizované úmluvy č. 108 je dostupné na adrese: <https://rm.coe.int/16808ade9d>.

⁵⁷ Sdělení Komise Evropskému parlamentu a Radě s názvem „Výměna a ochrana osobních údajů v globalizovaném světě“, COM/2017/07 final.

⁵⁸ Nařízení rovněž v rámci úsilí EU o usnadnění výměn údajů s mezinárodními organizacemi umožnilo uznat odpovídající ochranu v souvislosti s těmito subjekty.

Komise zároveň vítá, že další země zavedly nástroje pro předávání podobné nástrojům pro odpovídající ochranu stanoveným v nařízení, čímž uznávají, že EU sama i země, v nichž EU považuje ochranu za odpovídající, zajišťují požadovanou úroveň ochrany⁵⁹. Vznikl tak potenciál vytvořit síť zemí, ve kterých je možný volný pohyb údajů.

Kromě toho probíhá intenzivní spolupráce s dalšími třetími zeměmi, např. Kanadou, Novým Zélandem, Argentinou a Izraelem, jejímž cílem je zajistit, aby platnost rozhodnutí o odpovídající ochraně přijatých na základě směrnice o ochraně údajů z roku 1995 pokračovala i v rámci nařízení. Mezitím se štít mezi EU a USA pro ochranu osobních údajů ukázal jako užitečný nástroj pro zajištění transatlantických pohybů údajů na základě vysoké úrovně ochrany, do kterého je zapojeno více než 4 700 společností⁶⁰. Jeho každoroční přezkoumání zajišťuje pravidelnou kontrolu správného fungování tohoto rámce a včasné řešení nových problémů.

Protože pro pohyb údajů neexistuje jediné univerzální řešení, Komise rovněž spolupracuje se zúčastněnými subjekty i se sborem na využití celého potenciálu souboru nástrojů pro mezinárodní předávání vyplývajících z nařízení. Mezi tyto nástroje patří standardní smluvní doložky, vývoj certifikačních schémat, vypracování kodexů chování nebo administrativní ujednání pro veřejné orgány. V této souvislosti se Komise zajímá o výměnu zkušeností a osvědčených postupů s jinými systémy, které mohou mít pro některé z těchto nástrojů vyvinuté konkrétní odborné poznatky. Komise zváží využití pravomocí, které jí nařízení uděluje v oblasti těchto nástrojů pro předávání, především standardních smluvních doložek.

Kromě čistě dvoustranných nástrojů by také bylo vhodné se zabývat tím, zda by podobně naladěné země mohly v této oblasti zřídit nadnárodní rámec, když pohyb údajů představuje čím dál tím zásadnější složku obchodu, komunikací a sociálních interakcí. Takový nástroj by umožnil volný pohyb údajů mezi smluvními stranami a zároveň zajistil požadovanou úroveň ochrany na základě sdílených hodnot a sbližujících se systémů. Bylo by možné jej vypracovat například na základě modernizované úmluvy č. 108 nebo díky inspiraci z iniciativy Data Free Flow with Trust („důvěryhodný volný pohyb údajů“), která byla počátkem tohoto roku zahájena v Japonsku.

Rozvoj nových synergií mezi obchodem a nástroji na ochranu údajů

Kromě podpory sbližování norem ochrany údajů na mezinárodní úrovni je Komise rovněž odhodlána řešit digitální protekcionismus. Za tímto účelem vypracovala specifická ujednání o tocích údajů a ochraně údajů v obchodních dohodách, která při svých dvoustranných i mnohostranných jednáních systematicky předkládá, např. při právě probíhajících jednáních s WTO o elektronickém obchodu. Tato horizontální ujednání vylučují čistě protekcionistická opatření, např. požadavky na povinnou lokalizaci údajů, a zároveň zachovávají regulační samostatnost stran při ochraně základního práva na ochranu údajů.

⁵⁹ Tento postoj zaujaly například Argentina, Kolumbie, Izrael a Švýcarsko.

⁶⁰ To znamená, že do štítu pro ochranu osobních údajů je za první tři roky jeho existence zapojeno více společností než do předcházejícího nástroje „bezpečného přístavu“ – po 13 letech fungování.

Ačkoli dialogy o ochraně údajů a obchodní jednání musí probíhat samostatně, mohou se navzájem doplňovat: vzájemné ujednání o odpovídající ochraně mezi EU a Japonskem je nejlepším příkladem takových synergií, které ještě více usnadňují obchodní výměny, a tím posilují přínosy dohody o hospodářském partnerství. Tento druh sbližování založený na sdílených hodnotách a vysokých standardech a podpořený účinným prosazováním poskytuje nejspolehlivější základ pro výměnu osobních údajů, což naši mezinárodní partneři čím dál tím častěji uznávají⁶¹. Vzhledem k tomu, že společnosti působí čím dál více přes hranice a preferují uplatňování podobných souborů pravidel ve všech svých podnikatelských aktivitách po celém světě, pomáhá takové sbližování vytvářet prostředí, které podporuje přímé investice, usnadňuje obchod a zlepšuje důvěru mezi obchodními partnery.

Usnadňování výměny informací za účelem boje proti zločinu a terorismu na základě vhodných pojistek

Větší kompatibilita režimů ochrany údajů může rovněž významně usnadnit velmi potřebné výměny informací mezi EU a zahraničními regulačními, policejními a soudními orgány, a díky tomu přispět k účinnější a rychlejší spolupráci v oblasti prosazování práva⁶². Za tímto účelem Komise uvažuje o využití možnosti přijímat rozhodnutí o odpovídající ochraně v souladu se směrnicí o prosazování práva v oblasti ochrany údajů s cílem prohloubit spolupráci s klíčovými partnery v boji proti trestné činnosti a terorismu. Zastřešující dohodu mezi EU a USA⁶³, která vstoupila v platnost v únoru 2017, kromě toho lze použít jako vzor pro podobné dohody s jinými důležitými bezpečnostními partnery.

Další příklady, které ukazují na význam vysokých standardů ochrany údajů jako na základ stabilní spolupráce v oblasti prosazování práva se třetími zeměmi, zahrnují předávání záznamů ze jmenné evidence cestujících (PNR)⁶⁴ a výměnu operativních informací mezi Europolem a důležitými mezinárodními partnery. V této souvislosti právě probíhají jednání

⁶¹ Tato skutečnost byla uvedena např. ve zmínce o konceptu Data Free Flow with Trust v prohlášení vedoucích představitelů zemí G20 z Ósaky:

https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

⁶² Viz sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů s názvem „Evropský program pro bezpečnost“, COM(2015) 185 final.

⁶³ Dohoda mezi EU a USA o ochraně osobních údajů při jejich předávání a zpracování za účelem předcházení, vyšetřování, odhalování a stíhání trestných činů včetně terorismu v rámci policejní spolupráce a soudní spolupráce v trestních věcech: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A22016A1210%2801%29> (dále jen „zastřešující dohoda“). Zastřešující dohoda představuje první dvoustrannou mezinárodní dohodu v oblasti vymáhání práva, která poskytuje komplexní soubor práv a povinností v oblasti ochrany údajů v souladu s *acquis* EU. Jedná se o úspěšný příklad toho, jak lze posílit spolupráci s důležitým mezinárodním partnerem v oblasti prosazování práva díky vyjednání silného souboru pojistek v oblasti ochrany údajů.

⁶⁴ Rezoluce Rady bezpečnosti OSN č. 2396 ze dne 21. prosince 2017 vyzývá všechny členské státy OSN, aby vyvinuly schopnost shromažďovat, zpracovávat a analyzovat údaje PNR za plného dodržování lidských práv a základních svobod. Viz též sdělení Komise s názvem „Evropský program pro bezpečnost“, COM(2015) 185 final: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52015DC0185&qid=1564043138492&from=EN>.

o mezinárodních dohodách s několika zeměmi jižního sousedství nebo je jejich zahájení připraveno⁶⁵.

Silné pojistky v oblasti ochrany údajů budou také zásadní složkou jakékoli budoucí dohody o přeshraničním přístupu k elektronickým důkazům při vyšetřování trestných činů, a to jak na dvoustranné (dohoda mezi EU a USA), tak na mnohostranné úrovni (druhý dodatkový protokol k Budapešťské úmluvě Rady Evropy o počítačové kriminalitě)⁶⁶.

Podpora spolupráce mezi donucovacími orgány pro ochranu údajů

V době, kdy mohou problémy s dodržováním ochrany soukromí nebo bezpečnostní incidenty ovlivnit velký počet osob zároveň ve více jurisdikcích, mohou užší formy spolupráce mezi dozorovými úřady na mezinárodní úrovni pomoci zajistit jak účinnější ochranu jednotlivých práv, tak stabilnější prostředí pro hospodářské subjekty. V této souvislosti a v úzkém kontaktu se sborem bude Komise pracovat na způsobech, jak usnadnit spolupráci v oblasti vymáhání a vzájemnou pomoc mezi dozorovými úřady v EU i za jejími hranicemi, a to i prostřednictvím využití nových pravomocí, které jí nařízení v této oblasti přiděluje⁶⁷. To by mohlo zahrnovat různé formy spolupráce od vypracování společných výkladových nebo praktických nástrojů⁶⁸ až po výměny informací o probíhajících vyšetřováních.

Komise má rovněž v plánu posílit dialog s regionálními organizacemi a sítěmi, např. Sdružením národů jihovýchodní Asie (ASEAN), Africkou unií, fórem asijsko-tichomořských orgánů pro ochranu soukromí (APPA) nebo Iberoamerickou sítí pro ochranu údajů, jež hrají ve formování společných norem v oblasti ochrany údajů čím dál tím důležitější úlohu, podporují výměnu osvědčených postupů i spolupráci mezi donucovacími orgány. Kromě toho bude spolupracovat také s Organizací pro hospodářskou spolupráci a rozvoj a Asijsko-tichomořskou organizací pro hospodářskou spolupráci s cílem posilovat přibližování k vysoké úrovni ochrany údajů.

VII. Právní předpisy v oblasti ochrany údajů jakožto nedílná součást celé řady politik

Ochranu osobních údajů zajišťuje a obsahuje řada politik Unie.

Telekomunikační služby a služby elektronické komunikace

Komise v lednu 2017 přijala návrh nařízení o ochraně soukromí a ochraně osobních údajů v elektronických komunikacích⁶⁹. Cílem návrhu je chránit důvěrnost komunikace, jak stanoví

⁶⁵ https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en.

⁶⁶ http://europa.eu/rapid/press-release_IP-19-2891_en.htm.

⁶⁷ Viz článek 50 nařízení týkající se mezinárodní spolupráce v oblasti ochrany údajů. Toto ustanovení zahrnuje celou řadu forem spolupráce, od informací o právních předpisech pro oblast ochrany údajů až po postupování stížností a pomoc při vyšetřování.

⁶⁸ Např. společné šablony pro oznámení o porušení zabezpečení.

⁶⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>.

Listina základních práv, ale také chránit osobní údaje, které mohou být součástí komunikace, i koncová zařízení koncových uživatelů.

Návrh nařízení o ochraně soukromí a elektronických komunikacích upřesňuje a doplňuje nařízení tím, že pro výše uvedené účely stanoví specifická pravidla. Modernizuje současná pravidla EU ohledně soukromí a elektronických komunikací⁷⁰ s cílem zohlednit technologický a právní vývoj. Posiluje soukromí osob tím, že rozšiřuje oblast působnosti nových pravidel tak, aby se vztahovala i na poskytovatele komunikačních služeb typu over-the-top, čímž vytváří rovné podmínky pro všechny služby elektronických komunikací. Ačkoli Evropský parlament v říjnu 2017 schválil mandát k zahájení dialogů, Rada dosud obecný přístup neschválila. Komise se v nařízení o soukromí a elektronických komunikacích i nadále plně angažuje a podpoří spolunormotvůrce v jejich úsilí o dosažení rychlého přijetí navrhovaného nařízení.

Zdravotnictví a výzkum

V oblasti veřejného zdraví se z důvodů obecného zájmu stává čím dál tím důležitějším usnadnit mezi členskými státy výměnu zdravotních údajů, které podle nařízení spadají do kategorie citlivých údajů. Mezi tyto důvody patří poskytování zdravotní péče či léčby, ochrana před vážnými přeshraničními zdravotními hrozbami a zajištění vysokých norem kvality a bezpečnosti zdravotní péče a léčivých přípravků či zdravotnických prostředků. Nařízení stanoví pravidla, která zajistí zákonné a důvěryhodné zpracování a výměny zdravotních údajů napříč EU. Tato pravidla se uplatní i při přístupu třetích stran k lékařským údajům pacientů, a to včetně údajů uvedených v patientských souhrnech, elektronických receptech a v dlouhodobém horizontu i v komplexní elektronické zdravotní dokumentaci, jakož i při jejich využití pro účely vědeckého výzkumu. V konkrétní oblasti klinických hodnocení Komise rovněž připravila zvláštní soubor častých otázek a odpovědí týkajících se vzájemného působení nařízení o klinických hodnoceních⁷¹ a obecného nařízení o ochraně osobních údajů⁷².

Umělá inteligence

Se zvyšujícím se strategickým významem umělé inteligence se stává nezbytným formovat celosvětová pravidla pro její vývoj a využívání. Komise se při podpoře vývoje a zavádění umělé inteligence rozhodla pro přístup zaměřený na člověka, což znamená, že použití umělé inteligence musí být v souladu se základními právy⁷³. Pravidla stanovená nařízením v této

⁷⁰ 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).

⁷¹ <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32014R0536>.

⁷² https://ec.europa.eu/health/sites/health/files/documents/qa_clinicaltrials_gdpr_en.pdf.

⁷³ Sdělení Komise ze dne 8. dubna 2019 o budování důvěry v umělou inteligenci zaměřenou na člověka: <https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence>.

Etické pokyny pro důvěryhodnou umělou inteligenci představené dne 8. dubna 2019 odbornou skupinou na vysoké úrovni: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>. Viz též doporučení Rady OECD k umělé inteligenci: <https://legalinstruments.oecd.org/en/instruments/OECD->

souvislosti poskytují obecný rámec a obsahují konkrétní povinnosti a práva, jež jsou pro zpracování osobních údajů umělou inteligencí obzvláště důležité. Nařízení například obsahuje právo nebyt předmětem rozhodnutí založeného výhradně na automatickém zpracování (s výjimkou určitých situací)⁷⁴. Rovněž obsahuje konkrétní požadavky na transparentnost při používání automatizovaného rozhodování, konkrétně povinnost informovat o existenci takových rozhodnutí a poskytnout smysluplné informace a vysvětlit jejich význam, jakož i předpokládané důsledky takového zpracování pro danou osobu⁷⁵. Tyto hlavní zásady nařízení byly uznány odbornou skupinou na vysoké úrovni pro umělou inteligenci⁷⁶, Organizací pro hospodářskou spolupráci a rozvoj⁷⁷ a skupinou G20⁷⁸ jako obzvláště důležité pro řešení problémů a příležitostí vznikajících v souvislosti s umělou inteligencí. Evropský sbor pro ochranu osobních údajů určil umělou inteligenci za jedno z možných témat svého pracovního programu na období 2019–2020⁷⁹.

Doprava

Vývoj propojených automobilů a inteligentních měst se čím dál tím více spoléhá na zpracování a výměny velkých množství osobních údajů mezi více stranami, včetně automobilů, jejich výrobců, poskytovatelů telematických služeb a veřejných orgánů odpovědných za silniční infrastrukturu. Toto mnohostranné prostředí s sebou přináší určitou komplexnost, pokud jde o přidělování rolí a povinností jednotlivým subjektům zapojeným do zpracování osobních údajů a o způsob, jakým se zajistí zákonnost zpracování všemi subjekty. Dodržování nařízení a právních předpisů ohledně soukromí a elektronických komunikací je nezbytné pro úspěšné zavedení inteligentních dopravních systémů ve všech druzích dopravy a pro šíření digitálních nástrojů a služeb umožňujících vyšší míru mobility osob a zboží⁸⁰.

Energetika

Vývoj digitálních řešení v odvětví energetiky se čím dál tím častěji spoléhá na zpracování osobních údajů. Právní předpisy, které byly schváleny v rámci balíčku opatření nazvaného Čistá energie pro všechny Evropany⁸¹, zahrnují nová ustanovení, která umožňují digitalizaci odvětví energetiky, a pravidla pro přístup k údajům, správu údajů a vzájemnou provázanost. Díky tomu je možné spravovat údaje spotřebitelů v reálném čase za účelem dosažení úspor

[LEGAL-0449](#), zásady skupiny G20 pro umělou inteligenci podpořené jako součást prohlášení vedoucích představitelů zemí G20 z Ósaky: https://www.g20.org/pdf/documents/en/annex_08.pdf a prohlášení ministrů G20 o obchodu a digitální ekonomice: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

⁷⁴ Článek 22 nařízení.

⁷⁵ Čl. 13 odst. 2 písm. f) nařízení.

⁷⁶ <https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence>.

⁷⁷ Doporučení Rady týkající se umělé inteligence: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

⁷⁸ Prohlášení ministrů G20 o obchodu a digitální ekonomice:

https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

⁷⁹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_cs.pdf.

⁸⁰ Například usnadněním jejich plánování a používání různých dopravních prostředků v průběhu cesty.

⁸¹ Jedná se zejména o směrnici o elektrické energii:

<https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32009L0072>.

a podpory vlastní výroby a účasti na energetickém trhu. Dodržování pravidel ochrany údajů je proto pro úspěšné provádění těchto ustanovení velmi důležité.

Hospodářská soutěž

Zpracování osobních údajů je záležitost, kterou je třeba v čím dál vyšší míře zohledňovat v politice hospodářské soutěže⁸². Vzhledem k tomu, že orgány pro ochranu údajů jsou jedinými orgány, které jsou pověřeny posuzováním porušení pravidel ochrany údajů, spolupracují orgány na ochranu hospodářské soutěže, spotřebitelů a údajů mezi sebou a budou tak činit v případě potřeby i nadále, pokud dojde k propojení jejich příslušných oblastí působnosti. Komise bude takovou spoluprací podporovat a pozorně sledovat její vývoj.

Volební kontext

Komise ve svých pokynech pro používání osobních údajů ve volebním kontextu⁸³ vydaných v září 2018 jako součást volebního balíčku⁸⁴ upozornila na obzvláště důležitá pravidla pro subjekty zapojené do voleb, včetně otázek týkajících se cílení na jednotlivé voliče. Tyto pokyny byly připomenuty v prohlášení Evropského sboru na ochranu osobních údajů⁸⁵ a řada orgánů pro ochranu údajů vydala pokyny na vnitrostátní úrovni. Volební balíček obsahoval i výzvu každému členskému státu ke zřízení vnitrostátní volební sítě zahrnující vnitrostátní orgány odpovědné za volební otázky a za sledování a prosazování pravidel, např. v oblasti ochrany údajů nebo činností na internetu týkajících se voleb. Byla rovněž přijata nová opatření, jejichž cílem je zavést sankce za porušování pravidel ochrany údajů evropskými politickými stranami a nadacemi. Komise vydala doporučení, aby členské státy zaujaly stejný přístup i na vnitrostátní úrovni. Aspekty ochrany údajů zohlední rovněž hodnocení voleb do Evropského parlamentu 2019, které má být zveřejněno v říjnu 2019.

Prosazování práva

Účinná a skutečná bezpečnostní unie může být vybudována pouze za úplného dodržování základních práv ukotvených v Listině EU a v sekundárních právních předpisech EU, včetně odpovídajících záruk v oblasti ochrany údajů, jež mají umožnit bezpečnou výměnu osobních údajů pro účely prosazování práva. Pokud má dojít k jakémukoli omezení základního práva na soukromí a ochranu údajů, je třeba ověřit, že jsou tato omezení nezbytně nutná a přiměřená.

⁸² Např. věc Apple/Shazam, M.8788 a věc Microsoft/LinkedIn, M.8124.

⁸³ <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52018DC0638&qid=1563875255437&from=EN>.

⁸⁴ http://europa.eu/rapid/press-release_IP-18-5681_cs.htm.

⁸⁵ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

VIII. Závěr

Na základě informací, které jsou v současnosti dostupné, a dialogu se zúčastněnými stranami dospěla Komise k předběžnému závěru, že první rok uplatňování nařízení byl celkově pozitivní. Jak toto sdělení ovšem ukazuje, v řadě oblastí je nutný další pokrok.

Provádění a doplňování právního rámce:

- Tři členské státy, které dosud neaktualizovaly své vnitrostátní právní předpisy na ochranu údajů, tak musí bezodkladně učinit. Všechny členské státy by měly dokončit sjednocení svých odvětvových právních předpisů s požadavky nařízení.
- Komise využije všech nástrojů, které má k dispozici, včetně řízení o nesplnění povinnosti, aby zajistila, že členské státy nařízení dodržují, a omezila jakoukoli roztržičnost rámce na ochranu údajů.

Využití celého potenciálu nového správního systému:

- Členské státy by vnitrostátním orgánům pro ochranu údajů měly přidělit dostatečné lidské, finanční a technické zdroje.
- Orgány pro ochranu údajů by měly posílit vzájemnou spolupráci, např. v podobě společných vyšetřování. Členské státy by provádění takových vyšetřování měly usnadnit.
- Sbor by měl dále rozvíjet kulturu EU v oblasti ochrany údajů a plně využívat nástroje, které nařízení poskytuje, aby zajistil harmonizované uplatňování pravidel. Měl by i nadále pracovat na pokynech, zejména pro malé a střední podniky.
- Odborné poznatky sekretariátu sboru je třeba posílit za účelem účinnější podpory a účinnějšího vedení činnosti sboru.
- Komise bude i nadále podporovat orgány pro ochranu údajů a sbor, především aktivní účastí na činnosti sboru a upozorňováním na požadavky vyplývající z právních předpisů EU v průběhu provádění nařízení.
- Komise bude podporovat interakci mezi orgány pro ochranu údajů a jinými orgány, zejména v oblasti ochrany hospodářské soutěže, a zároveň plně respektovat jejich příslušné oblasti působnosti.

Podpora a zapojení zúčastněných stran:

- Sbor by měl posílit způsob, jakým do své činnosti zapojuje zúčastněné strany. Komise bude pokračovat ve finanční podpoře orgánů pro ochranu údajů, aby jim pomohla oslovit zúčastněné strany.
- Komise bude pokračovat ve své osvětové činnosti a ve své práci se zúčastněnými stranami.

Podpora sbližování na mezinárodní úrovni:

- Komise bude i nadále posilovat dialog o odpovídající ochraně se způsobilými klíčovými partnery, a to i v oblasti prosazování práva. Jejím cílem je zejména v nadcházejících měsících uzavřít probíhající jednání s Jižní Koreou. V roce 2020 bude informovat o přezkumu 11 rozhodnutí o odpovídající ochraně přijatých podle směrnice o ochraně údajů.
- Komise bude pokračovat ve své činnosti, a to i v podobě technické pomoci, výměny informací a osvědčených postupů, se zeměmi, jež mají zájem o přijetí moderních právních předpisů na ochranu soukromí, a podporovat spolupráci s dozorovými úřady a regionálními organizacemi třetích zemí.
- Komise se spojí s mnohostrannými a regionálními organizacemi s cílem podporovat vysoké standardy ochrany údajů jako faktor umožňující obchod a usnadňující spolupráci (např. v rámci iniciativy Data Free Flow with Trust, která byla spuštěna v Japonsku v kontextu skupiny G20).

Nařízení⁸⁶ Komisi ukládá povinnost, aby v roce 2020 informovala o jeho provádění. To bude příležitostí k posouzení dosaženého pokroku a skutečnosti, zda jsou různé prvky nového režimu na ochranu údajů po dvou letech uplatňování plně funkční. Za tímto účelem Komise zapojí Evropský parlament, Radu, členské státy, Evropský sbor na ochranu osobních údajů, příslušné zúčastněné strany a občany.

⁸⁶ Článek 97 nařízení.