Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Technická opatření pro plnění GDPR

Bakalářská práce

Autor: Leoš Karásek
Studijní obor: Aplikovaná Informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové Červenec 2019

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 1.8.2019 Leoš Karásek

Poděkování:
Děkuji vedoucímu bakalářské práce, Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, věcné připomínky, dobré rady a vstřícnost při konzultacích a vypracovávání bakalářské práce.

Anotace

KARÁSEK, Leoš. *Technická opatření pro plnění GDPR.* Hradec Králové: Fakulta informatiky a managementu Univerzity Hradec Králové, 2007. 87 s. Bakalářská práce.

Cílem této práce je posouzení dopadů „*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)*“, známé zejména jako obecné nařízení „Evropské unie o GDPR“ na správce informačních systémů podniku a možných technických opatření, vedoucích k naplnění tohoto obecného nařízení.

Povinnosti plynoucí z tohoto nařízení zasáhnou všechny podnikatelské subjekty všech velikostí a napříč všemi obory. Práce si klade za cíl zorientovat se v nařízení GDPR a navrhnout možná technická opatření k nakládání s daty občanů EU, vedoucích ke splnění podmínek plynoucích z obecného nařízení GDPR.

Hlavní přínos této práce spočívá v analýze obecného nařízení a povinnosti z něj plynoucích, následně pak v návrhu možných technických řešení ke splnění požadavků obecného nařízení pro podnikatelské subjekty napříč obory.

Annotation

Title: Technical measures for GDPR implementation

The goal of this Bachelors Theses is evaluation impacts of GDPR regulation to IT administrators of companies and technical steps to fulfill the directive GDPR(General Data Protection Regulation)..

The obligations under this Regulation will affect all business entities of all sizes and across all disciplines. The goal of this Bachelor theses is to orientate in the GDPR Regulation and to propose possible technical measures to handle the data of EU citizens leading to the fulfillment of the conditions under the General Regulation GDPR.

The main value of this work is in analyze of General Regulation GDPR obligations with impact to technical solution in companies IT infrastructure. And propose possible technical solutions necessary to fulfill the conditions under GDPR for companies across all segments of the business.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Dne 25. 5. 2018 vstoupilo v platnost *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)*“, známé spíše jako nařízení GDPR (General Data Protection Regulation).

Vzhledem ke stále se rozvíjející informační společnosti se data o lidech stávají velmi žádaným a ceněným obchodním artiklem. Tato data jsou na druhou stranu osobní a velmi citlivá. Žádný subjekt by bez souhlasu dotyčného nebo bez zákonné opory neměl taková data shromažďovat a využívat.

Jednotlivé státy Evropské unie tuto problematiku nejprve upravovaly ve vlastních národních legislativách, nakonec se ale ukázala potřeba jednotné regulace této problematiky.

2 Cíl práce

Cílem této práce je analyzovat NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, neboli směrnici GDPR. Nalézt ve směrnici části, které mohou mít dopad na technická opatření správců informačních technologii. Anebo naopak najít taková technická řešení, která pomohou podnikům naplnit požadavky obecného nařízení GDPR.

A nakonec navrhnout možná technická opatření.

Měla by tedy zodpovědět otázky:

Jaké bude mít technické dopady obecné nařízení GDPR na správce informačních technologií v podnicích? A jaké jsou možnosti řešení těchto dopadů?

3 Metodika zpracování

Prace se zabývá dvěma otázkami. Jsou to: Jaké bude mít technické dopady obecného nařízení GDPR na správce informačních technologií v podnicích? A jaké jsou možnosti řešení těchto dopadů?

První z otázek bude zodpovězena analýzou obecného nařízení GDPR.

Druhá z otázek bude vyřešena rešerší a následným návrhem jedné z možných cest.

4 Představení GDPR

4.1 Historie

Ochrana osobních údajů není v Evropské Unii (dále EU) samozřejmě nic nového, do května 2018 byla platná směrnice 95/46/ES o ochraně údajů z roku 1995. Tato směrnice ale řešila v podstatě pouze dva cíle: Ochranu osobních údajů, a jejich volný pohyb mezi členskými státy.

Směrnice je však stará více než 25 let a nepočítá např. s rozmachem sociálních sítí anebo cloudových úložišť.

Technický pokrok se však nezastaví a původní směrnice se stala brzo zastaralou. Nedokázala reflektovat nové potřeby problematiky ochrany osobních údajů, a proto bylo nutné vypracovat směrnici novou.

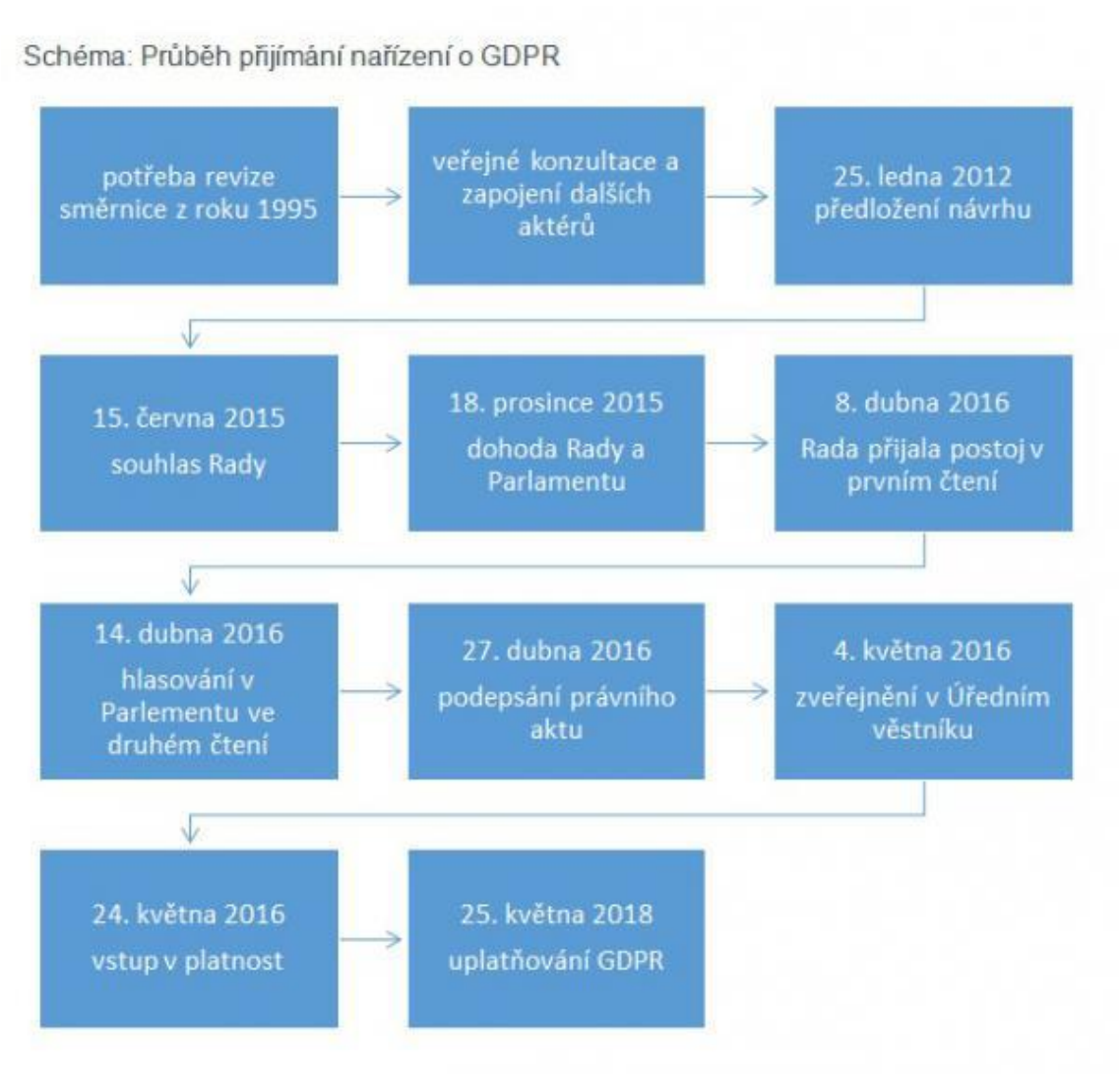
Jak uvádí server euroskop.cz, největším problémem původní směrnice byla její zastaralost a dále pak zjištění, že některé státy mimo EU shromažďují údaje o jejích občanech.

Právo na řádnou ochranu osobních údajů občanů je navíc garantováno Základní listinou práv EU jako jedno ze základních práv a také Lisabonskou smlouvou.

Nejprve tedy v roce 2009 až 2010 probíhaly diskuze o právním rámci pro základní právo na ochranu osobních údajů, konzultace o komplexním přístupu Komise k ochraně osobních údajů v EU, workshopy a semináře, kdy se k problematice mohli vyjadřovat orgány veřejné moci, soukromé organizace ale i občané.

Následně 25. 1. 2012 Evropská komise představila návrh směrnice, který byl projednáván v institucích EU do roku 2015, kdy rada dosáhla tzv. obecného přístupu, tedy v podstatě politické dohody.

Na začátku dubna 2016 novou směrnici schválil Evropský parlament. Následně bylo obecné nařízení 27. 4. 2015 podepsáno a účinnosti nabylo dne 25. 5. 2018.



Obrázek 1 - Průběh přijímaní nařízení o GDPR

Zdroj: KOMÍNKOVÁ, Magda. Jak vznikalo nařízení o ochraně osobních údajů (GDPR)?. *Euroskop.cz* [online]. 2018 [cit. 2018-09-27]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/

4.2 Co to vlastně je?

Díky ohromnému technologickému pokroku je lidstvo schopno sbírat a v poslední době už i relevantně analyzovat ohromné množství dat. Tím ale může docházet k podstatným zásahům do soukromí lidí a k zneužívání dat, která nazýváme osobními údaji. Všechny státy, kterým záleží na ochraně vlastních občanů, se nějakým způsobem snaží řešit ochranu osobních údajů. V naší zemi například zákonem 101/2000 Sb.

Nařízení GDPR má zejména harmonizovat pravidla pro nakládání s osobními údaji občanů EU a upravit pravidla pro případně nakládaní s těmito údaji mimo území EU.

Toto obecné nařízení na jedné straně dává občanům právo vědět, kdo a jaké osobní údaje o nich vede a v některých případech rozhodovat o tom, zda se mohou nadále využívat. A na druhou stranu nutí podniky mít v osobních údajích přehled a pořádek.

GDPR tedy především harmonizuje pravidla pro nakládání s osobními údaji napříč EU.

Zde je pro zajímavost uveden výňatek z desatera omylů, zpracovaných Úřadem pro ochranu osobních údajů

„ GDPR je revoluce

Není tomu tak; jediná novinka, kterou obecné nařízení přináší, je právo na přenositelnost údajů. Všechna ostatní práva a povinnosti obecného nařízení byla upravena různými jinými právními předpisy. A to dokonce i „údajná“ novinka - právo být zapomenut - byla řešena zákonem 101/2000 sb. Obecné nařízení tato pravidla sjednocuje, zpřesňuje a činí podrobnějšími.

Šifrování je povinné

Obecné nařízení neukládá povinnost použít pro zabezpečení zpracování některé specifické opatření.

Naopak, při stanovení povinnosti správce a zpracovatele zabezpečit osobní údaje se obecné nařízení výslovně dovolává ohledu na stav techniky, náklady na přijetí a provedení jednotlivých technických a organizačních opatření k zabezpečení osobních údajů, povaze, rozsahu, kontextu a účelům samotného zpracování a také k pravděpodobným rizikům pro práva a svobody, jež s sebou zpracování nese. Vlastní povinnost pak zahrnuje zavedení vhodných technických a organizačních opatření a začlenění do zpracování nezbytných záruk, a to jak v době určení prostředků pro

zpracování, tak v době vlastního zpracování. Šifrování je uvedeno jako jedno z vhodných opatření („případně včetně /…/ šifrování osobních údajů“). Při posuzování úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, jako náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů a neoprávněný přístup k takovým údajům.

Pokuty se počítají dle obratu

Horní hranice pokut je nová, ale jak je opakovaně v preambuli k obecnému nařízení uváděno, pokuty mají být v každém jednotlivém případě účinné, přiměřené a odrazující. Obecné nařízení současně respektuje zásady správního trestání, včetně kritérií pro stanovení výše pokut i podmínek pro určení odpovědnosti i vyvinění se (z trestu).“[1]

5 Analýza dopadových kritérií

K analýze dopadových kritérii je použita CS verze NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679. stažené z http://eur-lex.europa.eu dne 19. 10. 2017 (GDPR).

Nejsou brány v potaz různé výjimky a možnosti změkčení dopadů obecného nařízení, které se většinou týkají státních či vědeckých institucí nebo speciálních případů.

Z výše uvedeného dokumentu vyplývá, že bude vhodné přijmout určitá technická opatření k naplnění souladu s následujícími články obecného nařízení GDPR:

Článek 5:

V článku 5 se hovoří především o zásadách zpracování osobních údajů. Hned v písm. a) je poukazováno na nutnost data zpracovávat korektně a zákonným způsobem. Osobní údaje musí být shromažďovány za jasně definovaným a legitimním účelem a dle písm. c) musí být také minimalizovány na nezbytný rozsah.

[1] Zdroj: (Desatero omylů. *Úřad pro ochranu osobních údajů* [online]. [cit. 2018-10-25]. Dostupné z: https://www.uoou.cz/desatero-omylu-o-gdpr/ds-4818/archiv=0&p1=3938)

písm. d**)** hovoří o zásadě „přesnosti“, to znamená, že podnik musí být dále schopen osobní údaje nějakým efektivním způsobem aktualizovat, mazat či jinak spravovat a mít přehled, jaké osobní údaje a u koho jsou vedeny.
V písm. f) je podnikům ukládáno zpracovávat osobní údaje tak, aby byly náležitě zabezpečeny proti zneužití nebo ztrátě či poškození, tedy zásada „integrity“ a „důvěrnosti“ dat. Podniky jsou zodpovědné za data, která uchovávají.
To všechno budou muset být dle odstavce 2. podniky schopny řádně doložit.
Podniky budou muset mít jednoznačný přehled, jaké osobní údaje jsou kde uchovávány a za jakým účelem. Jako možné řešení navrhuji vytvoření centrálního, nejlépe elektronického, systému správy osobních údajů.

Článek 7:
Tento článek ukládá podnikům, přesněji řečeno jmenovaným správcům v těchto podnicích, povinnost být schopen prokázat, že subjekty údajů poskytly souhlas s uchováváním osobních údajů jednoznačně a bez jakýchkoli podmínek.
Následné potencionální odvolání souhlasu musí být stejně snadné, jako jeho udělení.
V praxi by to mohlo znamenat vytvoření jednotného způsobu udělování a odvolávání souhlasu a centrální evidence takovýchto souhlasů, případně vytvoření takového workflow, kde oba tyto úkony budou splňovat výše uvedené požadavky.

Článek 8:
Tento článek se svým obsahem dotýká udělování souhlasů nezletilými osobami.
Především odstavec 2. může mít dopad na technická opatření v podnicích. Ukládá totiž podnikům vyvíjet přiměřené úsilí k ověření rodičovských práv u osob, které udělují souhlas se spravováním osobních údajů jiných osob mladších 16 let. Tady se nabízí otázka, co je to přiměřené úsilí.

Po rozhovoru s architektem Základních registrů obyvatel, jsem našel možnost jak teoreticky využit k této validaci Základní registry obyvatel v kombinaci s Informačním systémem evidence obyvatel. Vztah rodič ev. opatrovník – nezletilý je v nich totiž uveden. Bohužel zatím tuto možnost registry nemají. Teoretická možnost je ověřit v základních registrech validitu údajů a pak v Informačním systému evidence obyvatel vztah rodič ev. opatrovník – nezletilý.

Článek 11:

Tento článek se týká situace, kdy podnik sbírá údaje, sice svou povahou osobní, ale v tak minimální míře, nebo takové povahy, že není možné na jejich základě určit konkrétního člověka. Např. samotná emailová adresa. V takové situaci není podnik povinen zjišťovat další údaje k zajištění souhlasu se zpracováním. Nicméně je podnik na žádost subjektu údajů povinen jím poskytnutá data doplnit a nadále s nimi nakládat příslušným způsobem. Tedy v praxi musí mít podnik nějaký mechanismus jak takováto data identifikovat a mít možnost je přesunout do příslušné kategorie pro další nakládání.

Článek 12:

Tento článek řeší především informační povinnost podniku vůči subjektům údajů. Podnik je povinen poskytnout informace, které jsou uvedeny v článcích 13 a 14 a dále informovat o právech subjektů dle článků 15 až 22. Podnik musí tyto informace zpřístupnit subjektu údajů ve vhodné strukturované formě. Dále bude vhodné informace uvedené v článcích 13 a 14 doplnit standardizovanými ikonami dle odstavce 7.
Jedná se o jednoduchou informaci o právech a povinnostech stran. Vhodným řešením by zde mohla být jednoduchá veřejná www stránka s požadovanými informacemi.
Dále je nutné vyřešit systém podávání žádosti subjektů a ověřování jejich totožnosti.

Článek 15:

Tento článek dává občanům právo na informace o tom, zda a jak jsou jejich osobní údaje zpracovávány, neboli nějakým způsobem využívány a dále právo vědět, jaké osobní údaje jsou o nich vedeny a jak je s nimi nakládáno. Podnik tedy musí mít především přehled, jaké údaje u dotyčných zpracovává a jak s nimi nakládá. V praxi tento článek bude podniky především nutit mít ve vedených osobních údajích pořádek a přehled.

Článek 16:

Tento článek opravňuje občany požadovat opravu osobních údajů, pokud zjistí, že jsou jeho vedené osobní údaje nepřesné nebo neúplné. Podniky tedy musí být opět schopny osobní údaje spravovat a jednoznačně identifikovat. Znovu se zde dostáváme k nutnosti sytému pro správu osobních údajů.

Článek 17:

Tento článek ukládá v odstavci 1 podnikům povinnost za definovaných podmínek, například v případě odvolání souhlasu subjektem, tyto údaje bezodkladně vymazat. V odstavci 2. je dokonce přidána povinnost informovat ostatní podniky, jimž tyto údaje zákonným způsobem poskytl, o tomto odvolání subjektem.

Podobně jako článek 16 nutí článek 17 podniky mít perfektní přehled o uchovávaných osobních údajích napříč všemi jeho systémy a navíc přidává povinnost mít přehled také o jejich pohybu.

Článek 18:

Tento článek řeší „Právo na omezené zpracovaní.“ Omezené zpracování je definováno v článku 4 odstavec 4 jako označení osobních údajů za účelem omezení jejich budoucího zpracování. V podstatě to znamená, že od okamžiku takového označení osobních údajů subjektu nesmějí být tyto nadále jakkoliv využívány a jsou pouze u podniku uloženy. Odstavec 3 podnikům navíc ukládá informační povinnost vůči subjektům při rušení takovéhoto omezení. V praxi bude nutné takové údaje označit příslušným parametrem a nadále s nimi podle toho nakládat.

Článek 19:

Tento článek ukládá oznamovací povinnost.

Obecné nařízení nám dává určité zákonné možnosti, jak osobní údaje subjektů předávat dál jiným podnikům, nicméně nám z tohoto článku vyplývá také povinnost takovéto podniky informovat o jakýchkoli změnách v osobních údajích subjektů, provedených na základě článků 16, čl. 17 odst. 1 a článku 18. Podniky jsou povinny za přiměřeného úsilí informovat své partnery o změnách v osobních údajích, odvolání souhlasu a omezení zpracování. K tomu budou podniky muset mít zejména přehled o takových změnách a navíc i o pohybu jimi spravovaných osobních údajů.

Článek 20:

Tento článek v podstatě dává právo vyžádat si vedené osobní údaje v nějakém strukturovaném, běžně strojově čitelném formátu, případně požádat o jejich předání

jinému podniku. V praxi by se mohlo jednat o jednoduchý export dat např. ve formátu CSV, XML ev. XLS.

Článek 21:

Tento článek dává subjektům právo kdykoliv vznést námitku proti zpracování osobních údajů. Jedná se zejména o případy, kdy jsou údaje zpracovávány na základě čl. 6 odst. 1 písm. e) nebo f), ale i o případné profilování na základě těchto údajů. V případě námitky proti zpracovávání osobních údajů z důvodů přímého marketingu a profilování je nutno zpracování v souladu s článkem 3 zastavit úplně a bez námitek.

Podnik je povinen zpracovaní neprodleně, *nejdéle však do 1 měsíce* [2], přerušit min. do doby, kdy prokáže závažné a oprávněné důvody proč ve zpracovávání pokračovat. V situaci, kdy subjekt vznese námitku, může tento článek ve svém důsledku znamenat povinnost přestat se zpracováním bez zbytečného průtahu. Technickým řešením by mohlo být zavedení příslušného parametru k označení osobních údajů nebo například použitím vhodné cookie v případě www stránek.

Dále je pak nutné věnovat pozornost odstavci 5. Kde je definována možnost vznést tuto námitku automatizovanými prostředky, to v praxi může nakonec znamenat např. nastavením prohlížeče ev. softwarem třetích stran.

Článek 22:

Tento článek dává subjektům právo nebýt předmětem žádného rozhodování založeného výhradně na automatizovaném zpracování. Jak uvádí UUOU „*Např. není možné udělit pokutu za rychlou jízdu pouze na základě rozhodnutí počítačem a bez lidského zásahu.“*[3] a oficiální internetové stránky Evropské unie „*Jsou sice možné výjimky, ale vždy je nutnésubjekt o takovémto rozhodnutí informovat, dát mu možnost takové rozhodnutí*

[2] Zdroj: *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679: 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)* [online]. 27.4.2016 [cit. 2018-01-26]. Dostupné z: http://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] Zdroj: Nejdůležitější pojmy. Úřad pro ochranu osobních údajů [online]. 2018 [cit. 2018-09-10]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaj/d-27276

napadnout a nakonec mu dát právo na prověření automatizovaného rozhodnutí člověkem.“[4]

Dále obecné nařízení GDPR zavadí pojem „Profilování“. Jinými slovy se jedná například o vyhodnocování chování člověka a následnou úpravu nabízeného obsahu, jako je třeba personalizace v případě www stránek nebo reklamní bannery „na míru“ uživateli. Navíc článek 22 implicitně ve svém znění předpokládá, že občan s profilováním nesouhlasí! Podniky budou tedy nuceny nejprve souhlas s profilováním od občanů získat, jinými slovy opět doplnit vedené osobní údaje o příslušný parametr nebo souhlas evidovat např. opět pomocí vhodných cookies v případě www stránek.

Z výše uvedených skutečností plyne potřeba subjektům poskytnout možnosti tato automatická rozhodnutí napadat a ev. žádat jejich přezkoumáni člověkem.

To pro podnik znamená mít možnost tato rozhodnutí a profilování nějakým způsobem kontrolovat.

Souhlasy s profilováním by bylo možné držet spolu s ostatními osobními údaji subjektů nebo držet tuto informaci pouze s jejich pseudonymizovaným, tokenem.

Pro případy automatického zpracování bude situace složitější a bude nezbytné zavést nějakou agendu pro zprávu námitek, nejlépe ve formě nějakého SW nástroje.

Článek 25:

Článek 25 se týká technických opatření k zabezpečení osobních údajů. Podnik je plně zodpovědný za údaje, jež shromažďuje a musí přijmout přiměřená opatření, která zabrání jejich ztrátě či zneužití.

Podniky budou muset zmapovat, kde všude se s osobními údaji nakládá a jak jsou tyto zabezpečeny. Dále budou muset učinit opatření k jejich ochraně. Například data šifrovat, pseudonymizovat, ale i minimalizovat množství ukládaných údajů, přijmout taková opatření, aby k osobním údajům měli přístup pouze oprávnění uživatelé a nakonec zabránit ukládání dat obsahujících osobní údaje na místa, která k tomu nebyla určena (HDD osobních počítačů, sdílené i veřejné složky serverů, přenosná media apod.)

---

[4] Zdroj: Ochrana osobních údajů podle nařízení GDPR. *Oficiální internetové stránky Evropské unie* [online]. 2018 [cit. 2018-09-27]. Dostupné z: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_cs.htm

Článek 30:

Článek 30 podnikům předepisuje vést agendu správců osobních údajů, jejich zástupců a pověřenců ochrany osobních údajů. Vymezuje jaké údaje a za jakých podmínek jsou povinni vést.

V praxi je soulad s tímto článkem možné řešit aplikací pro správu těchto údajů.

Článek 32:

Článek 32 předepisuje podnikům zabezpečit zpracovávání osobních údajů tak, aby byly údaje stále dostupné, integritní a zabezpečené. Vysloveně nařizuje, za předpokladu vynaložení úměrného úsilí, osobní údaje pseudonymizovat a šifrovat. Dále bude nezbytné zabezpečit pravidelné zálohování dat, vysokou dostupnost, nástroje k ověřování integrity dat a uchování historie operací provedených s osobními údaji, např. některým z nástrojů SIEM.

Článek 34:

Tento článek v podstatě řeší kroky po případné kompromitaci osobních údajů. Zavádí jednoznačně informační povinnost vůči subjektům zpracování údajů. Jinými slovy, podnik má povinnost informovat občany, jejichž osobní údaje zpracovává, o tom, že došlo ke kompromitaci ev. k úniku těchto dat.

Této povinnosti je podnik zbaven, pokud má údaje zabezpečeny tak, že jsou pro neoprávněného uživatele nesrozumitelné, tedy např. šifrováním. Dále pak v případě, že podnik přijal účinná opatření, o kterých lze pravděpodobně předpokládat, že zneužití uniklých dat zabrání. Nakonec, v případě nutnosti vynaložit přiměřené úsilí k informování všech dotčených subjektů. Třeba je možné zvolit formu veřejným oznámením.

Ideálním technickým opatřením k tomuto článku se zdá být účinné šifrování osobních údajů.

Po prostudování obecného nařízení GDPR je možné stanovit dopadová kritéria takto:

1. Podniky jsou plně zodpovědné za osobní údaje, které uchovávají. Musí mít o nich dokonalý přehled a mít možnost je kdykoli spravovat.

2. Podniky musí získávat a evidovat souhlasy se zpracováním osobních údajů a být schopny je doložit.
3. Občané mají právo na opravu osobních údajů, právo být zapomenut a právo na omezené zpracování. Tato práva musí podnik zajistit a garantovat.
4. Podniky mají také informační povinnost vůči třetím stranám, kterým osobní údaje zákonným způsobem poskytla. Jedná se zejména o situace vznikající při uplatnění práv subjektů z bodu 3.
5. Podniky také zodpovídají za nepřetržitou důvěrnost, integritu a dostupnost systémů zpracovávajících osobní údaje.

Některé body jsou podmíněny vynaložením přiměřeného úsilí a nákladů. V praxi se však na tuto formulaci nedá spoléhat. Není definováno, co jsou to přiměřené náklady a nakonec vždy bude stejně rozhodovat úřední moc.

6 Analýza možných technických opatření

Celé obecné nařízení GDPR nutí především podniky udělat si pořádek ve shromažďovaných osobních údajích a následně je zodpovědně spravovat. Pokud však chtějí podniky data řádně spravovat, musí nejprve mít přehled, kde a jaká data shromažďují a ukládají.

Při analýze jsou použity zejména on-line zdroje informací o nejnovějších technologiích, dále konzultace s odborníky a zkušenosti z dosavadní praxe autora.

Z předchozí analýzy dopadových kritérii vyplývají tři nosná témata, která mají nějaký dopad na technická opatření v podniku:

- pořádek v datech, tedy vědět, jaká data a kde máme,
- obecné zabezpečení dat,
- správa zpracovávaných osobních údajů.

6.1 Pořádek v datech

Zmapování dat, nejedná se doslova o technické opatření, nicméně bez důkladného zmapování, jaká data a kde se nacházejí, se budou příslušná citlivá data těžko spravovat.

Pro základní zmapování dat si můžeme udělat menší odskok z čistě technické oblasti GDPR do obecnější časti a zodpovědět pár základních otázek. Například dotazníkem používaným společností Mewburn Ellis pro datový audit.
Tyto odpovědi se nám následně budou hodit i při návrhu technických řešení dopadů obecného nařízení GDPR.

- ***Jaká osobní data shromažďujeme?*** *Např. Standardní osobní data, citlivá osobní data, data o osobách mladších 16 let?*
- ***Proč to děláme?*** *Na co taková data potřebujeme, jak je používáme a potřebujeme je opravdu v takovém rozsahu?*
- ***Jak data získáváme?*** *Tedy způsob, jakým se k nám data dostávají, on-line, off-line, existují procesy? Jsou data zabezpečena už při sběru?*
- ***Kdy data získáváme?*** *Kdy a při jakých příležitostech data shromažďujeme.*
- ***Kdo za data zodpovídá?*** *Kdo za data v podniku zodpovídá, a jakým způsobem? Existují směrnice pro nakládání s daty?*
- ***Co s nimi děláme?*** *Jak s daty v podniku pracujeme? Jsou předávány třetím stranám? Dokážeme říci, na co data vlastně potřebujeme?*[5]

K praktické realizaci nám může posloužit jednoduchý dotazník viz. Příloha 1.

Dále užitečné mohou být v tomto směru také závěry GAP analýzy.

GAP analýza, tedy v podstatě analýza mezer, řeší dvě základní otázky: Kde jsme? A kam chceme dojít? Kde jsme, z pohledu dat, záleží především na stávajícím vedení podniku a jeho důrazu či nedůrazu na dodržování elementárních zvyklostí a pravidel pro nakládání s daty. Výhodu mají ty podniky, které implementovaly předchozí směrnici EU o ochraně osobních údajů ev. požadavky zákona č. 101/200 sb. [6]

Jednoznačně zde tedy vzniká nutnost tuto, dost často neoblíbenou práci, udělat a často i ručně zmapovat, kde se jaké osobní údaje nacházejí a kdo k nim má přístup.

---

[5] Zdroj: Data Audit Checklist. *Http://mewburn.com/* [online]. [cit. 2018-10-25]. Dostupné z: http://mewburn.com/wp-content/uploads/2018/07/GDPR-Data-Audit-Checklist.pdf

[6] Zdroj: NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

6.2 Obecná bezpečnost dat

Mezi povinnostmi, které klade GDPR na podniky, je i dostatečné zabezpečení osobních údajů. Bezpečnost dat je důležitá i mimo oblast GDPR. V dnešní době může cena dat lehce mnohonásobně převyšovat cenu HW, na kterém jsou data uložena a mnohdy se jejich cena nedá ani stanovit. Ačkoliv problematika obecné bezpečnosti dat je velmi široká a přesahuje dalece rámec této bakalářské práce, jsou zde nastíněny obecné principy ochrany dat a možné hrozby.

6.2.1 Externí hrozby

Námi uchovávaná data mají obecně cenu nejenom pro nás, ale například i pro konkurenci nebo jiné zájmové skupiny. Data mohou být např. ohrožena úmyslným útokem, kdy útočník svou kriminální činností přímo kompromituje data, nebo jako sekundární únik, například krádež notebooku s citlivými daty, kdy primárním motivem útočníka není získání dat, ale i přesto nad nimi ztratíme kontrolu.

6.2.1.1 Hackerský útok

Ochrana proti úmyslným hackerským útokům bývá dnes ve většině podniku na poměrně slušné úrovni.

Základem zůstává zabezpečení vnějšího perimetru sítě kvalitním Firewallem a následná další opatření jako je vynucení kvality hesel a jejich obnovy, zásada minimálních přístupových práv k datům, kvalitní antivirová ochrana počítačů, zprovoznění demilitarizovaných zón, ale i taková opatření, jako je odpojení nepoužívaných datových zásuvek, zaheslováni wifi sítí atd.

V neposlední řadě jsou to i průběžná školení a vzdělávání uživatelů v bezpečnostní oblasti.

Krádež nebo ztráta fyzického zařízení:

Jedna z cest jak zabránit zneužití dat v tomto případě je jejich šifrování.

Když dojde k odcizení či ztrátě fyzického zařízení, jsou tato data bez příslušných klíčů nepoužitelná.

Základní ochranou je šifrování všech datových úložišť s osobními údaji v podniku. Společnost Microsoft nabízí nativně zabudovaný nástroj ve vlastním OS – Bitlocker. Linux umožňuje šifrování nástrojem LUKS.

V případě použití šifrování fyzických úložišť si musíme nicméně uvědomit, že jakákoliv obnova po HW havárii disku může být krajně obtížná, ne-li nemožná. Ztráta, byť jednoho bitu nám totiž znehodnotí celý blok dat. Je tedy zcela nezbytné, data zodpovědně zálohovat[7].

6.2.2 Interní hrozby

Uvádí se, že kolem 50 procent uniku dat je způsobeno interními zaměstnanci.
Z toho kolem 30 procent úniků je neúmyslných, způsobených chybou, či nedbalostí.
Kolem 20 procent dat je ukradeno za účelem získání nějakého profitu.
Dále si až 85 procent propuštěných zaměstnanců odnáší podniková data sebou.
V případě, že se jedna o osobní údaje nám obecné nařízení GDPR přímo nařizuje takovýmto únikům bránit.

6.2.2.1 Kontrola přístupových práv

Jedním ze znaků zodpovědného nakládání s daty v podnicích je zásada minimálních práv, tedy zaměstnanci mají přístup pouze k datům, která skutečně potřebují k plnění vlastních povinností. Přístup k ostatním datům je blokován.

Zavedení zásady minimálních práv se může zdát být snadným úkolem a je považováno za průmyslový standard, nicméně mnoho podniků mívá velké problémy se zavedením do praxe, naštěstí nejnovější generace nástrojů pro řízení uživatelských oprávnění tento proces usnadňují[8].

Těchto nástrojů je celá řada. Je možné použít nástroj 8MAN od stejnojmenné společnosti nebo Identity Management od společnosti CA.
Tyto nástroje umožnují projít celý proces zavedení zásady minimálních práv, přes prvotní analýzu stavu, zavedení do praxe, běžný provoz, ale i následnou kontrolu a audit.

---

[7] Zdroj: DOČEKAL, Michal. Proč a jak na šifrování disků v Linuxu? [online]. 22.5.2008 [cit. 2018-02-07]. Dostupné z: https://www.root.cz/clanky/proc-a-jak-na-sifrovani-disku-v-linuxu/
[8] Zdroj: *Network Security* [online]. Elsevier, 2013, **2013**(10) [cit. 2018-02-06]. ISSN 1353-4858. Dostupné z: https://doi.org/10.1016/S1353-4858(13)70114-4

6.2.2.2 Průběžný audit

Průběžný audit je zejména o vnitřních směrnicích podniku, spojených s vhodnými SW prostředky. Jeho hlavním cílem je zabránit přístupu interních zaměstnanců k datům, která jim nepřísluší a případně odhalit ať už úmyslné, nebo neúmyslné úniky dat a pokusy o ně. Na trhu je hodně pokročilých monitorovacích softwarových řešení, která logují akce uživatelů. Hledají souvislosti mezi nimi a dokážou i aktivně bránit případnému neautorizovanému pohybu dat. K dosažení souladu se článkem 32 by tento typ software měl být použit minimálně u uživatelů s přístupem k osobním údajům subjektů.

6.2.2.3 Deduplikace dat

Během každodenní činnosti v podniku vzniká mnoho duplicit používaných dat. Na serverech a počítačích se nachází mnoho verzí jednoho dokumentu. V emailových schránkách existují maily násobně přeposlané a hromadně rozeslané. Všude v těchto dokumentech se mohou nacházet osobní nebo i jinak citlivé údaje. Pokud chceme efektivně spravovat tato data, musíme mít dobrý přehled o tom, kde a jaká se nacházejí.

Podniky by měly zavést směrnice a postupy k zabránění vytváření a případně i k likvidaci duplicitních dat. Naštěstí existuje mnoho programů a technických řešení na bránění vzniku, ev. vyhledávání a likvidaci těchto duplicitních dat.

6.3 Centrální správa osobních údajů

Samotným jádrem technických opatření by mohl být nějaký centrální systém pro správu osobních údajů (dále CSSOU) a nakládání s nimi.

Jádrem CSSOU by mohla být šifrovaná databáze osobních údajů a všech potřebných parametrů vztahujících se k uděleným souhlasům, nesouhlasům, námitkám atd. Tato databáze by měla mít jednoznačně určená přístupová práva a měla by využívat nejmodernějších bezpečnostních technologii, jako je např. maskování sloupců, šifrování uložených a přenášených dat apod.

Osobní údaje subjektu budou v této databázi rozšířeny o anonymní token.

Všechny ostatní systémy podniku budou pracovat pouze s tokeny a v případě potřeby by si údaje v CSSOU pomocí REST ev. SOAP rozhraní dohledaly. To nám zajistí naplnění zásady pseudonymizace osobních údajů subjektů.

Pro potenciální zvýšení výkonu celého systému podniku bude ostatním systémům podniku povoleno držet si lokální šifrované cache a ty pouze pravidelně validovat vůči CSSOU. Obecné nařízení nám totiž umožňuje reagovat na požadavky subjektů s určitým zpožděním, a proto jsou cache, v případě rozumné retence ve validaci cache vůči CSSOU, přípustné.
Podobná validace bude využita i v případě obnovy dat ze zálohy, kdy součástí procesu obnovy dat bude i povinná validace vůči CSSOU. Tato validace musí proběhnout ještě dříve, než bude obnovená databáze prohlášená za provozní; jedině tak zaručíme, že v databázi nebudou přístupné tokeny subjektů, které požádaly o výmaz. Nebude tedy hrozit situace, kdy subjekt, který požádal například o výmaz, se stane znovu předmětem zpracování. To by bylo v rozporu se směrnicí GDPR a mohlo by to vyústit i v případné postihy vůči podniku.
CSSOU by sloužil jako úložiště aktuálního stavu osobních údajů a byl by autoritativní vůči ostatním systémům podniku.
Architektura bude CSSOU dělit na části:

- frontendovou, tedy rozhraní pro subjekty údajů, kde budou moci vyjadřovat svoje souhlasy, nesouhlasy, námitky atd.,
- -backendovou, sloužící pro správce a pověřené pracovníky podniku k vedení potřebných agend,
- databázovou, kde budou uložena samotná data a bude řešit i bezpečnost těchto dat,
- SOAP ev. REST API, pro komunikaci s ostatními systémy podniku.

Naplněním těchto tezí by se podniky měly dostat do souladu se směrnicí GDPR v otázce technických opatření

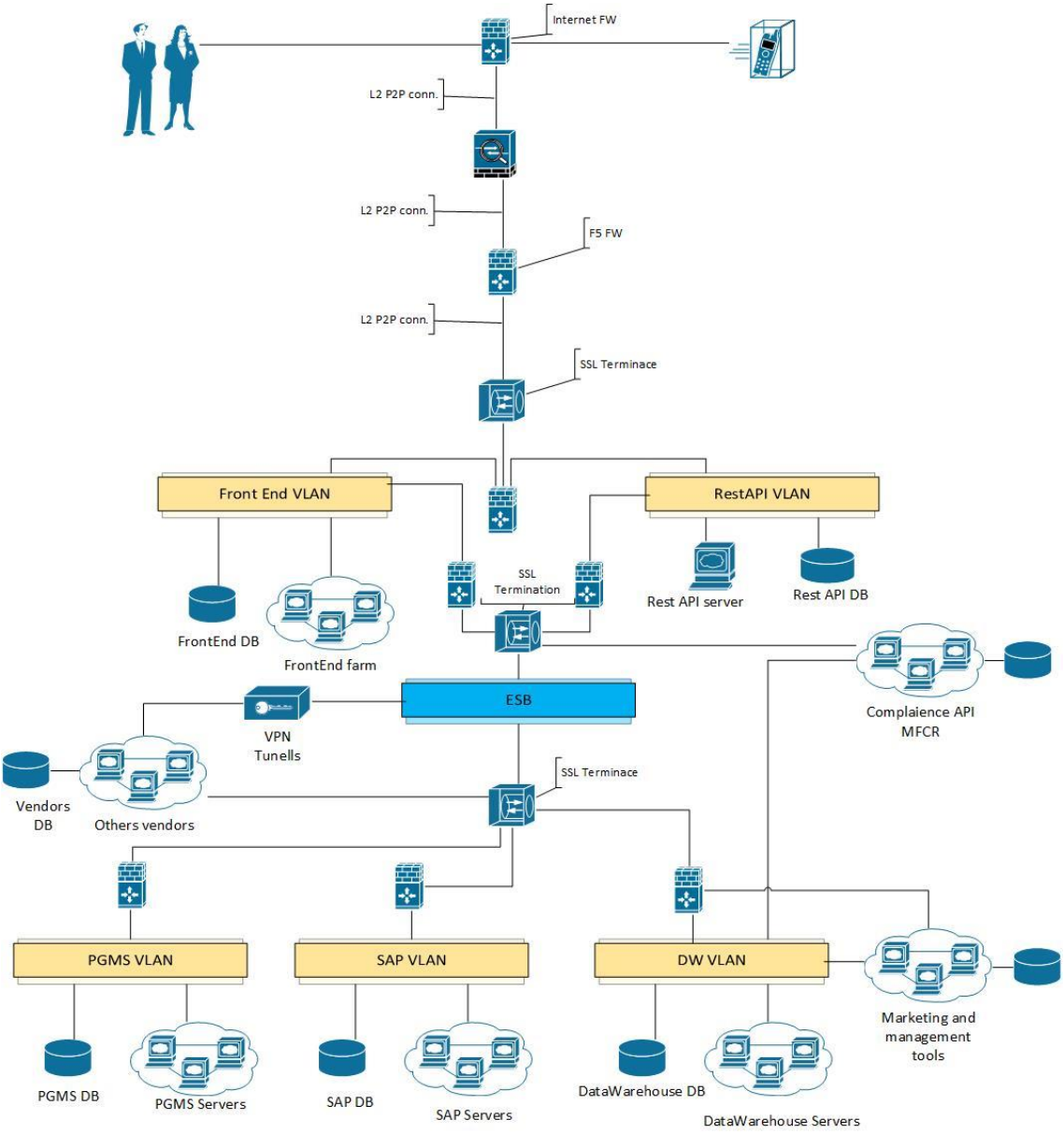
7 Případová studie

Pro případovou studii byl zvolen podnik střední velikosti a z regulovaného segmentu obchodu. Podnik má 450 zaměstnanců a jeho podnikání je regulováno zákonem 186/2016 Sb. Zákon o hazardních hrách. Dále je podnik také vázán certifikacemi
WLA Responsible Gaming Framework, WLA Security Control Standard, ISO 27001. WLA certifikace se týkají loterijního businessu a potvrzují zodpovědný přístup podniku k podnikání v tomto segmentu. Podnik prochází každoročně několika přísnými audity, jak finančním, tak audity k obnově certifikací.

Podnik také musí dbát na svou dobrou pověst, neboť vysoký goodwill je jeho nejcennějším aktivem.

Případová studie se věnuje popisu prostředí a technických opatření, zvolených k udržení souladu s nařízením GDPR. Z tohoto důvodu nejsou řešeny procesní úkony a audity jako např. posouzení vlivu DPIA, posouzení rizik atd. Předpokládá se, že tyto procesní úkony proběhly, a podnik jejich výsledky zohledňuje.

7.1 Schéma infrastruktury.



Obrázek 2 - Schéma infrastruktury

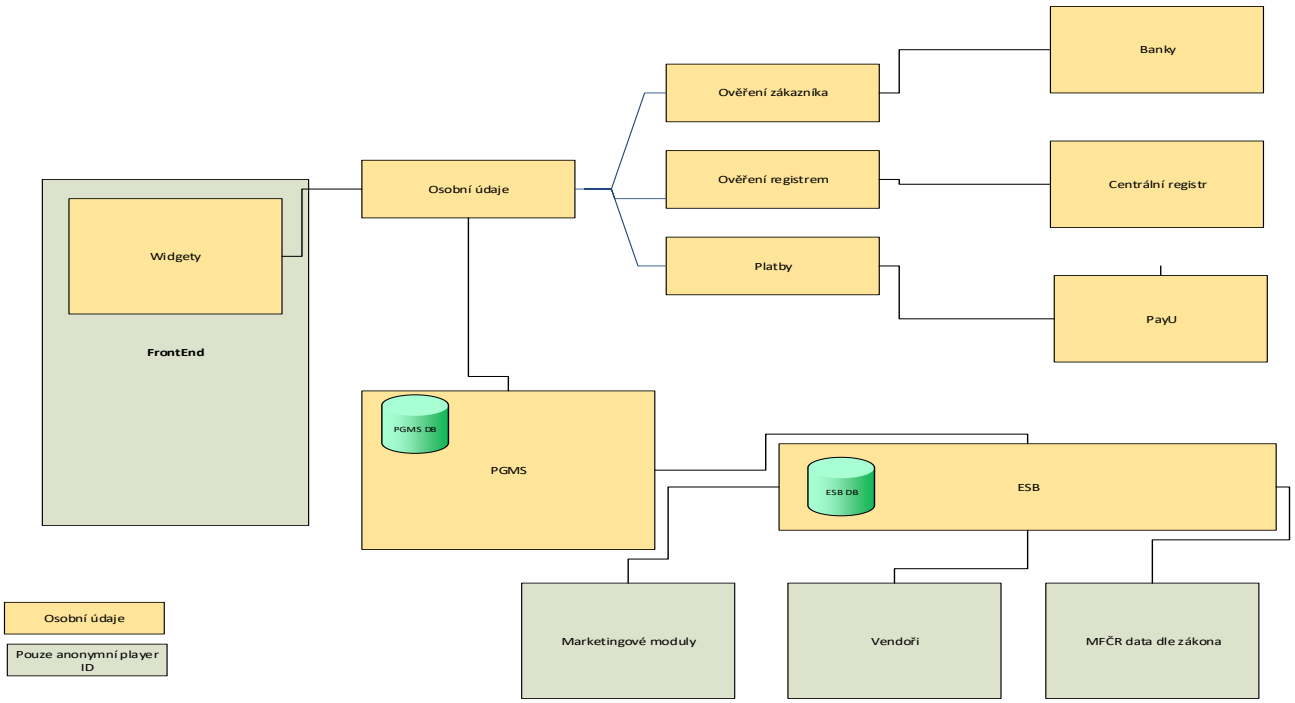
7.2 Rozsah zpracovávaných osobních údajů.

Jaké a jak jsou zpracovávány osobní údaje zákazníků podniku, vyplývá především z platné legislativy. Podnik je především zákonem zavazován ke zodpovědnému ověřování identity i věku zákazníka. K naplnění těchto povinností je nezbytné vyžadovat od svých zákazníků poměrně rozsáhlý soubor osobních údajů. Jedná se nejen o jména, adresy, rodná čísla a čísla bankovních účtů, ale v některých případech i o scany

občanských průkazů ev. jiných dokladů. Tyto údaje musí zákazník vyplnit pravdivě, protože jsou následně ověřovány proti základním registrům státní správy, a bez potvrzení správnosti údajů registrem není registrace zákazníka dokončena. Tedy, i když by zákazník použil falešné rodné číslo, které bude odpovídat formálním požadavkům (dělitelnost 11, poslední číslo je platná kontrolní číslice), tak neprojde validací v centrálním registru, a zákazníkovi není registrace umožněna.

Mimo těchto, ze zákona vyplývajících osobních údajů, podnik ještě zpracovává další údaje, jako jsou geolokační údaje, údaje o chování zákazníka na webu atd. údaje jsou využívány zejména pro marketingové účely a k naplnění legislativy některých států EU (geolokace a zabránění hraní lidem ze států, kde to není legální). Tato data jsou z velké části anonymizována a identifikace konkrétní osoby je dost obtížná.

7.3 Tok osobních údajů zákazníku systémem.



Obrázek 3 - Systémy dle přístupu k osobním údajům.

7.3.1 Registrace a ověření identity

Vstupním bodem osobních údajů do podniku je proces registrace zákazníka. Aby zákazník mohl využívat on-line možnosti sázení, tak musí projit procesem registrace. Samotná registrace probíhá pomoci widgetu z aplikace PGMS (Player and Management systém). Ten je spouštěn webovou aplikací na frontendu. Pro frontend jsou tedy osobní údaje klienta neviditelná a žádná se na něm nezpracovávají. Tyto osobní údaje jsou uloženy pouze v databázi PGMS.

Ověření osobních údajů probíhá vůči centrálnímu registru. PGMS komunikuje s centrálním registrem přes integrační platformu ESB a odesílá osobní údaje k ověření. Tyto jsou pak součástí auditního logu ESB. Tuto skutečnost je nutné zohlednit při ochraně osobních údajů zákazníků.

Samotné ověření identity člověka, tedy že se systémem komunikuje osoba, ke které se vážou poskytnuté osobní údaje je prováděna buď fyzickou kontrolou dokladů na provozovnách podniku, poskytnutím scanu dokumentů nebo ověřením identity pomocí bankovního účtu.

V případě fyzické kontroly je situace nejsnazší. Klientovi jsou zkontrolovány osobní dokumenty a pověřená obsluha klienta označí jako ověřeného. Žádné další údaje se neuchovávají. V případě, že zákazník zvolí ověření pomocí scanu dokumentu, je dokument možné buď přiložit jako přílohu ve standartních formátech, nebo použít fotoaparát mobilního telefonu. Dokument je pak strojově vyhodnocen technologii OCR. Po ověření jsou osobní údaje ve scanu dokumentu začerněny a scan je přiložen k účtu zákazníka. Při tomto typu ověření podnik dosahuje cca 10procentní chybovosti. Tyto stavy jsou řešeny následně ručně. Třetí možností je ověření pomocí bankovního účtu. Zde podnik využívá toho, že banky mají své klienty ověřeny. V případě zvolení této metody je zákazník přesměrován na stránky banky, a pokud řádně proběhne autentifikace, banka pošle pouze notifikaci o úspěšném ověření zákazníka.

7.3.2 Platby

Platby jsou realizovány třetí stranou a ochrana osobních údajů je zajištěna smluvně. Při požadavku na platbu, je zákazník přesměrován na stránku poskytovatele platebních služeb. Zpět jde pouze notifikace, zda byla platba úspěšná, či nikoliv. Čísla karet nejsou podniku vůbec známa a nejsou jím nijak zpracovávána. V případě bankovních

převodů jsou pouze ověřovány již podniku známé osobní údaje. Je tak ověřováno, zda bankovní účet je registrován na příslušného zákazníka.

7.3.3 Personalizace

Podnik pro marketingové účely dále pracuje s personalizací. Zákazníci jsou na základě svého chování na webu podniku řazeni do kategorií. Na základě těchto kategorií jim je pak upravován obsah samotného webu. Data jsou sice sbírána anonymně, nicméně toto může mít dopad na plnění článku 22 směrnice GDPR a je nutné získat souhlasy.

7.4 Řešení bezpečnosti jednotlivých částí systému.

7.4.1 Aplikace

Aplikační servery systému jsou vždy striktně odděleny od datových. Jedná se o fyzicky oddělené servery. Navíc je mezi nimi vždy umístěn virtuální firewall.
Dále je důležitým požadavkem na dodávané aplikace, jejich vývoj v souladu s doporučeními OWASP. Aplikace, které přicházejí do styku s osobními údaji, také vždy ukládají své logy pouze do chráněné databáze. Lokálně jsou ukládány pouze systémové logy, které osobní údaje neobsahují.

7.4.2 Databáze

Podnik má v podstatě dvě databáze, kde jsou uloženy osobní údaje zákazníků. První je databáze PGMS, kde jsou uloženy účty zákazníků se všemi zákonem vyžadovanými údaji. Druhou databází je auditní log integrační platformy ESB, kde se mohou vyskytnout dílčí osobní údaje zákazníků uložené v logách systému. Společnost má ještě databázi účetního a informačního systému, ve které jsou osobní údaje zaměstnanců a dodavatelů podniku. Tyto údaje podléhají jiným právním předpisům, jako je např. účetní zákon. Nicméně i na tyto databáze se vztahují stejná bezpečností opatření, jako na databáze se zákazníky.
Bezpečnost databází je řešena už v samotné architektuře systému. Databáze jsou fyzicky i síťově odděleny od aplikačních serverů. Síťová komunikace aplikačních serverů a databází je chráněna firewally.
Komunikovat s databází mohou pouze povolené IP adresy.

Samozřejmostí je také šifrování databází jejich nativními nástroji. Zde je dobré si uvědomit, že na vhodně zvoleném typu šifrování a úrovně klíčů může záviset následný výkon celého systému. Dobrou volbou, pro svět Microsoftu je šifrovat technologií TDE (Transparent Data Encryption), která je dostupná už od verze MS SQL 2008. Výhodou je, že toto šifrování je transparentní, a nejsou nutné žádné programové úpravy. Z aplikačního pohledu se databáze jeví jako nešifrovaná, ale datové soubory a zálohy jsou ve skutečnosti automaticky zašifrované. K dešifrování dat dochází až v paměti serveru.
Samotné nasazení je poměrně snadné. Nejprve je třeba vytvořit hlavní klíč (master key), následně vytvořit certifikát, chráněný hlavním klíčem. Tímto certifikátem se pak šifrují symetrické klíče pro šifrování databáze. V případě použití asymetrických klíčů jsou tyto šifrovány hlavním klíčem rovnou. Dále je nutné vygenerovat databázový šifrovací klíč chráněný certifikátem (symetrické šifrovaní). Nakonec zapnout TDE v databázi. Tím začnou být šifrovány databázové soubory, zálohy a tempDB.
TDE nabízí čtyři metody šifrování. Tři jsou AES s různou délkou klíče a doplňuje je 3DES. Jakou metodu zvolit záleží na potřebné míře zabezpečení, možného rizika a následného výkonu databáze. Symetrické šifrování databáze nemá takový dopad na výkon systému, nicméně použití asymetrických klíčů přináší vyšší bezpečnost, zejména v kombinaci s hardwarovým bezpečnostním modulem, kam je možné klíče uložit. Tím se stanou nedostupnými i pro administrátory systému.
Nicméně TDE neřeší nijak práva k datům. Zde je uplatněna zásada minimálních práv a jak uživatelé, tak i administrátoři systému mají pouze nezbytně nutná práva k systému. Například administrátor serveru nepotřebuje číst data v databázi, apod. Přístupová práva jsou řízena centrálně doménovými řadiči.

7.4.3 Síť

Síťová komunikace je v systému řešena výhradně jako point to point spoje na druhé vrstvě ISO/OSI. Jednotlivé systémy mají vlastní VLAN a mezi těmito sítěmi jsou navíc umístěny virtuální firewally. Jednotlivé části systému spolu komunikují přes integrační platformu ESB. Dále veškerá síťová komunikace využívá šifrovaného protokolu HTTPS. Jedná se o REST a SOAP volání.
Obecně známé slabé šifrovací algoritmy HTTPS nejsou vůbec povoleny.

Podnik má dále implementován systém Cisco ISE, který zabraňuje jakémukoliv neautorizovanému HW přistupovat do sítě společnosti.
Vzdálený přístup do systému je povolen pouze administrátorům systému z důvodu držení pohotovostí. Řešen je pomocí tunelu VPN. VPN je možné navázat pouze pomocí heslem zabezpečeného certifikátu. Po přihlášení do sítě tímto tunelem jsou aplikovány GPO a oprávnění, stejná jako v budově podniku. Úroveň bezpečnosti je tedy stejná jako v případě fyzické přítomnosti administrátora na pracovišti.
Tím je zajištěna maximální ochrana dat proti útokům na komunikační vrstvu.

7.4.4 Počítače

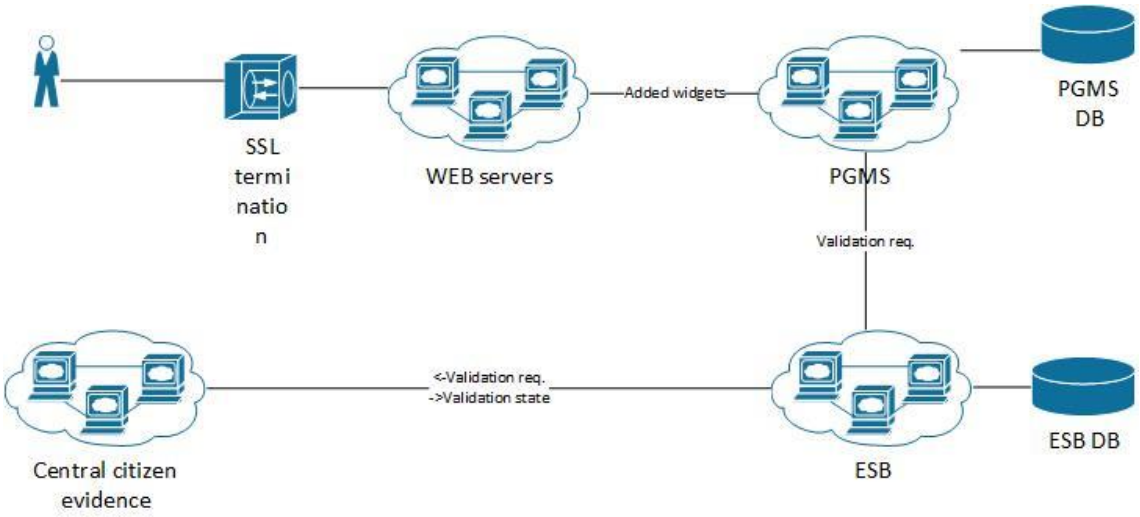
Při plnění pracovních úkolů zaměstnanců, se osobní údaje mohou dostat i na lokální počítače či notebooky. Ochrana těchto dat je řešena plošným šifrováním pevných disků počítačů a notebooků technologii Bitlocker v kombinaci s hardwarovým bezpečnostním modulem pro uložení klíčů. Na všech počítačích je samozřejmostí kvalitní antivirový program s centrální správou. Toto řešení umožnuje administrátorům udržet přehled o stavu antivirové ochrany jednotlivých počítačů a její dálkovou konfiguraci. Dále podnik používá software třetí strany ke klasifikaci a sledování dokumentů a emailů.
Každý dokument je doplněn o metadata, která říkají, jak citlivý obsah v dokumentu je a zda obsahuje nějaké osobní údaje. Následně jsou aplikovány politiky na ukládání těchto dokumentů na přenosná média, jejich tisk a posílání emailem. Jakákoliv podezřelá manipulace s citlivými dokumenty je automaticky reportována oddělení security. V některých případech může být i manipulaci aktivně bráněno.

7.4.5 Aktualizace, penetrační testy a hardening

Samozřejmou součástí ochrany dat jsou pravidelné bezpečnostní aktualizace operačních systémů serverů, počítačů a síťových prvků. Celý systém je také čtyřikrát do roka podrobován penetračním testům třetí stranou. Testy odpovídají opět doporučením OWASP. V neposlední řadě je prováděn tzv. hardening systému. Jinými slovy se podnik snaží průběžně systém dělat odolnější a bezpečnější. Průběžně je vyhodnocováno, jaké služby systém nabízí a jaké verze protokolů podporuje. Nepotřebné služby, či zastaralé ev. ne už bezpečné protokoly jsou zakazovány a odebírány.

7.5 Příklady toku dat (případy užití)

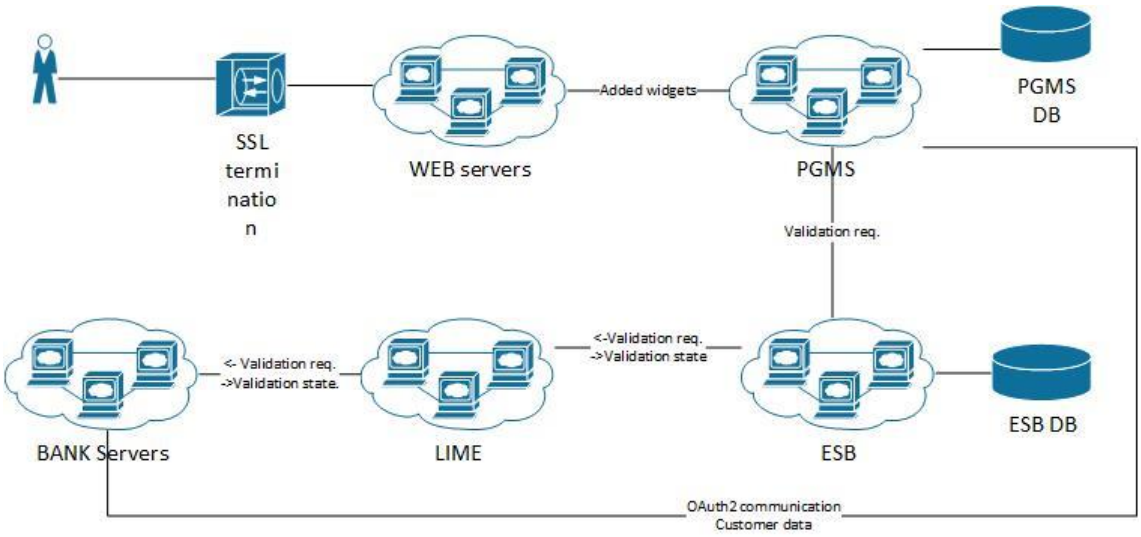
Registrace nového zákazníka:



Obrázek 4 - Registrace nového zákazníka

Proces registrace nového zákazníka se odehrává plně ve widgetu PGMS. Frontend se tedy k žádným osobním údajům nedostane. Zákazník vyplní zákonem vyžadované údaje, a pokud projdou prvotními kontrolami, např. platnost rodného čísla, formáty polí atd. je přistoupeno k validaci údajů s Centrálním registrem obyvatel. V případě úspěšného ověření je založen dočasný 30denní účet, který má omezení definovaná zákonem. Podnik ještě musí ověřit identitu, platební metodu a vlastnictví bankovního účtu zákazníka. To už jsou však samostatné případy užití.

Ověření identity bankou:



Obrázek 5 - Ověření identity Bankou

Podnik z legislativních důvodů musí dbát na ověření identity a plnoletosti svých zákazníků. Jako jedna z poměrně úspěšných cest, jak snadno online naplnit legislativní podmínky, se ukázala spolupráce s bankami. Podnik vycházel z předpokladu, že banky mají své zákazníky ověřeny a to včetně jejich plnoletosti. Tuto myšlenku přijalo i ministerstvo financí, a tento postup pro ověření zákazníků byl schválen.

Na obrázku 5. je naznačen design systému. Celý proces začíná na frontendu, kde je vložen widget z PGMS. V okamžiku, kdy zákazník požádá o ověření pomocí banky, je kontaktován server LIME, ten následně kontaktuje příslušnou banku a zprostředkuje následnou komunikaci mezi PGMS a bankou zabezpečeným protokolem OAuth2. PGMS pošle do banky údaje poskytnuté zákazníkem. Banka následně uloží zašifrovanou zprávu s výsledkem na server LIME, kde si jí PGMS vyzvedne a zákazníka validuje nebo zamítne.

7.5.1 SIEM

Nad všemi systémy podniku dohlíží SIEM QRadar od společnosti IBM. Logy ze všech systémů jsou sbírány a ukládaný na speciální úložiště a slouží k odhalování možných probíhajících útoků nebo k vyšetřování útoků již proběhlých. Výhodou SIEM je, že nad logy lze dělat sofistikované analýzy a dávat je do souvislostí napříč systémy.
Role operátorů a správců systému SIEM je opět oddělena od IT administrátorů systému a náleží plně oddělení Security. Je však třeba mít neustále na paměti, aby jeden člověk neměl příliš mnoho oprávnění najednou.

7.5.2 Dodavatelé

Vzhledem k rozsáhlosti hlavního systému, zvolil podnik strategii dodávek jednotlivých částí od různých dodavatelů. Z pohledu zabezpečení osobních údajů, je tento stav řešen tak, že dodavatelé do styku s osobními údaji nepřicházejí. V systému je pro komunikaci používané pouze pseudonymizované ID zákazníka. Klíč ke spojení osobních údajů zákazníka s jeho ID je pouze v PGMS a nikde jinde. Systémy dodavatelů se v případě potřeby, pouze obecnými dotazy doptávají na informace v PGMS. Jedná se pouze o dotazy „může toto ID vsadit“, „má toto ID dostatečný zůstatek na účtu“ atd. Od PGMS dostávají pouze informaci ano/ne. Tím je zaručeno, že se do systémů dodavatelů nedostanou žádné citlivé informace o identitě zákazníků, zůstatcích na účtech, nebo případně o výhrách.

8 Kritické zhodnocení navrženého řešení

Závěrem je možné říci, že „*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)*“, známější jako směrnice GDPR se není nutno obávat. Z počátku, zejména kvůli hrozbě likvidačních pokut, budila mezi podniky veliké obavy a na druhou stranu u fyzických osob vyvolávala neúměrná očekávání.
Podniky nevěděly, zda a za jaké náklady budou schopny směrnici plnit. S postupem času a implementace nařízení GDPR do podnikových procesů, se tyto obavy jeví jako liché.

V zásadě směrnice GDPR nutí podniky udělat si pořádek v datech, dbát o jejich bezpečnost a přehled o tom kdo s případnými osobními údaji nakládá a jak.
Směrnice GDPR neukládá nic, co by nebylo v dnešní informační společnosti, kdy data často bývají to nejcennější, samozřejmostí.
Technické požadavky směrnice GDPR se dají naplnit implementací známých a běžných technologií a postupů na obecnou ochranu dat. Při zodpovědném přístupu podniku k problematice informační bezpečnosti by podnik měl mít většinu technických opatření implementovánu bez ohledu na požadavky směrnice GDPR.
Studiem směrnice GDPR bylo dospěno k následujícím závěrům:

1. Podniky jsou plně zodpovědné za osobní údaje, které uchovávají. Musí mít o nich dokonalý přehled a mít možnost je kdykoli spravovat.
2. Podniky musí získávat a evidovat souhlasy se zpracováním osobních údajů a být schopny je doložit.
3. Občané mají právo na opravu osobních údajů, právo být zapomenut a právo na omezené zpracování. Tato práva musí podnik zajistit a garantovat.
4. Podniky mají také informační povinnost vůči třetím stranám, kterým osobní údaje zákonným způsobem poskytly. Jedná se zejména o situace vznikající při uplatnění práv subjektů z bodu 3.
5. Podniky také zodpovídají za nepřetržitou důvěrnost, integritu a dostupnost systémů zpracovávajících osobní údaje.

Nicméně k naplnění požadavků směrnice GDPR není potřeba vyvíjet nějaká speciální opatření, či technická řešení. Plně postačující je, aby podnik měl přehled kde, a za jakým účelem osobní údaje ukládá, řídil k nim přístup, měl vyřešené souhlasy se zpracováním, jejich odvolávání a přijal obecné zásady a technická řešení k ochraně dat.

Nad rámec navrhovaného, může podnik implementovat nějaké vlastní speciální softwarové řešení navržené na míru požadavkům GDPR. V tomto řešení by bylo možné zohlednit všechny povinnosti a záludnosti směrnice GDPR, vyřešit bezpečnost a v neposlední řadě i zálohování a obnovu osobních údajů tak, aby vždy odpovídala poskytnutým souhlasům. Jak je částečně naznačeno v kapitole 6.3 Centrální správa

osobních údajů. Nicméně implementaci obecných bezpečnostních opatření by se podnik neměl vyhýbat.

9 Závěr

Prvním cílem této práce byla analýza dopadů směrnice GDPR na technická opatření pro její plnění v prostředí soukromé firmy. Toto je řešeno v kapitole 5. Analýza dopadových kritérií. Ze směrnice byly vybrány články, které mají, nebo mohou k dosažení souladu se směrnicí GDPR vyžadovat nějaká technická opatření. Tyto pak byly následně jeden po druhém představeny, rozebrány a byl nastíněn směr možného technického řešení. K ověření správnosti rozboru byly využívány výklady Úřadu pro ochranu osobních údajů a EU.

V druhém bloku teoretické části - kapitola 6. Analýza možných technických opatření byly představeny obecná opatření a zásady ochrany dat, tedy i osobních údajů. Bylo nastíněno rozdělení problematiky na vnější a vnitřní hrozby. Tyto hrozby pak byly postupně identifikovány a bylo navrženo nějaké konkrétní opatření k jejich eliminaci.

V praktické časti - kapitola 7. Případová studie jsou navržena konkrétní technická opatření k naplnění požadavků směrnice GDPR v hlavním systému podniku. Podnik je z přísně regulovaného segmentu a podléhá, jak bankovnímu zákonu, tak i zákonu o hazardních hrách. Z tohoto vyplývá, že podnik musí klást velký důraz na bezpečnost svých dat.

Je navrženo řešení, jak z pohledu architektury systému podniku, tak i opatření na úrovni infrastruktury. Jednotlivé části jsou rozebrány a jsou předvedena konkrétní opatření k zajištění bezpečnosti dat, tedy i osobních údajů, které jsou v podniku ukládány. Řešení vychází z praxe autora a jeho funkčnost je ověřena každodenním provozem systému.

10 Seznam použité literatury

Online:

[1] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679: 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)* [online]. 27.4.2016 [cit. 2018-01-26]. Dostupné z: http://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[5] *Network Security* [online]. Elsevier, 2013, **2013**(10) [cit. 2018-02-06]. ISSN 1353-4858. Dostupné z: https://doi.org/10.1016/S1353-4858(13)70114-4

[6] DOČEKAL, Michal. Proč a jak na šifrování disků v Linuxu? [online]. 22.5.2008 [cit. 2018-02-07]. Dostupné z: https://www.root.cz/clanky/proc-a-jak-na-sifrovani-disku-v-linuxu/

[7] Ochrana osobních údajů podle nařízení GDPR. *Oficiální internetové stránky Evropské unie* [online]. 2018 [cit. 2018-09-27]. Dostupné z: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_cs.htm

[8] Nejdůležitější pojmy. Úřad pro ochranu osobních údajů [online]. 2018 [cit. 2018-09-10]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaj/d-27276

[9] KOMÍNKOVÁ, Magda. Jak vznikalo nařízení o ochraně osobních údajů (GDPR)?. *Euroskop.cz* [online]. 2018 [cit. 2018-09-27]. Dostupné z: https://www.euroskop.cz/9047/30715/clanek/jak-vznikalo-narizeni-o-ochrane-osobnich-udaju-gdpr/

[10] SOSNOVSKI, Rafal. Bitlocker: AES-XTS (new encryption type) [online]. 4 Března, 2016 [cit. 2019-04-28]. Dostupné z: https://blogs.technet.microsoft.com/dubaisec/2016/03/04/bitlocker-aes-xts-new-encryption-type/

11 Přílohy

Příloha č. 1

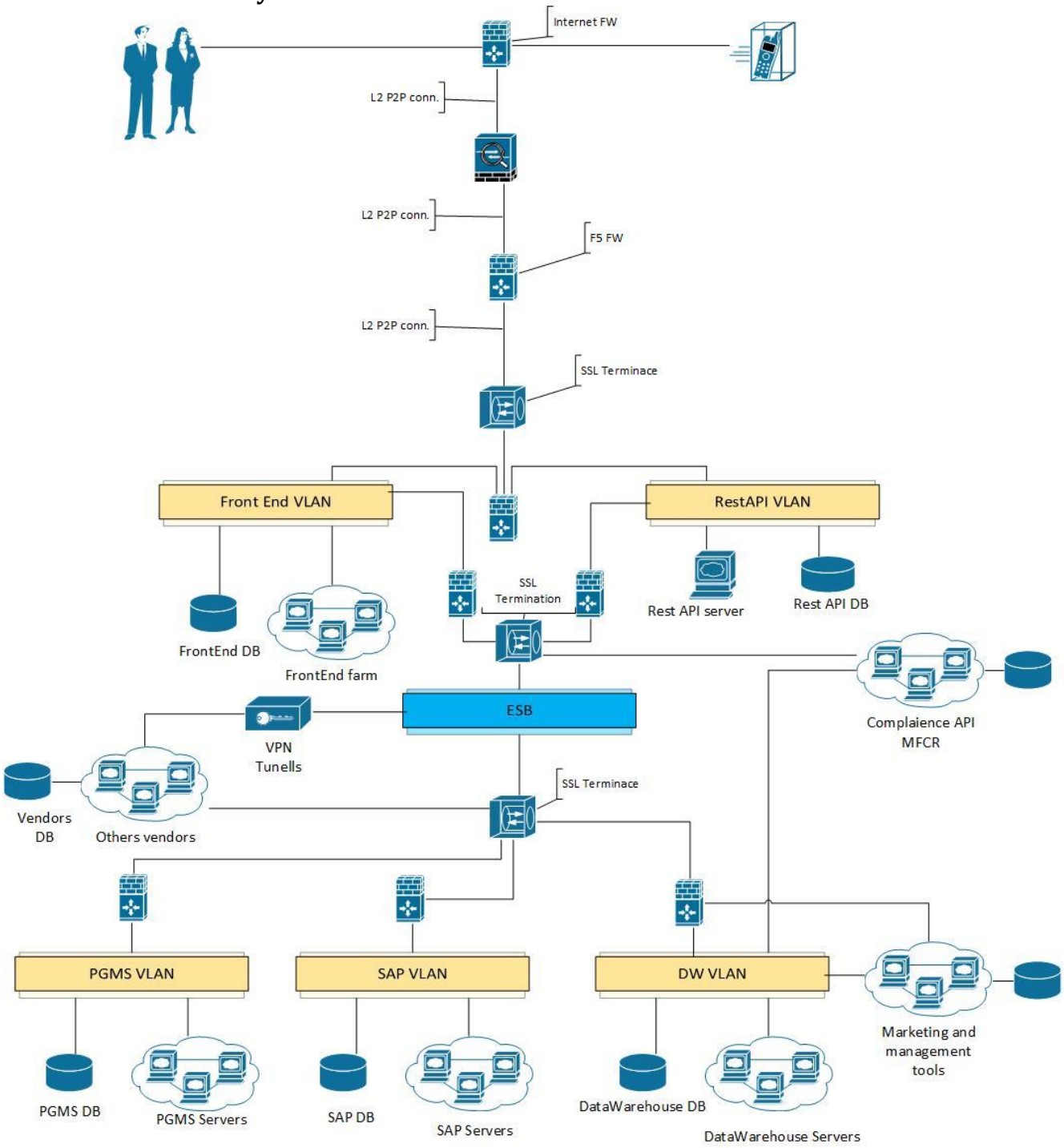
	Otázky	Odpovědi	Nutné kroky
1.	Jaká osobní data shromažďujeme [1)]		
2.	Proč to děláme [2)]		
3.	Jak data získáváme [3)]		
4.	Kdy data získáváme [4)]		
5.	Kdo je za data zodpovědný [5)]		
6.	Co se s daty u nás děje [6)]		

Tabulka 1 Dotazník datového auditu[9]

[9] Zdroj: Data Audit Checklist. *Http://mewburn.com/* [online]. [cit. 2018-10-25]. Dostupné z: http://mewburn.com/wp-content/uploads/2018/07/GDPR-Data-Audit-Checklist.pdf

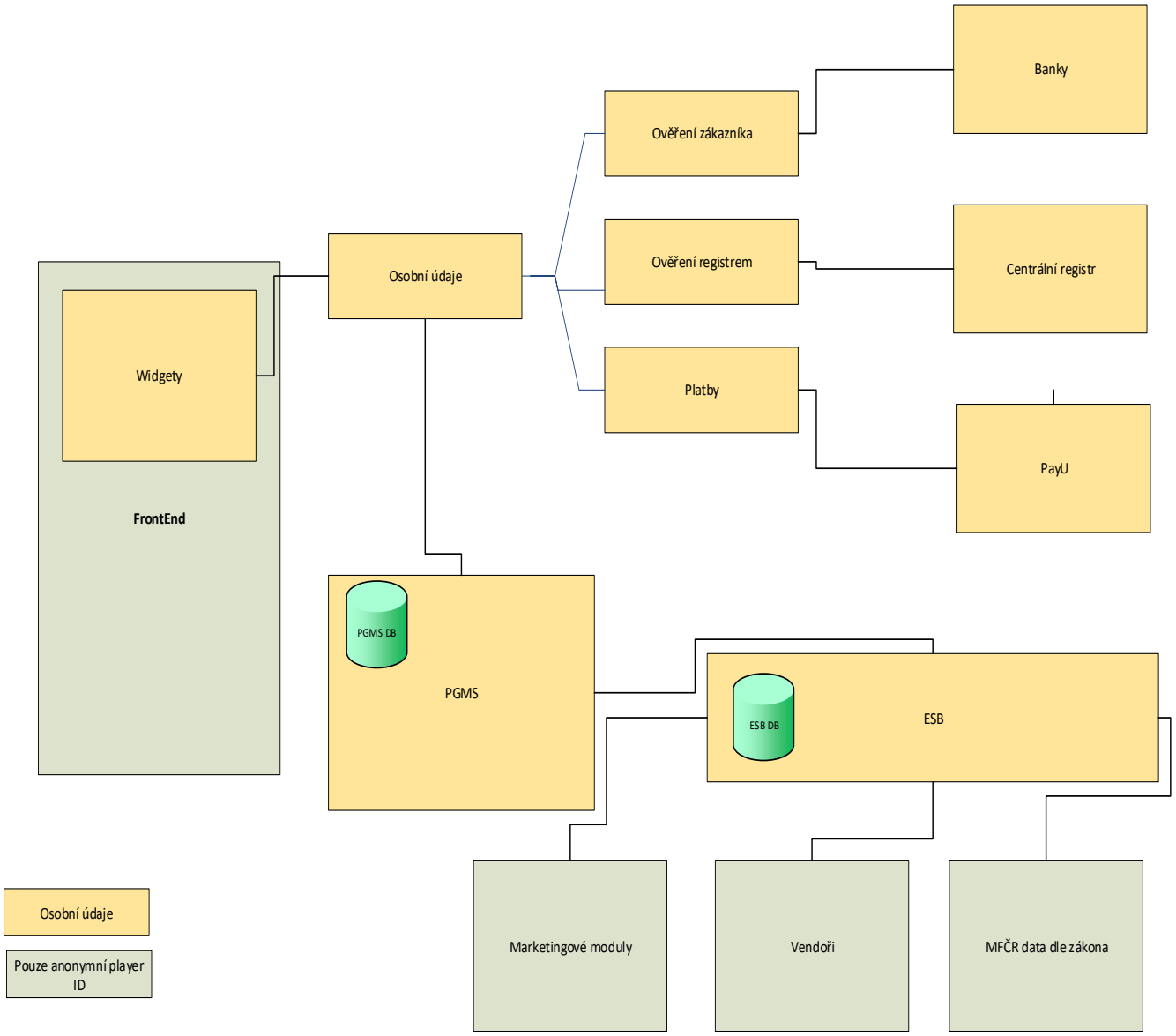
Příloha č. 2

Schéma infrastruktury



Příloha č. 3

Systémy dle přístupu k osobním údajům.



Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor: **Leoš Karásek**

Studium: I1500487

Studijní program: B1802 Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Název bakalářské práce: **Technická opatření pro plnění GDPR**

Název bakalářské práce AJ: Technical measures for GDPR implementation

Cíl, metody, literatura, předpoklady:

Cílem práce je analýza dopadů zavedení směrnice Evropské komise 95/46/ES (GDPR) na technická opatření pro její plnění v prostředí soukromé firmy. V teoretické části autor představí hlavní dopady plynoucí ze směrnice GDPR a provede analýzu technických opatření pro její plní. V praktické části pak autor na základě provedené analýzy navrhne a zrealizuje vhodná technická opatření s důrazem na správce systémů zpracovávající údaje podléhající GDPR, tak aby navržené technické řešení podpořilo komplexní plnění směrnice. Úvod Představení GDPR Analýza dopadových kritérií Analýza možných technických opatření Návrh a realizace tech. opatření Zhodnocení projektu Závěr

Regulation (EU) 2016/679 of the European Parliament [online]. EU, 2016 [cit. 2017-10-21]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501688126470&uri=CELEX:32016R0679 GDPR. UK: IT Governance Publishing, 2017. ISBN 978-1-84928-946-7. LAMBERT, Paul. The data protection officer: profession, rules, and role. New York: CRC Press, Taylor & Francis Group, 2017. ISBN 9781138031937.

Garantující pracoviště: Katedra informačních technologií,
Fakulta informatiky a managementu

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Datum zadání závěrečné práce: 21.10.2014

I

(Legislativní akty)

NAŘÍZENÍ

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)

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 16 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru ([1]),

s ohledem na stanovisko Výboru regionů ([2]),

v souladu s řádným legislativním postupem ([3]),

vzhledem k těmto důvodům:

(1) Ochrana fyzických osob v souvislosti se zpracováním osobních údajů je základním právem. Ustanovení čl. 8 odst. 1 Listiny základních práv Evropské unie (dále jen „Listina“) a čl. 16 odst. 1 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“) přiznávají každému právo na ochranu osobních údajů, které se jej týkají.

(2) Zásady a pravidla ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů by bez ohledu na jejich státní příslušnost nebo bydliště měly respektovat jejich základní práva a svobody, zejména právo na ochranu osobních údajů. Cílem tohoto nařízení je přispět k dotvoření prostoru svobody, bezpečnosti a práva a hospodářské unie, k hospodářskému a sociálnímu pokroku, k posílení a sblížení ekonomik v rámci vnitřního trhu a k dobrým životním podmínkám fyzických osob.

(3) Účelem směrnice Evropského parlamentu a Rady 95/46/ES ([4]) je harmonizovat právní předpisy o ochraně základních práv a svobod fyzických osob v souvislosti s činnostmi zpracování a zajistit volný pohyb osobních údajů mezi členskými státy.

([1]) Úř. věst. C 229, 31.7.2012, s. 90.
([2]) Úř. věst. C 391, 18.12.2012, s. 127.
([3]) Postoj Evropského parlamentu ze dne 12. března 2014 (dosud nezveřejněný v Úředním věstníku) a postoj Rady v prvním čtení ze dne 8. dubna 2016 (dosud nezveřejněný v Úředním věstníku). Postoj Evropského parlamentu ze dne 14. dubna 2016.
([4]) Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, s. 31).

(4) Zpracování osobních údajů by mělo sloužit lidem. Právo na ochranu osobních údajů není právem absolutním; musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy. Toto nařízení ctí všechna základní práva a dodržuje svobody a zásady uznávané Listinou, jak jsou zakotveny ve Smlouvách, zejména respektování soukromého a rodinného života, obydlí a komunikace, ochranu osobních údajů, svobodu myšlení, svědomí a náboženského vyznání, svobodu projevu a informací, svobodu podnikání, právo na účinnou právní ochranu a spravedlivý proces, jakož i kulturní, náboženskou a jazykovou rozmanitost.

(5) Hospodářská a sociální integrace vyplývající z fungování vnitřního trhu vedla ke značnému nárůstu přeshraničních toků osobních údajů. V celé Unii se zvýšila výměna osobních údajů mezi veřejnými a soukromými aktéry, včetně fyzických osob, sdružení a podniků. Právo Unie zavazuje vnitrostátní orgány členských států ke spolupráci a výměně osobních údajů, aby mohly plnit své povinnosti nebo provádět úkoly jménem orgánu jiného členského státu.

(6) Rychlý technologický rozvoj a globalizace s sebou přinesly nové výzvy pro oblast ochrany osobních údajů. Rozsah shromažďování a sdílení osobních údajů významně vzrostl. Technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu. Fyzické osoby stále častěji své osobní údaje zveřejňují, a to i v globálním měřítku. Technologie změnily ekonomiku i společenský život a měly by dále usnadňovat volný pohyb osobních údajů v rámci Unie a předávání do třetích zemí a mezinárodním organizacím a zároveň zajistit vysokou úroveň ochrany osobních údajů.

(7) Tento vývoj vyžaduje pevný a soudržnější rámec pro ochranu osobních údajů v Unii, jenž by se opíral o důsledné vymáhání práva, a to s ohledem na nezbytnost nastolit důvěru, která umožní rozvoj digitální ekonomiky na celém vnitřním trhu. Fyzické osoby by měly mít možnost kontrolovat své vlastní osobní údaje. Měla by být posílena právní a praktická jistota fyzických osob, hospodářských subjektů a orgánů veřejné moci.

(8) Stanoví-li toto nařízení upřesnění nebo omezení svých pravidel právem členského státu, mohou členské státy začlenit do svého vnitrostátního práva prvky tohoto nařízení, pokud je to nezbytné pro účely soudržnosti a pro učinění vnitrostátních předpisů srozumitelnými pro osoby, na něž se vztahují.

(9) Ačkoliv cíle a zásady směrnice 95/46/ES nadále platí, nezabránilo to roztříštěnosti v provádění ochrany údajů v celé Unii, právní nejistotě ani rozšířenému pocitu veřejnosti, že v souvislosti s ochranou fyzických osob existují značná rizika, zejména pokud jde o činnosti prováděné online. Rozdíly v úrovni ochrany práv a svobod fyzických osob, zejména práva na ochranu osobních údajů, v souvislosti se zpracováním osobních údajů v členských státech mohou bránit volnému pohybu osobních údajů v rámci Unie. Tyto rozdíly proto mohou být překážkou pro výkon hospodářských činností na úrovni Unie, mohou narušovat hospodářskou soutěž a bránit orgánům veřejné moci ve výkonu povinností, které jim ukládají právní předpisy Unie. Tato rozdílná úroveň ochrany je způsobena rozdíly v provádění a uplatňování směrnice 95/46/ES.

(10) S cílem zajistit soudržnou a vysokou úroveň ochrany fyzických osob a odstranit překážky bránící pohybu osobních údajů v rámci Unie by měla být úroveň ochrany práv a svobod fyzických osob v souvislosti se zpracováním těchto údajů rovnocenná ve všech členských státech. V celé Unii je třeba zajistit soudržné a jednotné uplatňování pravidel ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů. Pokud jde o zpracování osobních údajů z důvodu splnění právní povinnosti, provádění určitého úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, měly by mít členské státy možnost zachovat či zavést vnitrostátní předpisy za účelem dále konkretizovat uplatňování pravidel tohoto nařízení. Ve spojení s obecnými a horizontálními právními předpisy o ochraně údajů provádějícími směrnici 95/46/ES existuje v členských státech několik právních předpisů specifických pro určitá odvětví v oblastech, ve kterých je třeba přijmout konkrétnější ustanovení. Toto nařízení rovněž poskytuje členským státům určitý prostor ke stanovení vlastních pravidel, včetně pravidel pro zpracování zvláštních kategorií osobních údajů („citlivé osobní údaje“). V tomto rozsahu nařízení nevylučuje, aby právo členského státu stanovilo okolnosti konkrétních situací, při nichž dochází ke zpracování, včetně přesnějšího určení podmínek, za nichž je zpracování osobních údajů zákonné.

(11) Účinná ochrana osobních údajů v celé Unii vyžaduje nejen posílení a podrobné vymezení práv subjektů údajů a povinností těch, kdo osobní údaje zpracovávají a o jejich zpracování rozhodují, ale také rovnocenné pravomoci pro monitorování a zajišťování souladu s pravidly ochrany osobních údajů a rovnocenné sankce za jejich porušování v členských státech.

(12) Ustanovení čl. 16 odst. 2 Smlouvy o fungování EU zmocňuje Evropský parlament a Radu ke stanovení pravidel o ochraně fyzických osob při zpracování osobních údajů a pravidel o volném pohybu těchto údajů.

(13) Aby byla zajištěna jednotná úroveň ochrany fyzických osob v celé Unii a zamezilo se rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu, je nezbytné přijmout nařízení, které poskytne hospodářským subjektům, včetně mikropodniků a malých a středních podniků, právní jistotu a transparentnost, které fyzickým osobám ve všech členských státech zajistí stejnou úroveň práv vymahatelných právními prostředky a správcům a zpracovatelům uloží povinnosti a úkoly, které zajistí důsledné monitorování zpracování osobních údajů a rovnocenné sankce ve všech členských státech, jakož i účinnou spolupráci mezi dozorovými úřady jednotlivých členských států. Řádné fungování vnitřního trhu vyžaduje, aby volný pohyb osobních údajů v Unii nebyl z důvodů souvisejících s ochranou fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán. Aby byla zohledněna specifická situace mikropodniků a malých a středních podniků, obsahuje toto nařízení odchylku pro organizace s méně než 250 zaměstnanci týkající se uchovávání údajů. Kromě toho jsou orgány a instituce Unie, členské státy a jejich dozorové úřady podporovány v tom, aby specifické potřeby mikropodniků a malých a středních podniků zohledňovaly při uplatňování tohoto nařízení. Pojem mikropodniky a malé a střední podniky by měl vycházet z článku 2 přílohy doporučení Komise 2003/361/ES ([1]).

(14) Ochrana poskytovaná tímto nařízením by se měla týkat zpracování osobních údajů fyzických osob bez ohledu na jejich státní příslušnost nebo bydliště. Toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby.

(15) S cílem zabránit vzniku vážného rizika obcházení by ochrana fyzických osob měla být technologicky neutrální a nezávislá na použitých technologiích. Ochrana fyzických osob by se měla vztahovat jak na automatizované zpracování osobních údajů, tak na manuální zpracování, pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy. Záznamy nebo soubory záznamů ani jejich titulní strany, které nejsou uspořádány podle určených hledisek, by do oblasti působnosti tohoto nařízení spadat neměly.

(16) Toto nařízení se nevztahuje na otázky ochrany základních práv a svobod nebo volného pohybu osobních údajů v souvislosti s činnostmi, které nespadají do působnosti práva Unie, jako jsou činnosti týkající se národní bezpečnosti. Toto nařízení se rovněž nevztahuje na zpracování osobních údajů členskými státy při výkonu činností v rámci společné zahraniční a bezpečnostní politiky Unie.

(17) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ([2]) se vztahuje na zpracování osobních údajů orgány, institucemi a jinými subjekty Unie. Nařízení (ES) č. 45/2001 a další právní akty Unie týkající se takového zpracování osobních údajů by měly být uzpůsobeny zásadám a pravidlům zavedeným tímto nařízením a uplatňovány s ohledem na toto nařízení. S cílem zajistit pevný a soudržný rámec pro ochranu osobních údajů na úrovni Unie by po přijetí tohoto nařízení měly následovat nezbytné úpravy nařízení (ES) č. 45/2001, aby bylo možné jej uplatňovat zároveň s tímto nařízením.

(18) Toto nařízení se nevztahuje na zpracování osobních údajů fyzickou osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností. Činnosti osobní povahy nebo činnosti v domácnosti by mohly zahrnovat korespondenci a vedení

([1]) Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků (C(2003) 1422) (Úř. věst. L 124, 20.5.2003, s. 36).

([2]) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

adresářů nebo využívání sociálních sítí a internetu v souvislosti s těmito činnostmi. Toto nařízení se však vztahuje na správce nebo zpracovatele, kteří pro tyto činnosti osobní povahy či činnosti v domácnosti poskytují prostředky pro zpracování osobních údajů.

(19) Ochrana fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem předcházení trestným činům nebo jejich vyšetřování, odhalování či stíhání nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení a volný pohyb těchto údajů jsou upraveny zvláštním právním aktem Unie. Proto by se toto nařízení nemělo uplatňovat na činnosti zpracování za těmito účely. Na osobní údaje zpracovávané orgány veřejné moci podle tohoto nařízení, pokud jsou používány za těmito účely, by se však měl vztahovat konkrétnější právní akt Unie, totiž směrnice Evropského parlamentu a Rady (EU) 2016/680 ([1]). Členské státy mohou pověřit příslušné orgány ve smyslu směrnice (EU) 2016/680 i úkoly, které nemusí být nutně prováděny za účelem předcházení trestným činům a jejich vyšetřování, odhalování či stíhání nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, tak aby zpracování osobních údajů pro tyto jiné účely v rozsahu, v němž náleží do působnosti práva Unie, spadalo do oblasti působnosti tohoto nařízení.

Pokud jde o zpracování osobních údajů těmito příslušnými orgány pro účely spadající do oblasti působnosti tohoto nařízení, měly by mít členské státy možnost ponechat v platnosti nebo zavést konkrétnější ustanovení, aby používání pravidel tohoto nařízení přizpůsobily. Tato ustanovení mohou přesněji určit konkrétní požadavky na zpracování osobních údajů těmito příslušnými orgány pro uvedené jiné účely, s přihlédnutím k ústavní, organizační a správní struktuře daného členského státu. Pokud zpracování osobních údajů soukromými subjekty spadá do oblasti působnosti tohoto nařízení, mělo by toto nařízení členským státům umožnit, aby za určitých podmínek zákonem omezily některé povinnosti a práva, jestliže takové omezení představuje nezbytné a přiměřené opatření v demokratické společnosti na ochranu konkrétních důležitých zájmů, včetně veřejné bezpečnosti a předcházení trestným činům a jejich vyšetřování, odhalování či stíhání nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. To je relevantní například v rámci boje proti praní peněz nebo činností forenzních laboratoří.

(20) Toto nařízení se mimo jiné vztahuje na činnost soudů a dalších justičních orgánů, a proto by právo Unie nebo členského státu mohlo stanovit operace a postupy zpracování v souvislosti se zpracováním osobních údajů soudy a dalšími justičními orgány. Pravomoc dozorových úřadů by neměla zahrnovat zpracování osobních údajů, pokud soudy jednají v rámci svých soudních pravomocí, aby byla zajištěna nezávislost soudnictví při plnění soudních funkcí, včetně rozhodování. Dozor nad takovými operacemi zpracování by mělo být možné svěřit zvláštním subjektům v rámci justičního systému členského státu, které by zejména měly zajistit soulad s pravidly tohoto nařízení, posilovat povědomí členů justičních orgánů o jejich povinnostech podle tohoto nařízení a zabývat se stížnostmi souvisejícími s takovými operacemi zpracování.

(21) Tímto nařízením není dotčeno uplatňování směrnice Evropského parlamentu a Rady 2000/31/ES ([2]), zejména pokud jde o pravidla týkající se odpovědnosti poskytovatelů zprostředkovatelských služeb uvedená v článcích 12 až 15 uvedené směrnice. Cílem uvedené směrnice je přispět k řádnému fungování vnitřního trhu tím, že zajistí volný pohyb služeb informační společnosti mezi členskými státy.

(22) Jakékoliv zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii by mělo být prováděno v souladu s tímto nařízením bez ohledu na to, zda samotné zpracování probíhá v Unii nebo mimo ni. Provozovna předpokládá účinný a skutečný výkon činnosti prostřednictvím stálého zařízení. Právní forma této provozovny, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem.

([1]) 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 a o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (viz strana 89 v tomto čísle Úředního věstníku).

([2]) Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu) (Úř. věst. L 178, 17.7.2000, s. 1).

(23) Aby bylo zajištěno, že fyzickým osobám nebude odepřena ochrana, na niž mají podle tohoto nařízení nárok, mělo by se na zpracování osobních údajů subjektů údajů nacházejících se v Unii uskutečněné správcem nebo zpracovatelem, jenž není v Unii usazen, vztahovat toto nařízení, pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb těmto subjektům údajů bez ohledu na to, zda je spojena s platbou. Aby se určilo, zda takový správce nebo zpracovatel nabízí zboží nebo služby subjektům údajů nacházejícím se v Unii, je třeba zjistit, zda je zjevné, že má správce nebo zpracovatel v úmyslu nabízet služby subjektům údajů v jednom nebo více členských státech v Unii. Zatímco pouhá dostupnost internetových stránek správce, zpracovatele nebo zprostředkovatele v Unii, e-mailové adresy nebo jiných kontaktních údajů anebo používání jazyka obecně používaného ve třetí zemi, v níž je správce usazen, nepostačuje ke zjištění tohoto úmyslu, mohly by faktory, jako je používání jazyka nebo měny obecně používaných v jednom nebo více členských státech, spolu s možností objednat zboží a služby v tomto jiném jazyce nebo zmínky o zákaznících či uživatelích nacházejících se v Unii, být zjevným dokladem toho, že správce má v úmyslu nabízet zboží nebo služby subjektům údajů v Unii.

(24) Na zpracování osobních údajů subjektů údajů nacházejících se v Unii správcem nebo zpracovatelem, který není v Unii usazen, by se rovněž mělo vztahovat toto nařízení, pokud souvisí s monitorováním chování takových subjektů údajů v rozsahu, v němž k tomuto chování dochází v Unii. Aby se určilo, zda může být činnost zpracování považována za monitorování chování subjektu údajů, mělo by být zjištěno, zda jsou fyzické osoby sledovány na internetu, včetně případného následného použití technik zpracování osobních údajů, které spočívají v profilování fyzické osoby, zejména za účelem přijetí rozhodnutí, která se jí týkají, nebo za účelem analýzy či odhadu jejích osobních preferencí, postojů a chování.

(25) Pokud se právo členského státu uplatňuje na základě mezinárodního práva veřejného, mělo by se toto nařízení vztahovat také na správce, který není usazen v Unii, například na diplomatické misi nebo na konzulárním zastoupení členského státu.

(26) Zásady ochrany údajů by se měly uplatňovat na všechny informace týkající se identifikované nebo identifikovatelné fyzické osoby. Osobní údaje, na něž byla uplatněna pseudonymizace a jež by mohly být přiřazeny fyzické osobě na základě dodatečných informací, by měly být považovány za informace o identifikovatelné fyzické osobě. Při určování, zda je fyzická osoba identifikovatelná, by se mělo přihlédnout ke všem prostředkům, jako je například výběr vyčleněním, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby. Ke stanovení toho, zda lze rozumně předpokládat použití prostředků k identifikaci fyzické osoby, by měly být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím k technologii dostupné v době zpracování i k technologickému rozvoji. Zásady ochrany osobních údajů by se proto neměly vztahovat na anonymní informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným. Toto nařízení se tedy netýká zpracování těchto anonymních informací, včetně zpracování pro statistické nebo výzkumné účely.

(27) Toto nařízení se nevztahuje na osobní údaje zesnulých osob. Členské státy mohou stanovit pravidla týkající se zpracování osobních údajů zesnulých osob.

(28) Použití pseudonymizace osobních údajů může omezit rizika pro dotčené subjekty údajů a napomoci správcům a zpracovatelům splnit jejich povinnosti týkající se ochrany údajů. Výslovné zavedení „pseudonymizace“ v tomto nařízení nemá za cíl předem vyloučit jakákoliv další opatření týkající se ochrany údajů.

(29) S cílem vytvořit pobídky pro uplatňování pseudonymizace při zpracování osobních údajů by opatření pseudonymizace při současném umožnění obecné analýzy měla být možná v rámci téhož správce, pokud tento správce přijal technická a organizační opatření nezbytná k zajištění toho, aby bylo v případě daného zpracování provedeno toto nařízení a aby doplňkové informace pro přiřazení osobních údajů konkrétnímu subjektu údajů byly uchovány samostatně. Správce, který zpracovává osobní údaje, by rovněž měl označit oprávněné osoby v rámci téhož správce.

(30) Fyzickým osobám mohou být přiřazeny síťové identifikátory, které využívají jejich zařízení, aplikace, nástroje a protokoly, jako například adresy internetového protokolu či identifikátory cookies, nebo jiné identifikátory, jako jsou štítky pro identifikaci na základě rádiové frekvence. Tímto způsobem mohou být zanechány stopy, které mohou být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají, použity k profilování fyzických osob a k jejich identifikaci.

(31) Orgány veřejné moci, kterým jsou osobní údaje sdělovány na základě právní povinnosti pro účely výkonu jejich úředních povinností, jako jsou daňové a celní orgány, finanční vyšetřovací jednotky, nezávislé správní orgány nebo orgány finančního trhu příslušné pro regulaci trhů s cennými papíry a dohled nad nimi, by neměly být považovány za příjemce, pokud obdrží osobní údaje, které jsou nezbytné pro provedení konkrétního šetření v obecném zájmu v souladu s právem Unie či členského státu. Žádost o sdělení osobních údajů zaslaná orgány veřejné moci by měla být vždy písemná a odůvodněná, měla by se týkat jednotlivého případu a neměla by se vztahovat na celou evidenci ani vést k propojení evidencí. Zpracování osobních údajů těmito orgány veřejné moci by mělo být v souladu s platnými pravidly pro ochranu osobních údajů podle účelů zpracování.

(32) Souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení. Mohlo by se například jednat o zaškrtnutí políčka při návštěvě internetové stránky, volbu technického nastavení pro služby informační společnosti nebo jiné prohlášení či jednání, které v této souvislosti jasně signalizuje souhlas subjektu údajů s navrhovaným zpracováním jeho osobních údajů. Mlčení, předem zaškrtnutá políčka nebo nečinnost by tudíž neměly být považovány za souhlas. Souhlas by se měl vztahovat na veškeré činnosti zpracování prováděné pro stejný účel nebo stejné účely. Jestliže má zpracování několik účelů, měl by být souhlas udělen pro všechny. Má-li subjekt údajů vyjádřit souhlas na základě žádosti podané elektronickými prostředky, musí být žádost jasná a stručná a nesmí zbytečně narušit využívání služby, pro kterou je souhlas dáván.

(33) Často není možné v době shromažďování osobních údajů v plném rozsahu stanovit účel zpracování osobních údajů pro účely vědeckého výzkumu. Subjektům údajů by proto mělo být umožněno, aby udělily svůj souhlas ohledně určitých oblastí vědeckého výzkumu v souladu s uznávanými etickými normami pro vědecký výzkum. Subjekty údajů by měly mít možnost udělit svůj souhlas pouze pro některé oblasti výzkumu nebo části výzkumných projektů v rozsahu přípustném pro zamýšlený účel.

(34) Genetické údaje by měly být definovány jako osobní údaje týkající se zděděných nebo získaných genetických znaků určité fyzické osoby, které vyplývají z analýzy biologického vzorku dotčené fyzické osoby, zejména chromozomů nebo kyseliny deoxyribonukleové (DNA) či ribonukleové (RNA), anebo z analýzy jiného prvku, která umožňuje získat rovnocenné informace.

(35) Mezi osobní údaje o zdravotním stavu by měly být zahrnuty veškeré údaje související se zdravotním stavem subjektu údajů, které vypovídají o minulém, současném či budoucím tělesném nebo duševním zdraví subjektu údajů. To zahrnuje informace o dané fyzické osobě shromážděné v průběhu registrace pro účely zdravotní péče a jejího poskytování dotčené fyzické osobě podle směrnice Evropského parlamentu a Rady 2011/24/EU ([1]), číslo, symbol nebo specifický údaj přiřazený fyzické osobě za účelem její jedinečné identifikace pro zdravotnické účely, informace získané během provádění testů nebo vyšetřování části těla nebo tělesných látek, včetně z genetických údajů a biologických vzorků, a jakékoliv informace například o nemoci, postižení, riziku onemocnění, anamnéze, klinické léčbě nebo fyziologickém či biomedicínském stavu subjektu údajů nezávisle na jejich původu, tedy bez ohledu na to, zda pocházejí například od lékaře nebo jiného zdravotníka, z nemocnice, ze zdravotnického prostředku či diagnostických testů in vitro.

(36) Hlavní provozovnou správce v Unii by mělo být místo, kde se nachází jeho ústřední správa v Unii, ledaže by rozhodnutí ohledně účelů a prostředků zpracování osobních údajů byla přijímána v jiné provozovně správce v Unii, a v tom případě by za hlavní provozovnu měla být považována tato jiná provozovna. Hlavní provozovna

([1]) Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči (Úř. věst. L 88, 4.4.2011, s. 45).

správce v Unii by měla být určena na základě objektivních kritérií. Jedním z nich by měl být účinný a skutečný výkon řídících činností rozhodujících pro hlavní rozhodnutí ohledně účelů a prostředků zpracování v rámci stálého zařízení. Toto kritérium by nemělo záviset na tom, zda je zpracování osobních údajů prováděno na tomto místě. Existence a používání technických prostředků a technologií pro zpracování osobních údajů ani činnosti zpracování nezakládají samy o sobě hlavní provozovnu, a proto nejsou rozhodujícími kritérii pro její určení. Hlavní provozovna zpracovatele by měla být místem, kde se nachází jeho ústřední správa v Unii, nebo pokud v Unii nemá ústřední správu, pak místem, kde jsou v Unii prováděny hlavní činnosti zpracování. V případech týkajících se správce i zpracovatele by příslušným vedoucím dozorovým úřadem měl i nadále být dozorový úřad členského státu, v němž má správce hlavní provozovnu, avšak dozorový úřad zpracovatele by měl být považován za dotčený dozorový úřad a účastnit se postupu spolupráce stanoveného tímto nařízením. Dozorové úřady členského státu nebo členských států, v nichž má zpracovatel jednu nebo více provozoven, by v žádném případě neměly být považovány za dotčené dozorové úřady, pokud se návrh rozhodnutí týká pouze správce. Pokud zpracování provádí skupina podniků, měly by být za hlavní provozovnu této skupiny považována hlavní provozovna řídícího podniku, s výjimkou případů, kdy účely a způsob zpracování určuje jiný podnik.

(37) Skupina podniků by měla zahrnovat řídící podnik a jím řízené podniky, přičemž řídícím podnikem by měl být podnik, jenž může uplatňovat dominantní vliv na jiné podniky například na základě vlastnictví, finanční účasti nebo pravidel, kterými se podnik řídí, či pravomoci prosazovat pravidla týkající se ochrany osobních údajů. Podnik, který vykonává správu zpracování osobních údajů v podnicích k němu přidružených, by měl být společně s těmito podniky považován za skupinu podniků.

(38) Děti zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů. Tato zvláštní ochrana by se měla zejména vztahovat na používání osobních údajů dětí pro účely marketingu nebo vytváření osobnostních či uživatelských profilů a shromažďování osobních údajů týkajících se dětí při využívání služeb nabízených přímo dětem. Souhlas nositele rodičovské zodpovědnosti by neměl být nutný v případě preventivních či poradenských služeb nabízených přímo dětem.

(39) Jakékoliv zpracování osobních údajů by mělo být prováděno zákonným a spravedlivým způsobem. Pro fyzické osoby by mělo být transparentní, že osobní údaje, které se jich týkají, jsou shromažďovány, používány, konzultovány nebo jinak zpracovávány, jakož i v jakém rozsahu tyto osobní údaje jsou či budou zpracovány. Zásada transparentnosti vyžaduje, aby všechny informace a všechna sdělení týkající se zpracování těchto osobních údajů byly snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků. Tato zásada se dotýká zejména informování subjektů údajů o totožnosti správce a účelech zpracování a o dalších záležitostech v zájmu zajištění spravedlivého a transparentního zpracování ve vztahu k dotčeným fyzickým osobám a jejich práva získat potvrzení a na sdělení zpracovávaných osobních údajů, které se jich týkají. Fyzické osoby by měly být upozorněny na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a jak mají v souvislosti s tímto zpracováním uplatňovat svá práva. Zejména je zapotřebí, aby konkrétní účely, pro které jsou osobní údaje zpracovávány, byly jednoznačné a legitimní a aby byly stanoveny v okamžiku shromažďování osobních údajů. Osobní údaje by měly být přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelů, pro které jsou zpracovávány. Je nezbytné zejména zajistit, aby byla doba, po kterou jsou osobní údaje uchovávány, omezena na nezbytné minimum. Osobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky. Aby se zajistilo, že osobní údaje nebudou uchovávány déle, než je nezbytné, měl by správce stanovit lhůty pro výmaz nebo pravidelný přezkum. Měla by být přijata veškerá vhodná opatření, aby nepřesné osobní údaje byly opraveny nebo vymazány. Osobní údaje by měly být zpracovávány způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění neoprávněnému přístupu k osobním údajům a k zařízení používanému k jejich zpracování nebo jejich neoprávněnému použití.

(40) Aby bylo zpracování zákonné, měly by být osobní údaje zpracovávány na základě souhlasu subjektu údajů nebo s ohledem na nějaký jiný legitimní základ stanovený právními předpisy, buď v tomto nařízení, nebo v jiném

právním předpise Unie nebo členského státu, jak je uvedeno v tomto nařízení, mimo jiné i s ohledem na nezbytnost dodržení zákonné povinnosti, která se na správce vztahuje, nebo nezbytnost plnění smlouvy, jejíž stranou je subjekt údajů, nebo za účelem přijetí opatření na žádost subjektu údajů před uzavřením smlouvy.

(41) Odkazy v tomto nařízení na právní základ či legislativní opatření neznamenají nutně legislativní akt přijatý parlamentem, aniž jsou dotčeny požadavky vyplývající z ústavního řádu dotčeného členského státu. Tento právní základ či legislativní opatření by však měly být jasné a přesné a jejich použití by mělo být předvídatelné pro osoby, na něž se vztahují, jak to vyžaduje judikatura Soudního dvora Evropské unie (dále jen „Soudní dvůr“) a Evropského soudu pro lidská práva.

(42) Pokud je zpracování založeno na souhlasu subjektu údajů, měl by být správce schopen prokázat, že subjekt údajů vyjádřil s danou operací zpracování souhlas. Zejména v případě písemného prohlášení souvisejícího s jinou skutečností by mělo být pomocí záruk zajištěno, že si je subjekt údajů vědom toho, že dává souhlas a v jakém rozsahu. V souladu se směrnicí Rady 93/13/EHS ([1]) by prohlášení o souhlasu navržené správcem mělo být poskytnuto ve srozumitelném a snadno přístupném znění za použití jasného a jednoduchého jazyka a nemělo by obsahovat nepřiměřené podmínky. Aby se zajistilo, že souhlas bude informovaný, měl by subjekt údajů znát alespoň totožnost správce a účely zpracování, k nimž jsou jeho osobní údaje určeny. Souhlas by neměl být považován za svobodný, pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen.

(43) S cílem zajistit, aby byl souhlas svobodný, by vyjádření souhlasu nemělo představovat platný právní důvod pro zpracování osobních údajů ve zvláštním případě, kdy mezi subjektem údajů a správcem existuje jasná nerovnováha, zejména pokud je správce orgánem veřejné moci, a je tedy nepravděpodobné, že za všech okolností této konkrétní situace byl souhlas udělen svobodně. Lze předpokládat, že souhlas není svobodný, není-li možné vyjádřit samostatný souhlas s jednotlivými operacemi zpracování osobních údajů, i když je to v daném případě vhodné, nebo je-li plnění smlouvy, včetně poskytnutí služby učiněno závislým na souhlasu, i když to není pro toto plnění nezbytné.

(44) Zpracování by mělo být zákonné, pokud je nezbytné v souvislosti s plněním smlouvy nebo úmyslem smlouvu uzavřít.

(45) Pokud je zpracování prováděno v souladu se zákonnou povinností, která se na správce vztahuje, nebo pokud je zpracování nezbytné ke splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci, mělo by mít toto zpracování základ v právu Unie nebo členského státu. Toto nařízení nestanoví požadavek zvláštního právního předpisu pro každé jednotlivé zpracování. Jeden právní předpis jakožto základ pro více operací zpracování údajů založených na právní povinnosti, která se na správce vztahuje, nebo pokud je zpracování nezbytné ke splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci, může být dostačující. Právo Unie nebo členského státu by rovněž mělo stanovit účel zpracování. Toto právo by dále mohlo upřesnit obecné podmínky nařízení, kterými se řídí zákonnost zpracování osobních údajů, stanovit podrobnosti týkající se určení správce, typu osobních údajů, které mají být zpracovány, dotčených subjektů údajů, subjektů, kterým lze osobní údaje sdělit, účelového omezení, doby uložení a dalších opatření k zajištění zákonného a spravedlivého zpracování. Právo Unie nebo členského státu by rovněž mělo stanovit, zda by správcem plnícím úkol ve veřejném zájmu nebo při výkonu veřejné moci měl být orgán veřejné moci nebo jiná veřejnoprávní právnická osoba, nebo pokud je to odůvodněno veřejným zájmem, včetně oblasti zdraví, jako je veřejné zdraví a sociální ochrana a řízení zdravotnických služeb, fyzická osoba či soukromoprávní právnická osoba, například profesní sdružení.

(46) Zpracování osobních údajů by mělo být rovněž považováno za zákonné, pokud je nezbytné pro ochranu životně důležitého zájmu subjektu údajů nebo jiné fyzické osoby. Zpracování osobních údajů na základě životně

([1]) Směrnice Rady 93/13/EHS ze dne 5. dubna 1993 o nepřiměřených podmínkách ve spotřebitelských smlouvách (Úř. věst. L 95, 21.4.1993, s. 29).

důležitého zájmu jiné fyzické osoby by mělo v zásadě proběhnout pouze tehdy, pokud zjevně nemůže být založeno na jiném právním základě. Některé druhy zpracování mohou sloužit jak důležitým důvodům veřejného zájmu, tak životně důležitým zájmům subjektu údajů, například je-li zpracování nezbytné pro humanitární účely, včetně monitorování epidemií a jejich šíření nebo v naléhavých humanitárních situacích, zejména v případech přírodních a člověkem způsobených katastrof.

(47) Oprávněné zájmy správce, včetně správce, jemuž mohou být osobní údaje poskytnuty, nebo třetí strany se mohou stát právním základem zpracování za předpokladu, že nepřevažují zájmy nebo základní práva a svobody subjektu údajů, a to při zohlednění přiměřeného očekávání subjektu údajů na základě jeho vztahu se správcem. Tento oprávněný zájem by mohl být dán například v situaci, kdy existuje relevantní a odpovídající vztah mezi subjektem údajů a správcem, například pokud je subjekt údajů zákazníkem správce nebo mu naopak poskytuje služby. Existenci oprávněného zájmu je v každém případě třeba pečlivě posoudit, včetně toho, zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít. Zájmy a základní práva subjektu údajů by mohly převážit nad zájmy správce údajů zejména tehdy, jestliže ke zpracování osobních údajů dochází za okolností, kdy subjekt údajů jejich další zpracování důvodně neočekává. Jelikož právní základ pro zpracování osobních údajů orgány veřejné moci má upravit zákonodárce právním předpisem, neměl by se tento právní základ vztahovat na zpracování prováděné orgány veřejné moci při plnění jejich úkolů. Oprávněným zájmem dotčeného správce údajů je rovněž zpracování osobních údajů nezbytně nutné pro účely zamezení podvodům. Zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu oprávněného zájmu.

(48) Správci, kteří jsou součástí skupiny podniků nebo instituce přidružené k ústřednímu orgánu, mohou mít oprávněný zájem na předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků či zaměstnanců. Obecné zásady pro předávání osobních údajů v rámci skupiny podniků do podniku nacházejícího se ve třetí zemi zůstávají nedotčeny.

(49) Zpracování osobních údajů v rozsahu nezbytně nutném a přiměřeném pro zajištění bezpečnosti sítě a informací, to jest schopnosti sítě nebo informačního systému odolávat na dané úrovni spolehlivosti, náhodným událostem nebo protiprávnímu či zlovolnému jednání ohrožujícímu dostupnost, pravost, správnost a důvěrnost uložených či předávaných osobních údajů a bezpečnost souvisejících služeb poskytovaných či přístupných prostřednictvím těchto sítí a systémů, které provádějí orgány veřejné moci, skupiny pro reakci na počítačové hrozby (CERT), skupiny pro reakci na incidenty v oblasti počítačové bezpečnosti (CSIRT), poskytovatelé elektronických komunikačních sítí a služeb a poskytovatelé bezpečnostních technologií a služeb, představuje oprávněný zájem dotčeného správce údajů. Oprávněný zájem by například mohl spočívat v zabránění neoprávněnému přístupu k sítím elektronických komunikací a šíření škodlivých kódů a zamezení útokům, jejichž důsledkem je odepření služby, a škodám na počítačových systémech a systémech elektronických komunikací.

(50) Zpracování osobních údajů pro jiné účely, než jsou ty, pro které byly osobní údaje původně shromážděny, by mělo být povoleno pouze v případě, kdy je slučitelné s účely, pro které byly osobní údaje původně shromážděny. V takovém případě není třeba právní základ odlišný od toho, který umožnil shromáždění osobních údajů. Pokud je zpracování nezbytné ke splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce, mohou být v právu Unie nebo členského státu určeny a vymezeny úkoly a účely, pro které se další zpracování považuje za slučitelné a zákonné. Další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely by mělo být považováno za slučitelné zákonné operace zpracování. Právní základ pro zpracování osobních údajů podle práva Unie nebo členského státu může rovněž posloužit jako právní základ pro další zpracování. S cílem zjistit, zda je účel dalšího zpracování slučitelný s účelem, pro který byly osobní údaje původně shromážděny, by měl správce, po splnění všech požadavků na zákonnost původního zpracování, vzít mimo jiné v úvahu jakoukoliv vazbu mezi těmito účely a účely zamýšleného dalšího zpracování, kontext, v němž byly osobní údaje shromážděny, zejména

přiměřená očekávání ohledně dalšího použití osobních údajů, která mají subjekty údajů na základě svého vztahu se správcem, povahu osobních údajů, důsledky zamýšleného dalšího zpracování pro subjekty údajů a existenci vhodných záruk jak během původních, tak během zamýšlených dalších operací zpracování.

Pokud subjekt údajů udělil souhlas nebo pokud je zpracování na základě práva Unie nebo členského státu, které představuje v rámci demokratické společnosti nezbytné a přiměřené opatření s cílem zajistit zejména důležité cíle obecného veřejného zájmu, měl by správce mít možnost dalšího zpracování osobních údajů bez ohledu na slučitelnost účelů. V každém případě by mělo být zajištěno, že budou uplatňovány zásady stanovené v tomto nařízení, a zejména že bude subjekt údajů o těchto jiných účelech a o svých právech, včetně práva vznést námitku, informován. Oznámení případných trestných činů nebo hrozeb pro veřejnou bezpečnost správcem a předání dotčených osobních údajů příslušnému orgánu v jednotlivých případech nebo v několika případech týkajících se téhož trestného činu nebo hrozeb pro veřejnou bezpečnost by mělo být považováno za oprávněný zájem správce. Avšak takové přenesení oprávněného zájmu správce nebo další zpracování osobních údajů by mělo být zakázáno, jestliže není slučitelné s povinností mlčenlivosti vyplývající ze zákona či se závaznou povinností zachovávat profesní či jiné tajemství.

(51) Osobní údaje, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod, zasluhují zvláštní ochranu, jelikož by při jejich zpracování mohla vzniknout závažná rizika pro základní práv a svobody. Mezi tyto osobní údaje by měly patřit osobní údaje vypovídající o rasovém či etnickém původu, ovšem s tím, že použití slov „rasový původ“ v tomto nařízení neznamená, že Unie akceptuje teorie, které se pokoušejí určit existenci různých lidských ras. Zpracování fotografií by nemělo být systematicky považováno za zpracování zvláštních kategorií osobních údajů, neboť na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby. Tyto osobní údaje by neměly být zpracovávány, pokud není zpracování povoleno ve zvláštních případech stanovených tímto nařízením, a to se zohledněním skutečnosti, že v právu členských států mohou být stanovena zvláštní ustanovení o ochraně údajů s cílem přizpůsobit uplatňování pravidel tohoto nařízení za účelem dodržení zákonné povinnosti nebo splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce. Společně se zvláštními požadavky na takové zpracování by se měly uplatňovat obecné zásady a další pravidla tohoto nařízení, zejména pokud jde o podmínky pro zákonné zpracování. Odchylky od obecného zákazu zpracování těchto zvláštních kategorií osobních údajů by měly být výslovně stanoveny mimo jiné v případě, kdy subjekt údajů poskytuje svůj výslovný souhlas nebo jde-li o zvláštní potřeby, zejména pokud je toto zpracování prováděno v průběhu oprávněných činností některých sdružení či nadací, jejichž cílem je umožnit výkon základních svobod.

(52) Je třeba rovněž povolit odchylky od zákazu zpracování zvláštních kategorií osobních údajů, jsou-li stanoveny v právu Unie nebo členského státu a chráněny vhodnými zárukami na ochranu osobních údajů a jiných základních práv, je-li toto zpracování ve veřejném zájmu, zejména zpracování osobních údajů v oblasti pracovního práva a práva v oblasti sociální ochrany, včetně důchodů, a pro účely zdravotní bezpečnosti, monitorování a varování, předcházení přenosným chorobám a jiným závažným hrozbám pro zdraví nebo jejich kontroly. Tato odchylka může být učiněna z důvodů zdraví, včetně veřejného zdraví a řízení zdravotnických služeb, zejména v zájmu zajištění kvality a hospodárnosti v postupech používaných pro vyřizování nároků na plnění a služby v systému zdravotního pojištění, nebo pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Odchylka by rovněž měla umožnit zpracování těchto osobních údajů v případech, kdy je to nezbytné pro stanovení, výkon nebo ochranu právních nároků, ať již v soudním řízení, nebo ve správním či mimosoudním řízení.

(53) Zvláštní kategorie osobních údajů, které zasluhují vyšší stupeň ochrany, by měly být zpracovávány pouze pro zdravotní účely, je-li třeba těchto účelů dosáhnout ve prospěch fyzických osob a společnosti jako celku, zejména v souvislosti s řízením zdravotnických služeb či služeb sociální péče a systémů, což zahrnuje zpracování těchto údajů vedoucími pracovníky a ústředními vnitrostátními zdravotnickými orgány pro účely kontroly kvality, správy informací a obecného vnitrostátního a místního dozoru nad systémem zdravotní nebo sociální péče, a zajištění kontinuity zdravotní nebo sociální péče a přeshraniční zdravotní péče nebo zdravotní bezpečnosti, pro účely monitorování a varování nebo pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely na základě práva Unie nebo členského státu, které musí být ve veřejném zájmu, jakož i pro studie prováděné ve veřejném zájmu v oblasti veřejného zdraví. Proto by toto nařízení mělo stanovit harmonizované podmínky pro zpracování zvláštních kategorií osobních údajů o zdravotním stavu, pokud jde o zvláštní potřeby, zejména je-li zpracování takových údajů prováděno pro určité účely související se

zdravím osobou vázanou profesním tajemstvím podle právních předpisů. Právo Unie nebo členského státu by mělo stanovit zvláštní a vhodná opatření s cílem chránit základní práva a osobní údaje fyzických osob. Členské státy by měly mít možnost zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu. To by však nemělo omezovat volný pohyb osobních údajů v rámci Unie, pokud se tyto podmínky uplatní na přeshraniční zpracování takových údajů.

(54) Z důvodů veřejného zájmu v oblasti veřejného zdraví může být nezbytné zpracovávat zvláštní kategorie osobních údajů bez souhlasu subjektu údajů. Toto zpracování by mělo podléhat vhodným a zvláštním opatřením s cílem chránit práva a svobody fyzických osob. V této souvislosti by mělo být „veřejné zdraví" vykládáno ve smyslu definice v nařízení Evropského parlamentu a Rady (ES) č. 1338/2008 ([1]), totiž jako veškeré prvky týkající se zdraví, zejména zdravotní stav včetně nemocnosti a zdravotního postižení, determinanty ovlivňující tento zdravotní stav, potřeby zdravotní péče, prostředky přidělené na zdravotní péči, poskytování zdravotní péče a její všeobecná dostupnost, výdaje na zdravotní péči a její financování a příčiny úmrtnosti. Takové zpracování údajů o zdravotním stavu z důvodu veřejného zájmu by nemělo vést k tomu, aby třetí strany, jako jsou zaměstnavatelé nebo pojišťovny a bankovní společnosti, zpracovávaly osobní údaje pro jiné účely.

(55) Zpracování osobních údajů orgány veřejné moci za účelem dosažení cílů úředně uznaných náboženských sdružení, které jsou stanoveny ústavním právem nebo mezinárodním právem veřejným, se uskutečňuje z důvodů veřejného zájmu.

(56) Pokud v rámci činností spojených s volbami je pro fungování demokratického systému v členském státě nezbytné, aby politické strany shromažďovaly údaje o politických názorech osob, může být zpracování těchto osobních údajů povoleno z důvodu veřejného zájmu za předpokladu, že jsou stanoveny vhodné záruky.

(57) Pokud správce zpracovává osobní údaje, které mu neumožňují identifikovat fyzickou osobu, neměl by být povinen získat dodatečné informace pro zjištění totožnosti subjektu údajů výlučně za účelem dosažení souladu s některým ustanovením tohoto nařízení. Správce by však neměl odmítnout převzít dodatečné informace poskytnuté subjektem údajů s cílem podpořit výkon jeho práv. Součástí identifikace by měla být digitální identifikace subjektu údajů, například prostřednictvím mechanismu autentizace na základě stejných pověřovacích údajů, které subjekt údajů používá pro přihlášení k on-line službám poskytovaným správcem údajů.

(58) Zásada transparentnosti vyžaduje, aby všechny informace určené veřejnosti nebo subjektu údajů byly stručné, snadno přístupné a srozumitelné, podávané za použití jasných a jednoduchých jazykových prostředků a ve vhodných případech navíc i vizualizace. Pokud budou tyto informace určeny veřejnosti, mohly by být poskytovány v elektronické podobě, například prostřednictvím internetových stránek. To platí obzvláště v situacích, kdy zapojení celé řady aktérů a technologická složitost znesnadňují subjektu údajů, aby věděl a porozuměl tomu, zda jsou shromažďovány jeho osobní údaje a kdo a za jakým účelem je shromažďuje, jako je reklama na internetu. Jelikož děti zasluhují zvláštní ochranu, měly by být v případech, kdy je na ně zpracování zaměřeno, všechny informace a sdělení podávány za použití jasných a jednoduchých jazykových prostředků, aby jim děti snadno porozuměly.

(59) Je třeba stanovit postupy, které by usnadnily výkon práv subjektů údajů podle tohoto nařízení, včetně mechanismů pro podávání žádostí a případně bezplatného obdržení přístupu k osobním údajům a opravy nebo výmazu osobních údajů a pro uplatnění práva vznést námitku. Správce by měl rovněž zajistit podmínky pro to, aby žádosti mohly být podávány elektronicky, zejména v případě zpracování osobních údajů elektronickými prostředky. Správci by měla být uložena povinnost reagovat na žádosti subjektu údajů bez zbytečného odkladu a nejpozději do jednoho měsíce a uvést důvody v případě, že nemá v úmyslu těmto žádostem vyhovět.

([1]) Nařízení Evropského parlamentu a Rady (ES) č. 1338/2008 ze dne 16. prosince 2008 o statistice Společenství v oblasti veřejného zdraví a bezpečnosti a ochrany zdraví při práci (Úř. věst. L 354, 31.12.2008, s. 70).

(60) Zásady spravedlivého a transparentního zpracování vyžadují, aby byl subjekt údajů informován o probíhající operaci zpracování a jejích účelech. Správce by měl subjektu údajů poskytnout veškeré další informace nezbytné pro zajištění spravedlivého a transparentního zpracování, s přihlédnutím ke konkrétním okolnostem a kontextu, v němž jsou osobní údaje zpracovávány. Subjekt údajů by měl být dále informován o profilování a o jeho důsledcích. Pokud jsou osobní údaje získávány od subjektu údajů, měl by subjekt údajů být rovněž informován, zda je povinen tyto údaje poskytnout, a o důsledcích jejich případného neposkytnutí. Tyto informace mohou být doplněny standardizovanými ikonami s cílem poskytnout snadno viditelným, srozumitelným a jasně čitelným způsobem přehled o zamýšleném zpracování. Pokud jsou ikony prezentovány v elektronické podobě, měly by být strojově čitelné.

(61) Informování subjektu údajů o tom, že jsou zpracovávány jeho osobní údaje, by mělo proběhnout v okamžiku jejich shromáždění od subjektu údajů, nebo pokud jsou získávány z jiného zdroje, v přiměřené lhůtě v závislosti na okolnostech případu. Jestliže mohou být osobní údaje oprávněně sděleny jinému příjemci, měl by být subjekt údajů informován o jejich prvním sdělení tomuto příjemci. Pokud správce hodlá osobní údaje zpracovat pro jiný účel, než je účel, pro který byly shromážděny, měl by poskytnout subjektu údajů informace o tomto jiném účelu a další nezbytné informace ještě před uvedeným dalším zpracováním. Pokud z důvodu využití různých zdrojů nemůže být subjektu údajů sdělen původ osobních údajů, měly by být poskytnuty obecné informace.

(62) Povinnost poskytnout informace však není třeba ukládat v případech, kdy subjekt údajů již uvedené informace má, nebo kdy zaznamenání či zpřístupnění osobních údajů je výslovně stanoveno právními předpisy, nebo kdy poskytnutí těchto informací subjektu údajů není možné nebo by vyžadovalo neúměrné úsilí. Poskytnutí informací by mohlo vyžadovat neúměrné úsilí zejména tehdy, je-li zpracování prováděno pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. V tomto ohledu by se mělo přihlédnout k počtu subjektů údajů, ke stáří osobních údajů a k přijatým vhodným zárukám.

(63) Subjekt údajů by měl mít právo na přístup ke shromážděným osobním údajům, které se ho týkají, a měl by moci toto právo snadno a v přiměřených odstupech uplatňovat, aby byl o jejich zpracování informován a mohl si ověřit jeho zákonnost. To zahrnuje právo subjektů údajů na přístup k údajům o svém zdravotním stavu, například k údajům ve své lékařské dokumentaci, která obsahuje například informace o diagnóze, výsledky vyšetření, posudky ošetřujících lékařů a údaje o veškeré léčbě a provedených ošetřeních nebo zákrocích. Každý subjekt údajů by proto měl mít právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, případně období, po které budou uchovávány, kdo jsou příjemci osobních údajů, v čem spočívá logika automatizovaného zpracování osobních údajů a jaké mohou být důsledky takového zpracování přinejmenším v případech, kdy je zpracování založeno na profilování. Je-li to možné, měl by mít správce možnost poskytnout dálkový přístup k bezpečnému systému, který by subjektu údajů umožnil přímý přístup k jeho osobním údajům. Tímto právem by neměla být nepříznivě dotčena práva ani svobody ostatních, například obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení. Zohlednění těchto skutečností by ovšem nemělo vést k tomu, že by subjektu údajů bylo odepřeno poskytnutí všech informací. Pokud správce zpracovává velké množství informací týkajících se subjektu údajů, měl by mít možnost před poskytnutím informací požádat subjekt údajů, aby konkrétně uvedl, kterých informací nebo činností zpracování se jeho žádost týká.

(64) Správce by měl využít všech vhodných opatření k ověření identity subjektu údajů, který žádá o přístup, zejména v souvislosti s on-line službami a síťovými identifikátory. Správce by neměl uchovávat osobní údaje pouze za tím účelem, aby mohl reagovat na případné žádosti.

(65) Fyzická osoba by měla mít právo na opravu osobních údajů, které se jí týkají, a „právo být zapomenuta“, pokud uchovávání těchto údajů porušuje toto nařízení nebo právo Unie či členského státu, které se na správce vztahuje. Subjekt údajů by zejména měl mít právo na to, aby jeho osobní údaje byly vymazány a nebyly dále zpracovávány, pokud již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány, pokud subjekt údajů odvolal svůj souhlas se zpracováním nebo pokud vznesl námitku proti zpracování osobních údajů, které se jej týkají, anebo pokud je zpracování jeho osobních údajů v rozporu s tímto nařízením z jiných důvodů. Toto právo

je obzvláště důležité v případech, kdy subjekt údajů dal svůj souhlas v dětském věku a nebyl si plně vědom rizik spojených se zpracováním a později chce tyto osobní údaje zejména na internetu odstranit. Subjekt údajů by měl mít možnost toto právo uplatnit bez ohledu na skutečnost, že již není dítě. Další uchovávání osobních údajů by však mělo být zákonné, pokud je to nezbytné k uplatnění práva svobody projevu a informací, z důvodu splnění právní povinnosti, provádění určitého úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, z důvodů veřejného zájmu v oblasti veřejného zdraví, pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely nebo pro určení, výkon nebo obhajobu právních nároků.

(66) Aby bylo v internetovém prostředí posíleno právo být zapomenut, mělo by být rozšířeno právo na výmaz tím, že by správce, který zveřejnil osobní údaje, měl povinnost informovat správce, kteří osobní údaje zpracovávají, aby vymazali veškeré odkazy na dané osobní údaje či veškeré jejich kopie nebo replikace. Přitom by měl správce učinit vhodné kroky, s přihlédnutím k dostupné technologii a prostředkům, které má k dispozici, včetně uplatňování technických opatření, s cílem informovat správce, kteří tyto osobní údaje zpracovávají, o žádosti subjektu údajů.

(67) Způsoby, jak omezit zpracování osobních údajů, by mohly mimo jiné zahrnovat dočasný přesun vybraných údajů do jiného systému zpracování, znepřístupnění vybraných osobních údajů uživatelům nebo dočasné odstranění zveřejněných údajů z internetových stránek. V systémech automatizovaného zpracování by omezení zpracování mělo být v zásadě zajištěno technickými prostředky tak, aby se na osobní údaje již nevztahovaly žádné další operace zpracování a aby nemohly být změněny. Skutečnost, že zpracování osobních údajů je omezeno, by měla být v systému jasně vyznačena..

(68) Aby měl subjekt údajů větší kontrolu nad svými údaji, měl by v případě, kdy se osobní údaje zpracovávají automatizovaně, mít též právo získat osobní údaje, které se ho týkají, a jež poskytl správci, ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu a předat je jinému správci. Správce údajů je třeba podporovat v rozvíjení interoperabilních formátů umožňujících přenositelnost údajů. Toto právo by se mělo uplatnit v případě, kdy subjekt údajů poskytl osobní údaje na základě svého souhlasu, nebo pokud je zpracování potřebné za účelem plnění smlouvy. Nemělo by se uplatňovat v případě, kdy je zpracování založeno na jiném právním důvodu, než je souhlas nebo smlouva. Vzhledem ke své povaze by toto právo nemělo být uplatňováno vůči správcům, kteří zpracovávají osobní údaje v rámci výkonu veřejné moci. Proto by se nemělo uplatňovat v případě, kdy je zpracování osobních údajů nezbytné pro splnění právní povinnosti, která se na správce vztahuje, nebo pro vykonání úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce. Právo subjektu údajů předat nebo obdržet osobní údaje, které se ho týkají, by nemělo zakládat povinnost správců zavést nebo zachovávat technicky kompatibilní systémy zpracování. Pokud se určitý soubor osobních údajů týká více než jednoho subjektu údajů, neměla by právem obdržet osobní údaje být dotčena práva a svobody jiných subjektů údajů podle tohoto nařízení. Tímto právem by dále nemělo být dotčeno právo subjektu údajů dosáhnout výmazu osobních údajů a omezení uvedeného práva, jak je stanoveno v tomto nařízení, a zejména by toto právo nemělo znamenat výmaz osobních údajů týkajících se daného subjektu údajů, které tento subjekt údajů poskytl v rámci plnění smlouvy, v rozsahu, v němž jsou tyto osobní údaje nezbytné pro plnění dané smlouvy, a po dobu nezbytně nutnou pro toto plnění. Pokud je to technicky možné, měl by mít subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci jinému.

(69) Pokud mohou být osobní údaje zákonně zpracovávány, protože je toto zpracování nezbytné pro výkon úkolů vykonávaných ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, nebo z důvodu oprávněných zájmů správce nebo třetí strany, měl by každý dotčený subjekt údajů přesto mít právo vznést námitku proti zpracování osobních údajů, které se týkají jeho konkrétní situace. Mělo by být povinností správce, aby prokázal, že jeho závažné oprávněné zájmy převažují nad zájmy nebo základními právy a svobodami subjektu údajů.

(70) Jsou-li osobní údaje zpracovávány pro účely přímého marketingu, měl by mít subjekt údajů právo kdykoli bezplatně vznést námitku proti tomuto zpracování, včetně profilování, v rozsahu, v němž souvisí s daným přímým marketingem, ať již jde o počáteční, nebo další zpracování. Na toto právo by měl být subjekt údajů výslovně upozorněn a toto právo by mělo být uvedeno zřetelně a odděleně od jakýchkoli jiných informací.

(71) Subjekt údajů by měl mít právo nebýt předmětem žádného rozhodnutí, a to včetně opatření, které hodnotí osobní aspekty týkající se jeho osoby, vychází výlučně z automatizovaného zpracování a které má pro něj právní účinky nebo se jej podobně významně dotýká, jako jsou automatizované zamítnutí on-line žádosti o úvěr nebo postupy elektronického náboru bez jakéhokoliv lidského zásahu. Takové zpracování zahrnuje „profilování", jehož podstatou je jakákoliv forma automatizovaného zpracování osobních údajů hodnotící osobní aspekty vztahující se k fyzické osobě, zejména za účelem analýzy či předvídání aspektů souvisejících s pracovním výkonem subjektu údajů, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo chováním, místem pobytu či pohybu, pokud má pro něj právní účinky nebo se jí podobným způsobem významně dotýká. Rozhodování založené na takovém zpracování, včetně profilování, by však mělo být umožněno, pokud jej výslovně povoluje právo Unie nebo členského státu, které se na správce vztahuje, mimo jiné pro účely monitorování podvodů a daňových úniků a jejich předcházení, jež jsou v souladu s předpisy, normami a doporučeními orgánů Unie nebo vnitrostátních dozorových úřadů, a s cílem zajistit bezpečnost a spolehlivost služby poskytované správcem, nebo pokud je nezbytné pro uzavření nebo plnění smlouvy mezi subjektem údajů a správcem nebo pokud k tomu subjekt údajů dal svůj výslovný souhlas. V každém případě by se na takové zpracování měly vztahovat vhodné záruky, které by měly zahrnovat konkrétní informování subjektu údajů a právo na lidský zásah, na vyjádření svého názoru, na získání vysvětlení o rozhodnutí učiněném po takovém posouzení a na napadnutí tohoto rozhodnutí. Toto opatření by se nemělo týkat dítěte.

V zájmu zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů a s přihlédnutím ke konkrétním okolnostem a souvislostem, za kterých se dané osobní údaje zpracovávají, by měl správce použít vhodné matematické nebo statistické postupy profilování, zavést technická a organizační opatření, která zejména zajistí opravu faktorů vedoucích k nepřesnosti osobních údajů a minimalizaci rizika chyb, a zabezpečit osobní údaje takovým způsobem, který zohledňuje potenciální rizika pro zájmy a práva subjektu údajů a který mimo jiné předchází diskriminačním účinkům vůči fyzickým osobám na základě rasy nebo etnického původu, politických názorů, náboženského vyznání nebo přesvědčení, členství v odborech, genetických údajů nebo zdravotního stavu či sexuální orientace nebo předchází přijímání opatření, jež mají takové účinky. Automatizované rozhodování a profilování založené na zvláštních kategoriích osobních údajů by mělo být povoleno pouze za určitých podmínek.

(72) Na profilování se vztahují pravidla tohoto nařízení pro zpracování osobních údajů, jako jsou právní důvody zpracování nebo zásady ochrany údajů. Evropský sbor pro ochranu osobních údajů zřízený tímto nařízením (dále jen „sbor") by měl mít možnost vydat v této souvislosti pokyny.

(73) Právo Unie nebo členského státu může uložit omezení určitých zásad a práva na informace, na přístup a na opravu nebo na výmaz osobních údajů, práva na přenositelnost osobních údajů, práva vznést námitku, rozhodnutí založených na profilování, jakož i omezení týkající se oznamování případů porušení zabezpečení osobních údajů subjektu údajů nebo určitých souvisejících povinností správců, pokud je to v demokratické společnosti nutné a přiměřené pro zachování veřejné bezpečnosti, mimo jiné pro ochranu lidských životů, zejména v reakci na přírodní nebo člověkem způsobené katastrofy, pro předcházení trestným činům nebo jejich vyšetřování či stíhání nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, a pro předcházení porušování deontologických pravidel regulovaných povolání a jejich vyšetřování a stíhání, pro jiné významné cíle obecného veřejného zájmu Unie nebo členského státu, zejména jedná-li se o důležitý hospodářský či finanční zájem Unie nebo členského státu, vedení veřejných rejstříků z důvodů obecného veřejného zájmu, dalšího zpracování archivovaných osobních údajů s cílem poskytnout konkrétní informace související s politickým chováním za bývalého totalitního režimu nebo s ohledem na ochranu subjektu údajů či práv a svobod ostatních, včetně sociální ochrany, veřejného zdraví a humanitárních účelů. Tato omezení by měla být v souladu s požadavky stanovenými v Listině a v Evropské úmluvě o ochraně lidských práv a základních svobod.

(74) Měla by být stanovena odpovědnost správce za jakékoliv zpracování osobních údajů prováděné správcem nebo pro něj. Správce by měl být zejména povinen zavést vhodná a účinná opatření a být schopen doložit, že činnosti zpracování jsou v souladu s tímto nařízením, včetně účinnosti opatření. Tato opatření by měla zohledňovat povahu, rozsah, kontext a účely zpracování a riziko pro práva a svobody fyzických osob.

(75) Různě pravděpodobná a závažná rizika pro práva a svobody fyzických osob mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné nebo nehmotné újmě, zejména v případech, kdy by zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě důvěrnosti osobních údajů chráněných služebním tajemstvím, neoprávněnému zrušení pseudonymizace nebo jakémukoliv jinému významnému hospodářskému či společenskému znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje, kdy jsou zpracovávány osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech, kdy jsou zpracovávány genetické údaje či údaje o zdravotním stavu či sexuálním životě nebo odsouzení v trestních věcech a trestných činů či souvisejících bezpečnostních opatření, kdy jsou za účelem vytvoření či využití osobních profilů vyhodnocovány osobní aspekty, zejména prostřednictvím analýzy nebo odhadu aspektů týkajících se pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti nebo chování, místa pobytu a pohybu, kdy jsou zpracovávány osobní údaje zranitelných osob, především dětí, nebo kdy je zpracováván velký objem osobních údajů a zpracování se dotýká velkého počtu subjektů údajů.

(76) Pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů by měly být určeny na základě povahy, rozsahu, kontextu a účelům zpracování. Riziko by mělo být hodnoceno na základě objektivního posouzení, které stanoví, zda operace zpracování představují riziko či vysoké riziko.

(77) Pokyny pro zavádění vhodných opatření a pro prokázání souladu s požadavky tímto správcem nebo zpracovatelem, zejména pokud jde o zjištění rizika souvisejícího se zpracováním, jeho posouzení z hlediska původu, povahy, pravděpodobnosti a závažnosti, a stanovení osvědčených postupů ke snížení rizika by mohly být stanoveny zejména prostřednictvím schválených kodexů chování, schválených osvědčení, pokynů sboru nebo doporučení pověřence pro ochranu osobních údajů. Sbor může rovněž vydávat pokyny týkající se operací zpracování, u nichž se má za to, že je nepravděpodobné, že by mohly představovat vysoké riziko pro práva a svobody fyzických osob, a stanovit, jaká opatření mohou být v takových případech k řešení podobného rizika postačující.

(78) Pro ochranu práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů je třeba přijmout vhodná technická a organizační opatření, aby se zajistilo splnění požadavků vyplývajících z tohoto nařízení. Aby správce mohl doložit soulad s tímto nařízením, měl by přijmout vnitřní koncepce a zavést opatření, která dodržují zejména zásady záměrné a standardní ochrany osobních údajů. Tato opatření by mohla mimo jiné spočívat v minimalizaci zpracování osobních údajů, co nejrychlejší pseudonymizaci osobních údajů, transparentnosti s ohledem na funkce a zpracování osobních údajů, umožnění subjektům údajů monitorovat zpracování osobních údajů a umožnění správcům vytvářet a zlepšovat bezpečnostní prvky. Pokud jde o vývoj, koncepci, výběr a používání aplikací, služeb a produktů, které jsou založeny na zpracování osobních údajů nebo osobní údaje za účelem plnění svých funkcí zpracovávají, je třeba zhotovitele těchto produktů, služeb a aplikací vybízet k tomu, aby při vývoji a koncipování těchto produktů, služeb a aplikací zohledňovali právo na ochranu údajů a brali náležitý ohled na stav techniky s cílem zajistit, aby správci a zpracovatelé mohli plnit své povinnosti v oblasti ochrany údajů. Zásady záměrné a standardní ochrany osobních údajů by rovněž měly být zohledněny v souvislosti s veřejnými zakázkami.

(79) Ochrana práv a svobod subjektů údajů i odpovědnost správců a zpracovatelů, mimo jiné pokud jde o jejich monitorování a opatření vůči nim přijímaná dozorovými úřady, vyžadují, aby bylo jasně určeno, kdo má plnit jednotlivé povinnosti stanovené v tomto nařízení, včetně případů, kdy správce určuje účely a prostředky zpracování společně s jinými správci nebo kdy je operace zpracování prováděna pro správce.

(80) Pokud správce nebo zpracovatel, který není usazen v Unii, zpracovává osobní údaje subjektů údajů, které se nacházejí v Unii, a tyto činnosti zpracování souvisejí s nabídkou zboží nebo služeb takovým subjektům údajů v Unii bez ohledu na to, zda je vyžadována platba subjektu údajů, nebo souvisejí s monitorováním jejich chování v rozsahu, v němž k tomuto chování dochází v Unii, měl by daný správce nebo zpracovatel jmenovat svého zástupce, ledaže by dotčené zpracování bylo příležitostné, nezahrnovalo by rozsáhlé zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů a bylo by nepravděpodobné, že by s ohledem na svou povahu, souvislosti, rozsah a účely mohlo toto zpracování

představovat riziko pro práva a svobody fyzických osob, nebo ledaže by správce byl orgánem veřejné moci nebo veřejným subjektem. Zástupce by měl jednat jménem správce nebo zpracovatele a může se něj obracet kterýkoliv dozorový úřad. Zástupce by měl být výslovně jmenován na základě písemného zmocnění správcem nebo zpracovatelem, aby jednal jejich jménem v souvislosti s povinnostmi správce nebo zpracovatele stanovenými tímto nařízením. Jmenováním tohoto zástupce není dotčena odpovědnost správce nebo zpracovatele podle tohoto nařízení. Zástupce by měl vykonávat své úkoly podle zmocnění uděleného správcem nebo zpracovatelem, mimo jiné by měl spolupracovat s příslušnými dozorovými úřady při jakémkoliv úkonu prováděném s cílem zajistit soulad s tímto nařízením. Vůči jmenovanému zástupci by se v případě neplnění povinností správcem nebo zpracovatelem mělo uplatnit vymáhací řízení.

(81) Aby byl zajištěn soulad s požadavky tohoto nařízení v případě zpracování prováděného zpracovatelem jménem správce, měl by správce zpracováním pověřit pouze zpracovatele, kteří poskytují dostatečné záruky, zejména pokud jde o odborné znalosti, spolehlivost a zdroje, že zavedou technická a organizační opatření, která budou splňovat požadavky tohoto nařízení, včetně požadavků na bezpečnost zpracování. Jednou z možností, jak prokázat, že správce plní příslušné povinnosti, je dodržování schváleného kodexu chování nebo schváleného mechanismu pro vydávání osvědčení zpracovatelem. Provádění zpracování zpracovatelem by se mělo řídit smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které by zavazovaly zpracovatele vůči správci a v nichž by byl stanoven předmět a doba trvání zpracování, povaha a účely zpracování, typ osobních údajů a kategorie subjektů údajů, s přihlédnutím ke konkrétním úkolům a povinnosti zpracovatele v souvislosti se zpracováním, jež má být provedeno, a riziko pro práva a svobody subjektů údajů. Správce a zpracovatel se mohou rozhodnout, že použijí individuální smlouvu nebo standardní smluvní ustanovení, která přijme buď přímo Komise, nebo dozorový úřad v souladu s mechanismem jednotnosti a poté Komise. Po dokončení zpracování jménem správce by zpracovatel měl na základě rozhodnutí správce osobní údaje vrátit nebo vymazat, jestliže se nepožaduje uložení osobních údajů podle práva Unie nebo členského státu, které se na zpracovatele vztahuje.

(82) Aby správce nebo zpracovatel doložil soulad s tímto nařízením, měl by vést záznamy o činnostech zpracování, za které odpovídá. Každý správce a zpracovatel by měl být povinen spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit, aby na jejich základě mohly být tyto operace zpracování monitorovány.

(83) V zájmu zachování bezpečnosti a zabránění zpracování, které by bylo v rozporu s tímto nařízením, by měl správce nebo zpracovatel posoudit rizika spojená se zpracováním a přijmout opatření ke zmírnění těchto rizik, například šifrování. Tato opatření by měla zajistit náležitou úroveň bezpečnosti, včetně důvěrnosti, s ohledem na stav techniky, náklady na provedení v souvislosti s rizikem a povahu osobních údajů, které mají být chráněny. Při posuzování rizik pro zabezpečení osobních údajů by se měla vzít v úvahu rizika, která zpracování představuje, jako jsou náhodné nebo protiprávní zničení, ztráta, pozměnění, neoprávněné zpřístupnění nebo zpřístupnění předaných, uložených nebo jiným způsobem zpracovaných osobních údajů, které by mohly zejména vést k fyzické, hmotné nebo nehmotné újmě.

(84) S cílem přispět k zajištění souladu s tímto nařízením v případech, kdy je pravděpodobné, že operace zpracování budou představovat vysoké riziko pro práva a svobody fyzických osob, by měl být správce odpovědný za provedení posouzení vlivu na ochranu osobních údajů, aby vyhodnotil zejména původ, povahu, zvláštnost a závažnost tohoto rizika. Výsledek posouzení by měl být zohledněn při rozhodování o vhodných opatřeních, která by měla být přijata s cílem prokázat, že zpracování osobních údajů je v souladu s tímto nařízením. Pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že operace zpracování představují vysoké riziko, které správce nemůže vhodnými opatřeními zmírnit, s ohledem na dostupné technologie a náklady na provedení, měl by být před zpracováním konzultován dozorový úřad.

(85) Není-li porušení zabezpečení osobních údajů řešeno náležitě a včas, může to fyzickým osobám způsobit fyzickou, hmotnou či nehmotnou újmu, jako je ztráta kontroly nad jejich osobními údaji nebo omezení jejich práv, diskriminace, krádež nebo zneužití identity, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti, ztráta důvěrnosti osobních údajů chráněných služebním tajemstvím nebo jakékoliv jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob. Jakmile se tedy správce o

porušení zabezpečení osobních údajů dozví, měl by je bez zbytečného odkladu, a je-li to možné, do 72 hodin poté, co se o něm dozvěděl, ohlásit příslušnému dozorovému úřadu, ledaže může v souladu se zásadou odpovědnosti doložit, že je nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob. Není-li toto ohlášení možné učinit do 72 hodin, měly by být spolu s ním uvedeny důvody zpoždění a informace mohou být poskytnuty postupně bez zbytečného dalšího prodlení.

(86) Správce by měl porušení zabezpečení osobních údajů oznámit subjektu údajů bez zbytečného prodlení, pokud je pravděpodobné, že toto porušení bude mít za následek vysoké riziko pro práva a svobody fyzické osoby, aby mohl učinit nezbytná opatření. V oznámení by měla být popsána povaha daného případu porušení zabezpečení osobních údajů a obsažena doporučení pro dotčenou fyzickou osobu, jak případné nežádoucí účinky zmírnit. Tato oznámení by měla být subjektům údajů učiněna, jakmile je to proveditelné, v úzké spolupráci s dozorovým úřadem a v souladu s pokyny tohoto úřadu nebo jiných příslušných orgánů (například donucovacích orgánů). Například v případě potřeby zmírnit bezprostřední riziko způsobení újmy je nutné tuto skutečnost subjektům údajů neprodleně oznámit, zatímco v situaci, kdy je zapotřebí zavést vhodná opatření s cílem zabránit tomu, aby porušení zabezpečení osobních údajů pokračovalo nebo aby docházelo k podobným případům porušení, může být opodstatněna delší lhůta.

(87) Mělo by být zjištěno, zda byla zavedena veškerá vhodná technická a organizační opatření, aby se okamžitě stanovilo, zda došlo k porušení zabezpečení osobních údajů, a aby byly dozorový úřad a subjekt údajů neprodleně informovány. Skutečnost, že oznámení bylo provedeno bez zbytečného odkladu, se stanoví zejména s ohledem na povahu a závažnost daného porušení zabezpečení osobních údajů a jeho důsledky a nežádoucí účinky pro subjekt údajů. Toto oznámení může vést k zásahu dozorového úřadu v souladu s jeho úkoly a pravomocemi stanovenými v tomto nařízení.

(88) Při vytváření podrobných pravidel týkajících se formátu a postupů ohlašování případů porušení zabezpečení osobních údajů by měly být náležitě zohledněny okolnosti porušení, včetně otázky, zda byly osobní údaje chráněny vhodnými technickými opatřeními, jež pravděpodobnost zneužití totožnosti a jiných forem zneužívání účinně omezují. Tato pravidla a postupy by navíc měly vzít v úvahu oprávněné zájmy donucovacích orgánů v případech, kdy by předčasné zpřístupnění mohlo zbytečně ztížit vyšetřování okolností porušení zabezpečení osobních údajů.

(89) Směrnice 95/46/ES stanovila obecnou povinnost ohlašovat zpracování osobních údajů dozorovým úřadům. Tato povinnost přináší administrativní a finanční zátěž, avšak nepřispěla ve všech případech ke zlepšení ochrany osobních údajů. Proto by měla být tato nerozlišená obecná ohlašovací povinnost zrušena a nahrazena účinnými postupy a mechanismy, které by se místo toho zaměřily na takové typy operací zpracování, jež mohou s ohledem na svou povahu, rozsah, kontext a účely představovat vysoké riziko pro práva a svobody fyzických osob. Mezi tyto typy operací zpracování mohou patřit ty, při nichž jsou zejména používány nové technologie, nebo které jsou zcela nového druhu a u nichž správce dosud neprovedl posouzení vlivu na ochranu osobních údajů, nebo které se staly nezbytnými z důvodu času, který uplynul od prvotního zpracování.

(90) V těchto případech by měl správce před zpracováním provést posouzení vlivu na ochranu osobních údajů s cílem posoudit konkrétní pravděpodobnost a závažnost vysokého rizika a zohlednit přitom povahu, rozsah, kontext a účely zpracování a zdroje rizika. Toto posouzení vlivu by mělo zejména obsahovat zamýšlená opatření, záruky a mechanismy pro snížení tohoto rizika, pro zajištění ochrany osobních údajů a prokázání souladu s tímto nařízením.

(91) To by mělo platit zejména pro rozsáhlé operace zpracování, jež mají sloužit ke zpracování značného množství osobních údajů na regionální, celostátní nebo nadnárodní úrovni, jež by mohly mít dopad na velký počet subjektů údajů a u nichž je pravděpodobné, že budou představovat vysoké riziko, například vzhledem k jejich citlivosti, pokud se v souladu s dosaženou úrovní technických znalostí použije ve velkém rozsahu nová technologie, jakož i pro jiné operace zpracování, které představují vysoké riziko pro práva a svobody subjektů údajů, zejména v případech, kdy s ohledem na tyto operace je pro subjekty údajů obtížnější uplatnit svá práva.

Posouzení vlivu na ochranu osobních údajů by mělo být vypracováno i v případech, kdy se osobní údaje zpracovávají za účelem přijetí rozhodnutí o konkrétních fyzických osobách v návaznosti na jakékoliv systematické a rozsáhlé hodnocení osobních aspektů týkajících se fyzických osob na základě profilování těchto údajů nebo v návaznosti na zpracování zvláštních kategorií osobních údajů, biometrických údajů, nebo údajů o odsouzení v trestních věcech a o trestných činech či souvisejících bezpečnostních opatřeních. Posouzení vlivu na ochranu osobních údajů je rovněž zapotřebí v případě monitorování veřejně přístupných prostor prováděného ve velkém rozsahu, zejména pokud se k němu používá optických elektronických přístrojů, nebo v případě jakýchkoliv jiných operací, kdy má příslušný dozorový úřad za to, že je pravděpodobné, že zpracování bude představovat vysoké riziko pro práva a svobody subjektů údajů, zejména proto, že tyto úkony brání subjektům údajů v uplatňování některého z jejich práv nebo v používání některé služby či smlouvy, nebo proto, že jsou prováděny systematicky a ve velkém rozsahu. Zpracování osobních údajů by nemělo být považováno za zpracování velkého rozsahu, pokud se jedná o zpracování osobních údajů pacientů nebo klientů jednotlivými lékaři, zdravotníky nebo právníky. V takových případech by posouzení vlivu na ochranu osobních údajů nemělo být povinné.

(92) Za určitých okolností může být přiměřené a účelné, aby byl předmět posouzení vlivu na ochranu osobních údajů širší a nevztahoval se pouze na jeden projekt, například když orgány veřejné moci nebo veřejné subjekty mají v úmyslu vytvořit společnou aplikaci nebo platformu zpracování, nebo když několik správců hodlá zavést společnou aplikaci nebo zpracovatelské prostředí pro celé průmyslové odvětví nebo pro určitý segment nebo pro široce užívanou horizontální činnost.

(93) V souvislosti s přijetím právního předpisu členského státu, na jehož základě orgán veřejné moci nebo veřejný subjekt plní své úkoly a který danou operaci nebo soubor operací zpracování upravuje, mohou členské státy považovat za nutné provést výše uvedené posouzení před činnostmi zpracování.

(94) Pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by zpracování v případě, že neexistují záruky, bezpečnostní opatření ani mechanismy ke zmenšení rizika, představovalo vysoké riziko pro práva a svobody fyzických osob, a pokud je správce toho názoru, že riziko nelze zmenšit prostředky přiměřenými z hlediska dostupných technologií a nákladů na provedení, je třeba před zahájením zpracování konzultovat s dozorovým úřadem. Je pravděpodobné, že toto vysoké riziko vznikne v souvislosti s určitým typem zpracování a rozsahem a četností zpracování, což rovněž může vést ke vzniku škody nebo zásahu do práv a svobod dotčené fyzické osoby. Dozorový úřad by měl na žádost o konzultaci reagovat ve stanovené lhůtě. Skutečností, že dozorový úřad v této lhůtě nezareaguje, by však neměl být dotčen žádný zásah tohoto úřadu prováděný v souladu s jeho úkoly a pravomocemi stanovenými v tomto nařízení, včetně pravomoci zakázat operace zpracování. V rámci tohoto procesu konzultací může být výsledek posouzení vlivu na ochranu osobních údajů, které bylo provedeno v souvislosti s daným zpracováním, předložen dozorovému úřadu, zejména zamýšlená opatření ke zmírnění rizika pro práva a svobody fyzických osob.

(95) Zpracovatel by měl být v případě potřeby a na požádání správci nápomocen při zajišťování dodržování povinností vyplývajících z provádění posouzení vlivu na ochranu osobních údajů a z předchozí konzultace s dozorovým úřadem.

(96) V průběhu příprav legislativního nebo regulačního opatření, jímž bude stanoveno zpracování osobních údajů, by měl být rovněž konzultován dozorový úřad, aby byl zajištěn soulad zamýšleného zpracování s tímto nařízením, a zejména zmírněno související riziko pro subjekt údajů.

(97) Pokud je zpracování prováděno orgánem veřejné moci, s výjimkou soudů nebo nezávislých justičních orgánů jednajících v rámci svých justičních pravomocí, pokud jej v soukromém sektoru provádí správce, jehož hlavní činnosti spočívají v operacích zpracování, jež vyžadují pravidelné a systematické monitorování subjektů údajů ve velkém rozsahu nebo pokud hlavní činnosti správce nebo zpracovatele spočívají ve zpracování zvláštních kategorií osobních údajů a údajů týkajících se rozsudků v trestních věcech a trestných činů, měla by být správci nebo zpracovateli při monitorování toho, zda je zajištěn vnitřní soulad s tímto nařízením, nápomocna osoba s odbornými znalostmi v oblasti právních předpisů a postupů týkajících se ochrany údajů. V soukromém sektoru souvisejí hlavní činnosti správce s jeho základními činnostmi a nevztahují se na zpracování osobních údajů jakožto pomocnou činnost. Potřebná úroveň odborných znalostí by se měla určit zejména podle prováděných

operací zpracování a podle ochrany, která se vyžaduje pro osobní údaje zpracovávané správcem nebo zpracovatelem. Tito pověřenci pro ochranu osobních údajů, bez ohledu na to, zda se jedná o zaměstnance správce, by měli být schopni plnit své povinnosti a úkoly nezávislým způsobem.

(98) Sdružení nebo jiné subjekty zastupující různé kategorie správců nebo zpracovatelů by měly být vybízeny k tomu, aby v mezích tohoto nařízení vypracovaly kodexy chování s cílem usnadnit účinné uplatňování tohoto nařízení, a to při zohlednění zvláštní povahy zpracování prováděného v některých odvětvích a specifických potřeb mikropodniků a malých a středních podniků. Tyto kodexy chování by zejména mohly upřesňovat povinnosti správců a zpracovatelů s přihlédnutím k riziku, které ze zpracování pravděpodobně vyplyne pro práva a svobody fyzických osob.

(99) Při vypracovávání kodexu chování nebo při jeho změně či rozšíření by sdružení a jiné subjekty zastupující různé kategorie správců nebo zpracovatelů měly konzultovat příslušné zúčastněné strany, pokud možno i subjekty údajů, a měly by zohledňovat návrhy a stanoviska vyjádřené v reakci na tyto konzultace.

(100) S cílem zvýšit transparentnost a lépe zajistit soulad s tímto nařízením je třeba vybízet k zavedení mechanismů pro vydávání osvědčení, jakož i pečetí a známek dokládajících ochranu údajů, aby subjekty údajů mohly u příslušných produktů a služeb rychle posoudit úroveň ochrany údajů.

(101) Pro rozvoj mezinárodního obchodu a mezinárodní spolupráce jsou nezbytné toky osobních údajů do zemí mimo Unii a do mezinárodních organizací a z těchto zemí a organizací. Nárůst těchto toků s sebou přinesl nové výzvy a obavy týkající se ochrany osobních údajů. Pokud jsou však osobní údaje předávány z Unie správcům, zpracovatelům nebo jiným příjemcům ve třetích zemích nebo v mezinárodních organizacích, neměla by být úroveň ochrany fyzických osob zajištěná v Unii tímto nařízením oslabována, a to ani v případech dalšího předání osobních údajů ze třetí země nebo mezinárodní organizace správcům nebo zpracovatelům ve stejné nebo jiné třetí zemi nebo mezinárodní organizaci. V každém případě lze předání do třetích zemí a mezinárodním organizacím provést pouze za plného dodržování tohoto nařízení. K předání by mělo docházet pouze tehdy, pokud s výhradou ostatních ustanovení tohoto nařízení správce nebo zpracovatel splňují podmínky stanovené v tomto nařízení vztahující se na předávání osobních údajů do třetích zemí nebo mezinárodním organizacím.

(102) Tímto nařízením nejsou dotčeny mezinárodní dohody uzavřené mezi Unií a třetími zeměmi o předávání osobních údajů, které zahrnují vhodné záruky pro subjekty údajů. Členské státy mohou uzavírat mezinárodní dohody, které zahrnují předání osobních údajů do třetích zemí nebo mezinárodním organizacím, pokud takové dohody nemají vliv na toto nařízení nebo jakákoliv jiná ustanovení práva Unie a obsahují odpovídající úroveň ochrany základních práv subjektů údajů.

(103) Komise by měla být schopna s účinkem pro celou Unii rozhodnout, že určitá třetí země, určité území či konkrétní odvětví v určité třetí zemi nebo určitá mezinárodní organizace poskytují odpovídající úroveň ochrany osobních údajů, a zajistit tak právní jistotu a jednotný přístup v celé Unii ve vztahu k dané třetí zemi nebo mezinárodní organizaci, u níž se má za to, že takovou úroveň ochrany poskytuje. V těchto případech by mělo být možné předat osobní údaje do této země nebo této mezinárodní organizaci bez potřeby získat další povolení. Komise by měla být schopna rovněž rozhodnout o zrušení takového rozhodnutí, pokud o tom dotčenou třetí zemi nebo mezinárodní organizaci vyrozumí s plným uvedením důvodů.

(104) V souladu se základními hodnotami, na kterých je Unie založena a mezi něž patří zejména ochrana lidských práv, by Komise měla při svém hodnocení určité třetí země nebo určitého území nebo konkrétního odvětví v určité třetí zemi zohlednit skutečnost, jak tato třetí země dodržuje zásady právního státu a přístupu ke spravedlnosti, jakož i mezinárodní normy a standardy v oblasti lidských práv a příslušné obecné a odvětvové právní předpisy, včetně právních předpisů týkajících se veřejné bezpečnosti, obrany a národní bezpečnosti, jakož i veřejného pořádku a trestního práva. Přijetí rozhodnutí o odpovídající ochraně ve vztahu k určitému území nebo konkrétnímu odvětví v určité třetí zemi by mělo zohlednit jasná a objektivní kritéria, jako jsou určité činnosti zpracování a oblast působnosti použitelných právních standardů a právních předpisů platných v dané třetí zemi.

Třetí země by měla nabídnout záruky zajišťující odpovídající úroveň ochrany v zásadě rovnocennou úrovni ochrany zajištěné v Unii, zejména pokud jsou osobní údaje zpracovávány v jednom nebo více konkrétních odvětvích. Daná třetí země by zejména měla zajistit účinný nezávislý dozor nad ochranou údajů a měla by stanovit mechanismy spolupráce s úřady členských států pro ochranu osobních údajů, přičemž subjektům údajů by měla být poskytnuta účinná a vymahatelná práva a účinná správní a soudní ochrana.

(105) Vedle mezinárodních závazků, které daná třetí země nebo mezinárodní organizace přijala, by Komise měla zohlednit povinnosti vyplývající z účasti dané třetí země nebo mezinárodní organizace na mnohostranných nebo regionálních systémech, zejména ve vztahu k ochraně osobních údajů, jakož i plnění těchto povinností. Zohledněno by mělo být zejména přistoupení dané třetí země k Úmluvě Rady Evropy ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat a jejímu dodatkovému protokolu. Komise by měla při posuzování úrovně ochrany ve třetích zemích nebo mezinárodních organizacích konzultovat sbor.

(106) Komise by měla monitorovat fungování rozhodnutí o úrovni ochrany v určité třetí zemi, na určitém území či v konkrétním odvětví v určité třetí zemi nebo v určité mezinárodní organizaci a fungování rozhodnutí přijatých na základě čl. 25 odst. 6 nebo čl. 26 odst. 4 směrnice 95/46/ES. Ve svých rozhodnutích o odpovídající ochraně by Komise měla stanovit mechanismus pravidelného přezkumu jejich fungování. Tento pravidelný přezkum by měl probíhat za konzultace s dotčenou třetí zemí nebo mezinárodní organizací a měl by zohlednit veškerý relevantní vývoj v dané třetí zemi nebo mezinárodní organizaci. Pro účely monitorování a provádění pravidelných přezkumů by Komise měla zohlednit názory a zjištění Evropského parlamentu a Rady, jakož i jiné příslušné orgány a zdroje. Komise by měla v přiměřené lhůtě vyhodnotit fungování posledně uvedených rozhodnutí a veškerá relevantní zjištění sdělovat výboru ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ([1]), jak je stanoven v tomto nařízení, Evropskému parlamentu a Radě.

(107) Komise by měla být schopna konstatovat, že určitá třetí země, určité území či konkrétní odvětví v určité třetí zemi nebo určitá mezinárodní organizace již odpovídající úroveň ochrany údajů nezajišťuje. Předání osobních údajů do této třetí země nebo této mezinárodní organizaci by tudíž mělo být povoleno, jen pokud jsou splněny požadavky článků tohoto nařízení týkající se předání na základě vhodných záruk, závazných podnikových pravidel a odchylek ve zvláštních situacích. V tomto případě by měly být stanoveny konzultace mezi Komisí a těmito třetími zeměmi nebo mezinárodními organizacemi. Komise by měla včas informovat danou třetí zemi nebo mezinárodní organizaci o důvodech a zahájit s ní konzultace za účelem nápravy situace.

(108) Nebude-li přijato rozhodnutí o odpovídající ochraně, měl by správce nebo zpracovatel v zájmu odstranění nedostatků v oblasti ochrany údajů ve třetí zemi přijmout opatření, která subjektu údajů poskytnou vhodné záruky. Tyto vhodné záruky mohou spočívat ve využívání závazných podnikových pravidel, standardních doložek o ochraně údajů přijatých Komisí, standardních doložek o ochraně údajů přijatých dozorovým úřadem nebo smluvních doložek jím schválených. Tyto záruky by měly zajistit splnění požadavků na ochranu údajů a dodržení práv subjektů údajů v rozsahu odpovídajícím zpracování v Unii, včetně dostupnosti vymahatelných práv subjektu údajů a účinné právní ochrany, včetně práva na účinnou správní nebo soudní ochranu a na požadování náhrady škody v Unii nebo ve třetí zemi. Měly by se týkat zejména souladu s obecnými zásadami pro zpracování osobních údajů a zásad záměrné a standardní ochrany osobních údajů. Předání mohou provést rovněž orgány veřejné moci nebo veřejné subjekty s orgány veřejné moci nebo veřejný subjekty ve třetích zemích nebo s mezinárodními organizacemi s odpovídajícími povinnostmi nebo funkcemi, a to i na základě ustanovení, která mají být vložena do správních ujednání, jako je memorandum o porozumění, a která stanoví vymahatelná a účinná práva subjektů údajů. Povolení příslušného dozorového úřadu by mělo být obdrženo, jestliže jsou záruky stanoveny ve správních ujednáních.

(109) Skutečnost, že správci a zpracovatelé mohou používat standardní doložky o ochraně údajů přijaté Komisí nebo dozorovým úřadem, by neměla správcům ani zpracovatelům bránit v tom, aby zahrnuli standardní doložky

([1]) Nařízení Evropského parlamentu a Rady (EU) č 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

o ochraně údajů i do rozsáhlejších smluv, jako je smlouva mezi zpracovatelem a dalším zpracovatelem, nebo doplnili jiné doložky či další záruky, pokud tyto nejsou v přímém nebo nepřímém rozporu se standardními smluvními doložkami přijatými Komisí nebo dozorovým úřadem nebo pokud se nedotýkají základních práv či svobod subjektů údajů. Správci a zpracovatelé by měli být vybízeni k poskytování dalších záruk prostřednictvím smluvních závazků, které doplní standardní doložky o ochraně údajů.

(110) Skupina podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost by měly mít možnost používat pro mezinárodní předávání údajů z Unie organizacím ve stejné skupině podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost schválená závazná podniková pravidla za podmínky, že tato pravidla obsahují veškeré základní zásady a vymahatelná práva v zájmu zajištění vhodných záruk pro předávání nebo kategorie předávání osobních údajů.

(111) Měla by být stanovena možnost předat údaje za určitých okolností, pokud subjekt údajů dal svůj výslovný souhlas nebo pokud je předání příležitostné a nezbytné v souvislosti se smluvními či právními nároky, bez ohledu na to, zda probíhá v soudním řízení nebo ve správním či jakémkoli mimosoudním řízení, včetně řízení před regulačními orgány. Rovněž by měla být stanovena možnost převádět údaje, pokud je to nutné z důležitých důvodů veřejného zájmu stanovených právem Unie nebo členského státu nebo pokud je předání prováděno z rejstříku zřízeného na základě právních předpisů a určeného k nahlížení pro veřejnost nebo osoby s oprávněným zájmem. V tomto případě by se takové předání nemělo týkat všech osobních údajů ani celých kategorií osobních údajů obsažených v tomto rejstříku, a pokud má být rejstřík přístupný osobám s oprávněným zájmem, mělo by být předání uskutečněno pouze na žádost těchto osob nebo pokud jsou tyto osoby jejich příjemci, přičemž je třeba plně zohlednit zájmy a základní práva subjektu údajů.

(112) Tyto výjimky by se měly uplatnit zejména v případech, kdy je předání údajů vyžadováno a je nutné z důležitých důvodů veřejného zájmu, například v případech mezinárodní výměny údajů mezi orgány pro hospodářskou soutěž, daňovými či celními správami, orgány finančního dohledu, útvary příslušnými v oblasti sociálního zabezpečení nebo veřejného zdraví, například v případě vysledování kontaktů v souvislosti s nakažlivými chorobami nebo za účelem omezení nebo odstranění dopingu ve sportu. Předání osobních údajů by mělo být považováno za zákonné rovněž tehdy, pokud je nezbytné pro ochranu životně důležitého zájmu subjektu údajů nebo jiné osoby, včetně fyzické integrity nebo života, není-li subjekt údajů schopen udělit souhlas. V případě neexistence rozhodnutí o odpovídající ochraně může právo Unie nebo členského státu z důležitých důvodů veřejného zájmu výslovně stanovit omezení předání konkrétních kategorií údajů třetí zemi nebo mezinárodní organizaci. Členské státy by taková ustanovení měly oznámit Komisi. Jakékoliv předání osobních údajů subjektu údajů, který není fyzicky nebo právně způsobilý udělit souhlas s předáním, mezinárodní humanitární organizaci za účelem vykonání úkolu svěřeného na základě ženevských úmluv nebo uplatňování mezinárodního humanitárního práva použitelného v ozbrojených konfliktech by mohlo být považováno za nezbytné z důležitého důvodu veřejného zájmu nebo z důvodu životně důležitého zájmu subjektu údajů.

(113) Předání, o nichž lze konstatovat, že nejsou opakovaná a že se týkají pouze omezeného počtu subjektů údajů, by rovněž mohla být uskutečňována pro účely závažných oprávněných zájmů správce, pokud nad těmito zájmy nepřevažují zájmy nebo práva a svobody subjektu údajů a pokud správce posoudil všechny okolnosti daného předání údajů. Správce by měl zvážit zvláště povahu osobních údajů, účel a dobu trvání navrhované operace nebo operací zpracování, jakož i situaci v zemi původu, v dané třetí zemi a v zemi konečného určení, a měl by poskytnout vhodné záruky pro ochranu základních práv a svobod fyzických osob, pokud jde o zpracování jejich osobních údajů. Taková předání by měla být možná pouze v okrajových případech, kdy se nepoužije žádný z ostatních důvodů pro převod. Pro účely vědeckého či historického výzkumu nebo pro statistické účely by měla být zohledněna oprávněná očekávání společnosti ohledně zvyšování znalostí. Správce by o takovém předání měl informovat dozorový úřad a subjekt údajů.

(114) Pokud Komise nepřijala rozhodnutí o odpovídající úrovni ochrany údajů ve třetí zemi, správce nebo zpracovatel by měl v každém případě využít řešení, která subjektům údajů poskytnou vymahatelná a účinná práva, pokud jde o zpracování jejich osobních údajů v Unii po jejich předání, tak aby i nadále požívali základních práv a záruk.

(115) Některé třetí země přijímají právní předpisy a jiné právní akty, které mají přímo upravovat činnosti zpracování fyzickými a právnickými osobami spadající do pravomoci členských států. Může se mimo jiné jednat o rozsudky soudů či rozhodnutí správních orgánů ve třetích zemích, v nichž se od správce nebo zpracovatele vyžaduje předání či zpřístupnění osobních údajů a které nejsou založeny na platných mezinárodních dohodách, jako je například smlouva o vzájemné právní pomoci, mezi danou třetí zemí a Unií nebo členským státem. Extrateritoriální používání těchto právních předpisů a jiných právních aktů může být v rozporu s mezinárodním právem a znesnadnit zajištění ochrany fyzických osob zajištěné v Unii tímto nařízením. Předání údajů by mělo být povoleno jen tehdy, jsou-li splněny podmínky předání údajů do třetích zemí stanovené v tomto nařízení. Tak tomu může být mimo jiné v případě, kdy je sdělení údajů nezbytné z důležitého důvodu veřejného zájmu, jenž je uznán v právu Unie nebo členského státu, které se na správce vztahuje.

(116) Předání osobních údajů přes hranice mimo území Unie může fyzické osoby vystavit zvýšenému riziku, že nebudou moci uplatnit svá práva na ochranu osobních údajů, a zejména se chránit před protiprávním použitím nebo poskytnutím těchto údajů. Zároveň se může stát, že dozorové úřady nebudou schopny vyřizovat stížnosti nebo provádět šetření týkající se činností prováděných za hranicemi svého státu. Překážkou pro jejich úsilí o přeshraniční spolupráci mohou být také nedostatečné preventivní nebo nápravné pravomoci, rozdíly v právní úpravě a praktické překážky, například omezené zdroje. Proto je třeba podporovat užší spolupráci mezi dozorovými úřady zabývajícími se ochranou osobních údajů s cílem napomoci jim při výměně informací a provádění šetření ve spolupráci s příslušnými mezinárodními partnery. Pro účely vypracování mechanismů mezinárodní spolupráce s cílem usnadnit a poskytovat vzájemnou mezinárodní pomoc při prosazování právních předpisů na ochranu osobních údajů by si Komise a dozorové úřady měly při činnostech souvisejících s výkonem svých pravomocí vyměňovat informace a spolupracovat s příslušnými orgány ve třetích zemích, na základě vzájemnosti a v souladu s tímto nařízením.

(117) je Zásadním prvkem ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů je zřízení dozorových úřadů, jež mohou v členských státech plnit své úkoly a vykonávat své pravomoci zcela nezávisle. Členské státy by měly mít možnost zřídit více než jeden dozorový úřad, aby zohlednily své ústavní, organizační a správní uspořádání.

(118) Nezávislost dozorových úřadů by neměla znamenat, že se na ně nemůže vztahovat mechanismus kontroly nebo monitorování, pokud jde o jejich finanční výdaje, nebo soudní přezkum.

(119) Pokud členský stát zřídí více dozorových úřadů, měl by právním předpisem zavést mechanismy, které zajistí jejich účinnou účast v mechanismu jednotnosti. Tento členský stát by měl zejména určit dozorový úřad, který bude fungovat jako jediné kontaktní místo pro účinnou účast těchto úřadů v mechanismu, s cílem zajistit rychlou a plynulou spolupráci s ostatními dozorovými úřady, sborem a Komisí.

(120) Každému dozorovému úřadu by měly být poskytnuty finanční a lidské zdroje, prostory a infrastruktura, které potřebuje pro účinné plnění svých úkolů, včetně úkolů souvisejících se vzájemnou pomocí a spoluprací s jinými dozorovými úřady v celé Unii. Každý dozorový úřad by měl mít samostatný veřejný roční rozpočet, který může být součástí celkového zemského nebo státního rozpočtu.

(121) Obecné podmínky pro člena nebo členy dozorového úřadu by měly být v každém členském státě upraveny právním předpisem, a zejména by měly stanovit, že tito členové mají být jmenováni transparentním způsobem parlamentem, vládou nebo hlavou dotčeného členského státu na návrh vlády nebo člena vlády, parlamentu nebo jeho komory, anebo nezávislým subjektem pověřeným právem členského státu. V zájmu zajištění nezávislosti dozorového úřadu by jeho člen nebo členové měli jednat poctivě a zdržet se jakéhokoliv jednání neslučitelného s výkonem jejich funkce a během svého funkčního období by neměli vykonávat žádnou výdělečnou ani nevýdělečnou pracovní činnost neslučitelnou s touto funkcí. Dozorový úřad by měl mít vlastní pracovníky, které vybere dozorový úřad nebo nezávislý orgán zřízený podle práva členského státu a kteří by měli podléhat výhradně vedení člena či členů daného dozorového úřadu.

(122) Každý dozorový úřad by měl být na území svého vlastního členského státu příslušný k výkonu pravomocí a plnění úkolů, které mu byly svěřeny v souladu s tímto nařízením. To by se mělo týkat zejména zpracování

v souvislosti s činnostmi provozovny správce nebo zpracovatele na území jejich vlastního členského státu, zpracování osobních údajů prováděného orgány veřejné moci nebo soukromými subjekty jednajícími ve veřejném zájmu, zpracování dotýkajícího se subjektů údajů na jeho území nebo zpracování prováděného správcem či zpracovatelem, který není usazen v Unii, v případě zacílení na subjekty údajů mající bydliště na jeho území. To by dále mělo zahrnovat vyřizování stížností podaných subjekty údajů, provádění šetření ohledně uplatňování tohoto nařízení a zvyšování povědomí veřejnosti o rizicích, pravidlech, zárukách a právech, pokud jde o zpracování osobních údajů.

(123) Dozorové úřady by měly sledovat uplatňování ustanovení tohoto nařízení a přispívat k jejich jednotnému uplatňování v celé Unii s cílem chránit fyzické osoby v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů v rámci vnitřního trhu. Za tímto účelem by dozorové úřady měly spolupracovat mezi sebou a s Komisí, aniž by byla zapotřebí jakákoliv dohoda mezi členskými státy o poskytování vzájemné pomoci nebo o takové spolupráci.

(124) Pokud ke zpracování osobních údajů dochází v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii a tento správce nebo zpracovatel je usazen ve více než jednom členském státě, nebo pokud zpracování prováděné v souvislosti s činnostmi jediné provozovny správce či zpracovatele v Unii se podstatně dotýká či pravděpodobně dotkne subjektů údajů ve více než jednom členském státě, měl by úlohu vedoucího dozorového úřadu plnit dozorový úřad pro hlavní provozovnu správce či zpracovatele nebo pro jedinou provozovnu správce či zpracovatele. Měl by spolupracovat s ostatními dotčenými dozorovými úřady vzhledem k tomu, že správce nebo zpracovatel má na území jejich členského státu provozovnu, že subjekty údajů mající bydliště na jejich území jsou podstatně dotčeny, nebo že u těchto úřadů byla podána stížnost. Rovněž v případě, kdy subjekt údajů nemající bydliště v daném členském státě podal stížnost, měl by být dozorový úřad, u nějž byla taková stížnost podána, rovněž dotčeným dozorovým úřadem. V rámci svých úkolů vydávat pokyny k veškerým otázkám týkajícím se uplatňování tohoto nařízení by měl mít sbor možnost vydávat pokyny, zejména ohledně kritérií, která je třeba zohlednit za účelem zjištění, zda jsou daným zpracováním podstatně dotčeny subjekty údajů ve více než jednom členském státě, a ohledně toho, co se rozumí relevantní a odůvodněnou námitkou.

(125) Vedoucí dozorový úřad by měl být příslušný k přijímání závazných rozhodnutí o opatřeních, aby tak uplatnil pravomoci, které svěřuje toto nařízení. Ve své funkci vedoucího dozorového úřadu by měl do rozhodovacího procesu úzce zapojit dotčené dozorové úřady a jejich činnost koordinovat. Pokud se rozhodne o zamítnutí stížnosti subjektu údajů zcela či částečně, měl by toto rozhodnutí přijmout dozorový úřad, u nějž byla stížnost podána.

(126) Rozhodnutí by mělo být odsouhlaseno společně vedoucím dozorovým úřadem a dotčenými dozorovými úřady, mělo by být určeno hlavní či jediné provozovně správce nebo zpracovatele a mělo by být pro správce i zpracovatele závazné. Správce nebo zpracovatel by měl přijmout opatření nezbytná k zajištění souladu s tímto nařízením a provádění rozhodnutí oznámeného vedoucím dozorovým úřadem hlavní provozovně správce nebo zpracovatele, pokud jde o zpracování prováděné v Unii.

(127) Každý dozorový úřad, který nejedná jako vedoucí dozorový úřad, by měl být příslušný k projednávání místních případů, kdy je správce nebo zpracovatel usazen ve více než jednom členském státě, avšak předmět určitého zpracování se týká pouze zpracování prováděného v jediném členském státě a zahrnuje pouze subjekty údajů v tomto jediném členském státě, například jsou-li předmětem zpracování osobní údaje zaměstnanců v konkrétním zaměstnaneckém kontextu určitého členského státu. V takových případech by měl tento dozorový úřad o této záležitosti neprodleně informovat vedoucí dozorový úřad. Po obdržení těchto informací by měl vedoucí dozorový úřad rozhodnout, zda se bude danou záležitostí zabývat podle ustanovení o spolupráci mezi vedoucím dozorovým úřadem a dalšími dotčenými dozorovými úřady, či zda se jí má na místní úrovni zabývat dozorový úřad, který vedoucí dozorový úřad informoval. Při rozhodování o tom, zda se bude záležitostí zabývat, by měl vedoucí dozorový úřad zohlednit, zda se v členském státě dozorového úřadu, který jej informoval, nachází provozovna správce nebo zpracovatele, s cílem zajistit účinný výkon rozhodnutí vůči správci nebo zpracovateli.

Pokud vedoucí dozorový úřad rozhodne, že se záležitostí zabývat bude, měl by mít dozorový úřad, který jej informoval, možnost předložit návrh rozhodnutí, které by vedoucí dozorový úřad měl co nejvíce zohlednit při přípravě svého návrhu rozhodnutí v rámci tohoto mechanismu jediného kontaktního místa.

(128) Pravidla týkající se vedoucího dozorového úřadu a mechanismu jediného kontaktního místa by se neměla vztahovat na případy, kdy zpracování provádějí orgány veřejné moci nebo soukromé subjekty ve veřejném zájmu. V takových případech by jediným dozorovým úřadem příslušným k výkonu pravomocí, které mu byly svěřeny podle tohoto nařízení, měl být dozorový úřad členského státu, v němž je orgán veřejné moci či soukromý subjekt usazen.

(129) Aby se zajistilo jednotné monitorování a prosazování tohoto nařízení v celé Unii, měly by mít dozorové úřady v každém členském státě tytéž úkoly a účinné pravomoci, včetně pravomocí provádět šetření, ukládat nápravná opatření a sankce, vydávat povolení a poskytovat poradenství, zejména v případech stížností fyzických osob, a aniž jsou dotčeny pravomoci orgánů příslušných podávat obžalobu podle práva členského státu, pravomoci upozorňovat justiční orgány na porušení tohoto nařízení a obrátit se na soud. Mezi tyto pravomoci by měla rovněž patřit pravomoc vydávat dočasné nebo trvalé omezení zpracování, včetně jeho zákazu. Členské státy mohou vymezit další úkoly související s ochranou osobních údajů podle tohoto nařízení. Pravomoci dozorových úřadů by měly být vykonávány v souladu s vhodnými procesními zárukami stanovenými v právu Unie a členského státu, nestranně, spravedlivě a v přiměřených lhůtách. Každé opatření by zejména mělo být vhodné, nezbytné a přiměřené, aby byl s přihlédnutím k okolnostem každého jednotlivého případu zajištěn soulad s tímto nařízením, mělo by respektovat právo všech osob být vyslechnuty dříve, než bude přijato jakékoliv individuální opatření, které by na ně mělo nepříznivý dopad, a nemělo by pro dotčené osoby znamenat zbytečné náklady a přílišné obtíže. Pravomoci provádět šetření, pokud jde o přístup do prostor, by měly být vykonávány v souladu s příslušnými požadavky procesního práva členského státu, jako je například požadavek obstarat si předem soudní povolení. Každé právně závazné opatření dozorového úřadu by mělo mít písemnou formu, být jasné a jednoznačné, uvádět dozorový úřad, který je vydal, a datum svého vydání, mělo by být opatřeno podpisem vedoucího či vedoucím zmocněného člena dozorového úřadu a obsahovat odůvodnění opatření a odkaz na právo na účinnou právní ochranu. Tím by však neměly být vyloučeny další požadavky podle procesního práva členského státu. Přijetí právně závazného rozhodnutí znamená, že může dojít k soudnímu přezkumu v členském státě dozorového úřadu, který rozhodnutí přijal.

(130) Pokud dozorový úřad, jemuž byla stížnost podána, není vedoucím dozorovým úřadem, měl by s ním vedoucí dozorový úřad úzce spolupracovat v souladu s ustanoveními o spolupráci a jednotnosti obsaženými v tomto nařízení. V těchto případech by vedoucí dozorový úřad měl při přijetí opatření s právními účinky, včetně uložení správních pokut, v maximální míře zohlednit stanovisko dozorového úřadu, jemuž byla stížnost podána a jenž by měl i nadále mít pravomoc provádět společně s příslušným dozorovým úřadem jakékoliv šetření na území svého členského státu.

(131) V případech, kdy by měl jiný dozorový úřad jednat jako vedoucí dozorový úřad pro činnosti zpracování prováděné správcem nebo zpracovatelem, ale kdy se konkrétní předmět stížnosti nebo možné porušení týkají pouze činností zpracování prováděných správcem či zpracovatelem v tom členském státě, v němž byla stížnost podána nebo zjištěno možné porušení, a daná záležitost se podstatným způsobem nedotýká či pravděpodobně nedotkne subjektů údajů v dalších členských státech, by dozorový úřad, jenž obdržel stížnost nebo odhalil situace, které představují možné porušení tohoto nařízení, nebo byl o těchto situacích informován jiným způsobem, měl usilovat o smírné řešení se správcem, a nebude-li v tomto úsilí úspěšný, měl by uplatnit veškerou škálu svých pravomocí. Mělo by sem mimo jiné patřit zvláštní zpracování prováděné na území členského státu daného dozorového úřadu nebo zpracování týkající se subjektů údajů na území tohoto členského státu, zpracování prováděné v souvislosti s nabídkou zboží nebo služeb konkrétně zaměřenou na subjekty údajů na území členského státu daného dozorového úřadu, nebo zpracování, které musí být posouzeno s ohledem na příslušné právní závazky podle práva členského státu.

(132) Činnosti dozorových úřadů, jejichž cílem je zvyšování povědomí veřejnosti, by měly zahrnovat specifická opatření zaměřená na správce a zpracovatele, včetně mikropodniků a malých a středních podniků, jakož i na fyzické osoby, zejména v kontextu vzdělávání.

(133) Dozorové úřady by si při plnění svých úkolů měly být vzájemně nápomocny, aby bylo zajištěno jednotné uplatňování a prosazování tohoto nařízení na vnitřním trhu. Dozorový úřad, který požádal o vzájemnou pomoc, může přijmout prozatímní opatření, pokud neobdrží odpověď na žádost o vzájemnou pomoc do jednoho měsíce od obdržení této žádosti jiným dozorovým úřadem.

(134) Každý dozorový úřad by se měl ve vhodných případech účastnit společných postupů dozorových úřadů. Dožádaný dozorový úřad by měl mít povinnost reagovat na žádost ve stanovené lhůtě.

(135) Aby bylo zajištěno jednotné uplatňování tohoto nařízení v celé Unii, měl by být zaveden mechanismus jednotnosti pro spolupráci mezi dozorovými úřady. Tento mechanismus by se měl použít především tehdy, má-li některý dozorový úřad v úmyslu přijmout opatření s právními účinky ve vztahu k operacím zpracování, které se podstatně dotýkají významného počtu subjektů údajů v několika členských státech. Měl by se použít také v případě, kdy kterýkoli dotčený dozorový úřad nebo Komise žádají, aby byla daná záležitost vyřešena v rámci mechanismu jednotnosti. Tímto mechanismem by neměla být dotčena jiná opatření, která by Komise mohla přijmout při výkonu svých pravomocí podle Smluv.

(136) Při použití mechanismu jednotnosti by sbor měl ve stanovené lhůtě vydat stanovisko, pokud tak rozhodne většina jeho členů nebo pokud o to požádá kterýkoli dotčený dozorový úřad či Komise. Sbor by rovněž měl být zmocněn k přijímání právně závazných rozhodnutí v případě sporů mezi dozorovými úřady. Pro tyto účely by měl vydávat v zásadě se souhlasem dvoutřetinové většiny svých členů právně závazná rozhodnutí v jasně určených případech, kdy mezi dozorovými úřady existují protikladná stanoviska, zejména v rámci mechanismu spolupráce mezi vedoucím dozorovým úřadem a dotčenými dozorovými úřady, pokud jde o podstatu věci, zejména o to, zda došlo k porušení tohoto nařízení.

(137) Může se vyskytnout naléhavá potřeba konat z důvodu ochrany práv a svobod subjektů údajů, zejména pokud hrozí, že výkon některého z práv subjektu údajů by mohl být značně ztížen. Dozorový úřad by proto měl mít možnost v řádně odůvodněných případech přijmout na svém území prozatímní opatření se stanovenou dobou platnosti, která by neměla být delší než tři měsíce.

(138) Použití takového mechanismu by mělo být podmínkou legality opatření s právními účinky přijatého dozorovým úřadem v těch případech, kdy je jeho použití povinné. V ostatních případech s přeshraničním rozměrem by se měl použít mechanismus spolupráce mezi vedoucím dozorovým úřadem a dotčenými dozorovými úřady a dotčené dozorové úřady by si na dvoustranné nebo mnohostranné úrovni mohly poskytovat vzájemnou pomoc a provádět společné postupy, aniž by mechanismus jednotnosti použily.

(139) Za účelem podpory důsledného uplatňování tohoto nařízení by sbor měl být zřízen jako nezávislý subjekt Unie. Aby sbor mohl plnit své cíle, měl by mít právní subjektivitu. Sbor by měl zastupovat jeho předseda. Sbor by měl nahradit pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, zřízenou směrnicí 95/46/ES. Měl by být složen z vedoucího dozorového úřadu každého členského státu a evropského inspektora ochrany údajů nebo jejich příslušných zástupců. Komise by se měla na jeho činnosti sboru podílet bez hlasovacího práva a evropský inspektor ochrany údajů by měl mít zvláštní hlasovací práva. Sbor by měl přispívat k jednotnému uplatňování tohoto nařízení v celé Unii, například poskytovat Komisi poradenství, zejména ohledně úrovně ochrany ve třetích zemích nebo v mezinárodních organizacích, a podporovat spolupráci dozorových úřadů v celé Unii. Sbor by měl při plnění svých úkolů jednat nezávisle.

(140) Sboru by měl být nápomocen sekretariát, jehož služby zajistí evropský inspektor ochrany údajů. Pracovníci evropského inspektora ochrany údajů podílející se na plnění úkolů svěřených sboru tímto nařízením by měli své úkoly plnit výhradně na základě pokynů a pod vedením předsedy sboru.

(141) Každý subjekt údajů by měl mít právo podat stížnost u jediného dozorovému úřadu, zejména v členském státě, kde má své obvyklé bydliště, a právo na účinnou soudní ochranu v souladu s článkem 47 Listiny, jestliže se

domnívá, že byla porušena jeho práva podle tohoto nařízení, nebo pokud dozorový úřad na stížnost nereaguje, stížnost zcela či částečně odmítne či zamítne, nebo pokud nekoná, přestože je to nutné z důvodu ochrany práv subjektu údajů. Šetření, které následuje po podání stížnosti, by mělo být s výhradou soudního přezkumu provedeno v rozsahu, jenž je v daném případě přiměřený. Dozorový úřad by měl subjekt údajů v přiměřené lhůtě informovat o pokroku v řešení stížnosti a o jeho výsledku. Je-li v dané věci zapotřebí další šetření nebo koordinace s jiným dozorovým úřadem, měl by být subjekt údajů informován průběžně. S cílem usnadnit podávání stížností by měl každý dozorový úřad přijmout určitá opatření, například poskytnout formulář pro podání stížnosti, který lze vyplnit i elektronicky, aniž by byly vyloučeny další komunikační prostředky.

(142) Pokud se subjekt údajů domnívá, že jeho práva podle tohoto nařízení byla porušena, měl by být oprávněn pověřit určitý neziskový subjekt, organizaci nebo sdružení, které jsou zřízeny v souladu s právem členského státu, jejichž statutární cíle jsou ve veřejném zájmu a které působí v oblasti ochrany osobních údajů, aby podaly jeho jménem stížnost u dozorového úřadu, uplatnily právo na soudní ochranu jménem subjektu údajů nebo uplatnily jménem subjektu údajů právo na odškodnění, je-li stanoveno v právu členského státu. Členský stát může stanovit, že tento subjekt, organizace nebo sdružení má právo podat v daném členském státě stížnost nezávisle na pověření od subjektu údajů a právo na účinnou soudní ochranu, pokud mají důvod se domnívat, že došlo k porušení práva subjektu údajů v důsledku zpracování osobních údajů, které je porušením tohoto nařízení. Tento subjekt, organizace nebo sdružení nesmí požadovat jménem subjektu údajů náhradu škody, aniž by ho tím subjekt údajů pověřil.

(143) Každá fyzická nebo právnická osoba má právo podat žalobu na neplatnost rozhodnutí sboru u Soudního dvora za podmínek stanovených v článku 263 Smlouvy o fungování EU. Jakožto orgány, jimž jsou taková rozhodnutí určena, musí dotčené dozorové úřady, které chtějí tato rozhodnutí napadnout, v souladu s článkem 263 Smlouvy o fungování EU žalobu podat ve lhůtě dvou měsíců ode dne, kdy jim byla rozhodnutí oznámena. Pokud se rozhodnutí sboru bezprostředně a osobně dotýkají správce, zpracovatele nebo stěžovatele, mohou tyto osoby podat žalobu na neplatnost těchto rozhodnutí a v souladu s článkem 263 Smlouvy o fungování EU ve lhůtě dvou měsíců od jejich zveřejnění na internetových stránkách sboru. Aniž je dotčeno toto právo podle článku 263 Smlouvy o fungování EU, měla by mít každá fyzická nebo právnická osoba právo na účinnou soudní ochranu u příslušného vnitrostátního soudu proti rozhodnutím dozorového úřadu, která vůči ní zakládají právní účinky. Taková rozhodnutí se týkají zejména výkonu vyšetřovacích, nápravných a povolovacích pravomocí dozorovým úřadem nebo odmítnutí či zamítnutí stížností. Právo na účinnou soudní ochranu se však nevztahuje na další opatření dozorových úřadů, která nejsou právně závazná, jako jsou stanoviska vydávaná dozorovým úřadem nebo poradenství jím poskytované. Řízení proti dozorovému úřadu by mělo být zahájeno u soudů toho členského státu, v němž je daný dozorový úřad zřízen, a mělo by probíhat podle procesního práva tohoto členského státu. Tyto soudy by měly vykonávat soudní pravomoc v plném rozsahu, která by měla zahrnovat pravomoc řešit všechny skutkové a právní otázky, které jsou pro jimi projednávaný spor relevantní.

Pokud dozorový úřad odmítl nebo zamítl stížnost, může se stěžovatel obrátit na soudy v tomtéž členském státě. Pokud jde o soudní ochranu související s uplatňováním tohoto nařízení, vnitrostátní soudy, které zvažují rozhodnutí o otázce nezbytné pro vydání jejich rozsudku, mohou, nebo v případě uvedeném v článku 267 Smlouvy o fungování EU musí, požádat Soudní dvůr o rozhodnutí o předběžné otázce týkající se výkladu práva Unie včetně tohoto nařízení. Kromě toho pokud je rozhodnutí dozorového úřadu, kterým se provádí rozhodnutí sboru, napadeno u vnitrostátního soudu a předmětem sporu je platnost daného rozhodnutí sboru, nemá tento vnitrostátní soud pravomoc prohlásit rozhodnutí sboru za neplatné, nýbrž se musí v případě, že je považuje za neplatné, obrátit v otázce platnosti na Soudní dvůr v souladu s článkem 267 Smlouvy o fungování EU. Vnitrostátní soud se však nemůže s otázkou platnosti rozhodnutí sboru obrátit na Soudní dvůr na žádost fyzické či právnické osoby, která měla možnost podat žalobu na neplatnost tohoto rozhodnutí, zejména pokud se jí rozhodnutí bezprostředně a osobně dotýkalo, avšak ve lhůtě stanovené v článku 263 Smlouvy o fungování EU tak neučinila.

(144) Domnívá-li se soud vedoucí řízení proti rozhodnutí dozorového úřadu, že před příslušným soudem v jiném členském státě je vedeno řízení týkající se stejného zpracování, jako je například stejný předmět, pokud jde o zpracování prováděné stejným správcem nebo zpracovatelem, nebo stejný důvod činnosti, měl by tento soud kontaktovat, aby ověřil existenci takových souvisejících řízení. Není-li související řízení před soudem v jiném členském státě dosud vyřízeno, mohou všechny soudy, u nichž nebylo řízení zahájeno jako první, svá řízení

přerušit nebo se mohou na žádost zúčastněné strany příslušnosti vzdát ve prospěch soudu, u něhož bylo řízení zahájeno jako první, jestliže je soud, u něhož bylo řízení zahájeno jako první, příslušný pro daná řízení a spojení těchto souvisejících řízení je podle práva státu tohoto soudu přípustné. Má se za to, že řízení spolu navzájem souvisejí, pokud je mezi nimi tak úzký vztah, že jejich společné projednání a rozhodnutí je vhodné k tomu, aby se zabránilo vydání vzájemně si odporujících rozhodnutí v oddělených řízeních.

(145) Při řízeních proti správci nebo zpracovateli by žalobce měl mít možnost volby, zda podá žalobu u soudů členského státu, kde má správce nebo zpracovatel provozovnu nebo kde má subjekt údajů bydliště, s výjimkou případů, kdy je správce orgánem veřejné moci členského státu, který jedná v rámci výkonu veřejné moci.

(146) Veškerou újmu, která může osobám vzniknout v důsledku zpracování, které porušuje toto nařízení, by měl nahradit správce nebo zpracovatel. Správce nebo zpracovatel by však měl být odpovědnosti zproštěn, pokud prokáže, že za újmu nenese žádným způsobem odpovědnost. Výklad pojmu „újma" by měl být široký a opírat se o judikaturu Soudního dvora při plném zohlednění cílů tohoto nařízení. Tím nejsou dotčeny jakékoliv nároky uplatňované v případě újmy způsobené porušením jiných pravidel práva Unie nebo členského státu. Zpracování, které porušuje toto nařízení, zahrnuje rovněž zpracování, které porušuje akty v přenesené pravomoci a prováděcí akty přijaté v souladu s tímto nařízením a právními předpisy členského státu upřesňující pravidla tohoto nařízení. Subjekty údajů by měly obdržet plnou a účinnou náhradu újmy, kterou utrpěly. Jsou-li správci nebo zpracovatelé zapojeni do téhož zpracování, měl by každý správce nebo zpracovatel nést odpovědnost za celkovou újmu. Jsou-li však tito správci nebo zpracovatelé v souladu s právem členského státu spojeni v tomtéž řízení, může být náhrada újmy rozvržena podle odpovědnosti každého správce nebo zpracovatele za újmu způsobenou zpracováním, za podmínky, že je zajištěno úplné a účinné odškodnění subjektu údajů, jenž újmu utrpěl. Kterýkoli správce nebo zpracovatel, který uhradil plnou náhradu újmy, může následně zahájit soudní řízení proti jiným správcům nebo zpracovatelům zapojeným do téhož zpracování.

(147) Jsou-li v tomto nařízení obsažena zvláštní pravidla o soudní příslušnosti, zejména pokud jde o řízení týkající se žádosti o soudní ochranu, včetně odškodnění, vedené proti správci nebo zpracovateli, nemělo by uplatnění těchto zvláštních pravidel být dotčeno obecnými pravidly o soudní příslušnosti, jako jsou například pravidla stanovená v nařízení Evropského parlamentu a Rady (EU) č. 1215/2012 ([1]).

(148) S cílem posílit prosazování pravidel tohoto nařízení by za jakékoliv jeho porušení měly být uloženy sankce včetně správních pokut, a to vedle nebo namísto vhodných opatření uložených dozorovým úřadem podle tohoto nařízení. V méně závažných případech porušení nebo pokud by pokuta, která bude pravděpodobně uložena, představovala pro fyzickou osobu nepřiměřenou zátěž, může být namísto pokuty uloženo napomenutí. Náležitě by se však měla zohlednit povaha, závažnost a doba trvání porušení, úmyslný charakter porušení, kroky, které byly učiněny s cílem zmírnit způsobenou škodu, míra odpovědnosti nebo jakékoli relevantní předchozí porušení, způsob, jakým se dozorový úřad o daném porušení dozvěděl, dodržování opatření, která byla vůči správci nebo zpracovateli nařízena, dodržování kodexu chování nebo jakýkoli jiný přitěžující nebo polehčující faktor. Uložení sankcí včetně správních pokut by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami právních předpisů Unie a Listiny, včetně účinné právní ochrany a spravedlivého procesu.

(149) Členské státy by měly mít možnost stanovit pravidla týkající se trestních sankcí za porušení tohoto nařízení, včetně porušení vnitrostátních pravidel přijatých podle tohoto nařízení a v jeho mezích. Tyto trestní sankce mohou rovněž zahrnovat odebrání zisků získaných na základě porušení tohoto nařízení. Uložení trestních sankcí za porušení těchto vnitrostátních pravidel a správních pokut by však nemělo vést k porušení zásady *ne bis in idem*, jak ji vykládá Soudní dvůr.

(150) Aby byly posíleny a harmonizovány správní sankce za porušení tohoto nařízení, měl by každý dozorový úřad mít pravomoc uložit správní pokuty. V tomto nařízení by měly být uvedeny porušení a maximální hranice

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 1215/2012 ze dne 12. prosince 2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech (Úř. věst. L 351, 20.12.2012, s. 1).

a kritéria pro stanovení souvisejících správních pokut, jež by měl v každém jednotlivém případě určit příslušný dozorový úřad při zohlednění všech příslušných okolností konkrétní situace s náležitým přihlédnutím zejména k povaze, závažnosti a době trvání tohoto porušení a k jeho důsledkům a opatřením přijatým v zájmu zajištění souladu s povinnostmi vyplývajícími z tohoto nařízení a v zájmu prevence či zmírnění důsledků tohoto porušení. Pro účely uložení správních pokut podniku by měl být podnik chápán ve smyslu článků 101 a 102 Smlouvy o fungování EU. Jsou-li správní pokuty uloženy osobám, které nejsou podnikem, měl by dozorový úřad při rozhodování o odpovídající výši pokuty zohlednit obecnou úroveň příjmů v daném členském státě, jakož i ekonomickou situaci dané osoby. K prosazování důsledného uplatňování správních pokut je možné využít rovněž mechanismus jednotnosti. Zda a do jaké míry by se měly správní pokuty vztahovat na orgány veřejné moci, by měl určit členský stát. Uložení správní pokuty nebo varování nemá vliv na uplatňování dalších pravomocí dozorových úřadů nebo dalších sankcí podle tohoto nařízení.

(151) Právní systémy Dánska a Estonska neumožňují uložení správních pokut v podobě stanovené tímto nařízením. Pravidla týkající se správních pokut mohou být uplatňována tak, že v Dánsku pokutu uloží příslušný vnitrostátní soud jakožto trestní sankci a v Estonsku pokutu uloží dozorový úřad v přestupkovém řízení, pokud takové uplatnění pravidel má v uvedených členských státech účinek, který je rovnocenný správním pokutám uloženým dozorovými úřady. Příslušné vnitrostátní soudy by tedy měly zohlednit doporučení dozorového úřadu, který dal podnět k uložení pokuty. Uložené pokuty by v každém případě měly být účinné, přiměřené a odrazující.

(152) Nejsou-li správní sankce harmonizovány tímto nařízením nebo v případě potřeby v jiných případech, jako jsou závažná porušení tohoto nařízení, měly by členské státy zavést systém, který zajistí uložení účinných, přiměřených a odrazujících pokut. Povaha těchto trestních nebo správních sankcí by měla být stanovena právem členského státu.

(153) Právo členského státu by měly uvádět pravidla upravující svobodu projevu a informací, včetně novinářského, akademického, uměleckého nebo literárního projevu, do souladu s právem na ochranu osobních údajů podle tohoto nařízení. Na zpracování osobních údajů prováděné výhradně pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu by se měly vztahovat odchylky nebo výjimky z některých ustanovení tohoto nařízení, je-li to nutné za účelem uvedení práva na ochranu osobních údajů do souladu s právem na svobodu projevu a informací, jak je zakotveno v článku 11 Listiny. To by mělo platit zejména pro zpracování osobních údajů v audiovizuální oblasti a ve zpravodajských a tiskových archivech. Členské státy by proto měly přijmout legislativní opatření stanovující výjimky a odchylky nezbytné pro vyvážení těchto základních práv. Členské státy by měly tyto výjimky a odchylky přijímat s ohledem na obecné zásady, práva subjektu údajů, správce a zpracovatele, předávání osobních údajů do třetích zemí nebo mezinárodním organizacím, nezávislé dozorové úřady a na spolupráci a jednotné použití a zvláštní případy zpracování osobních údajů. Pokud se tyto výjimky a odchylky v jednotlivých členských státech liší, mělo by se použít právo členského státu, které se na správce vztahuje. Aby byl zohledněn význam práva na svobodu projevu v každé demokratické společnosti, je třeba vykládat pojmy související s touto svobodou, například žurnalistika, šířeji.

(154) Toto nařízení umožňuje, aby při jeho provádění byla zohledněna zásada přístupu veřejnosti k úředním dokumentům. Lze mít za to, že přístup veřejnosti k úředním dokumentům je ve veřejném zájmu. Orgán veřejné moci nebo veřejný subjekt by měl mít možnost zpřístupnit veřejnosti osobní údaje v dokumentech, které jsou v jeho držení, pokud je toto zpřístupnění stanoveno právem Unie nebo členského státu, které se na tento orgán nebo subjekt vztahuje. Tyto právní předpisy by měly zajišťovat soulad přístupu veřejnosti k úředním dokumentům a opakovaného použití informací veřejného sektoru s právem na ochranu osobních údajů, a mohou proto stanovit nezbytné zajištění souladu s právem na ochranu osobních údajů podle tohoto nařízení. Odkaz na orgány veřejné moci a veřejné subjekty by v tomto kontextu měl zahrnovat všechny orgány nebo jiné subjekty, na něž se vztahuje právo členského státu v oblasti přístupu veřejnosti k dokumentům. Směrnice Evropského parlamentu a Rady 2003/98/ES [1] ponechává nedotčenu a nijak neovlivňuje úroveň ochrany

[1] Směrnice Evropského parlamentu a Rady 2003/98/ES ze dne 17. listopadu 2003 o opakovaném použití informací veřejného sektoru (Úř. věst. L 345, 31.12.2003, s. 90).

fyzických osob v souvislosti se zpracováním osobních údajů podle práva Unie a členských států, a zejména nemění povinnosti a práva podle tohoto nařízení. Uvedená směrnice by se zejména neměla vztahovat na dokumenty, k nimž je vyloučen nebo omezen přístup na základě režimů přístupu z důvodu ochrany osobních údajů, a na části dokumentů přístupné podle těchto režimů, které obsahují osobní údaje, jejichž opakované použití bylo právně vymezeno jako jednání v rozporu s právními předpisy na ochranu fyzických osob v souvislosti se zpracováním osobních údajů.

(155) Právo členského státu nebo kolektivní smlouvy (včetně „podnikových dohod“) mohou stanovit zvláštní pravidla, která upraví zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména podmínky, za nichž lze osobní údaje v souvislosti se zaměstnáním zpracovávat na základě souhlasu zaměstnance, za účelem náboru, plnění pracovní smlouvy včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a různorodosti na pracovišti, zdraví a bezpečnosti na pracovišti, dále za účelem individuálního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru.

(156) Zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely by mělo podléhat vhodným zárukám týkajícím se práv a svobod subjektu údajů podle tohoto nařízení. Tyto záruky by měly zajistit, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit dodržování zásady minimalizace údajů. Další zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely má být provedeno, pokud správce usoudil, že je možné splnit tyto účely na základě zpracování osobních údajů, které neumožňují nebo již neumožňují identifikaci subjektů údajů, za podmínky existence vhodných záruk (jako je například pseudonymizace osobních údajů). Členské státy by měly stanovit vhodné záruky týkající se zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely. Členské státy by měly mít v souvislosti se zpracováním osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely možnost stanovit, za zvláštních podmínek podléhajícím vhodným zárukám pro subjekty údajů, upřesnění a odchylky týkající se požadavků na informace a práva na opravu nebo výmaz osobních údajů, práva být zapomenut, práva na omezení zpracování, práva na přenositelnost údajů a práva vznést námitku. S danými podmínkami a zárukami mohou být spojeny zvláštní postupy určené subjektům údajů pro uplatňování těchto práv, je-li to vhodné s ohledem na účely daného konkrétního zpracování, spolu s technickými a organizačními opatřeními, jejichž cílem je minimalizovat zpracování osobních údajů při uplatňování zásad přiměřenosti a nutnosti. Zpracování osobních údajů pro vědecké účely by mělo být v souladu i s dalšími příslušnými právními předpisy, upravujícími například klinická hodnocení.

(157) Díky propojení informací z registrů mohou výzkumní pracovníci získat velmi cenné poznatky o rozšířených onemocněních, jako jsou kardiovaskulární onemocnění, rakovina a deprese. Na základě informací z registrů mohou být výsledky výzkumů posíleny, neboť takové výzkumy vycházejí z rozsáhlejšího vzorku populace. V rámci společenských věd umožňuje výzkum vycházející z informací obsažených v registrech výzkumným pracovníkům získat základní poznatky o dlouhodobém vztahu mezi řadou sociálních podmínek, jako je stav nezaměstnanosti a úroveň vzdělání, a jinými životními proměnnými. Výsledky výzkumu získané prostřednictvím registrů poskytují spolehlivé a velmi kvalitní poznatky, které mohou sloužit jako základ pro formulaci a provádění znalostní politiky, zvýšit kvalitu života řady osob a zlepšit účinnost sociálních služeb. S cílem usnadnit vědecký výzkum mohou být osobní údaje zpracovávány pro účely vědeckého výzkumu s výhradou vhodných podmínek a záruk stanovených v právu Unie nebo členského státu.

(158) Toto nařízení by se mělo vztahovat i na případy zpracování osobních údajů pro účely archivace, přičemž je třeba mít na paměti, že by se nemělo vztahovat na osobní údaje zesnulých osob. Orgány veřejné moci či veřejné nebo soukromé subjekty, které mají v držení záznamy veřejného zájmu, by měly být útvary, které mají na základě práva Unie nebo členského státu právní povinnost získávat, uchovávat, posuzovat, uspořádat, popisovat, sdělovat, podporovat a šířit záznamy trvalé hodnoty pro obecný veřejný zájem a poskytovat k nim přístup. Členské státy by rovněž měly mít možnost stanovit, že osobní údaje mohou být dále zpracovávány pro účely archivace, například s cílem poskytnout konkrétní informace související s politickým chováním za bývalých totalitních režimů, s genocidou, zločiny proti lidskosti, zejména holokaustem, nebo válečnými zločiny.

(159) Jsou-li osobní údaje zpracovávány pro účely vědeckého výzkumu, toto nařízení by se mělo vztahovat i na takové zpracování. Pro účely tohoto nařízení by zpracování osobních údajů pro účely vědeckého výzkumu mělo být chápáno v širokém smyslu a zahrnovat například technologický vývoj a technologické demonstrace, základní výzkum, aplikovaný výzkum a výzkum financovaný ze soukromých zdrojů. Kromě toho by mělo zohledňovat cíl Unie podle čl. 179 odst. 1 Smlouvy o fungování EU, jímž je vytvoření evropského výzkumného prostoru. K účelům vědeckého výzkumu by rovněž měly patřit studie prováděné ve veřejném zájmu v oblasti veřejného zdraví. V zájmu dodržení specifických podmínek zpracování osobních údajů pro vědecké účely by měly platit zvláštní podmínky zejména pro zveřejňování nebo jiné zpřístupnění osobních údajů v souvislosti s účely vědeckého výzkumu. Vyplynou-li z vědeckého výzkumu, zejména v souvislosti se zdravím, důvody pro přijetí dalších opatření v zájmu subjektu údajů, měla by se s ohledem na tato opatření uplatňovat obecná pravidla tohoto nařízení.

(160) Jsou-li osobní údaje zpracovávány pro účely historického výzkumu, toto nařízení by se mělo vztahovat i na takové zpracování. K takovým účelům by rovněž měl patřit historický výzkum a výzkum pro genealogické účely, přičemž je třeba mít na paměti, že by se toto nařízení nemělo vztahovat na zesnulé osoby.

(161) Pro účely vyslovení souhlasu s účastí ve vědeckém výzkumu v klinických hodnoceních by měla platit příslušná ustanovení nařízení Evropského parlamentu a Rady (EU) č. 536/2014 ([1]).

(162) Jsou-li osobní údaje zpracovávány pro statistické účely, toto nařízení by se mělo vztahovat na takové zpracování. Právo Unie nebo členského státu by mělo v mezích tohoto nařízení určit statistický obsah, kontrolu přístupu, zvláštní podmínky zpracování osobních údajů pro statistické účely a vhodná opatření k zaručení práv a svobod subjektu údajů a k zajištění statistické důvěrnosti. Statistickými účely se rozumí jakékoli operace shromažďování a zpracování osobních údajů nezbytné pro statistická zjišťování nebo pro generování statistických výsledků. Tyto statistické výsledky mohou být dále použity pro různé účely, včetně účelů vědeckého výzkumu. Jestliže se jedná o statistické účely, výsledkem zpracování nejsou osobní údaje, ale souhrnné údaje, a tento výsledek ani dané osobní údaje nejsou používány na podporu opatření nebo rozhodnutí týkajících se konkrétní fyzické osoby.

(163) Důvěrné informace, které statistické orgány Unie a členských států shromažďují za účelem vypracovávání úředních evropských a vnitrostátních statistik, by měly být chráněny. Evropské statistiky by měly být sestavovány, vypracovávány a šířeny v souladu se statistickými zásadami stanovenými v čl. 338 odst. 2 Smlouvy o fungování EU, zatímco vnitrostátní statistiky by měly splňovat rovněž požadavky práva členského státu. Další upřesnění o statistické důvěrnosti evropské statistiky poskytuje nařízení Evropského parlamentu a Rady (ES) č. 223/2009 ([2]).

(164) Pokud jde o pravomoci dozorových úřadů získat od správce nebo zpracovatele přístup k osobním údajům a přístup do jejich prostor, mohou členské státy v mezích tohoto nařízení právním předpisem přijmout zvláštní pravidla pro zajištění povinnosti zachovávat služební nebo jiné rovnocenné tajemství, pokud je to nezbytné pro uvedení práva na ochranu osobních údajů do souladu s povinností zachovávat služební tajemství. Nejsou tím dotčeny stávající povinnosti členských států přijmout pravidla o uplatňování služebního tajemství tam, kde to vyžadují právní předpisy Unie.

(165) V souladu s článkem 17 Smlouvy o fungování EU toto nařízení uznává postavení, které podle stávajícího ústavního práva mají církve a náboženská sdružení či společenství v členských státech, a nedotýká se jej.

(166) Aby byly splněny cíle tohoto nařízení, zejména chránit základní práva a svobody fyzických osob a především jejich právo na ochranu osobních údajů a zajistit volný pohyb osobních údajů v rámci Unie, měla by být na

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 536/2014 ze dne 16. dubna 2014 o klinických hodnoceních humánních léčivých přípravků a o zrušení směrnice 2001/20/ES (Úř. věst. L 158, 27.5.2014, s. 1).

([2]) Nařízení Evropského parlamentu a Rady (ES) č. 223/2009 ze dne 11. března 2009 o evropské statistice a zrušení nařízení (ES, Euratom) č. 1101/2008 o předávání údajů, na které se vztahuje statistická důvěrnost, Statistickému úřadu Evropských společenství, nařízení Rady (ES) č. 322/97 o statistice Společenství a rozhodnutí Rady 89/382/EHS, Euratom, kterým se zřizuje Výbor pro statistické programy Evropských společenství (Úř. věst. L 87, 31.3.2009, s. 164).

Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování EU. Akty v přenesené pravomoci by měly být přijímány především s ohledem na kritéria a požadavky týkající se mechanismů pro vydávání osvědčení, informace, které mají být poskytovány pomocí standardizovaných ikon a postupy pro prezentaci takových ikon. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni. Při přípravě a vypracovávání aktů v přenesené pravomoci by Komise měla zajistit, aby byly příslušné dokumenty předány současně, včas a vhodným způsobem Evropskému parlamentu a Radě.

(167) V zájmu zajištění jednotných podmínek pro provádění tohoto nařízení je třeba svěřit Komisi prováděcí pravomoci v případech stanovených tímto nařízením. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011. Komise by v této souvislosti měla zvážit zvláštní opatření, pokud jde o mikropodniky a malé a střední podniky.

(168) Přezkumný postup by se měl použít při přijímání prováděcích aktů, pokud jde o standardní smluvní doložky mezi správci a zpracovateli a mezi zpracovateli navzájem, kodexy chování; technické normy a mechanismy pro vydávání osvědčení; odpovídající úroveň ochrany poskytovanou určitou třetí zemí, určitým územím či konkrétním odvětvím v určité třetí zemi nebo určitou mezinárodní organizací; přijetí standardních ustanovení o ochraně údajů; formáty a postupy pro výměnu informací elektronickými prostředky mezi správci, zpracovateli a dozorovými úřady pro účely závazných podnikových pravidel; vzájemnou pomoc; ujednání pro výměnu informací elektronickými prostředky mezi dozorovými úřady navzájem a mezi dozorovými úřady a sborem.

(169) Je-li to nezbytné v závažných, naléhavých a řádně odůvodněných případech, jestliže dostupné důkazy poukazují na to, že určitá třetí země, určité území či konkrétní odvětví zpracování v určité třetí zemi nebo určitá mezinárodní organizace nezajišťuje odpovídající úroveň ochrany, a jedná-li se o krajně naléhavé případy, měla by Komise přijmout okamžitě použitelné prováděcí akty.

(170) Jelikož cíle tohoto nařízení, totiž zajištění přiměřené úrovně ochrany fyzických osob a volného pohybu osobních údajů v Unii, nemůže být dosaženo uspokojivě členskými státy, ale spíše jej, z důvodu rozsahu nebo účinků tohoto nařízení, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii (dále jen „Smlouva o EU“). V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení tohoto cíle.

(171) Směrnice 95/46/ES by tudíž měla být tímto nařízením zrušena. Zpracování, které již ke dni použitelnosti tohoto nařízení probíhá, by mělo být uvedeno v soulad s tímto nařízením ve lhůtě dvou let ode dne vstupu tohoto nařízení v platnost. Je-li toto zpracování založeno na souhlasu podle směrnice 95/46/ES, není nutné, aby subjekt údajů znovu udělil svůj souhlas, pokud je způsob udělení daného souhlasu v souladu s podmínkami tohoto nařízení, s cílem umožnit správci pokračovat v tomto zpracování i po dni použitelnosti tohoto nařízení. Přijatá rozhodnutí Komise a schválení dozorových úřadů vycházející ze směrnice 95/46/ES by měla zůstat v platnosti, dokud nebudou změněna, nahrazena nebo zrušena.

(172) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 a vydal stanovisko dne 7. března 2012 ([1]).

(173) Toto nařízení by se mělo použít na všechny záležitosti týkající se ochrany základních práv a svobod při zpracování osobních údajů, na které se nevztahují specifické povinnosti stanovené ve směrnici Evropského parlamentu a Rady 2002/58/ES ([2]) a sledující stejný cíl, včetně povinností správce a práv fyzických osob. Za účelem vyjasnění vztahu mezi tímto nařízením a směrnicí 2002/58/ES by měla být uvedená směrnice odpovídajícím způsobem změněna. Jakmile bude toto nařízení přijato, směrnice 2002/58/ES by měla být podrobena přezkumu, zejména s cílem zajistit soudržnost s tímto nařízením,

([1]) Úř. věst. C 192, 30.6.2012, s. 7.
([2]) 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).

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

Obecná ustanovení

Článek 1

Předmět a cíle

1. Toto nařízení stanoví pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů a pravidla týkající se volného pohybu osobních údajů.

2. Toto nařízení chrání základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů.

3. Volný pohyb osobních údajů v Unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán.

Článek 2

Věcná působnost

1. Toto nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.

2. Toto nařízení se nevztahuje na zpracování osobních údajů prováděné:

a) při výkonu činností, které nespadají do oblasti působnosti práva Unie;

b) členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU;

c) fyzickou osobou v průběhu výlučně osobních či domácích činností;

d) příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

3. Na zpracování osobních údajů orgány, institucemi a jinými subjekty Unie se vztahuje nařízení (ES) č. 45/2001. Nařízení (ES) č. 45/2001 a další právní akty Unie týkající se takového zpracování osobních údajů jsou uzpůsobeny zásadám a pravidlům tohoto nařízení podle článku 98.

4. Tímto nařízením není dotčeno uplatňování směrnice 2000/31/ES, zejména pokud jde o pravidla týkající se odpovědnosti poskytovatelů zprostředkovatelských služeb uvedená v článcích 12 až 15 uvedené směrnice.

Článek 3

Místní působnost

1. Toto nařízení se vztahuje na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii bez ohledu na to, zda zpracování probíhá v Unii či mimo ni.

2. Toto nařízení se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí:

a) s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba; nebo

b) s monitorováním jejich chování, pokud k němu dochází v rámci Unie.

3. Toto nařízení se vztahuje na zpracování osobních údajů správcem, který není usazen v Unii, ale na místě, kde se právo členského státu uplatňuje na základě mezinárodního práva veřejného.

Článek 4

Definice

Pro účely tohoto nařízení se rozumí:

1) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

2) „zpracováním“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;

3) „omezením zpracování“ označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;

4) „profilováním“ jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;

5) „pseudonymizací“ zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

6) „evidencí“ jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;

7) „správcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;

8) „zpracovatelem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;

9) „příjemcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní

údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování;

10) „třetí stranou“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů;

11) „souhlasem“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

12) „porušením zabezpečení osobních údajů“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

13) „genetickými údaji“ osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby;

14) „biometrickými údaji“ osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

15) „údaji o zdravotním stavu“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;

16) „hlavní provozovnou“:

a) v případě správce s provozovnami ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, ledaže jsou rozhodnutí o účelech a prostředcích zpracování osobních údajů přijímána v jiné provozovně správce v Unii a tato jiná provozovna má pravomoc vymáhat provádění těchto rozhodnutí, přičemž v takovém případě je za hlavní provozovnu považována provozovna, která tato rozhodnutí přijala;

b) v případě zpracovatele s provozovnami ve více než jednom členském státě místo, kde se nachází jeho ústřední správa v Unii, nebo pokud zpracovatel nemá v Unii žádnou ústřední správu, pak ta provozovna zpracovatele v Unii, kde probíhají hlavní činnosti zpracování v souvislosti s činnostmi provozovny zpracovatele, v rozsahu, v jakém se na zpracovatele vztahují specifické povinnosti podle tohoto nařízení;

17) „zástupcem“ jakákoli fyzická nebo právnická osoba usazená v Unii, která je správcem nebo zpracovatelem určena písemně podle článku 27 k tomu, aby správce nebo zpracovatele zastupovala, pokud jde o příslušné povinnosti správce nebo zpracovatele ve smyslu tohoto nařízení;

18) „podnikem“ jakákoli fyzická nebo právnická osoba vykonávající hospodářskou činnost bez ohledu na její právní formu, včetně osobních společností nebo sdružení, která běžně vykonávají hospodářskou činnost;

19) „skupinou podniků“ skupina zahrnující řídící podnik a jím řízené podniky;

20) „závaznými podnikovými pravidly“ koncepce ochrany osobních údajů, kterou dodržuje správce nebo zpracovatel usazený na území členského státu při jednorázových nebo souborných předáních osobních údajů správci nebo zpracovateli v jedné nebo více třetích zemích v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost;

21) „dozorovým úřadem“ nezávislý orgán veřejné moci zřízený členským státem podle článku 51;

22) „dotčeným dozorovým úřadem“ dozorový úřad, kterého se zpracování osobních údajů dotýká, neboť:

a) správce či zpracovatel je usazen na území členského státu tohoto dozorového úřadu;

b) subjekty údajů s bydlištěm v členském státě tohoto dozorového úřadu jsou nebo pravděpodobně budou zpracováním podstatně dotčeny, nebo

c) u něj byla podána stížnost;

23) „přeshraničním zpracováním“ buď:

a) zpracování osobních údajů, které probíhá v souvislosti s činnostmi provozoven ve více než jednom členském státě správce či zpracovatele v Unii, je-li tento správce či zpracovatel usazen ve více než jednom členském státě; nebo

b) zpracování osobních údajů, které probíhá v souvislosti s činnostmi jediné provozovny správce či zpracovatele v Unii, ale kterým jsou nebo pravděpodobně budou podstatně dotčeny subjekty údajů ve více než jednom členském státě;

24) „relevantní a odůvodněnou námitkou“ námitka vůči návrhu rozhodnutí za účelem posouzení, zda došlo k porušení tohoto nařízení, nebo zda je zamýšlený úkon v souvislosti se správcem či zpracovatelem v souladu s tímto nařízením, která jasně dokazuje významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně volný pohyb osobních údajů v rámci Unie;

25) „službou informační společnosti“ služba ve smyslu čl. 1 odst. 1 písm. b) směrnice (EU) 2015/1535 ([1]);

26) „mezinárodní organizací“ organizace a jí podřízené subjekty podléhající mezinárodnímu právu veřejnému nebo jiný subjekt zřízený dohodou mezi dvěma nebo více zeměmi nebo na jejím základě.

KAPITOLA II

Zásady

Článek 5

Zásady zpracování osobních údajů

1. Osobní údaje musí být:

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely („účelové omezení“);

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);

d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“);

([1]) Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1).

e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);

f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“);

2. Správce odpovídá za dodržení odstavce 1 a musí být schopen toto dodržení souladu doložit („odpovědnost“).

Článek 6

Zákonnost zpracování

1. Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.

2. Členské státy mohou zachovat nebo zavést konkrétnější ustanovení, aby přizpůsobily používání pravidel tohoto nařízení ohledně zpracování ke splnění odst. 1 písm. c) a e) tím, že přesněji určí konkrétní požadavky na zpracování a jiná opatření k zajištění zákonného a spravedlivého zpracování, a to i u jiných zvláštních situací, při nichž dochází ke zpracování, jak stanoví kapitola IX.

3. Základ pro zpracování podle odst. 1 písm. c) a e) musí být stanoven:

a) právem Unie nebo

b) právem členského státu, které se na správce vztahuje.

Účel zpracování musí vycházet z tohoto právního základu, nebo pokud jde o zpracování uvedené v odst. 1 písm. e), musí být toto zpracování nutné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce. Tento právní základ může obsahovat konkrétní ustanovení pro přizpůsobení uplatňování pravidel tohoto nařízení, včetně obecných podmínek, kterými se řídí zákonnost zpracování správcem, typu osobních údajů, které mají být zpracovány, dotčených subjektů údajů, subjektů, kterým lze osobní údaje poskytnout, a účelu tohoto poskytování, účelového omezení, doby uložení a jednotlivých operací zpracování a postupů zpracování, jakož i dalších

opatření k zajištění zákonného a spravedlivého zpracování, jako jsou opatření pro jiné zvláštní situace, při nichž dochází ke zpracování, než stanoví kapitola IX. Právo Unie nebo členského státu musí splňovat cíl veřejného zájmu a musí být přiměřené sledovanému legitimnímu cíli.

4. Pokud zpracování pro jiný účel, než pro který byly osobní údaje shromážděny, není založeno na souhlasu subjektu údajů nebo na právu Unie či členského státu, který v demokratické společnosti představuje nutné a přiměřené opatření k zajištění cílů uvedených v čl. 23 odst. 1, zohlední správce v zájmu zjištění toho, zda je zpracování pro jiný účel slučitelné s účely, pro něž byly osobní údaje původně shromážděny, mimo jiné:

a) jakoukoli vazbu mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování;

b) okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem;

c) povahu osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů podle článku 9 nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů podle článku 10;

d) možné důsledky zamýšleného dalšího zpracování pro subjekty údajů;

e) existenci vhodných záruk, mezi něž může patřit šifrování nebo pseudonymizace.

Článek 7

Podmínky vyjádření souhlasu

1. Pokud je zpracování založeno na souhlasu, musí být správce schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů.

2. Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí být žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Jakákoli část tohoto prohlášení, která představuje porušení tohoto nařízení, není závazná.

3. Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

4. Při posuzování toho, zda je souhlas svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné.

Článek 8

Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti

1. Pokud se použije čl. 6 odst. 1 písm. a) v souvislosti s nabídkou služeb informační společnosti přímo dítěti, je zpracování osobních údajů dítěte zákonné, je-li dítě ve věku nejméně 16 let. Je-li dítě mladší 16 let, je takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.

Členské státy mohou pro uvedené účely právním předpisem stanovit nižší věk, ne však nižší než 13 let.

2. Správce vyvine přiměřené úsilí s ohledem na dostupnou technologii, aby v takovýchto případech ověřil, že byl souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.

3. Odstavcem 1 není dotčeno obecné smluvní právo členských států, například pravidla týkající se platnosti, uzavírání nebo účinků smlouvy vzhledem k dítěti.

Článek 9

Zpracování zvláštních kategorií osobních údajů

1. Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

2. Odstavec 1 se nepoužije, pokud jde o některý z těchto případů:

a) subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů, s výjimkou případů, kdy právo Unie nebo členského státu stanoví, že zákaz uvedený v odstavci 1 nemůže být subjektem údajů zrušen;

b) zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany, pokud je povoleno právem Unie nebo členského státu nebo kolektivní dohodou podle práva členského státu, v němž se stanoví vhodné záruky týkající se základních práv a zájmů subjektu údajů;

c) zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;

d) zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;

e) zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;

f) zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí;

g) zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;

h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4;

i) zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků, na základě práva Unie nebo členského státu, které stanoví odpovídající a zvláštní opatření pro zajištění práv a svobod subjektu údajů, zejména služebního tajemství;

j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely v souladu s čl. 89 odst. 1 na základě práva Unie nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů.

3. Osobní údaje uvedené v odstavci 1 mohou být zpracovávány pro účely uvedené v odst. 2 písm. h), jsou-li tyto údaje zpracovány pracovníkem vázaným služebním tajemstvím nebo na jeho odpovědnost podle práva Unie nebo členského státu nebo pravidel stanovených příslušnými vnitrostátními orgány nebo jinou osobou, na niž se rovněž vztahuje povinnost mlčenlivosti podle práva Unie nebo členského státu nebo pravidel stanovených příslušnými vnitrostátními orgány.

4. Členské státy mohou zachovat nebo zavést další podmínky, včetně omezení, pokud jde o zpracování genetických údajů, biometrických údajů či údajů o zdravotním stavu.

Článek 10

Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů

Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření na základě čl. 6 odst. 1 se může provádět pouze pod dozorem orgánu veřejné moci nebo pokud je oprávněné podle práva Unie nebo členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů. Jakýkoli souhrnný rejstřík trestů může být veden pouze pod dozorem orgánu veřejné moci.

Článek 11

Zpracování, které nevyžaduje identifikaci

1. Pokud účely, pro něž správce zpracovává osobní údaje, od správce nevyžadují nebo již nevyžadují identifikaci subjektu údajů, nemá správce povinnost uchovávat, získávat nebo zpracovávat dodatečné informace za účelem identifikace subjektu údajů výlučně kvůli dosažení souladu s tímto nařízením.

2. Je-li v případech uvedených v odstavci 1 tohoto článku správce s to doložit, že není schopen identifikovat subjekt údajů, informuje o této skutečnosti subjekt údajů, pokud je to možné. V takovýchto případech se neuplatní články 15 až 20, s výjimkou případů, kdy subjekt údajů za účelem výkonu svých práv podle uvedených článků poskytne dodatečné informace umožňující jeho identifikaci.

KAPITOLA III

Práva subjektu údajů

Oddíl 1

Transparentnost a postupy

Článek 12

Transparentní informace, sdělení a postupy pro výkon práv subjektu údajů

1. Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

2. Správce usnadňuje výkon práv subjektu údajů podle článků 15 až 22. V případech uvedených v čl. 11 odst. 2 správce neodmítne vyhovět žádosti subjektu údajů za účelem výkonu jeho práv podle článků 15 až 22, ledaže doloží, že nemůže zjistit totožnost subjektu údajů.

3. Správce poskytne subjektu údajů na žádost podle článků 15 až 22 informace o přijatých opatřeních, a to bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce. Správce informuje subjekt údajů o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.

4. Pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti subjekt údajů o důvodech nepřijetí opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.

5. Informace podle článků 13 a 14 a veškerá sdělení a veškeré úkony podle článků 15 až 22 a 34 se poskytují a činí bezplatně. Jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď:

a) uložit přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo sdělení nebo s učiněním požadovaných úkonů; nebo

b) odmítnout žádosti vyhovět.

Zjevnou nedůvodnost nebo nepřiměřenost žádosti dokládá správce.

6. Aniž je dotčen článek 11, pokud má správce důvodné pochybnosti o totožnosti fyzické osoby, která podává žádost podle článků 15 až 21, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů.

7. Informace, které mají být subjektům údajů poskytnuty podle článků 13 a 14, mohou být doplněny standardizovanými ikonami s cílem poskytnout snadno viditelným, srozumitelným a jasným způsobem přehled o zamýšleném zpracování. Pokud jsou ikony prezentovány v elektronické formě, musí být strojově čitelné.

8. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 92 za účelem určení informací, které mají být sděleny pomocí ikon, a postupů pro poskytování standardizovaných ikon.

Oddíl 2

Informace a přístup k osobním údajům

Článek 13

Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů

1. Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne správce v okamžiku získání osobních údajů subjektu údajů tyto informace:

a) totožnost a kontaktní údaje správce a jeho případného zástupce;

b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů;

c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;

d) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);

e) případné příjemce nebo kategorie příjemců osobních údajů;

f) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.

2. Vedle informací uvedených v odstavci 1 poskytne správce subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování:

a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

b) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

c) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;

d) existence práva podat stížnost u dozorového úřadu;

e) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;

f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

3. Pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace uvedené v odstavci 2.

4. Odstavce 1, 2 a 3 se nepoužijí, pokud subjekt údajů již uvedené informace má, a do té míry, v níž je má.

Článek 14

Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů

1. Jestliže osobní údaje nebyly získány od subjektu údajů, poskytne správce subjektu údajů tyto informace:

a) totožnost a kontaktní údaje správce a případně jeho zástupce;

b) případně kontaktní údaje případného pověřence pro ochranu osobních údajů;

c) účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;

d) kategorie dotčených osobních údajů;

e) případné příjemce nebo kategorie příjemců osobních údajů;

f) případný záměr správce předat osobní údaje příjemci ve třetí zemi nebo mezinárodní organizaci a existence či neexistence rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo v čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.

2. Kromě informací uvedených v odstavci 1 poskytne správce subjektu údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování ve vztahu k subjektu údajů:

a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;

b) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);

c) existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz anebo omezení zpracování a práva vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;

d) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;

e) existence práva podat stížnost u dozorového úřadu;

f) zdroj, ze kterého osobní údaje pocházejí, a případně informace o tom, zda údaje pocházejí z veřejně dostupných zdrojů;

g) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

3. Správce poskytne informace uvedené v odstavcích 1 a 2:

a) v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;

b) nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace; nebo

c) nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

4. Pokud správce hodlá osobní údaje dále zpracovat pro jiný účel, než pro který byly získány, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace uvedené v odstavci 2.

5. Odstavce 1 a 4 se nepoužijí, pokud a do té míry, v níž:

a) subjekt údajů již uvedené informace má;

b) se ukáže, že poskytnutí takových informací není možné nebo by vyžadovalo nepřiměřené úsilí; to platí zejména v případě zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely s výhradou podmínek a záruk uvedených v čl. 89 odst. 1, nebo pokud je pravděpodobné, že uplatnění povinnosti uvedené v odstavci 1 tohoto článku by znemožnilo nebo výrazně ztížilo dosažení cílů uvedeného zpracování. V takových případech přijme správce vhodná opatření na ochranu práv, svobod a oprávněných zájmů subjektu údajů, včetně zpřístupnění daných informací veřejnosti;

c) je získávání nebo zpřístupnění výslovně stanoveno právem Unie nebo členského státu, které se na správce vztahuje a v němž jsou stanovena vhodná opatření na ochranu oprávněných zájmů subjektu údajů; nebo

d) osobní údaje musí zůstat důvěrné s ohledem na povinnost zachovávat služební tajemství upravenou právem Unie nebo členského státu, včetně zákonné povinnosti mlčenlivosti.

Článek 15

Právo subjektu údajů na přístup k osobním údajům

1. Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:

a) účely zpracování;

b) kategorie dotčených osobních údajů;

c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;

d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;

e) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování a nebo vznést námitku proti tomuto zpracování;

f) právo podat stížnost u dozorového úřadu;

g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;

h) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

2. Pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách podle článku 46, které se vztahují na předání.

3. Správce poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

4. Právem získat kopii uvedenou v odstavci 3 nesmějí být nepříznivě dotčena práva a svobody jiných osob.

Oddíl 3

Oprava a výmaz

Článek 16

Právo na opravu

Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

Článek 17

Právo na výmaz („právo být zapomenut“)

1. Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:

a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;

b) subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování;

c) subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 1 a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 2;

d) osobní údaje byly zpracovány protiprávně;

e) osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje;

f) osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1.

2. Jestliže správce osobní údaje zveřejnil a je povinen je podle odstavce 1 vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně technických opatření, aby informoval správce, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby vymazali veškeré odkazy na tyto osobní údaje, jejich kopie či replikace.

3. Odstavce 1 a 2 se neuplatní, pokud je zpracování nezbytné:

a) pro výkon práva na svobodu projevu a informace;

b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;

c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3;

d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely v souladu s čl. 89 odst. 1, pokud je pravděpodobné, že by právo uvedené v odstavci 1 znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování;

e) pro určení, výkon nebo obhajobu právních nároků.

Článek 18

Právo na omezení zpracování

1. Subjekt údajů má právo na to, aby správce omezil zpracování, v kterémkoli z těchto případů:

a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;

b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;

c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;

d) subjekt údajů vznesl námitku proti zpracování podle čl. 21 odst. 1, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

2. Pokud bylo zpracování omezeno podle odstavce 1, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Unie nebo některého členského státu.

3. Subjekt údajů, který dosáhl omezení zpracování podle odstavce 1, je správcem předem upozorněn na to, že bude omezení zpracování zrušeno.

Článek 19

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

Správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování provedené v souladu s článkem 16, čl. 17 odst. 1 a článkem 18, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.

Článek 20

Právo na přenositelnost údajů

1. Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že:

a) zpracování je založeno na souhlasu podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) nebo na smlouvě podle čl. 6 odst. 1 písm. b); a

b) zpracování se provádí automatizovaně.

2. Při výkonu svého práva na přenositelnost údajů podle odstavce 1 má subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.

3. Výkonem práva uvedeného v odstavci 1 tohoto článku není dotčen článek 17. Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.

4. Právem uvedeným v odstavci 1 nesmí být nepříznivě dotčena práva a svobody jiných osob.

Oddíl 4

Právo vznést námitku a automatizované individuální rozhodování

Článek 21

Právo vznést námitku

1. Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají, na základě čl. 6 odst. 1 písm. e) nebo f), včetně profilování založeného na těchto ustanoveních. Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

2. Pokud se osobní údaje zpracovávají pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů, které se ho týkají, pro tento marketing, což zahrnuje i profilování, pokud se týká tohoto přímého marketingu.

3. Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány.

4. Subjekt údajů je na právo uvedené v odstavcích 1 a 2 výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.

5. V souvislosti s využíváním služeb informační společnosti, a aniž je dotčena směrnice 2002/58/ES, může subjekt údajů uplatnit své právo vznést námitku automatizovanými prostředky pomocí technických specifikací.

6. Jsou-li osobní údaje zpracovávány pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, má subjekt údajů, z důvodů týkajících se jeho konkrétní situace, právo vznést námitku proti zpracování osobních údajů, které se ho týkají, ledaže je zpracování nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu.

Článek 22

Automatizované individuální rozhodování, včetně profilování

1. Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.

2. Odstavec 1 se nepoužije, pokud je rozhodnutí:

a) nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů;

b) povoleno právem Unie nebo členského státu, které se na správce vztahuje a které rovněž stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů; nebo

c) založeno na výslovném souhlasu subjektu údajů.

3. V případech uvedených v odst. 2 písm. a) a c) provede správce údajů vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí.

4. Rozhodnutí uvedená v odstavci 2 se neopírají o zvláštní kategorie osobních údajů uvedené v čl. 9 odst. 1, pokud se neuplatní čl. 9 odst. 2 písm. a) nebo g) a nejsou zavedena vhodná opatření pro zajištění práv a svobod a oprávněných zájmů subjektu údajů.

Oddíl 5

Omezení

Článek 23

Omezení

1. Právo Unie nebo členského státu, které se na správce nebo zpracovatele vztahuje, může prostřednictvím legislativního opatření omezit rozsah povinností a práv uvedených v článcích 12 až 22 a v článku 34, jakož i v článku 5, v rozsahu, v jakém ustanovení tohoto článku odpovídají právům a povinnostem stanoveným v článcích 12 až 22, jestliže takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti s cílem zajistit:

a) národní bezpečnost;

b) obranu;

c) veřejnou bezpečnost;

d) prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;

e) jiné důležité cíle obecného veřejného zájmu Unie nebo členského státu, zejména důležitý hospodářský nebo finanční zájem Unie nebo členského státu, včetně peněžních, rozpočtových a daňových záležitostí, veřejného zdraví a sociálního zabezpečení;

f) ochranu nezávislosti soudnictví a soudních řízení;

g) prevenci, vyšetřování, odhalování a stíhání porušování etických pravidel regulovaných povolání;

h) monitorovací, inspekční nebo regulační funkci spojenou, i pouze příležitostně, s výkonem veřejné moci v případech uvedených v písmenech a) až e) a g);

i) ochranu subjektu údajů nebo práv a svobod druhých;

j) vymáhání občanskoprávních nároků.

2. Každé legislativní opatření uvedené v odstavci 1 zejména obsahuje konkrétní ustanovení, alespoň, je-li to relevantní, pokud jde o:

a) účely zpracování nebo kategorie zpracování;

b) kategorie osobních údajů;

c) rozsah zavedených omezení;

d) záruky proti zneužití údajů nebo protiprávnímu přístupu k nim či jejich protiprávnímu předání;

e) specifikaci správců nebo kategorie správců;

f) doby uložení a platné záruky s ohledem na povahu, rozsah a účely zpracování nebo kategorie zpracování;

g) rizika z hlediska práv a svobod subjektů údajů; a

h) právo subjektů údajů být informováni o daném omezení, pokud toto informování nemůže být na újmu účelu omezení.

KAPITOLA IV

Správce a zpracovatel

Oddíl 1

Obecné povinnosti

Článek 24

Odpovědnost správce

1. S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.

2. Pokud je to s ohledem na činnosti zpracování přiměřené, zahrnují opatření uvedená v odstavci 1 uplatňování vhodných koncepcí v oblasti ochrany údajů správcem.

3. Jedním z prvků, jimiž lze doložit, že správce plní příslušné povinnosti, je dodržování schválených kodexů chování uvedených v článku 40 nebo schválených mechanismů pro vydávání osvědčení uvedených v článku 42.

Článek 25

Záměrná a standardní ochrana osobních údajů

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů.

2. Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

3. Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavcích 1 a 2 tohoto článku, je schválený mechanismus pro vydávání osvědčení podle článku 42.

Článek 26

Společní správci

1. Pokud účely a prostředky zpracování stanoví společně dva nebo více správců, jsou společnými správci. Společní správci mezi sebou transparentním ujednáním vymezí své podíly na odpovědnosti za plnění povinností podle tohoto nařízení, zejména pokud jde o výkon práv subjektu údajů, a své povinnosti poskytovat informace uvedené v článcích 13 a 14, pokud tuto odpovědnost správců nestanoví právo Unie nebo členského státu, které se na správce vztahuje. V ujednání může být určeno kontaktní místo pro subjekty údajů.

2. Ujednání uvedené v odstavci 1 náležitě zohlední úlohy společných správců a jejich vztahy vůči subjektům údajů. Subjekt údajů musí být o podstatných prvcích ujednání informován.

3. Bez ohledu na podmínky ujednání uvedeného v odstavci 1 může subjekt údajů vykonávat svá práva podle tohoto nařízení u každého ze správců i vůči každému z nich.

Článek 27

Zástupci správců nebo zpracovatelů, kteří nejsou usazeni v Unii

1. Pokud se použije čl. 3 odst. 2, správce nebo zpracovatel písemně jmenuje svého zástupce v Unii.

2. Povinnost uvedená v odstavci 1 tohoto článku se nevztahuje na:

a) zpracování, které je příležitostné, nezahrnuje, ve velkém měřítku, zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10, a u něhož je nepravděpodobné, že by s ohledem na svou povahu, kontext, rozsah a účely představovalo riziko pro práva a svobody fyzických osob; nebo

b) orgán veřejné moci nebo veřejný subjekt.

3. Zástupce je usazen v jednom z členských států, ve kterém se vyskytují subjekty údajů, jejichž osobní údaje jsou zpracovávány v souvislosti s nabízeným zbožím či službami, nebo jejichž chování je monitorováno.

4. Zástupce je správcem nebo zpracovatelem zmocněn v tom smyslu, že se na něj vedle správce nebo zpracovatele nebo místo nich mohou obracet zejména dozorové úřady a subjekty údajů ohledně všech otázek souvisejících se zpracováním za účelem zajištění souladu s tímto nařízením.

5. Tím, že správce nebo zpracovatel jmenuje svého zástupce, nejsou dotčeny právní kroky, které by mohly být zahájeny proti správci nebo zpracovateli samotnému.

Článek 28

Zpracovatel

1. Pokud má být zpracování provedeno pro správce, využije správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.

2. Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky.

3. Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:

a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;

b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

c) přijme všechna opatření požadovaná podle článku 32;

d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4;

e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;

f) je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;

g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;

h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.

Pokud jde o první pododstavec písm. h), informuje zpracovatel neprodleně správce v případě, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy Unie nebo členského státu týkající se ochrany údajů.

4. Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle odstavce 3, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto nařízení. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel.

5. Jedním z prvků, jimiž lze doložit dostatečné záruky podle odstavců 1 a 4 tohoto článku, je skutečnost, že zpracovatel dodržuje schválený kodex chování uvedených v článku 40 nebo schválený mechanismus pro vydávání osvědčení uvedený v článku 42.

6. Aniž jsou dotčeny individuální smlouvy mezi správcem a zpracovatelem, mohou být smlouvy nebo jiné právní akty podle odstavců 3 a 4 tohoto článku založeny zcela nebo částečně na standardních smluvních doložkách podle odstavců 7 a 8 tohoto článku, mimo jiné i v případě, že jsou součástí osvědčení uděleného správci či zpracovateli podle článků 42 a 43.

7. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky stanovit Komise přezkumným postupem podle čl. 93 odst. 2.

8. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky přijmout dozorový úřad v souladu s mechanismem jednotnosti uvedeným v článku 63.

9. Smlouva nebo jiný právní akt podle odstavců 3 a 4 musí být vyhotoveny písemně, v to počítaje i elektronickou formu.

10. Aniž jsou dotčeny články 82, 83 a 84, pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce.

Článek 29

Zpracování z pověření správce nebo zpracovatele

Zpracovatel a jakákoliv osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, může tyto osobní údaje zpracovávat pouze na pokyn správce, ledaže jí jejich zpracování ukládá právo Unie nebo členského státu.

Článek 30

Záznamy o činnostech zpracování

1. Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto informace:

a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;

b) účely zpracování;

c) popis kategorií subjektů údajů a kategorií osobních údajů;

d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;

e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;

f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;

g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.

2. Každý zpracovatel a jeho případný zástupce vede záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují:

a) jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů;

b) kategorie zpracování prováděného pro každého ze správců;

c) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;

d) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.

3. Záznamy podle odstavců 1 a 2 se vyhotovují písemně, v to počítaje i elektronickou formu.

4. Správce, zpracovatel nebo případný zástupce správce nebo zpracovatele poskytne záznamy na požádání dozorového úřadu.

5. Povinnosti uvedené v odstavcích 1 a 2 se nepoužijí pro podnik nebo organizaci zaměstnávající méně než 250 osob, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.

Článek 31

Spolupráce s dozorovým úřadem

Správce a zpracovatel a případný zástupce správce nebo zpracovatele spolupracují na požádání s dozorovým úřadem při plnění jeho úkolů.

Oddíl 2

Zabezpečení osobních údajů

Článek 32

Zabezpečení zpracování

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování osobních údajů;

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

3. Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je dodržování schváleného kodexu chování uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42.

4. Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

Článek 33

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1. Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.

2. Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

3. Ohlášení podle odstavce 1 musí přinejmenším obsahovat:

a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;

c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;

d) popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

4. Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

5. Správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto článkem.

Článek 34

Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

1. Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů.

2. V oznámení určeném subjektu údajů podle odstavce 1 tohoto článku se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a opatření uvedené v čl. 33 odst. 3 písm. b), c) a d).

3. Oznámení subjektu údajů uvedené v odstavci 1 se nevyžaduje, je-li splněna kterákoli z těchto podmínek:

a) správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;

b) správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví;

c) vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

4. Jestliže správce dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek vysoké riziko, požadovat, aby tak učinil, nebo může rozhodnout, že je splněna některá z podmínek uvedených v odstavci 3.

Oddíl 3

Posouzení vlivu na ochranu osobních údajů a předchozí konzultace

Článek 35

Posouzení vlivu na ochranu osobních údajů

1. Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

2. Při provádění posouzení vlivu na ochranu osobních údajů si správce vyžádá posudek pověřence pro ochranu osobních údajů, byl-li jmenován.

3. Posouzení vlivu na ochranu osobních údajů podle odstavce 1 je nutné zejména v těchto případech:

a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;

b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

4. Dozorový úřad sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů podle odstavce 1. Dozorový úřad uvedené seznamy předá sboru.

5. Dozorový úřad může rovněž sestavit a zveřejnit seznam druhů operací zpracování, u nichž není posouzení vlivu na ochranu osobních údajů nutné. Dozorový úřad uvedené seznamy předá sboru.

6. Před přijetím seznamů podle odstavců 4 a 5 použije příslušný dozorový úřad mechanismus jednotnosti uvedený v článku 63, pokud tyto seznamy zahrnují činnosti zpracování související s nabídkou zboží či služeb subjektům údajů nebo s monitorováním jejich chování v několika členských státech, nebo jestliže dané seznamy mohou výrazně ovlivnit volný pohyb osobních údajů v rámci Unie.

7. Posouzení obsahuje alespoň:

a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;

b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;

c) posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci 1; a

d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

8. Dodržování schválených kodexů chování podle článku 40 příslušnými správci nebo zpracovateli se řádně zohlední při posuzování dopadu operací zpracování prováděných těmito správci či zpracovateli, zejména pro účely posouzení vlivu na ochranu osobních údajů.

9. Správce ve vhodných případech získá k zamýšlenému zpracování stanovisko subjektů údajů nebo jejich zástupců, aniž by byla dotčena ochrana obchodních či veřejných zájmů nebo bezpečnost operací zpracování.

10. Pokud má zpracování podle čl. 6 odst. 1 písm. c) nebo e) právní základ v právu Unie nebo členského státu, které se na správce vztahuje, a toto právo upravuje konkrétní operaci nebo soubor operací zpracování a pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu, odstavce 1 až 7 se nepoužijí, ledaže by členské státy považovaly provedení tohoto posouzení před činnostmi zpracování za nezbytné.

11. Správce případně provede přezkum s cílem posoudit, zda je zpracování prováděno v souladu s posouzením vlivu na ochranu osobních údajů alespoň v případech, kdy dojde ke změně rizika, jež představují operace zpracování.

Článek 36

Předchozí konzultace

1. Správce konzultuje před zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů podle článku 35 vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.

2. Pokud se dozorový úřad domnívá, že by zamýšlené zpracování uvedené v odstavci 1 porušilo toto nařízení, zejména pokud správce nedostatečně určil či zmírnil riziko, upozorní na to správce a případně zpracovatele údajů písemně ve lhůtě nejvýše osmi týdnů od obdržení žádosti o konzultaci a může uplatnit kteroukoli ze svých pravomocí uvedených v článku 58. Tato lhůta může být s ohledem na složitost zamýšleného zpracování prodloužena o šest týdnů. Dozorový úřad informuje správce a případně zpracovatele o každém takovém prodloužení a o jeho důvodech do jednoho měsíce od obdržení žádosti o konzultaci. Tyto lhůty mohou být pozastaveny, dokud dozorový úřad neobdrží veškeré informace, o které požádal pro účely konzultace.

3. Při konzultaci s dozorovým úřadem podle odstavce 1 mu správce poskytne informace o těchto aspektech:

a) ve vhodných případech rozdělení odpovědnosti správce, společných správců a zpracovatelů zapojených do zpracování, zejména v případě zpracování v rámci skupiny podniků;

b) účely a způsoby zamýšleného zpracování;

c) opatření a záruky poskytnuté za účelem ochrany práv a svobod subjektů údajů podle tohoto nařízení;

d) kontaktní údaje případného pověřence pro ochranu osobních údajů;

e) posouzení vlivu na ochranu osobních údajů podle článku 35 a

f) veškeré další informace, o které dozorový úřad požádá.

4. Členské státy konzultují s dozorovým úřadem během přípravy návrhu legislativního opatření, které má přijmout vnitrostátní parlament, nebo návrhu regulačního opatření založeného na takovém legislativním opatření, jež souvisí se zpracováním.

5. Bez ohledu na odstavec 1 může právo členského státu od správců vyžadovat, aby konzultovali s dozorovým úřadem a získali od něj předchozí povolení, pokud jde o zpracování správcem za účelem vykonání úkolu ve veřejném zájmu, včetně zpracování v souvislosti se sociální ochranou a veřejným zdravím.

Oddíl 4

Pověřenec pro ochranu osobních údajů

Článek 37

Jmenování pověřence pro ochranu osobních údajů

1. Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:

a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;

b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo

c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.

2. Skupina podniků může jmenovat jediného pověřence pro ochranu osobních údajů, pokud je snadno dosažitelný z každého podniku.

3. Je-li správce nebo zpracovatel orgánem veřejné moci či veřejným subjektem, může být s přihlédnutím k jejich organizační struktuře a velikosti jmenován jediný pověřenec pro ochranu osobních údajů pro několik takových orgánů nebo subjektů.

4. V jiných případech, než jaké jsou uvedeny v odstavci 1, mohou nebo, vyžaduje-li to právo Unie nebo členského státu, musí pověřence pro ochranu osobních údajů jmenovat správce nebo zpracovatel nebo sdružení a jiné subjekty zastupující kategorie správců či zpracovatelů. Pověřenec pro ochranu osobních údajů může jednat ve prospěch takovýchto sdružení a jiných subjektů zastupujících správce nebo zpracovatele.

5. Pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů a své schopnosti plnit úkoly stanovené v článku 39.

6. Pověřenec pro ochranu osobních údajů může být pracovníkem správce či zpracovatele, nebo může úkoly plnit na základě smlouvy o poskytování služeb.

7. Správce nebo zpracovatel zveřejní kontaktní údaje pověřence pro ochranu osobních údajů a sdělí je dozorovému úřadu.

Článek 38

Postavení pověřence pro ochranu osobních údajů

1. Správce a zpracovatel zajistí, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů.

2. Správce a zpracovatel podporují pověřence pro ochranu osobních údajů při plnění úkolů uvedených v článku 39 tím, že mu poskytují zdroje nezbytné k plnění těchto úkolů, k přístupu k osobním údajům a operacím zpracování a k udržování jeho odborných znalostí.

3. Správce a zpracovatel zajistí, aby pověřenec pro ochranu osobních údajů nedostával žádné pokyny týkající se výkonu těchto úkolů. V souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován. Pověřenec pro ochranu osobních údajů je přímo podřízen vrcholovým řídícím pracovníkům správce nebo zpracovatele.

4. Subjekty údajů se mohou obracet na pověřence pro ochranu osobních údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle tohoto nařízení.

5. Pověřenec pro ochranu osobních údajů je v souvislosti s výkonem svých úkolů vázán tajemstvím nebo důvěrností, v souladu s právem Unie nebo členského státu.

6. Pověřenec pro ochranu osobních údajů může plnit i jiné úkoly a povinnosti. Správce nebo zpracovatel zajistí, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.

Článek 39

Úkoly pověřence pro ochranu osobních údajů

1. Pověřenec pro ochranu osobních údajů vykonává alespoň tyto úkoly:

a) poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;

b) monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;

c) poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35;

d) spolupráce s dozorovým úřadem a

e) působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci.

2. Pověřenec pro ochranu osobních údajů bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.

Oddíl 5

Kodexy chování a vydávání osvědčení

Článek 40

Kodexy chování

1. Členské státy, dozorové úřady, sbor a Komise podporují vypracování kodexů chování, které mají přispět k řádnému uplatňování tohoto nařízení s ohledem na konkrétní povahu různých odvětví provádějících zpracování a na konkrétní potřeby mikropodniků a malých a středních podniků.

2. Sdružení nebo jiné subjekty zastupující různé kategorie správců nebo zpracovatelů mohou vypracovávat kodexy chování nebo tyto kodexy upravovat či rozšiřovat, a to s cílem upřesnit uplatňování ustanovení tohoto nařízení, mimo jiné pokud jde o:

a) spravedlivé a transparentní zpracování;

b) oprávněné zájmy, jež správci v konkrétních situacích sledují;

c) shromažďování osobních údajů;

d) pseudonymizaci osobních údajů;

e) informace poskytované veřejnosti a subjektů údajů;

f) výkon práv subjektů údajů;

g) informace poskytované dětem a jejich ochranu a způsob získávání souhlasu nositele rodičovské zodpovědnosti nad dítětem;

h) opatření a postupy uvedené v článcích 24 a 25 a opatření k zajištění bezpečnosti zpracování podle článku 32;

i) ohlašování případů porušení zabezpečení osobních údajů dozorovým úřadům a oznamování těchto případů porušení subjektům údajů;

j) předávání osobních údajů do třetích zemí nebo mezinárodním organizacím; nebo

k) mimosoudní vyrovnání a jiné postupy pro řešení sporů mezi správci a subjekty údajů v souvislosti se zpracováním, aniž by byla dotčena práva subjektů údajů podle článků 77 a 79.

3. Vedle správců a zpracovatelů, na něž se vztahuje toto nařízení vztahuje, mohou kodexy chování schválené podle odstavce 5 tohoto článku a mající všeobecnou platnost podle odstavce 9 tohoto článku dodržovat i správci nebo zpracovatelé, na něž se podle článku 3 toto nařízení nevztahuje, s cílem poskytnout vhodné záruky v rámci předání osobních údajů do třetích zemí nebo mezinárodním organizacím za podmínek uvedených v čl. 46 odst. 2 písm. e). Za účelem uplatňování těchto vhodných záruk, a to i pokud jde o práva subjektů údajů, přijmou tito správci nebo zpracovatelé prostřednictvím smluvních nástrojů nebo jiných právně závazných nástrojů závazné a vymahatelné závazky.

4. Kodex chování uvedený v odstavci 2 tohoto článku obsahuje mechanismy, které umožňují subjektu uvedenému v čl. 41 odst. 1 provádět povinné monitorování dodržování jeho ustanovení správci nebo zpracovateli, kteří se zavázali jej dodržovat, aniž tím jsou dotčeny úkoly a pravomoci dozorových úřadů, které jsou příslušné podle článku 55 nebo 56.

5. Sdružení nebo jiné subjekty uvedené v odstavci 2 tohoto článku, které mají v úmyslu vypracovat kodex chování nebo upravit či rozšířit existující kodex, předloží návrh kodexu či návrhy na úpravu či rozšíření kodexu dozorového úřadu, který je příslušný podle článku 55. Dozorový úřad vydá stanovisko k tomu, zda je daný návrh kodexu nebo návrh na úpravu či rozšíření kodexu v souladu s tímto nařízením, a pokud shledá, že tento návrh nebo návrh na úpravu ný či rozšíření kodexu poskytuje dostatečné vhodné záruky, schválí jej.

6. Je-li kodex chování nebo návrh na úpravu či rozšíření kodexu schválen v souladu s odstavcem 5 a jestliže se kodex chování nevztahuje na činnosti zpracování v několika členských státech, dozorový úřad daný kodex zaregistruje a zveřejní.

7. Pokud se návrh kodexu chování týká činností zpracování v několika členských státech, předloží dozorový úřad příslušný podle článku 55 návrh kodexu nebo návrh na úpravu či rozšíření kodexu před jeho schválením v rámci postupu podle článku 63 sboru a ten vydá stanovisko k tomu, zda je návrh kodexu nebo návrh na úpravu či rozšíření kodexu v souladu s tímto nařízením nebo zda v situaci uvedené v odstavci 3 tohoto článku poskytuje vhodné záruky.

8. Pokud se ve stanovisku uvedeném v odstavci 7 potvrdí, že kodex chování nebo návrh na úpravu či rozšíření kodexu je v souladu s tímto nařízením nebo že v situaci uvedené v odstavci 3 poskytují vhodné záruky, předloží sbor své stanovisko Komisi.

9. Komise může prostřednictvím prováděcích aktů rozhodnout, že schválený kodex chování, jeho úprava či rozšíření, které jí byly předloženy podle odstavce 8 tohoto článku, mají všeobecnou platnost v rámci Unie. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 93 odst. 2.

10. Komise zajistí odpovídající zveřejnění schválených kodexů, o nichž bylo v souladu s odstavcem 9 rozhodnuto, že mají všeobecnou platnost.

11. Sbor všechny schválené kodexy chování a jejich úpravy či rozšíření shromáždí v registru a vhodným způsobem je zpřístupní veřejnosti.

Článek 41

Monitorování schválených kodexů chování

1. Aniž jsou dotčeny úkoly a pravomoci příslušného dozorového úřadu podle článků 57 a 58, může monitorování souladu s kodexem chování podle článku 40 provádět subjekt, který má ohledně předmětu kodexu příslušnou úroveň odborných znalostí a je pro tento účel akreditován příslušným dozorovým úřadem.

2. Subjekt uvedený v odstavci 1 může být akreditován pro monitorování souladu s kodexem chování, pokud tento subjekt:

a) prokázal ke spokojenosti příslušného dozorového úřadu svoji nezávislost a odborné znalosti ohledně předmětu kodexu;

b) stanovil postupy, které mu umožňují posoudit způsobilost dotčených správců a zpracovatelů, pokud jde o uplatňování kodexu, monitorovat, zda jeho ustanovení dodržují, a pravidelně přezkoumávat jeho fungování;

c) stanovil postupy a struktury pro řešení stížností na porušování kodexu nebo na způsob, jak správce nebo zpracovatel kodex uplatňoval nebo uplatňuje, a učinil tyto postupy a struktury pro subjekty údajů a pro veřejnost transparentními; a

d) ke spokojenosti příslušného dozorového úřadu prokázal, že jeho úkoly a povinnosti nevedou ke střetu zájmů.

3. Příslušný dozorový úřad předloží návrh kritérií pro akreditaci subjektu uvedeného v odstavci 1 tohoto článku sboru podle mechanismu jednotnosti uvedeného v článku 63.

4. Aniž jsou dotčeny úkoly a pravomoci příslušného dozorového úřadu a aniž je dotčena kapitola VIII, přijme subjekt uvedený v odstavci 1 tohoto článku s výhradou vhodných záruk v případech porušování kodexu správcem nebo zpracovatelem vhodná opatření, včetně pozastavení účasti daného správce nebo zpracovatele na kodexu nebo jeho vyloučení z této účasti. O těchto opatřeních a důvodech jejich přijetí informuje příslušný dozorový úřad.

5. Příslušný dozorový úřad zruší akreditaci subjektu uvedeného v odstavci 1, jestliže nejsou nebo již přestaly být dodržovány podmínky akreditace nebo jestliže je činnosti tohoto subjektu v rozporu s tímto nařízením.

6. Tento článek se netýká zpracování prováděného orgány veřejné moci a veřejnými subjekty.

Článek 42

Vydávání osvědčení

1. Členské státy, dozorové úřady, sbor a Komise podpoří, zejména na úrovni Unie, zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s tímto nařízením v případě operací zpracování prováděných správci a zpracovateli. Zohlední se specifické potřeby mikropodniků a malých a středních podniků.

2. Vedle dodržování správci a zpracovateli, na něž se vztahuje toto nařízení, mohou být mechanismy pro vydávání osvědčení o ochraně údajů a příslušné pečetě či známky schválené podle odstavce 5 tohoto článku zavedeny rovněž za účelem prokázání existence vhodných záruk poskytnutých správci nebo zpracovateli, na něž se podle článku 3 toto nařízení nevztahuje, v rámci předávání osobních údajů do třetích zemí nebo mezinárodním organizacím za podmínek uvedených v čl. 46 odst. 2 písm. f). Za účelem uplatňování těchto vhodných záruk, a to i pokud jde o práva subjektů údajů, přijmou tito správci nebo zpracovatelé prostřednictvím smluvních nebo jiných právně závazných nástrojů závazné a vymahatelné závazky.

3. Vydávání osvědčení je dobrovolné a dostupné prostřednictvím postupu, který je transparentní.

4. Osvědčením podle tohoto článku se nesnižuje odpovědnost správce nebo zpracovatele za soulad s tímto nařízením a nejsou jím dotčeny úkoly a pravomoci dozorových úřadů, které jsou příslušné podle článku 55 nebo 56.

5. Osvědčení podle tohoto článku vydávají subjekty pro vydávání osvědčení uvedené v článku 43 nebo příslušný dozorový úřad na základě kritérií jím schválených podle čl. 58 odst. 3 nebo schválených sborem podle článku 63. Jsou-li kritéria schválena sborem, může to vést k vydání společného osvědčení, evropské pečeti ochrany údajů.

6 Správce nebo zpracovatel, který předloží své zpracování mechanismu pro vydávání osvědčení, poskytne subjektu pro vydávání osvědčení uvedenému v článku 43 nebo případně příslušnému dozorovému úřadu veškeré informace a přístup ke svým činnostem zpracování, které jsou pro provedení postupu vydávání osvědčení nezbytné.

7. Osvědčení se vydává správci nebo zpracovateli na dobu nejvýše tří let a lze je obnovit za stejných podmínek, pokud jsou i nadále plněny příslušné požadavky. Nejsou-li požadavky na osvědčení plněny, nebo pokud již přestaly být plněny, subjekty pro vydávání osvědčení podle článku 43 nebo příslušný dozorový úřad uvedené osvědčení odeberou.

8. Sbor všechny mechanismy pro vydávání osvědčení o ochraně údajů a příslušné pečetě či známky shromáždí v registru a vhodným způsobem je zpřístupní veřejnosti.

Článek 43

Subjekty pro vydávání osvědčení

1. Aniž jsou dotčeny úkoly a pravomoci příslušného dozorového úřadu podle článků 57 a 58, osvědčení vydává a obnovuje subjekt pro vydávání osvědčení, který má příslušnou úroveň odborných znalostí ohledně ochrany údajů, a to poté, co informoval dozorový úřad s cílem umožnit případně výkon jeho pravomocí podle čl. 58 odst. 2 písm. h). Členské státy zajistí, aby byly tyto subjekty pro vydávání osvědčení akreditovány jedním nebo oběma z následujících orgánů:

a) dozorovým úřadem, který je příslušný podle článku 55 nebo 56; nebo

b) vnitrostátním akreditačním orgánem určeným v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008 ([1]), v souladu s normou EN-ISO/IEC 17065/2012 a s dodatečnými požadavky stanovenými dozorovým úřadem, který je příslušný podle článku 55 nebo 56.

2. Subjekt pro vydávání osvědčení uvedený v odstavci 1 je pro tento účel akreditován v souladu s uvedeným odstavcem, pouze pokud:

a) prokázal ke spokojenosti příslušného dozorového úřadu svoji nezávislost a odborné znalosti ohledně předmětu osvědčení;

([1]) Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

b) se zavázal dodržovat kritéria uvedená v čl. 42 odst. 5 a schválená dozorovým úřadem, který je příslušný podle článku 55 nebo 56, nebo sborem podle článku 63;

c) stanovil postupy pro vydávání, pravidelný přezkum a odebírání osvědčení, pečetí a známek dokládajících ochranu údajů;

d) stanovil postupy a struktury pro řešení stížností týkajících se porušování osvědčení nebo způsobu, jak správce nebo zpracovatel osvědčení uplatňoval nebo uplatňuje, a učinil tyto postupy a struktury pro subjekty údajů a pro veřejnost transparentními; a

e) ke spokojenosti příslušného dozorového úřadu doložil, že jeho úkoly a povinnosti nevedou ke střetu zájmů.

3. Akreditace subjektů pro vydávání osvědčení uvedených v odstavcích 1 a 2 tohoto článku probíhá na základě kritérií schválených dozorovým úřadem, který je příslušný podle článku 55 nebo 56, nebo sborem podle článku 63. V případě akreditace podle odst. 1 písm. c) tohoto článku tyto požadavky doplňují požadavky stanovené v nařízení (ES) č. 765/2008 a technická pravidla, která popisují metody a postupy subjektů pro vydávání osvědčení.

4. Subjekty pro vydávání osvědčení uvedené v odstavci 1 jsou odpovědné za řádné posouzení vedoucí k vydání osvědčení nebo k jeho odebrání, aniž je dotčena odpovědnost správce nebo zpracovatele za soulad s tímto nařízením. Akreditace se vydává na období nejvýše pěti let a lze ji obnovit za stejných podmínek, pokud daný subjekt pro vydávání osvědčení splňuje příslušné požadavky stanovené tímto článkem.

5. Subjekty pro vydávání osvědčení uvedené v odstavci 1 sdělí příslušným dozorovým úřadům důvody pro vydání nebo odebrání požadovaného osvědčení.

6. Požadavky podle odstavce 3 tohoto článku a kritéria podle čl. 42 odst. 5 zveřejní dozorový úřad ve snadno přístupné formě. Dozorové úřady je předají také sboru. Sbor všechny mechanismy pro vydávání osvědčení a pečetě dokládající ochranu údajů shromáždí v registru a vhodným způsobem je zpřístupní veřejnosti.

7. Aniž je dotčena kapitola VIII, zruší příslušný dozorový úřad nebo vnitrostátní akreditační orgán akreditaci, kterou udělil subjektu pro vydávání osvědčení podle odstavce 1 tohoto článku, jestliže nejsou nebo již přestaly být dodržovány podmínky akreditace, nebo kroky tohoto subjektu pro vydávání osvědčení porušují toto nařízení.

8. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 92 za účelem upřesnění požadavků, které je třeba zohlednit v souvislosti s mechanismy pro vydávání osvědčení o ochraně údajů podle čl. 42 odst. 1.

9. Komise může přijmout prováděcí akty, kterými stanoví technické normy pro mechanismy vydávání osvědčení a pro pečeti a známky dokládající ochranu údajů a mechanismy pro prosazování a uznávání mechanismů vydávání osvědčení a pečetí a známek dokládajících ochranu údajů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 93 odst. 2.

KAPITOLA V

Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím

Článek 44

Obecná zásada pro předávání

K jakémukoli předání osobních údajů, které jsou předmětem zpracování nebo které jsou určeny ke zpracování po předání do třetí země nebo mezinárodní organizaci, může dojít pouze tehdy, splní-li správce a zpracovatel v závislosti na dalších ustanoveních tohoto nařízení podmínky stanovené v této kapitole, včetně podmínek pro další předávání osobních údajů z dané třetí země nebo mezinárodní organizace do jiné třetí země nebo jiné mezinárodní organizaci. Veškerá ustanovení této kapitoly se použijí s cílem zajistit, aby úroveň ochrany fyzických osob zaručená tímto nařízením nebyla znehodnocena.

Článek 45

Předání založené na rozhodnutí o odpovídající ochraně

1. Předávání osobních údajů do určité třetí země nebo určité mezinárodní organizaci se může uskutečnit, jestliže Komise rozhodla, že tato třetí země, určité území nebo jedno či více konkrétních odvětví v této třetí zemi, nebo tato mezinárodní organizace zajišťují odpovídající úroveň ochrany. Takovéto předání nevyžaduje žádné zvláštní povolení.

2. Při posuzování odpovídající úrovně ochrany vezme Komise v úvahu zejména tyto prvky:

a) právní stát, dodržování lidských práv a základních svobod, příslušné právní předpisy, obecné i odvětvové, včetně těch, které se týkají veřejné bezpečnosti, obrany, národní bezpečnosti a trestního práva a přístupu orgánů veřejné moci k osobním údajům, jakož i provádění těchto právních předpisů, pravidla ochrany údajů, profesní pravidla a související bezpečnostní opatření, včetně pravidel dalšího předávání osobních údajů do další třetí země nebo mezinárodní organizaci, která jsou v dané třetí zemi nebo mezinárodní organizaci dodržována, judikaturu, jakož i existenci účinných a vymahatelných práv subjektu údajů a účinné správní a soudní ochrany pro subjekty údajů, jejichž osobní údaje se předávají;

b) existenci a účinné fungování jednoho nebo více nezávislých dozorových úřadů, které působí v dané třetí zemi nebo kterým podléhá daná mezinárodní organizace, příslušných zajišťovat a vymáhat souladu s pravidly pro ochranu údajů, včetně přiměřených vymáhacích pravomocí, poskytovat pomoc a poradenství subjektům údajů při výkonu jejich práv a spolupracovat s dozorovými úřady členských států, a

c) mezinárodní závazky, které daná třetí země nebo mezinárodní organizace přijala, nebo jiné závazky vyplývající z právně závazných úmluv nebo nástrojů, jakož i z její účasti v mnohostranných či regionálních systémech, zejména pokud jde o ochranu osobních údajů.

3. Komise může po posouzení odpovídající úrovně ochrany prostřednictvím prováděcího aktu rozhodnout, že určitá třetí země, určité území či jedno nebo více konkrétních odvětví v určité třetí zemi nebo určitá mezinárodní organizace zajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku. Uvedený prováděcí akt stanoví mechanismus pro pravidelný přezkum prováděný nejméně každé čtyři roky, který zohlední veškerý relevantní vývoj v dotčené třetí zemi nebo mezinárodní organizaci. Stanoví také svou územní a odvětvovou působnost a případně určí dozorový úřad nebo úřady uvedené v odst. 2 písm. b) tohoto článku. Tento prováděcí akt se přijímá přezkumným postupem podle čl. 93 odst. 2.

4. Komise průběžně sleduje vývoj ve třetích zemích a mezinárodních organizacích, jenž by mohl ovlivnit fungování rozhodnutí přijatých podle odstavce 3 tohoto článku a rozhodnutí přijatých na základě čl. 25 odst. 6 směrnice 95/46/ES.

5. Komise v případě, že to vyplyne z dostupných informací, zejména na základě přezkumu uvedeného v odstavci 3 tohoto článku, rozhodne, že určitá třetí země, určité území nebo konkrétní odvětví v určité třetí zemi nebo určitá mezinárodní organizace již nezajišťuje odpovídající úroveň ochrany ve smyslu odstavce 2 tohoto článku, v nezbytné míře rozhodnutí uvedené v odstavci 3 tohoto článku prováděcími akty bez zpětné působnosti zruší nebo změní anebo pozastaví jeho použitelnost. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 93 odst. 2.

V závažných, naléhavých a řádně odůvodněných případech přijme Komise postupem podle čl. 93 odst. 3 okamžitě použitelné prováděcí akty.

6. Komise zahájí s danou třetí zemí nebo mezinárodní organizací konzultace s cílem napravit stav, který vedl k rozhodnutí podle odstavce 5.

7. Rozhodnutím podle odstavce 5 tohoto článku není dotčeno předávání osobních údajů do dané třetí země, na určité území nebo jednomu nebo více konkrétním odvětvím v dané třetí zemi nebo dané mezinárodní organizaci podle článků 46 až 49.

8. Komise zveřejní v *Úředním věstníku Evropské unie* a na svých internetových stránkách seznam třetích zemí, území a konkrétních odvětví ve třetích zemích a mezinárodních organizací, v nichž podle jejího rozhodnutí odpovídající úroveň ochrany je, nebo naopak již není zajištěna.

9. Rozhodnutí přijatá Komisí na základě čl. 25 odst. 6 směrnice 95/46/ES zůstávají platná až do chvíle, kdy je Komise změní, nahradí nebo zruší rozhodnutím přijatým podle odstavce 3 nebo 5 tohoto článku.

Článek 46

Předávání založené na vhodných zárukách

1. Jestliže neexistuje rozhodnutí podle čl. 45 odst. 3, správce nebo zpracovatel mohou předat osobní údaje do třetí země nebo mezinárodní organizaci, pouze pokud správce nebo zpracovatel poskytl vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů.

2. Vhodné záruky uvedené v odstavci 1 mohou být stanoveny, aniž je zapotřebí jakékoli zvláštní povolení dozorového úřadu, pomocí:

a) právně závazného a vymahatelného nástroje mezi orgány veřejné moci nebo veřejnými subjekty;

b) závazných podnikových pravidel v souladu s článkem 47;

c) standardních doložek o ochraně osobních údajů přijatých Komisí přezkumným postupem podle čl. 93 odst. 2;

d) standardních doložek o ochraně údajů přijatých dozorovým úřadem a schválených Komisí přezkumným postupem podle čl. 93 odst. 2;

e) schváleného kodexu chování podle článku 40 spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů; nebo

f) schváleného mechanismu pro vydání osvědčení podle článku 42 spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to i ohledně práv subjektů údajů.

3. S výhradou povolení od příslušného dozorového úřadu mohou být vhodné záruky uvedené v odstavci 1 rovněž stanoveny zejména pomocí:

a) smluvních doložek mezi správcem nebo zpracovatelem a správcem, zpracovatelem nebo příjemcem osobních údajů ve třetí zemi nebo v mezinárodní organizaci; nebo

b) ustanovení určených k vložení do správních ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektu údajů.

4. Dozorový úřad použije mechanismus jednotnosti v případech uvedených v čl. 63 odst. 3 tohoto článku.

5. Povolení členského státu nebo dozorového úřadu na základě čl. 26 odst. 2 směrnice 95/46/ES zůstávají platná až do chvíle, kdy je dozorový úřad v případě potřeby změní, nahradí nebo zruší. Rozhodnutí přijatá Komisí na základě čl. 26 odst. 4 směrnice 95/46/ES zůstávají platná až do chvíle, kdy je Komise podle potřeby změní, nahradí nebo zruší rozhodnutím přijatým podle odstavce 2 tohoto článku.

Článek 47

Závazná podniková pravidla

1. Příslušný dozorový úřad schvaluje v souladu s mechanismem jednotnosti stanoveným v článku 63 závazná podniková pravidla za předpokladu, že:

a) jsou právně závazná a platná pro všechny a prosazovaná všemi dotčenými členy skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, včetně jejich zaměstnanců;

b) subjektům údajů výslovně přiznávají vymahatelná práva v souvislosti se zpracováním jejich osobních údajů; a

c) splňují požadavky stanovené v odstavci 2.

2. Závazná podniková pravidla uvedená v odstavci 1 vymezují přinejmenším:

a) strukturu a kontaktní údaje skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a každého z jejích členů;

b) předání údajů nebo soubor předání, včetně kategorií osobních údajů, typu zpracování a jeho účelů, typu dotčených subjektů údajů a určení dané třetí země nebo daných třetích zemí;

c) svoji právně závaznou povahu, a to interně i externě;

d) použití obecných zásad pro ochranu údajů, zejména účelové omezení, minimalizaci údajů, omezenou dobu uložení, kvalitu údajů, záměrná a standardní ochranu osobních údajů, právní základ pro zpracování, zpracování zvláštních kategorií osobních údajů; opatření k zajištění zabezpečení údajů a požadavky ohledně dalšího předávání subjektům, které podnikovými pravidly nejsou vázány;

e) práva subjektů údajů v souvislosti se zpracováním jejich osobních údajů a prostředky jejich výkonu, včetně práva nebýt předmětem rozhodnutí založených výhradně na automatizovaném zpracování, včetně profilování v souladu s článkem 22, práva podat stížnost u příslušného dozorového úřadu a příslušných soudů členských států v souladu s článkem 79, právní ochrany a případně i práva na odškodnění v případě porušení závazných podnikových pravidel;

f) přijetí odpovědnosti správcem nebo zpracovatelem usazeným na území některého členského státu za jakékoli porušení závazných podnikových pravidel kterýmkoli dotčeným členem neusazeným v Unii; správce nebo zpracovatel se může této odpovědnosti zcela nebo zčásti zprostit, pouze pokud prokáže, že za okolnost, jež vedla ke vzniku škody, není daný člen odpovědný;

g) způsob poskytování informací o závazných podnikových pravidlech, zejména o ustanoveních uvedených v písmenech d), e) a f) tohoto odstavce, subjektům údajů, vedle informací uvedených v článcích 13 a 14;

h) úkoly všech pověřenců pro ochranu osobních údajů jmenovaných v souladu s článkem 37, nebo jakékoli jiné osoby či subjektu pověřeného monitorováním souladu se závaznými podnikovými pravidly v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a sledování školení a vyřizování stížností;

i) postupy pro vyřizování stížností;

j) mechanismy, které mají v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost zajistit ověřování souladu se závaznými podnikovými pravidly. Tyto mechanismy zahrnují audity ochrany údajů a metody zajištění opravných opatření pro ochranu práv subjektu údajů. Výsledky takového ověření by měly být oznámeny osobě nebo subjektu uvedenému v písmenu h) a radě řídícího podniku skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a na požádání by měly být zpřístupněny příslušnému dozorovému úřadu;

k) mechanismy pro podávání zpráv a pro zaznamenávání změn pravidel a hlášení těchto změn dozorovému úřadu;

l) mechanismus spolupráce s dozorovým úřadem, který zajistí dodržování pravidel každým členem skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost, zejména zpřístupňování výsledků ověřování opatření uvedených v písmenu j) dozorovému úřadu;

m) mechanismy pro podávání zpráv příslušnému dozorovému úřadu o právních požadavcích, kterým je člen skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost podřízen ve třetí zemi a které mohou mít podstatný negativní účinek na záruky poskytované závaznými podnikovými pravidly; a

n) vhodnou odbornou přípravu v oblasti ochrany údajů pro pracovníky, kteří mají k osobním údajům trvalý nebo pravidelný přístup.

3. Komise může u závazných podnikových pravidel ve smyslu tohoto článku určit formát a postupy pro výměnu informací mezi správci, zpracovateli a dozorovými úřady. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 93 odst. 2.

Článek 48

Předání či zveřejnění údajů nepovolená právem Unie

Rozhodnutí soudního orgánu a rozhodnutí správního orgánu třetí země, jež po správci nebo zpracovateli požadují předání nebo zpřístupnění osobních údajů, lze jakýmkoli způsobem uznat nebo vymáhat, pouze pokud vycházejí z mezinárodní dohody, například úmluvy o vzájemné právní pomoci, která je v platnosti mezi žádající třetí zemí a Unií nebo členským státem, aniž jsou dotčeny jiné důvody pro převod podle této kapitoly.

Článek 49

Výjimky pro specifické situace

1. Jestliže neexistuje rozhodnutí o odpovídající ochraně podle čl. 45 odst. 3 ani vhodné záruky podle článku 46, včetně závazných podnikových pravidel, může se předání nebo soubor předání osobních údajů do třetí země nebo mezinárodní organizaci uskutečnit pouze při splnění jedné z následujících podmínek:

a) daný subjekt údajů byl informován o možných rizicích, která pro něj v důsledku absence rozhodnutí o odpovídající ochraně a vhodných záruk vyplývají, a následně k navrhovanému předání vydal svůj výslovný souhlas;

b) předání je nezbytné pro splnění smlouvy mezi subjektem údajů a správcem nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost subjektu údajů;

c) předání je nezbytné pro uzavření nebo splnění smlouvy, která byla uzavřena v zájmu subjektu údajů mezi správcem a jinou fyzickou nebo právnickou osobou;

d) předání je nezbytné z důležitých důvodů veřejného zájmu;

e) předání je nezbytné pro určení, výkon nebo obhajobu právních nároků;

f) předání je nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo jiných osob v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit svůj souhlas;

g) k předání dochází z rejstříku, který je na základě práva Unie nebo členského státu určen pro informování veřejnosti a je přístupný k nahlížení veřejnosti obecně nebo jakékoli osobě, která může prokázat oprávněný zájem, avšak pouze pokud jsou v daném případě splněny podmínky pro nahlížení stanovené právem Unie nebo členského státu.

Jestliže by některé předání nemohlo být založeno na některém z ustanovení článku 45 nebo 46, včetně ustanovení o závazných podnikových pravidlech, a žádná z výjimek pro specifickou situaci uvedených v prvním pododstavci není použitelná, může k předání do třetí země nebo mezinárodní organizaci dojít pouze tehdy, pokud tento převod není opakovaný, týká se pouze omezeného počtu subjektů údajů, je nezbytný pro účely závažných oprávněných zájmů správce, které nejsou převáženy zájmy nebo právy a svobodami subjektu údajů, a pokud správce posoudil všechny okolnosti daného předání údajů a na základě tohoto posouzení poskytl vhodné záruky pro ochranu osobních údajů. Správce o takovém předání informuje dozorový úřad. Správce musí kromě poskytnutí informací uvedených v článcích 13 a 14 subjekt údajů informovat o předání a o závažných legitimních zájmech, které sledoval.

2. Předmětem předání podle odst. 1 prvního pododstavce písm. g) nejsou veškeré osobní údaje nebo veškeré kategorie osobních údajů, které jsou v rejstříku obsaženy. Má-li rejstřík sloužit k nahlížení osobám majícím oprávněný zájem, předání se uskuteční, pouze pokud o to tyto osoby požádají nebo pokud tyto osoby mají být příjemcem.

3. Ustanovení odst. 1 prvního pododstavce písm. a), b) a c) a druhého pododstavce se nevztahují na činnosti prováděné orgány veřejné moci při výkonu jejich úředních pravomocí.

4. Veřejný zájem uvedený v odst. 1 prvním pododstavci písm. d) musí být uznáván právem Unie nebo právem členského státu, které se na správce vztahuje.

5. V případě absence rozhodnutí o odpovídající ochraně může právo Unie nebo členského státu z důležitých důvodů veřejného zájmu výslovně stanovit omezení předání konkrétních kategorií osobních údajů do třetí země nebo mezinárodní organizaci. Členské státy ohlásí taková ustanovení Komisi.

6. Správce nebo zpracovatel zaznamená posouzení i vhodné záruky uvedené v odst. 1 druhém pododstavci tohoto článku v záznamech uvedených v článku 30.

Článek 50

Mezinárodní spolupráce v zájmu ochrany osobních údajů

Ve vztahu k třetím zemím a mezinárodním organizacím podniknou Komise a dozorové úřady vhodné kroky v zájmu:

a) rozvoje mechanismů pro mezinárodní spolupráci, aby se usnadnilo účinné prosazování právních předpisů na ochranu osobních údajů;

b) poskytování vzájemné pomoci na mezinárodní úrovni při prosazování právních předpisů na ochranu osobních údajů, a to i formou oznamování, postupování stížností, pomoci při vyšetřování a výměny informací, pod podmínkou vhodných záruk ochrany osobních údajů a jiných základních práv a svobod;

c) zapojení příslušných zúčastněných stran do diskuse a činností zacílených na prohlubování mezinárodní spolupráce při prosazování právních předpisů na ochranu osobních údajů;

d) podpoření výměny a dokumentace v souvislosti s právními předpisy a praxí v oblasti ochrany osobních údajů, mimo jiné o kompetenčních sporech se třetími zeměmi.

KAPITOLA VI

Nezávislé dozorové úřady

Oddíl 1

Nezávislost postavení

Článek 51

Dozorový úřad

1. Každý členský stát stanoví, že jeden nebo více nezávislých orgánů veřejné moci jsou pověřeny monitorováním uplatňování tohoto nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů a usnadnit volný pohyb osobních údajů uvnitř Unie (dále jen „dozorový úřad“).

2. Každý dozorový úřad přispívá k jednotnému uplatňování tohoto nařízení v celé Unii. Dozorové úřady za tímto účelem spolupracují mezi sebou a s Komisí v souladu s kapitolou VII.

3. Pokud je v některém členském státě zřízen více než jeden dozorový úřad, určí tento členský stát dozorový úřad, jenž má tyto úřady zastupovat ve sboru, a stanoví mechanismus, který zajistí, že budou ostatní dozorové úřady dodržovat pravidla týkající se mechanismu jednotnosti uvedeného v článku 63.

4. Každý členský stát oznámí Komisi do 25. května 2018 právní ustanovení, která přijme podle této kapitoly, a bez zbytečného odkladu jakékoliv následné změny týkající se těchto ustanovení.

Článek 52

Nezávislost

1. Každý dozorový úřad jedná při plnění úkolů a při výkonu svých pravomocí podle tohoto nařízení zcela nezávisle.

2. Člen či členové každého dozorového úřadu musí být při plnění svých úkolů a výkonu svých pravomocí podle tohoto nařízení i nadále nezávislí na vnějším vlivu, přímém či nepřímém, a od nikoho nesmějí vyžadovat ani přijímat pokyny.

3. Člen či členové každého dozorového úřadu se zdrží jakéhokoli jednání neslučitelného s jejich funkcí a během svého funkčního období nesmějí vykonávat žádnou výdělečnou ani nevýdělečnou pracovní činnost neslučitelnou s touto funkcí.

4. Každý členský stát zajistí, aby byl každý dozorový úřad vybaven lidskými, technickými a finančními zdroji, prostorami a infrastrukturou, které bude potřebovat pro účinné plnění svých úkolů a výkon svých pravomocí, včetně úkolů a pravomocí, jež je třeba plnit v rámci vzájemné pomoci, spolupráce a účasti ve sboru.

5. Každý členský stát zajistí, aby každý dozorový úřad vybíral a měl své vlastní zaměstnance, kteří podléhají výlučně řízení členem či členy tohoto dozorového úřadu.

6. Každý členský stát zajistí, aby každý dozorový úřad podléhal finanční kontrole, která neovlivní jeho nezávislost, a aby měl samostatný veřejný roční rozpočet, který může být součástí celkového zemského nebo státního rozpočtu.

Článek 53

Obecné podmínky pro členy dozorového úřadu

1. Členské státy stanoví, že každý člen jejich dozorových úřadů je jmenován transparentním způsobem:

— parlamentem,

— vládou,

— hlavou státu, nebo

— nezávislým subjektem, kterému toto jmenování svěří právo členského státu.

2. Každý člen musí mít kvalifikaci, zkušenosti a dovednosti, zejména v oblasti ochrany osobních údajů, potřebné k plnění svých povinností a výkonu svých pravomocí.

3. Povinnosti člena končí uplynutím jeho funkčního období, odstoupením nebo povinným odchodem do důchodu v souladu s právem daného členského státu.

4. Člena může být odvolán pouze v případě závažného pochybení nebo pokud přestane splňovat podmínky pro plnění svých povinností.

Článek 54

Pravidla pro zřízení dozorového úřadu

1. Každý členský stát upraví právním předpisem všechny tyto záležitosti:

a) zřízení každého dozorového úřadu;

b) kvalifikaci a podmínky způsobilosti požadované pro jmenování členem každého dozorového úřadu;

c) pravidla a postupy pro jmenování člena nebo členů každého dozorového úřadu;

d) délku funkčního období člena či členů každého dozorového úřadu, která činí nejméně čtyři roky, s výjimkou prvního jmenování po 24. květnu 2016, kdy někteří členové mohou být jmenováni na dobu kratší, je-li k ochraně nezávislosti dozorového úřadu nutný proces postupného jmenování;

e) zda a případně na kolik funkčních období mohou být člen či členové každého dozorového úřadu jmenováni opětovně;

f) podmínky, jimiž se řídí povinnosti člena nebo členů a pracovníků každého dozorového úřadu, zákaz jednání a pracovních činností a využívání výhod neslučitelných s těmito podmínkami během funkčního období a po jeho skončení a pravidla, jimiž se řídí ukončení zaměstnání.

2. Člen či členové a pracovníci každého dozorového úřadu jsou, v souladu s právem Unie nebo členského státu, vázáni během funkčního období i po jeho skončení služebním tajemstvím, pokud jde o veškeré důvěrné informace, o nichž se dozvědí během plnění svých úkolů či výkonu svých pravomocí. Během jejich funkčního období se tato povinnost zachovávat služební tajemství vztahuje zejména na ohlášení porušení tohoto nařízení učiněná fyzickými osobami.

Oddíl 2

Příslušnost, úkoly a pravomoci

Článek 55

Příslušnost

1. Každý dozorový úřad je na území svého členského státu příslušný k plnění úkolů a výkonu pravomocí, které mu byly svěřeny v souladu s tímto nařízením.

2. Pokud zpracování provádějí orgány veřejné moci nebo soukromé subjekty jednající na základě čl. 6 odst. 1 písm. c) nebo e), je příslušným dozorový úřad dotčeného členského státu. V takových případech se nepoužije článek 56.

3. Dozorové úřady nejsou příslušné k dozoru nad operacemi zpracování, které provádějí soudy jednající v rámci svých soudních pravomocí.

Článek 56

Příslušnost vedoucího dozorového úřadu

1. Aniž je dotčen článek 55, je dozorový úřad pro hlavní nebo jedinou provozovnu správce či zpracovatele příslušný k tomu, aby jednal jako vedoucí dozorový úřad v případě přeshraničního zpracování prováděného tímto správcem či zpracovatelem v souladu s postupem stanoveným v článku 60.

2. Odchylně od odstavce 1 je každý dozorový úřad příslušný k tomu, aby se zabýval stížnostmi, které u něj byly podány, nebo možným porušením tohoto nařízení, pokud se daná záležitost týká pouze provozovny v jeho členském státě nebo jsou touto záležitostí podstatným způsobem dotčeny subjekty údajů pouze v jeho členském státě.

3. V případech uvedených v odstavci 2 tohoto článku daný dozorový úřad o této záležitosti neprodleně informuje vedoucí dozorový úřad. Ve lhůtě tří týdnů po obdržení těchto informací vedoucí dozorový úřad rozhodne, zda se postupem podle článku 60 bude danou věcí zabývat či nikoli, a zohlední přitom, zda se v členském státě dozorového úřadu, který jej informoval, nachází provozovna správce nebo zpracovatele či nikoli.

4. Pokud vedoucí dozorový úřad rozhodne, že se věcí zabývat bude, použije se postup podle článku 60. Dozorový úřad, který vedoucí dozorový úřad informoval, může vedoucímu dozorovému úřadu předložit návrh rozhodnutí. Vedoucí dozorový úřad tento návrh co nejvíce zohlední při přípravě návrhu rozhodnutí podle čl. 60 odst. 3.

5. Pokud vedoucí dozorový úřad rozhodne, že se věcí zabývat nebude, zabývá se jí v souladu s články 61 a 62 dozorový úřad, který informoval vedoucí dozorový úřad.

6. Provádějí-li správce či zpracovatel přeshraniční zpracování, je pro ně jediným příslušným orgánem vedoucí dozorový úřad.

Článek 57

Úkoly

1. Aniž jsou dotčeny další úkoly stanovené tímto nařízením, každý dozorový úřad na svém území:

a) monitoruje a vymáhá uplatňování tohoto nařízení;

b) zvyšuje povědomí veřejnosti o rizicích, pravidlech, zárukách a právech v souvislosti se zpracováním a podporuje porozumění těmto otázkám. Zvláštní pozornost se přitom věnuje akcím, které jsou určeny speciálně pro děti;

c) v souladu s právem členského státu poskytuje poradenství vnitrostátnímu parlamentu, vládě a dalším orgánům a institucím ohledně legislativních a správních opatření týkajících se ochrany práv a svobod fyzických osob v souvislosti se zpracováním;

d) podporuje povědomí správců a zpracovatelů o jejich povinnostech podle tohoto nařízení;

e) na požádání poskytuje všem subjektům údajů informace ohledně výkonu jejich práv podle tohoto nařízení a, je-li to vhodné, spolupracuje za tímto účelem s dozorovými úřady v jiných členských státech;

f) zabývá se stížnostmi, které mu podá subjekt údajů nebo subjekt, organizace či sdružení v souladu s článkem 80, a ve vhodné míře prošetřuje předmět stížnosti a v přiměřené lhůtě informuje stěžovatele o vývoji a výsledku šetření, zejména v případech, kdy je zapotřebí další šetření nebo koordinace s jiným dozorovým úřadem;

g) s cílem zajistit jednotné uplatňování a prosazování tohoto nařízení spolupracuje s dalšími dozorovými úřady, mimo jiné formou sdílení informací, a s těmito úřady si vzájemně poskytuje pomoc;

h) provádí šetření o uplatňování tohoto nařízení, mimo jiné na základě informací obdržených od jiného dozorového úřadu či jiného orgánu veřejné moci;

i) monitoruje vývoj v relevantních oblastech, pokud má vliv na ochranu osobních údajů, zejména vývoj informačních a komunikačních technologií a obchodních praktik;

j) přijímá standardní smluvní doložky uvedené v čl. 28 odst. 8 a čl. 46 odst. 2 písm. d);

k) připravuje a udržuje seznam v souvislosti s požadavkem provádět posouzení vlivu na ochranu osobních údajů podle čl. 35 odst. 4;

l) poskytuje poradenství o operacích zpracování uvedených v čl. 36 odst. 2;

m) podporuje vypracování kodexů chování podle čl. 40 odst. 1, vydává stanoviska a schvaluje takové kodexy chování, které poskytují dostatečné záruky podle čl. 40 odst. 5;

n) vybízí k zavedení mechanismů pro vydávání osvědčení o ochraně údajů a pečetí a známek dokládajících ochranu údajů podle čl. 42 odst. 1 a schvaluje kritéria pro vydávání osvědčení podle čl. 42 odst. 5;

o) případně provádí pravidelný přezkum osvědčení vydaných v souladu s čl. 42 odst. 7;

p) navrhuje a zveřejňuje kritéria pro schvalování subjektu pro monitorování kodexů chování podle článku 41 a subjektu pro vydávání osvědčení podle článku 43;

q) provádí schvalování subjektu pro monitorování kodexů chování podle článku 41 a subjektu pro vydávání osvědčení podle článku 43;

r) schvaluje smluvní doložky a ustanovení uvedené v čl. 46 odst. 3;

s) schvaluje závazná podniková pravidla podle článku 47;

t) přispívá k činnostem sboru;

u) vede interní záznamy o porušeních tohoto nařízení a o opatřeních přijatých podle čl. 58 odst. 2; a

v) plní veškeré další úkoly související s ochranou osobních údajů.

2. Každý dozorový úřad usnadňuje podávání stížností uvedených v odst. 1 písm. f) takovými opatřeními, jako je poskytnutí formuláře pro podávání stížností, který lze vyplnit i v elektronické formě, aniž jsou vyloučeny jiné komunikační prostředky.

3. Provádění úkolů každého dozorového úřadu je pro subjekty údajů a pro případné pověřence pro ochranu osobních údajů bezplatné.

4. Jestliže jsou požadavky zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může dozorový úřad uložit přiměřený poplatek na základě svých administrativních nákladů nebo odmítnout žádosti vyhovět. Zjevnou nedůvodnost nebo nepřiměřenost žádosti dokládá dozorový úřad.

Článek 58

Pravomoci

1. Každý dozorový úřad má všechny tyto vyšetřovací pravomoci:

a) nařídit správci a zpracovateli, případně zástupci správce nebo zpracovatele, aby mu poskytli veškeré informace, které potřebuje k plnění svých úkolů;

b) provádět vyšetřování formou auditů ochrany údajů;

c) provádět přezkum osvědčení vydaných v souladu s čl. 42 odst. 7;

d) ohlásit správci nebo zpracovateli údajné porušení tohoto nařízení;

e) získat od správce a zpracovatele přístup ke všem osobním údajům a ke všem informacím, které potřebuje k výkonu svých úkolů;

f) získat přístup do všech prostor, v nichž správce a zpracovatel působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů, v souladu s procesním právem Unie nebo členského státu.

2. Každý dozorový úřad má všechny tyto nápravné pravomoci:

a) upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení;

b) udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily toto nařízení;

c) nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení;

d) nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;

e) nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů;

f) uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu;

g) nařídit opravu či výmaz osobních údajů nebo omezení zpracování podle článků 16, 17 a 18 a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny podle čl. 17 odst. 2 a článku 19;

h) odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení vydané podle článků 42 a 43, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny;

i) uložit správní pokutu podle článku 83 vedle či namísto opatření uvedených v tomto odstavci, podle okolností každého jednotlivého případu;

j) nařídit přerušení toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.

3. Každý dozorový úřad má všechny tyto povolovací a poradní pravomoci:

a) poskytovat poradenství správci v souladu s postupem předchozí konzultace podle článku 36;

b) z vlastního podnětu nebo na požádání vydávat stanoviska určená vnitrostátnímu parlamentu, vládě členského státu nebo v souladu s právem členského státu dalším institucím a subjektům, jakož i veřejnosti, ohledně veškerých otázek souvisejících s ochranou osobních údajů;

c) povolovat zpracování uvedené v čl. 36 odst. 5, pokud právo členského státu takové předchozí povolení vyžaduje;

d) vydávat stanoviska a schvalovat návrhy kodexů chování podle čl. 40 odst. 5;

e) akreditovat subjekty pro vydávání osvědčení podle článku 43;

f) vydávat osvědčení a schvalovat kritéria pro vydávání osvědčení podle čl. 42 odst. 5;

g) přijímat standardní doložky o ochraně údajů podle čl. 28 odst. 8 a čl. 46 odst. 2 písm. d);

h) povolovat smluvní doložky podle čl. 46 odst. 3 písm. a);

i) povolovat správní ujednání podle čl. 46 odst. 3 písm. b);

j) schvalovat závazná podniková pravidla podle článku 47.

4. Výkon pravomocí svěřených tímto článkem dozorovému úřadu podléhá vhodným zárukám, včetně účinné soudní ochrany a spravedlivého procesu, stanoveným v právu Unie a členského státu v souladu s Listinou.

5. Každý členský stát v právních předpisech stanoví, že jeho dozorový úřad má pravomoc upozornit na porušení tohoto nařízení justiční orgány, a pokud je to vhodné, zahájit soudní řízení či se do něj jinak zapojit s cílem vymoci dodržení tohoto nařízení.

6. Každý členský stát může v právních předpisech stanovit, že jeho dozorový úřad má další pravomoci než ty uvedené v odstavcích 1, 2 a 3. Výkon těchto pravomocí nesmí narušit účinné fungování kapitoly VII.

Článek 59

Zprávy o činnosti

Každý dozorový úřad vypracovává výroční zprávy o své činnosti, které mohou obsahovat seznam druhů ohlášených porušení a druhů opatření přijatých podle čl. 58 odst. 2. Tyto zprávy předkládá vnitrostátnímu parlamentu, vládě a dalším orgánům určeným právem dotčeného členského státu. Dále je zpřístupní veřejnosti, Komisi a sboru.

KAPITOLA VII

Spolupráce a jednotnost

Oddíl 1

Spolupráce

Článek 60

Spolupráce mezi vedoucím dozorovým úřadem a dalšími dotčenými dozorovými úřady

1. Vedoucí dozorový úřad spolupracuje s ostatními dotčenými dozorovými úřady v souladu s tímto článkem ve snaze dosáhnout konsensu. Vedoucí dozorový úřad a dotčené dozorové úřady si vzájemně vyměňují veškeré relevantní informace.

2. Vedoucí dozorový úřad může kdykoliv požádat další dotčené dozorové úřady o poskytnutí vzájemné pomoci podle článku 61 a může provádět společné postupy podle článku 62, zejména pokud jde o vedení šetření nebo monitorování provádění opatření týkajících se správce či zpracovatele usazených v jiném členském státě.

3. Vedoucí dozorový úřad neprodleně sdělí relevantní informace o dané záležitosti ostatním dotčeným dozorovým úřadům. Neprodleně předloží ostatním dotčeným dozorovým úřadům návrh rozhodnutí, aby se k němu vyjádřily, a řádně zohlední jejich stanoviska.

4. Pokud ve lhůtě čtyř týdnů kterýkoliv z ostatních dotčených dozorových úřadů poté, co byl v souladu s odstavcem 3 tohoto článku konzultován, vznese k návrhu rozhodnutí relevantní a odůvodněnou námitku, postoupí vedoucí dozorový úřad v případě, že relevantní a odůvodněnou námitku nesdílí nebo ji považuje za irelevantní či nedůvodnou, záležitost k řešení v rámci mechanismu jednotnosti uvedeného v článku 63.

5. Pokud má vedoucí dozorový úřad v úmyslu vznesenou relevantní a odůvodněnou námitku zohlednit, předloží ostatním dotčeným dozorovým úřadům revidovaný návrh rozhodnutí k vyjádření. Tento revidovaný návrh rozhodnutí podléhá postupu uvedenému v odstavci 4 v rámci dvoutýdenní lhůty.

6. Pokud ve lhůtě uvedené v odstavcích 4 a 5 nevznesl žádný z ostatních dotčených dozorových úřadů námitku proti návrhu rozhodnutí předloženému vedoucím dozorovým úřadem, má se za to, že vedoucí dozorový úřad a dotčené dozorové úřady s tímto návrhem rozhodnutí souhlasí a toto rozhodnutí je pro ně závazné.

7. Vedoucí dozorový úřad dané rozhodnutí přijme, ohlásí je hlavní nebo jediné provozovně správce či zpracovatele a o daném rozhodnutí včetně shrnutí relevantních skutečností a důvodů informuje ostatní dotčené dozorové úřady a sbor. Dozorový úřad, u nějž byla podána stížnost, informuje o daném rozhodnutí stěžovatele.

8. Odchylně od odstavce 7, pokud je stížnost odmítnuta nebo zamítnuta, přijme rozhodnutí dozorový úřad, u nějž byla stížnost podána; tento úřad oznámí rozhodnutí stěžovateli a informuje o něm správce.

9. Pokud se vedoucí dozorový úřad a dotčené dozorové úřady shodnou na tom, že určité části stížnosti odmítnou nebo zamítnou a že budou reagovat na jiné části této stížnosti, přijme se pro každou z těchto částí dané věci samostatné rozhodnutí. Vedoucí dozorový úřad přijme rozhodnutí o části týkající se úkonů souvisejících se správcem, ohlásí je hlavní nebo jediné provozovně správce či zpracovatele na území svého členského státu a informuje o něm stěžovatele, zatímco dozorový úřad stěžovatele přijme rozhodnutí o části týkající se odmítnutí či zamítnutí této stížnosti, oznámí je danému stěžovateli a informuje o něm správce nebo zpracovatele.

10. Poté, co mu bylo oznámeno rozhodnutí vedoucího dozorového úřadu podle odstavců 7 a 9, přijme správce nebo zpracovatel opatření nezbytná k zajištění souladu s daným rozhodnutím, pokud jde o činnosti zpracování prováděné v souvislosti se všemi jeho provozovnami v Unii. Správce nebo zpracovatel oznámí opatření přijatá k zajištění souladu s daným rozhodnutí vedoucímu dozorovému úřadu, který o tom informuje ostatní dotčené dozorové úřady.

11. Pokud má za výjimečných okolností dotčený dozorový úřad důvody se domnívat, že je třeba naléhavě jednat, aby byly ochráněny zájmy subjektů údajů, použije se postup pro naléhavé případy podle článku 66.

12. Vedoucí dozorový úřad a ostatní dotčené dozorové úřady si vzájemně poskytují informace požadované podle tohoto článku, a to v elektronické formě za použití standardizovaného formátu.

Článek 61

Vzájemná pomoc

1. Dozorové úřady si vzájemně poskytují relevantní informace a pomoc v zájmu soudržného provádění a uplatňování tohoto nařízení a zavedou opatření pro účinnou vzájemnou spolupráci. Vzájemná spolupráce zahrnuje zejména žádosti o informace a opatření v oblasti dozoru, například žádosti o předchozí povolení a konzultace, inspekce a šetření.

2. Každý dozorový úřad přijme všechna vhodná opatření, která jsou požadována v odpověď na žádost jiného dozorového úřadu, a to bez zbytečného odkladu a nejpozději do jednoho měsíce od obdržení této žádosti. K těmto opatřením může patřit zejména předání relevantních informací o průběhu šetření.

3. Žádost o pomoc musí obsahovat všechny potřebné informace včetně svého účelu a důvodů. Vyměňované informace se použijí pouze pro účely, pro které byly vyžádány.

4. Dožádaný dozorový úřad nesmí odmítnout žádosti vyhovět, ledaže:

a) není pro předmět žádosti nebo pro opatření, o jejichž výkon je žádán, příslušný; nebo

b) vyhověním žádosti by došlo k porušení tohoto nařízení nebo práva Unie či členského státu, které se na dožádaný dozorový úřad vztahuje.

5. Dožádaný dozorový úřad informuje žádající dozorový úřad o výsledcích nebo případně o pokroku či opatřeních, jež byla přijata k vyřízení žádosti. Jestliže dožádaný dozorový úřad žádosti nevyhoví na základě odstavce 4, uvede důvody svého rozhodnutí.

6. Dožádané dozorové úřady poskytují informace, které po nich žádají jiné dozorové úřady, zpravidla v elektronické formě za použití standardizovaného formátu.

7. Dožádané dozorové úřady za žádné úkony, které provedou na základě žádosti o vzájemnou pomoc, neúčtují poplatky. Ve výjimečných případech se mohou dozorové úřady dohodnout na pravidlech pro vzájemné odškodnění za zvláštní výdaje vyplývající z poskytnutí vzájemné pomoci.

8. Pokud dozorový úřad neposkytne informace uvedené v odstavci 5 tohoto článku do jednoho měsíce od obdržení žádosti jiného dozorového úřadu, může dožadující dozorový úřad přijmout na území svého členského státu předběžné opatření podle čl. 55 odst. 1. V takovém případě se nutnost naléhavě jednat podle čl. 66 odst. 1 považuje za splněnou, což vyžaduje přijetí naléhavého závazného rozhodnutí sboru podle čl. 66 odst. 2.

9. Komise může prostřednictvím prováděcích aktů určit formát a postupy pro vzájemnou pomoc podle tohoto článku a může určit, jak má probíhat elektronická výměna informací mezi dozorovými úřady navzájem a mezi dozorovými úřady a sborem, zejména pak může určit standardizovaný formát uvedený v odstavci 6 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 93 odst. 2.

Článek 62

Společné postupy dozorových úřadů

1. Dozorové úřady podle potřeby provádějí společné postupy, včetně společných šetření a společných donucovacích opatření, do nichž jsou zapojeni členové nebo pracovníci dozorových úřadů z jiných členských států.

2. Pokud má správce nebo zpracovatel provozovny v několika členských státech, nebo pokud je pravděpodobné, že operacemi zpracování bude podstatně dotčen významný počet subjektů údajů ve více než jednom členském státě, má dozorový úřad každého z těchto členských států právo účastnit se společných postupů. Dozorový úřad příslušný podle čl. 56 odst. 1 nebo 4 vyzve dozorový úřad každého z těchto členských států k účasti na těchto společných postupech a na žádost některého dozorového úřadu o účast bez odkladu odpoví.

3. Dozorový úřad může v souladu s právem členského státu a s povolením vysílajícího dozorového úřadu svěřovat pravomoci včetně vyšetřovacích pravomocí členům nebo pracovníkům vysílajícího dozorového úřadu zapojeným do společných postupů, nebo pokud to umožňuje právo členského státu hostitelského dozorového úřadu, povolit členům nebo pracovníkům vysílajícího dozorového úřadu, aby vykonávali své vyšetřovací pravomoci v souladu s právem členského státu vysílajícího dozorového úřadu. Tyto vyšetřovací pravomoci mohou být vykonávány pouze pod vedením a za přítomnosti členů nebo pracovníků hostitelského dozorového úřadu. Na členy nebo pracovníky vysílajícího dozorového úřadu se vztahuje právo členského státu hostitelského dozorového úřadu.

4. Pokud pracovníci vysílajícího dozorového úřadu působí v souladu s odstavcem 1 v jiném členském státě, přijímá členský stát hostitelského dozorového úřadu odpovědnost za jejich jednání, včetně odpovědnosti za škody, které tito pracovníci během svých úkonů způsobí, v souladu s právem členského státu, na jehož území působí.

5. Členský stát, na jehož území byla škoda způsobena, nahradí tuto škodu za stejných podmínek, jaké se vztahují na škody způsobené jeho vlastními pracovníky. Členský stát vysílajícího dozorového úřadu, jehož pracovníci způsobí škodu jakékoli osobě na území jiného členského státu, nahradí tomuto jinému členskému státu v plné výši částky, které tento stát jménem dotčených pracovníků vyplatil oprávněným osobám.

6. V případě uvedeném v odstavci 1 a s výjimkou odstavce 5 se každý členský stát zřekne požadavků vůči jinému členskému státu na náhradu škody uvedené v odstavci 4, aniž jsou dotčena jeho práva vůči třetím stranám.

7. Jestliže je plánován společný postup a některý dozorový úřad nesplní do jednoho měsíce povinnost stanovenou v odst. 2 tohoto článku druhé větě, mohou ostatní dozorové úřady přijmout na území svého členského státu v souladu s článkem 55 předběžné opatření. V takovém případě se nutnost naléhavě jednat podle čl. 66 odst. 1 považuje za splněnou, což vyžaduje přijetí naléhavého stanoviska nebo naléhavého závazného rozhodnutí sboru podle čl. 66 odst. 2.

Oddíl 2

Jednotnost

Článek 63

Mechanismus jednotnosti

S cílem přispět k jednotnému uplatňování tohoto nařízení v celé Unii spolupracují dozorové úřady mezi sebou navzájem a ve vhodných případech s Komisí prostřednictvím mechanismu jednotnosti stanoveného v tomto oddíle.

Článek 64

Stanovisko sboru

1. Sbor vydá stanovisko, hodlá-li příslušný dozorový úřad přijmout některé z níže uvedených opatření. Za tímto účelem příslušný dozorový úřad oznámí sboru návrh rozhodnutí, pokud:

a) má za cíl přijmout seznam operací zpracování podléhajících požadavku na posouzení vlivu na ochranu osobních údajů podle čl. 35 odst. 4;

b) se týká záležitosti podle čl. 40 odst. 7, zda je návrh kodexu chování nebo změna či rozšíření kodexu chování v souladu s tímto nařízením;

c) má za cíl schválit kritéria pro akreditaci subjektu podle čl. 41 odst. 3 nebo subjektu pro vydávání osvědčení podle čl. 43 odst. 3;

d) má za cíl stanovit standardní doložky o ochraně údajů podle čl. 46 odst. 2 písm. d) a čl. 28 odst. 8;

e) má za cíl schválit smluvní doložky podle čl. 46 odst. 3 písm. a); nebo

f) má za cíl schválit závazná podniková pravidla ve smyslu článku 47.

2. Kterýkoli dozorový úřad, předseda sboru nebo Komise mohou požádat, aby sbor posoudil jakoukoli záležitost s obecnou působností nebo s účinky ve více než jednom členském státě za účelem získání stanoviska, zejména v případě, kdy příslušný dozorový úřad nesplní povinnosti související se vzájemnou pomocí podle článku 61 nebo se společnými postupy podle článku 62.

3. V případech uvedených v odstavcích 1 a 2 vydá sbor stanovisko k záležitosti, která mu byla předložena, pokud již stanovisko ke stejné záležitosti nevydal. Toto stanovisko se přijme do osmi týdnů prostou většinou členů sboru. Tato lhůta může být prodloužena o dalších šest týdnů s ohledem na složitost dané záležitosti. Pokud jde o návrh rozhodnutí uvedený v odstavci 1 zaslaný členům sboru v souladu s odstavcem 5, má se za to, že členové, kteří v přiměřené lhůtě stanovené předsedou nevznesli námitky, s návrhem rozhodnutí souhlasí.

4. Dozorové úřady a Komise elektronickými prostředky a za použití standardizovaného formátu bez zbytečného odkladu oznamují sboru veškeré relevantní informace, případně včetně shrnutí skutečností, návrhu rozhodnutí, důvodů, pro které je nezbytné takové opatření přijmout, a stanoviska dalších dotčených dozorových úřadů.

5. Předseda sboru bez zbytečného odkladu elektronickými prostředky sděluje:

a) členům sboru a Komisi veškeré relevantní informace, které byly radě pro ochranu údajů sděleny, a to za použití standardizovaného formátu. V nezbytných případech poskytne sekretariát sboru překlady relevantních informací; a

b) dozorovému úřadu uvedenému v odstavcích 1 a 2 a Komisi stanovisko, které zveřejní.

6. Během lhůty uvedené v odstavci 3 nepřijme příslušný dozorový úřad svůj návrh rozhodnutí podle odstavce 1.

7. Dozorový úřad uvedený v odstavci 1 stanovisko sboru co nejvíce zohlední a do dvou týdnů po obdržení stanoviska v elektronické formě sdělí předsedovi sboru, zda svůj návrh rozhodnutí zachová nebo jej změní, a rozhodne-li se je změnit, zašle mu pozměněný návrh rozhodnutí za použití standardizovaného formátu.

8. Pokud ve lhůtě uvedené v odstavci 7 tohoto článku informuje dotčený dozorový úřad předsedu sboru o tom, že nemá v úmyslu se stanoviskem sboru řídit, ať již zcela nebo částečně, a uvede relevantní důvody, použije se čl. 65 odst. 1.

Článek 65

Řešení sporů sborem

1. S cílem zajistit, aby toto nařízení bylo v jednotlivých případech správně a důsledně uplatňováno, přijme sbor závazné rozhodnutí v těchto případech:

a) pokud v případě uvedeném v čl. 60 odst. 4 vznesl dotčený dozorový úřad relevantní a odůvodněnou námitku vůči návrhu rozhodnutí vedoucího dozorového úřadu nebo pokud vedoucí dozorový úřad zamítl tuto námitku jako irelevantní či nedůvodnou. Závazné rozhodnutí se týká všech záležitostí, které jsou předmětem relevantní a odůvodněné námitky, zejména dojde-li k porušení tohoto nařízení;

b) pokud existují protikladné názory ohledně toho, který dotčený dozorový úřad je příslušný pro hlavní provozovnu;

c) pokud v případech uvedených v čl. 64 odst. 1 příslušný dozorový úřad nepožádá o stanovisko sboru nebo pokud se tento úřad neřídí stanoviskem sboru vydaným podle článku 64. V takovém případě může danou záležitost ohlásit sboru kterýkoliv dotčený dozorový úřad nebo Komise.

2. Rozhodnutí uvedené v odstavci 1 přijmou do jednoho měsíce od postoupení dané záležitosti členové sboru dvoutřetinovou většinou. Tato lhůta může být z důvodu složitosti dané záležitosti prodloužena o další měsíc. Rozhodnutí uvedené v odstavci 1 musí být odůvodněno a určeno vedoucímu dozorovému úřadu a všem dotčeným dozorovým úřadům a je pro ně závazné.

3. Pokud sbor nemohl rozhodnutí přijmout ve lhůtách uvedených v odstavci 2, přijme své rozhodnutí do dvou týdnů po uplynutí druhého měsíce uvedeného v odstavci 2 prostou většinou svých členů. Pokud členové sboru hlasují nerozhodně, rozhodnutí se přijme na základě hlasu jeho předsedy.

4. Během lhůt uvedených v odstavcích 2 a 3 nepřijmou dotčené dozorové úřady žádné rozhodnutí o záležitosti předložené sboru podle odstavce 1.

5. Předseda sboru bez zbytečného odkladu oznámí rozhodnutí uvedené v odstavci 1 dotčeným dozorovým úřadům. Uvědomí o tom Komisi. Rozhodnutí se neprodleně zveřejní na internetových stránkách sboru poté, co dozorový úřad oznámil konečné rozhodnutí podle odstavce 6.

6. Vedoucí dozorový úřad nebo dozorový úřad, u nějž byla stížnost podána, přijme své konečné rozhodnutí na základě rozhodnutí uvedeného v odstavci 1 tohoto článku bez zbytečného odkladu a nejpozději do jednoho měsíce poté, co sbor oznámil své rozhodnutí. Vedoucí dozorový úřad nebo dozorový úřad, u nějž byla stížnost podána, informuje sbor o dni oznámení svého konečného rozhodnutí správci nebo zpracovateli a subjektu údajů. Konečné rozhodnutí dotčených dozorových úřadů se přijme podle čl. 60 odst. 7, 8 a 9. Konečné rozhodnutí musí odkazovat na rozhodnutí uvedené v odstavci 1 tohoto článku a uvádět, že rozhodnutí zmíněné v uvedeném odstavci bude zveřejněno na internetových stránkách sboru v souladu s odstavcem 5 tohoto článku. Ke konečnému rozhodnutí se přiloží rozhodnutí uvedené v odstavci 1 tohoto článku.

Článek 66

Postup pro naléhavé případy

1. Dotčený dozorový úřad se za výjimečných okolností, kdy se domnívá, že je třeba naléhavě jednat v zájmu ochrany práv a svobod subjektů údajů, může odchýlit od mechanismu jednotnosti uvedeného v článcích 63, 64 a 65 nebo od postupu uvedeného v článku 60 a okamžitě přijmout předběžná opatření s právními účinky na svém území a se stanovenou dobou platnosti, která nepřesáhne tři měsíce. Tento dozorový úřad neprodleně oznámí tato opatření a důvody pro jejich přijetí ostatním dotčeným dozorovým úřadům, sboru a Komisi.

2. Pokud některý dozorový úřad přijal opatření podle odstavce 1 a domnívá se, že je třeba naléhavě přijmout konečná opatření, může požádat sbor o naléhavé stanovisko nebo naléhavé závazné rozhodnutí, přičemž svou žádost o takové stanovisko nebo rozhodnutí odůvodní.

3. O naléhavé stanovisko nebo o naléhavé závazné rozhodnutí může sbor požádat kterýkoli dozorový úřad, jestliže příslušný dozorový úřad nepřijal vhodné opatření v situaci, kdy je třeba naléhavě jednat v zájmu ochrany práv a svobod subjektů údajů, přičemž svou žádost o takové stanovisko či rozhodnutí odůvodní, stejně jako naléhavou potřebu jednat.

4. Odchylně od čl. 64 odst. 3 a čl. 65 odst. 2 se naléhavé stanovisko nebo naléhavé závazné rozhodnutí uvedená v odstavcích 2 a 3 tohoto článku přijímají do dvou týdnů prostou většinou členů sboru.

Článek 67

Výměna informací

Komise může přijímat prováděcí akty s obecnou působností za účelem určení toho, jak bude probíhat elektronická výměna informací mezi dozorovými úřady navzájem a mezi dozorovými úřady a sborem, zejména určení standardizovaného formátu uvedeného v článku 64.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 93 odst. 2.

Oddíl 3

Evropský sbor pro ochranu osobních údajů

Článek 68

Evropský sbor pro ochranu osobních údajů

1. Zřizuje se Evropský sbor pro ochranu osobních údajů (dále jen „sbor“) jako subjekt Unie s právní subjektivitou.

2. Sbor zastupuje jeho předseda.

3. Sbor tvoří vedoucí jednoho dozorového úřadu z každého členského státu a evropský inspektor ochrany údajů nebo jejich zástupci.

4. Pokud je v některém členském státě za monitorování toho, zda jsou uplatňována ustanovení tohoto nařízení, odpovědný více než jeden dozorový úřad, je v souladu s právem tohoto členského státu jmenován společný zástupce.

5. Komise má právo účastnit se činností a schůzek sboru, aniž by měla hlasovací právo. Komise jmenuje svého zástupce. Předseda sboru informuje Komisi o činnostech sboru.

6. V případech uvedených v článku 65 má evropský inspektor ochrany údajů hlasovací právo pouze pro rozhodnutí týkající se zásad a pravidel použitelných pro orgány, instituce a jiné subjekty Unie, jež v podstatě odpovídají požadavkům tohoto nařízení.

Článek 69

Nezávislost

1. Sbor jedná při plnění svých úkolů nebo výkonu svých pravomocí podle článků 70 a 71 nezávisle.

2. Aniž jsou dotčeny žádosti Komise uvedené v čl. 70 odst. 1 písm. b) a odst. 2, sbor při plnění svých úkolů nebo výkonu svých pravomocí od nikoho nevyžaduje ani nepřijímá pokyny.

Článek 70

Úkoly sboru

1. Sbor zajišťuje jednotné uplatňování tohoto nařízení. Za tímto účelem sbor z vlastního podnětu nebo případně na žádost Komise zejména:

a) monitoruje a zajišťuje řádné uplatňování tohoto nařízení v případech uvedených v článcích 64 a 65, aniž jsou dotčeny úkoly vnitrostátních dozorových úřadů;

b) poskytuje poradenství Komisi ve veškerých záležitostech souvisejících s ochranou osobních údajů v Unii včetně jakýchkoli navrhovaných změn tohoto nařízení;

c) poskytuje poradenství Komisi ohledně formy a postupů výměny informací mezi správci, zpracovateli a dozorovými úřady pro závazná podniková pravidla;

d) vydává pokyny, doporučení a osvědčené postupy týkající se postupů pro výmaz odkazů, kopií nebo replikací osobních údajů z veřejně dostupných komunikačních služeb, jak je uvedeno v čl. 17 odst. 2;

e) prošetřuje z vlastního podnětu, na žádost některého ze svých členů nebo na žádost Komise veškeré otázky týkající se uplatňování tohoto nařízení a vydává pokyny, doporučení a osvědčené postupy, aby podporoval soudržné uplatňování tohoto nařízení;

f) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce za účelem dalšího vymezení kritérií a podmínek, které mají platit pro rozhodnutí založená na profilování podle čl. 22 odst. 2;

g) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce, jak zjistit případy porušení zabezpečení osobních údajů a jak určit zbytečný odklad podle čl. 33 odst. 1 a 2 a konkrétní okolnosti, za nichž jsou správce a zpracovatel povinni porušení ohlásit;

h) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem b) tohoto odstavce, pokud jde o okolnosti, za jakých je pravděpodobné, že porušení zabezpečení osobních údajů bude mít z následek vysoké riziko pro práva a svobody fyzických osob, jak je uvedeno v čl. 34 odst. 1;

i) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce za účelem dalšího vymezení kritérií a požadavků pro předávání osobních údajů na základě závazných podnikových pravidel, kterými se řídí správci, a závazných podnikových pravidel, kterými se řídí zpracovatelé, a dalších požadavků potřebných k zajištění ochrany osobních údajů dotčených subjektů údajů uvedených v článku 47;

j) vydává pokyny, doporučení a osvědčené postupy v souladu s písmenem e) tohoto odstavce za účelem dalšího vymezení kritérií a požadavků pro předávání osobních údajů na základě čl. 49 odst. 1;

k) vypracovává pokyny pro dozorové úřady o uplatňování opatření uvedených v čl. 58 odst. 1, 2 a 3 a stanoví správní pokuty podle článku 83;

l) přezkoumává praktické uplatňování pokynů, doporučení a osvědčených postupů uvedených v písmenech e) a f);

m) vydává pokyny, doporučení a osvědčené postupy v souladu písmenem e) tohoto odstavce pro zavedení společných postupů pro podávání zpráv fyzickými osobami v případě porušení tohoto nařízení podle čl. 54 odst. 2;

n) podporuje vypracování kodexů chování a zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů podle článků 40 a 42;

o) provádí akreditaci subjektů pro vydávání osvědčení a její pravidelný přezkum podle článku 43 a provozuje veřejný registr akreditovaných subjektů podle čl. 43 odst. 6 a akreditovaných správců či zpracovatelů usazených ve třetích zemích podle čl. 42 odst. 7;

p) stanoví požadavky uvedené v čl. 43 odst. 3 pro účely akreditace subjektů pro vydávání osvědčení podle článku 42;

q) poskytuje Komisi stanovisko k požadavkům na vydání osvědčení uvedeným v čl. 43 odst. 8;

r) poskytuje Komisi stanovisko k ikonám uvedeným v čl. 12 odst. 7;

s) poskytuje Komisi stanovisko pro posouzení odpovídající úrovně ochrany ve třetí zemi nebo v mezinárodní organizaci, i pro posouzení, zda určitá třetí země, určité území nebo jedno či více konkrétních odvětví v určité třetí zemi nebo určitá mezinárodní organizace již nezajišťuje odpovídající úroveň ochrany. Za tímto účelem poskytne Komise sboru veškerou potřebnou dokumentaci, včetně korespondence s vládou dané třetí země s ohledem na tuto třetí zemi, území či konkrétní odvětví nebo s mezinárodní organizací;

t) vydává stanoviska k návrhům rozhodnutí dozorových úřadů podle mechanismu jednotnosti uvedeného v čl. 64 odst. 1, k záležitostem předloženým podle čl. 64 odst. 2 a vydává závazná rozhodnutí podle článku 65, včetně v případech uvedených v článku 66;

u) podporuje spolupráci a účinnou dvoustrannou a vícestrannou výměnu informací a osvědčených postupů mezi dozorovými úřady;

v) podporuje společné školicí programy a usnadňuje výměny pracovníků mezi dozorovými úřady a případně i s dozorovými úřady třetích zemí nebo s mezinárodními organizacemi;

w) podporuje výměnu znalostí a dokumentů o právních předpisech v oblasti ochrany údajů a zavedených postupech s dozorovými úřady pro ochranu údajů po celém světě;

x) vydává stanoviska ke kodexům chování vypracovaným na úrovni Unie podle čl. 40 odst. 9); a

y) provozuje veřejně přístupný elektronický registr rozhodnutí přijatých dozorovými úřady a soudy k otázkám řešeným v rámci mechanismu jednotnosti.

2. Jestliže Komise žádá sbor o poradenství, může uvést určitou lhůtu s přihlédnutím k naléhavosti dané záležitosti.

3. Sbor zasílá svá stanoviska, pokyny, doporučení a osvědčené postupy Komisi a výboru uvedenému v článku 93 a zveřejňuje je.

4. Sbor ve vhodných případech konzultuje zúčastněné strany a poskytne jim možnost se v rozumné lhůtě vyjádřit. Sbor výsledky postupu konzultace veřejně zpřístupní, aniž je tím dotčen článek 76.

Článek 71

Zprávy

1. Sbor vypracovává výroční zprávy, pokud jde o ochranu fyzických osob v souvislosti se zpracováním v Unii, případně ve třetích zemích a v mezinárodních organizacích. Zprávy se zveřejňují a předávají Evropskému parlamentu, Radě a Komisi.

2. Výroční zprávy obsahují posouzení praktického uplatňování pokynů, doporučení a osvědčených postupů uvedených v čl. 70 odst. 1 písm. l), jakož i závazných rozhodnutí uvedených v článku 65.

Článek 72

Postup

1. Sbor přijímá rozhodnutí prostou většinou svých členů, pokud v tomto nařízení není stanoveno jinak.

2. Sbor přijme dvoutřetinovou většinou svých členů svůj jednací řád a připraví si vlastní provozní opatření.

Článek 73

Předseda

1. Sbor si prostou většinou zvolí z řad svých členů předsedu a dva místopředsedy.

2. Funkční období předsedy a místopředsedů trvá pět let a lze je jednou prodloužit.

Článek 74

Úkoly předsedy

1. Předseda plní následující úkoly:

a) svolává zasedání sboru a připravuje pro ně pořad jednání;

b) oznamuje rozhodnutí přijatá sborem podle článku 65 vedoucímu dozorovému úřadu a dotčeným dozorovým úřadům;

c) zajišťuje včasné plnění úkolů sborem, zejména v souvislosti s mechanismem jednotnosti uvedeným v článku 63.

2. Sbor stanoví ve svém jednacím řádu rozdělení úkolů mezi předsedu a místopředsedy.

Článek 75

Sekretariát

1. Sbor má k dispozici sekretariát, jehož služby poskytuje evropský inspektor ochrany údajů.

2. Sekretariát plní své úkoly výlučně v souladu s pokyny předsedy sboru.

3. Na pracovníky evropského inspektora ochrany údajů podílející se na plnění úkolů svěřených sboru tímto nařízením se vztahují jiné hierarchické linie než na pracovníky podílející se na plnění úkolů svěřených evropskému inspektorovi ochrany údajů.

4. Sbor s evropským inspektorem ochrany údajů v případě potřeby vypracují a zveřejní memorandum o porozumění, jímž se provádí tento článek a vymezují podmínky jejich spolupráce a jenž je použitelný pro pracovníky evropského inspektora ochrany údajů podílející se na plnění úkolů svěřených sboru tímto nařízením.

5. Sekretariát zajišťuje sboru analytickou, administrativní a logistickou podporu.

6. Sekretariát odpovídá zejména za:

a) každodenní fungování sboru;

b) komunikaci mezi členy sboru, jeho předsedou a Komisí;

c) komunikaci s jinými institucemi a veřejností;

d) využívání elektronických prostředků k interní a externí komunikaci;

e) překlady relevantních informací;

f) přípravu zasedání sboru a navazující opatření;

g) přípravu, navrhování a zveřejňování stanovisek, rozhodnutí o urovnání sporů mezi dozorovými úřady a jiných textů přijímaných sborem.

Článek 76

Důvěrnost

1. Pokládá-li to sbor za nezbytné, jsou jeho jednání důvěrná, jak je stanoveno v jednacím řádu sboru.

2. Přístup k dokumentům předkládaným členům sboru, odborníkům a zástupcům třetích stran se řídí nařízením Evropského parlamentu a Rady (ES) č. 1049/2001 ([1]).

KAPITOLA VIII

Právní ochrana, odpovědnost a sankce

Článek 77

Právo podat stížnost u dozorového úřadu

1. Aniž jsou dotčeny jakékoliv jiné prostředky správní nebo soudní ochrany, má každý subjekt údajů právo podat stížnost u některého dozorového úřadu, zejména v členském státě svého obvyklého bydliště, místa výkonu zaměstnání nebo místa, kde došlo k údajnému porušení, pokud se subjekt údajů domnívá, že zpracováním jeho osobních údajů je porušeno toto nařízení.

2. Dozorový úřad, kterému byla stížnost podána, informuje stěžovatele o pokroku v řešení stížnosti a o jeho výsledku, jakož i o možnosti soudní ochrany podle článku 78.

Článek 78

Právo na účinnou soudní ochranu vůči dozorovému úřadu

1. Aniž je dotčena jakákoli jiná správní či mimosoudní ochrana, má každá fyzická nebo právnická osoba právo na účinnou soudní ochranu proti právně závaznému rozhodnutí dozorového úřadu, které se jí týká.

2. Aniž je dotčena jakákoli jiná správní či mimosoudní ochrana, má každý subjekt údajů právo na účinnou soudní ochranu, pokud se dozorový úřad, který je příslušný podle článků 55 a 56, stížností nezabývá nebo pokud neinformuje subjekt údajů do tří měsíců o pokroku v řešení stížnosti podané podle článku 77 či o jeho výsledku.

3. Řízení proti dozorovému úřadu se zahajuje u soudů toho členského státu, v němž je daný dozorový úřad zřízen.

4. Je-li zahájeno řízení proti rozhodnutí dozorového úřadu, kterému předcházelo stanovisko nebo rozhodnutí sboru v rámci mechanismu jednotnosti, dozorový úřad toto stanovisko nebo rozhodnutí předloží soudu.

Článek 79

Právo na účinnou soudní ochranu vůči správci nebo zpracovateli

1. Aniž je dotčena jakákoli dostupná správní či mimosoudní ochrana, včetně práva na podání stížnosti u dozorového úřadu podle článku 77, má každý subjekt údajů právo na účinnou soudní ochranu, pokud má za to, že jeho práva podle tohoto nařízení byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto nařízením.

2. Řízení proti správci nebo zpracovateli se zahajuje u soudů toho členského státu, v němž má daný správce nebo zpracovatel provozovnu. Řízení se může popřípadě zahájit i u soudů členského státu, kde má subjekt údajů své obvyklé bydliště, s výjimkou případů, kdy je správce nebo zpracovatel orgánem veřejné moci některého členského státu, který jedná v rámci výkonu veřejné moci.

([1]) Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (Úř. věst. L 145, 31.5.2001, s. 43).

Článek 80

Zastupování subjektů údajů

1. Subjekt údajů má právo pověřit neziskový subjekt, organizaci nebo sdružení, jež byly řádně založeny v souladu s právem některého členského státu, jejichž statutární cíle jsou ve veřejném zájmu a jež vyvíjejí činnost v oblasti ochrany práv a svobod subjektů údajů ohledně ochrany jejich osobních údajů, aby jeho jménem podal stížnost, uplatnil práva uvedená v článcích 77, 78 a 79 a, pokud tak stanoví právo členského státu, uplatnil právo na odškodnění podle článku 82.

2. Členské státy mohou stanovit, že jakýkoliv subjekt, organizace nebo sdružení uvedené v odstavci 1 tohoto článku má bez ohledu na pověření od subjektu údajů právo podat v daném členském státě stížnost u dozorového úřadu příslušného podle článku 77 a vykonávat práva uvedená v článcích 78 a 79, pokud se domnívá, že v důsledku zpracování byla porušena práva subjektu údajů podle tohoto nařízení.

Článek 81

Přerušení řízení

1. Má-li příslušný soud členského státu informace o tom, že u soudu jiného členského státu probíhá řízení týkající se stejného předmětu, pokud jde o zpracování prováděné týmž správcem nebo zpracovatelem, kontaktuje daný soud jiného členského státu, aby existenci takového řízení ověřil.

2. Probíhá-li u soudu jiného členského státu řízení týkající se stejného předmětu, pokud jde o zpracování prováděné týmž správcem nebo zpracovatelem, kterýkoliv z příslušných soudů, u nichž nebylo řízení zahájeno jako první, může své řízení přerušit.

3. Pokud toto řízení probíhá v prvním stupni, kterýkoliv ze soudů, u nichž nebylo řízení zahájeno jako první, se může na návrh jedné ze stran také prohlásit za nepříslušný, je-li soud, u něhož bylo řízení zahájeno jako první, příslušný pro daná řízení a spojení těchto řízení je podle práva státu tohoto soudu přípustné.

Článek 82

Právo na náhradu újmy a odpovědnost

1. Kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy.

2. Správce zapojený do zpracování je odpovědný za újmu, kterou způsobí zpracováním, jež porušuje toto nařízení. Zpracovatel je za újmu způsobenou zpracováním odpovědný pouze v případě, že nesplnil povinnosti stanovené tímto nařízením konkrétně pro zpracovatele nebo že jednal nad rámec zákonných pokynů správce nebo v rozporu s nimi.

3. Správce nebo zpracovatel jsou odpovědnosti podle odstavce 2 zproštěni, pokud prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.

4. Je-li do téhož zpracování zapojen více než jeden správce nebo zpracovatel, nebo správce i zpracovatel, a nesou-li podle odstavců 2 a 3 odpovědnost za jakoukoliv škodu způsobenou daným zpracováním, nese každý správce nebo zpracovatel odpovědnost za celou újmu, tak aby byla zajištěna účinná náhrada újmy subjektu údajů.

5. Jestliže některý správce nebo zpracovatel zaplatil v souladu s odstavcem 4 plnou náhradu způsobené újmy, má právo žádat od ostatních správců nebo zpracovatelů zapojených do téhož zpracování vrácení části náhrady, která odpovídá jejich podílu na odpovědnosti za újmu v souladu s podmínkami v odstavci 2.

6. Soudní řízení za účelem výkonu práva na náhradu újmy se zahajují u soudů příslušných podle práva členského státu uvedeného v čl. 79 odst. 2.

Článek 83

Obecné podmínky pro ukládání správních pokut

1. Každý dozorový úřad zajistí, aby ukládání správních pokut v souladu s tímto článkem ohledně porušení tohoto nařízení podle odstavců 4, 5 a 6 bylo v každém jednotlivém případě účinné, přiměřené a odrazující.

2. Správní pokuty se ukládají podle okolností každého jednotlivého případu kromě či namísto opatření uvedených v čl. 58 odst. 2 písm. a) až h) a j). Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se řádně zohlední tyto okolnosti:

a) povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena;

b) zda k porušení došlo úmyslně nebo z nedbalosti;

c) kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů;

d) míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedeným podle článků 25 a 32;

e) veškerá relevantní předchozí porušení správcem či zpracovatelem;

f) míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků;

g) kategorie osobních údajů dotčené daným porušením;

h) způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře;

i) v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízena opatření uvedená v čl. 58 odst. 2, splnění těchto opatření;

j) dodržování schválených kodexů chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 a

k) jakoukoliv jinou přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

3. Pokud správce nebo zpracovatel úmyslně či z nedbalosti u stejných nebo souvisejících operací zpracování poruší více ustanovení tohoto nařízení, nesmí celková výše správní pokuty překročit výši stanovenou pro nejzávažnější porušení.

4. Za porušení následujících ustanovení lze v souladu s odstavcem 2 uložit správní pokuty až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší:

a) povinnosti správce a zpracovatele podle článků 8, 11, 25 až 39, 42 a 43;

b) povinnosti subjektu pro vydávání osvědčení podle článků 42 a 43;

c) povinnosti subjektu pro vydávání osvědčení podle čl. 41 odst. 4.

5. Za porušení následujících ustanovení lze v souladu s odstavcem 2 uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší:

a) základní zásady pro zpracování, včetně podmínek týkajících se souhlasu podle článků 5, 6, 7 a 9;

b) práva subjektů údajů podle článků 12 až 22;

c) předání osobních údajů příjemci ve třetí zemi nebo mezinárodní organizaci podle článků 44 až 49;

d) jakékoli povinnosti vyplývající z právních předpisů členského státu přijatých na základě kapitoly IX;

e) nesplnění příkazu nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem podle čl. 58 odst. 2 nebo neposkytnutí přístupu v rozporu s čl. 58 odst. 1.

6. Za nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2 lze v souladu s odstavcem 2 tohoto článku uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok, podle toho, co je vyšší.

7. Aniž jsou dotčeny nápravné pravomoci dozorových úřadů podle čl. 58 odst. 2, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.

8. Na výkon pravomocí dozorovým úřadem podle tohoto článku se vztahují vhodné procesní záruky v souladu s právem Unie a členského státu, včetně účinné soudní ochrany a spravedlivého procesu.

9. Neumožňuje-li právo členského státu uložení správních pokut, může se použít tento článek tak, aby podnět k uložení pokuty dal příslušný dozorový úřad a aby pokuta byla uložena příslušnými vnitrostátními soudy, a současně je třeba zajistit, aby tyto prostředky právní ochrany byly účinné a aby jejich účinek byl rovnocenný se správními pokutami, jež ukládají dozorové úřady. Uložené pokuty musí být v každém případě účinné, přiměřené a odrazující. Tyto členské státy oznámí Komisi do 25. května 2018 příslušná ustanovení svých právních předpisů, která přijmou podle tohoto odstavce, a bez prodlení jakékoliv následné novely nebo změny týkající se těchto ustanovení.

Článek 84

Sankce

1. Členské státy stanoví pravidla pro jiné sankce, jež se mají ukládat za porušení tohoto nařízení, zejména za porušení, na něž se nevztahují správní pokuty podle článku 83, a učiní veškerá opatření nezbytná k zajištění jejich uplatňování. Tyto sankce musí být účinné, přiměřené a odrazující.

2. Každý členský stát oznámí Komisi do 25. května 2018 právní předpisy, které přijme podle odstavce 1, a bez zbytečného odkladu jakékoliv následné změny týkající se těchto ustanovení.

KAPITOLA IX

Ustanovení týkající se zvláštních situací, při nichž dochází ke zpracování

Článek 85

Zpracování a svoboda projevu a informací

1. Členské státy uvedou prostřednictvím právních předpisů právo na ochranu osobních údajů podle tohoto nařízení do souladu s právem na svobodu projevu a informací, včetně zpracování pro novinářské účely a pro účely akademického, uměleckého či literárního projevu.

2. Pro zpracování pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu členské státy stanoví odchylky a výjimky z kapitoly II (zásady), kapitoly III (práva subjektu údajů), kapitoly IV (správce a zpracovatel), kapitoly V (předávání osobních údajů do třetí země nebo mezinárodní organizaci), kapitoly VI (nezávislé dozorové úřady), kapitoly VII (spolupráce a jednotnost) a kapitoly IX (zvláštní situace, při nichž dochází ke zpracování osobních údajů), pokud je to nutné k uvedení práva na ochranu osobních údajů do souladu se svobodou projevu a informací.

3. Každý členský stát ohlásí Komisi právní ustanovení, která přijme podle odstavce 2, a bez prodlení jakékoliv následné novely nebo změny týkající se těchto ustanovení.

Článek 86

Zpracování a přístup veřejnosti k úředním dokumentům

Osobní údaje v úředních dokumentech, které jsou v držení orgánu veřejné moci či veřejného nebo soukromého subjektu za účelem plnění úkolu ve veřejném zájmu, může tento orgán či subjekt zpřístupnit v souladu s právem Unie nebo členského státu, kterému podléhá, aby tak zajistil soulad mezi přístupem veřejnosti k úředním dokumentům a právem na ochranu osobních údajů podle tohoto nařízení.

Článek 87

Zpracování národních identifikačních čísel

Členské státy mohou dále stanovit zvláštní podmínky pro zpracování národních identifikačních čísel nebo jakýchkoliv jiných všeobecně uplatňovaných identifikátorů. V takovém případě se národní identifikační číslo nebo jakýkoliv jiný všeobecně uplatňovaný identifikátor použije pouze v závislosti na vhodných zárukách práv a svobod daného subjektu údajů podle tohoto nařízení.

Článek 88

Zpracování v souvislosti se zaměstnáním

1. Členské státy mohou právním předpisem nebo kolektivními smlouvami stanovit konkrétnější pravidla k zajištění ochrany práv a svobod ve vztahu ke zpracování osobních údajů zaměstnanců v souvislosti se zaměstnáním, zejména za účelem náboru, plnění pracovní smlouvy včetně plnění povinností stanovených zákonem nebo kolektivními smlouvami, řízení, plánování a organizace práce, za účelem zajištění rovnosti a rozmanitosti na pracovišti, zdraví a bezpečnosti na pracovišti, ochrany majetku zaměstnavatele nebo majetku zákazníka, dále za účelem individuálního a kolektivního výkonu a požívání práv a výhod spojených se zaměstnáním a za účelem ukončení zaměstnaneckého poměru.

2. Tato pravidla zahrnují zvláštní a vhodná opatření zajišťující ochranu lidské důstojnosti, oprávněných zájmů a základních práv subjektů údajů, především pokud jde o transparentnost zpracování, předávání osobních údajů v rámci skupiny podniků nebo uskupení podniků vykonávajících společnou hospodářskou činnost a systémy monitorování na pracovišti.

3. Každý členský stát oznámí Komisi do 25. května 2018 právní ustanovení, která přijme podle odstavce 1, a bez zbytečného odkladu jakékoliv následné změny týkající se těchto ustanovení.

Článek 89

Záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely

1. Zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podléhá v souladu s tímto nařízením vhodným zárukám práv a svobod subjektu údajů. Tyto záruky zajistí, aby byla zavedena technická a organizační opatření, zejména s cílem zajistit dodržování zásady minimalizace

údajů. Tato opatření mohou zahrnovat pseudonymizaci za podmínky, že lze tímto způsobem splnit sledované účely. Pokud mohou být sledované účely splněny dalším zpracováním, které neumožňuje nebo které přestane umožňovat identifikaci subjektů údajů, musí být tyto účely splněny tímto způsobem.

2. Jsou-li osobní údaje zpracovány pro účely vědeckého či historického výzkumu nebo pro statistické účely, může právo Unie nebo členského státu stanovit odchylky od práv uvedených v článcích 15, 16, 18 a 21, s výhradou podmínek a záruk uvedených v odstavci 1 tohoto článku, pokud je pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění zvláštních účelů, a tyto odchylky jsou pro splnění těchto účelů nezbytné.

3. Jsou-li osobní údaje zpracovány pro účely archivace ve veřejném zájmu, může právo Unie nebo členského státu stanovit odchylky od práv uvedených v článcích 15, 16, 18, 19, 20 a 21, s výhradou podmínek a záruk uvedených v odstavci 1 tohoto článku, pokud je pravděpodobné, že by daná práva znemožnila nebo vážně ohrozila splnění zvláštních účelů, a tyto odchylky jsou pro splnění těchto účelů nezbytné.

4. Pokud typ zpracování uvedený v odstavcích 2 a 3 slouží zároveň k jinému účelu, povolené odchylky se vztahují pouze na zpracování pro účely uvedené ve zmíněných odstavcích.

Článek 90

Povinnost mlčenlivosti

1. Je-li to nutné a přiměřené pro soulad práva na ochranu osobních údajů s povinností mlčenlivosti, mohou členské státy přijmout zvláštní pravidla, aby stanovily pravomoci dozorových úřadů podle čl. 58 odst. 1 písm. e) a f) ve vztahu ke správcům nebo zpracovatelům, jež podle práva Unie nebo členského státu anebo pravidel stanovených příslušnými orgány členských států podléhají povinnosti zachovávat služební tajemství nebo jiným rovnocenným povinnostem mlčenlivosti. Tato pravidla platí pouze ve vztahu k osobním údajům, které správce nebo zpracovatel obdržel nebo získal při činnosti podléhající této povinnosti mlčenlivosti.

2. Každý členský stát oznámí Komisi do 25. května 2018 pravidla, která přijme podle odstavce 1, a bez odkladu jakékoliv následné změny týkající se těchto ustanovení.

Článek 91

Zavedená pravidla pro ochranu údajů uplatňovaná církvemi a náboženskými sdruženími

1. Jestliže církve a náboženská sdružení nebo společenství v některém členském státě v době vstupu tohoto nařízení v platnost uplatňují komplexní pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním, tato pravidla mohou nadále platit za předpokladu, že se uvedou do souladu s tímto nařízením.

2. Na církve a náboženská sdružení uplatňující komplexní pravidla v souladu s odstavcem 1 tohoto článku dohlíží nezávislý dozorový úřad, který může být zvláštní, za předpokladu, že splňuje podmínky stanovené v kapitole VI.

KAPITOLA X

Akty v přenesené pravomoci a prováděcí akty

Článek 92

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci svěřená Komisi podléhá podmínkám stanoveným v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 12 odst. 8 a čl. 43 odst. 8 je svěřena Komisi na dobu neurčitou počínaje dnem 24. května 2016.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 12 odst. 8 a čl. 43 odst. 8 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie*, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

5. Akt v přenesené pravomoci přijatý podle čl. 12 odst. 8 a čl. 43 odst. 8 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě tří měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o tři měsíce.

Článek 93

Postupy projednávání ve výboru

1. Komisi je nápomocen výbor. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

3. Odkazuje-li se na tento odstavec, použije se článek 8 nařízení (EU) č. 182/2011 ve spojení s článkem 5 uvedeného nařízení.

KAPITOLA XI

Závěrečná ustanovení

Článek 94

Zrušení směrnice 95/46/ES

1. Směrnice 95/46/ES se zrušuje s účinkem ode dne 25. května 2018.

2. Odkazy na zrušenou směrnici se považují za odkazy na toto nařízení. Odkazy na pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízenou článkem 29 směrnice 95/46/ES se považují za odkazy na Evropský sbor pro ochranu osobních údajů zřízený tímto nařízením.

Článek 95

Vztah ke směrnici 2002/58/ES

Toto nařízení neukládá žádné další povinnosti fyzickým nebo právnickým osobám, pokud jde o zpracování ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v Unii, co se týče záležitostí, u nichž se na ně vztahují konkrétní povinnosti s týmž cílem stanovené ve směrnici 2002/58/ES.

Článek 96

Vztah k dříve uzavřeným dohodám

Mezinárodní dohody zahrnující předávání osobních údajů do třetích zemí či mezinárodním organizacím, které byly uzavřeny členskými státy přede dnem 24. května 2016 a jsou v souladu s právem Unie použitelným před tímto dnem, zůstávají v platnosti, dokud nebudou změněny, nahrazeny či zrušeny.

Článek 97

Zprávy Komise

1. Do 25. května 2020 a poté každé čtyři roky předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení.

2. V souvislosti s hodnoceními a přezkumy uvedenými v odstavci 1 Komise přezkoumá zejména uplatňování a fungování:

a) kapitoly V o předávání osobních údajů do třetích zemí nebo mezinárodním organizacím, se zvláštním zřetelem na rozhodnutí přijatá podle čl. 45 odst. 3 tohoto nařízení a rozhodnutí přijatá podle čl. 25 odst. 6 směrnice 95/46/ES;

b) kapitoly VII o spolupráci a jednotnosti.

3. Pro účel odstavce 1 může Komise požádat členské státy a dozorové úřady o informace.

4. Při provádění hodnocení a přezkumů podle odstavců 1 a 2, vezme Komise v úvahu postoje a zjištění Evropského parlamentu, Rady a dalších relevantních subjektů nebo zdrojů.

5. Komise v případě potřeby předloží návrhy na změnu tohoto nařízení, zvláště s přihlédnutím k vývoji informačních technologií a dosaženému pokroku v informační společnosti.

Článek 98

Přezkum jiných právních aktů Unie v oblasti ochrany údajů

Bude-li to vhodné, předloží Komise legislativní návrhy s cílem změnit jiné právní akty Unie v oblasti ochrany osobních údajů, a zajistit tak jednotnou a soudržnou ochranu fyzických osob v souvislosti se zpracováním osobních údajů. Jedná se zejména o pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a pravidla týkající se volného pohybu těchto údajů.

Článek 99

Vstup v platnost a použitelnost

1. Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

2. Toto nařízení se použije ode dne 25. května 2018.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 27. dubna 2016.

Za Evropský parlament	*Za Radu*
předseda	*předsedkyně*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT