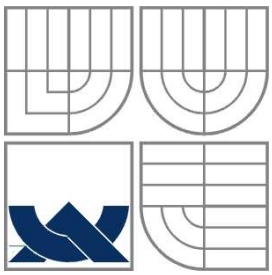
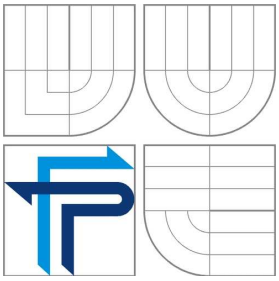


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY (UI)

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF INFORMATICS

OCHRANA OSOBNÍCH ÚDAJŮ V INFORMAČNÍM SYSTÉMU

PROTECTION OF PERSONAL DATA IN INFORMATION SYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — VENDULA OPLETALOVÁ
AUTHOR

VEDOUCÍ PRÁCE — JUDr. TOMÁŠ SOUKUP
SUPERVISOR

BRNO 2007

Abstrakt

Pojmy *osobní údaje* a *ochrana osobních údajů* doprovázejí běžný společenský život v České republice teprve pár let. V oblasti ochrany osobních údajů je nutné přijímat opatření k zamezení zneužití osobních údajů a tím se vyvarovat následnému postihu. Problematika ochrany osobních údajů je složitá, diskuse a polemiky jsou vedeny i ve sdělovacích prostředcích.

Abstract of the Thesis

The terms *personal data* and *personal data protection* have accopmanied ordinary social life of people in the Czech Republic only for several years. In the area of personal data protection it is necessary to receive measures to prevent misuse of personal data and thereby to avoid resulting sanction. Problems of personal data protection is complicated, discussion and polemics are hold even in media.

Klíčová slova

osobní údaj, ochrana osobních údajů, informační systém, Úřad na ochranu osobních údajů, legislativa, kryptografie

Keywords

personal data, personal data protection, information system, The office for personal data protection, legislation, cryptograph

Bibliografická citace mé práce:

OPLETALOVÁ, V. *Ochrana osobních údajů v informačním systému.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2007. 116 s. Vedoucí bakalářské práce JUDr. Tomáš Soukup.

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma Ochrana osobních údajů v informačním systému vypracovala samostatně s použitím pramenů uvedených v seznamu literatury a po odborných konzultacích.

V Jedovnicích dne 28. 5. 2007

Vendula Opletalová

Poděkování

Tímto bych chtěla poděkovat panu JUDr. Tomáši Soukupovi, Ing. Romaně Bašné za ochotu zhostit se úkolu oponenta mojí bakalářské práce a v neposlední řadě společnosti Synthon, s.r.o. za poskytnutí informací nutných ke zpracování práce.

Vendula Opletalová

OBSAH

1. Úvod

[1]Dnešní moderní doba bývá někdy označována **informačním věkem**. Co si pod zmíněným termínem představit? Člověk si uvědomuje nezastupitelnost úlohy informací pro kvalitu svého života. Společnost jako celek zjišťuje, že jediným jejím opravdu nevyčerpatelným zdrojem jsou právě informace.

V prvé řadě jsou tu nové **informační a komunikační technologie**, které překonávají bariéry prostoru a času a které umožňují efektivní uchovávání a opětovné vyhledávání údajů. Je pravda, že usnadňují lidem práci, ale zároveň však nynější vývoj přináší dříve neznámá potenciální nebezpečí, respektive by se dalo říci nárůst těch nebezpečí již známých. A to je důvodem, aby společnost stanovila pravidla, která by zabránila tomu, aby nesporné výhody, které přinášejí nové technologie, nebyly provázeny oslabením pozice osob, o kterých údaje vypovídají. To vše znamená vymezit nové hranice soukromí, které nahradí čas a prostor a které dokáží ochránit člověka před diskriminujícím mechanizujícím a počítačovým použitím údajů, které se k němu vztahují. Ty jsou pak předpokladem pro to, aby moderní informační a komunikační technologie, které jsou objektivně pro lidstvo přínosem, nepůsobily v jeho neprospěch.

Aktuální situace ve využívání výpočetní techniky je ale bohužel taková, že většině komerčně dostupných systémů nelze svěřit adekvátní ochranu informačních zdrojů. Ochrana dat přenášených v počítačové síti je všude ve světě prvořadým úkolem každé společnosti, která takovou sítí disponuje.

Informace jsou sbírány tak dlouho, kam až sahá lidská paměť. Za dávných časů nebylo třeba se příliš bránit existenci obrovských „smetišť“ obsahujících „hromady“ údajů, najít požadovanou informaci v požadovaném čase se doslova rovnalo malému zázraku. Avšak zcela jiná situace nastala v okamžiku, kdy s revoluční změnou

[1] Čerpáno z literatury: ŠMÍD, Vladimír. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 227/2000 Sb., zákona č. 177/2001 Sb., zákona č. 450/2001 Sb., zákona č. 107/2002 Sb., zákona č. 310/2002 Sb., zákona č. 517/2002 Sb., zákona č. 439/2004 Sb., zákona č. 480/2004 Sb., zákona č. 626/2004 Sb., zákona č. 413/2005 Sb. a zákona č. 444/2005 Sb. – komen*tář. Brno, 2005. Masarykova univerzita v Brně. 69s.

informačních technologií lze informace mnohem rychleji třídit, vybírat a analyzovat. Další dimenze tohoto problému spočívá také v tom, že pokud dříve měl finanční a technické možnosti s rozsáhlými údajovými základnami nakládat zpravidla jenom stát, s rozvojem výpočetní techniky se tyto možnosti stávají dostupné v podstatě komukoliv, kdo vlastní běžný počítač vybavený běžným softwarem a hardwarem a navíc volně nakládá byť jen obecným právem na získávání informací v kontextu základních lidských práv.

Nicméně, ještě speciálnější charakter než informace mají **osobní údaje**. Jedním z důvodů je ten, že se jedná o neoddělitelné a nezcizitelné vlastnictví naprosto každého člověka bez ohledu na jeho ekonomickou situaci a společenské postavení. Druhou zásadní odlišností je fakt, že pokud takové informace získá někdo jiný, může si vytvořit takový profil osoby, který souvisí nejen obecně s důstojností a pověstí člověka ve společenství lidí, ale může mít zcela přirozené pozitivní i negativní následky z hlediska nejrůznějších konkrétních aktivit.

Teoretické přístupy k řešení těchto problémů by mohly být v zásadě dva:

- *umožnit shromažďovat veškeré informace o jedinci* na jednom místě s cílem jakoukoliv stránku jeho osobnosti informačně podchytit tak, aby jejich držitel mohl mít přehled o tom, co ho zajímá, a to jak ve smyslu působit ve prospěch daného člověka, tak ve smyslu bránit se před jeho negativní činností;
- *neshromažďovat vůbec žádné informace*, protože všechno, co se týká jedince, je jeho výlučnou záležitostí a nikdo nemá právo jakkoliv do jeho soukromí zasahovat.

V každém případě je jasné, že jádro souvisejících problémů spočívá v nalezení vhodného a přijatelného kompromisu mezi oběmi volbami.

2. Vymezení problému a cíle práce

Bakalářská práce **Ochrana osobních údajů v informačním systému** si klade za cíl analýzu této oblasti (nejen) právní vědy. Důvodem zpracování mojí práce na dané téma byl zájem o problematiku a také vidina proniknutí do jedné z mnoha právních a technických oblastí. Jelikož dokument je výsledkem mého tříletého působení na podnikatelské fakultě se zaměřením na oblast informačních technologií, na příštích stranách se nebudu „jen" zabývat zákony a právními pojmy. Ochrana osobních údajů je taktéž úzce spjata s právě již zmiňovanými informačními technologiemi, což znamená, že mojí snahou bude spojit dvě stránky – právní a technickou – zmíněného oboru a podat čtenářům ucelený přehled o ochraně osobních údajů v informačním systému.

V úvodu jsem nastínila, o čem se v bakalářské práci budu zabývat. Tak tedy bude v ní řeč o ochraně osobních údajů v IS z hlediska právního, kdy se o ní začalo poprvé mluvit, proč je vůbec důležité osobní údaje v informačních systémech chránit, zmíním se též o zákonech, které se k téhle problematice vztahují a o Úřadě pro ochranu osobních údajů. Dále se zaměřím na druhou stránku tohoto tématu a to technickou. V mnou vybrané firmě jsem analyzovala jejich systém ochrany osobních údajů v IS a následně navrhnu nějaká doporučení, které by pomohly společnosti se v této oblasti rychleji a snadněji orientovat.

3. Teoretická východiska

3.1. Počátky

[2]Na začátek bych pro zajímavost ráda uvedla, jak to bylo s právní ochranou osobních údajů za I. republiky. Ve způsobu ochrany osobních údajů I. republika navazovala a v zásadě pokračovala v praxi z doby Rakouska-Uherska. Ani její ústava z roku 1920 negarantovala výslovně ochranu soukromí, ale pouze jeho jednotlivé aspekty (o ochraně osobních údajů se ani v této době ještě stále neuvažovalo).

Je známo, že **informace** o občanech jsou sbírány odedávna. Ovšem až zhruba v posledních třiceti letech, což přímo souvisí s masivním vstupem výpočetní techniky do všech oblastí lidské činnosti, je jejich ochraně věnována velká pozornost a řada civilizovaných států světa upravuje podmínky zacházení s osobními údaji právními normami.

[3]Pojmy **osobní údaje** a **ochrana osobních údajů** doprovázejí běžný společenský život v České republice teprve pár let. Jako lidmi pociťovaný problém byly prvně zaznamenány na počátku 90. let minulého století, na přelomu tisíciletí se pak staly – řekněme v poněkud zjednodušené podobě – také mediálním sloganem.

3.2. Co se rozumí pod pojmem „osobní údaj“?

[4]Pro účely zákona o ochraně osobních údajů se **osobním údajem** rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo

---

[2] Čerpáno z literatury: Ochrana dat za 1. republiky. *Právní ochrana osobních údajů za I. republiky* [online]. [cit. 2007-05-05]. Dostupný z WWW: <http://www.czso.cz/sldb/sldb.nsf/i/ochrana_dat_za_1_republiky>.

[3] Čerpáno z literatury: MATOUŠKOVÁ, Miroslava. *Ochrana osobních údajů: v otázkách a odpovědích*. ASPI Publishing, 2005. 157s. ISBN 80-7357-037.

identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Určité údaje ale někdy osobními údaji jsou a někdy nejsou. To platí pro údaje, které mají smysl a význam bez uvedení do vztahu k určité fyzické osobě. Typickým příkla - dem takových údajů jsou adresy nebo čísla bankovních účtů. Obecně je možné takové údaje společně označit jako popisné. Osobními údaji jsou pouze, pokud se **vztahují k** nějaké **fyzické osobě** – v terminologii zákona o ochraně osobních údajů určené nebo určitelné osobě. Velká skupina údajů je osobním údajem zpravidla; patří sem všechny identifikační údaje skutečně žijících fyzických osob. Ty nejsou osobními údaji podle zákona a podle mezinárodních předpisů upravujících ochranu osobních údajů například pokud byly vytvořeny jako údaje fiktivní. Vezmeme si například rodné číslo: pokud již bylo přiděleno nějakému člověku, osobním údajem je a nemůže jím přestat být.

Obecně však neexistuje žádná definice, která by obecně určila, co jsou to údaje dostatečně určující konkrétní subjekt údajů. Je zřejmé, že v běžné situaci by mělo stačit jméno, příjmení a adresa bydliště. Nicméně například bydlí-li v jednom domě několik rodinných příslušníků více generací se stejnými jmény a příjmeními, budeme potřebovat další identifikátor (např. datum narození). Naopak však může docházet k situacím, kdy zcela jiný elementární údaj konkrétní subjekt údajů jednoznačně identifikuje (např. předseda vlády ČR ve funkci k datu 1.ledna 2002).

3.3. Proč chránit osobní údaje v IS?

[5]Je řada důvodu, proč chránit osobní údaje (nejen) v informačních systémech. Nyní tyto důvody shrnu. Nejdříve bych uvedla dvě odlišné odpovědi, z nichž jedna („*filozofická*“) se týká společenských mravů a druhá („*pragmatická*“) samotného porušování zákona.

[4] Čerpáno z literatury: MATOUŠKOVÁ, Miroslava. Ochrana osobních údajů: v otázkách a odpovědích. ASPI Publishing, 2005. 157 s. ISBN 80-7357-037-8.

a) filozofická odpověď

Jednoduše řečeno, protože se jedná o součást ochrany osobnosti. Pokud se k sobě mají lidé chovat slušně, pak by součástí tohoto slušného chování mělo být i odpovědně nakládat s jejich osobními údaji. Povinnosti stanovené zákonem na ochranu osobních údajů představují pouze uzákonění něčeho, co slušní lidé, kteří mají k dispozici osobní údaje jiných lidí, stejně dělají. Ochrana osobních údajů by tak měla být součástí lidské slušnosti.

[6]**Osobní údaje se mohou stát bránou do soukromí všech. Je jen na každém z nás, koho necháme vstoupit, koho necháme projít a koho necháme před těmito pomyslnými branami stát**. Uvedu zde jeden ilustrující příklad: S přicházejícím večerem většina z nás zatahuje doma závěsy, protože přirozeně cítíme, že prostor, který obýváme a který je určen nám, naší rodině či přátelům, je naším soukromím, do kterého nechceme, aby někdo cizí nahlížel. Své osobní doklady, různé rodinné dokumenty či jinak důležitá potvrzení se také snažíme mít v pořádku, zbytečně je nevystavujeme na obdiv a snažíme se je neztratit, či o ně jiným způsobem nepřijít. Soukromím je také naše osobnost, se všemi niternými pocity a vztahy, naše zdraví a intimní život, majetek i naše politické názory. Opět můžeme říci, že většina z nás se snaží zbytečně nevydávat v plen vše o svém nitru, protože přirozeně cítíme, že tím naše osobnost něco ztrácí.

b) pragmatická odpověď

Plnit povinnosti stanovené zákonem na ochranu osobních údajů je třeba, protože za jejich neplnění hrozí sankce. S těmito povinnostmi se každý člověk nemusí ztotožnit, může na ně nadávat, ale pokud je nedodržuje, vystavuje se tak postihu. Je to obdobné jako např. placení daní. Platit daně a vyplňovat daňová přiznání je velká otrava, která nás připravuje o čas i peníze. Pokud bychom však daně neplatili, vystavujeme se finanč-

---

[5] Čerpáno z literatury: Ochrana osobních údajů. *Proč se zabývat ochranou osobních údajů?* [online]. [cit.2007-04-12]. Dostupný z WWW: <http://www.oou.cz/index.php?file=ochrana_dat_proc_chranit_osobni_udaje>.

[6] Čerpáno z literatury: Úřad pro ochranu osobních údajů [online]. [cit. 2007-04-10]. Dostupný z WWW:<www.uoou.cz/zpravodaj/bulletin_2000_02.pdf>.

nímu nebo jinému postihu (např. trest odnětí svobody). S ochranou osobních údajů je to stejné jako s daněmi. Sankce za nerespektování ochrany osobních údajů jsou přitom ve srovnání se sankcemi za neplacení daní mnohem přísnější.

3.4. Ochrana osobních údajů

[7]Problematika **ochrany osobních údajů** je jednou z oblastí v již tak rozmanité krajině práva. Jak je zřejmé z názvu, právo na ochranu osobních údajů vzniklo za účelem ochrany osobních údajů lidí před jejich možným zneužitím. Svou povahou je toto právo nejbližší právu na soukromí, ze kterého se vývojem společnosti oddělilo. Představy lidí, co vlastně soukromí znamená, se možná v něčem trochu odlišují, ale jedno je jisté, že soukromí potřebujeme, že je pro nás důležité a že bez soukromí bychom byli tak trochu loutkami na scéně života.

Ochrana osobních údajů je v současné době ale komplikovaná, dynamická a jistým způsobem závislá na bouřlivém rozvoji informačních technologií. Před 20 – 30 lety ještě nikoho nenapadlo, že již dnes neodmyslitelnou součástí života bude třeba mobilní telefon či že nás budou sledovat kamerové systémy nebo čipy. Chytré technologie nám jakoby usnadňují denní život, ale současně vnímáme jejich negativní dopad na naše soukromí. A jen těžko lze předvídat, co ještě přinese jejich další vývoj. Je zde na místě otázka: „Je důvod k obavám?“ V naší aktuální informační společnosti, která je přeplněná množstvím nejrůznějších databází a registrů, napadne některé z nás znepokojivá myšlenka na nebezpečí orwellovského státu a jeho Velkého bratra, v němž jsou osobní údaje občanů nekontrolovaně shromažďovány, předávány a různě využívány.

Ochrana osobních údajů je téma, které stále rychleji a intenzivněji proniká do našeho každodenního života a nabývá na významu. Je tedy zapotřebí, aby se zásady ochrany osobních údajů rovněž stávaly součástí znalostí, kterými je každý člověk dosta-

[7] Čerpáno z literatury: Úřad pro ochranu osobních údajů [online]. [cit. 2007-04-24]. Dostupný z WWW:<www.uoou.cz/zpravodaj/bulletin_2000_02.pdf>.

tečně vybaven. Závažnosti a aktuálnosti problematiky odpovídá i pozornost, kterou ochraně osobních údajů věnuje Evropská unie. S právem EU harmonizovala svou legislativu i Česká republika.

[8]Ochrana osobních údajů v teorii i praxi se skládá z těchto částí (složek):

- Automatizovaná rozhodnutí
- Důvody zpracování
- Kategorie osobních údajů
- Kategorie příjemců
- Kategorie subjektů údajů
- Legislativa
- Povinnosti správce
- Prostředky zpracování
- Správce a zpracovatel
- Účel zpracování
- Zdroje osobních údajů
- Způsoby zpracování osobních údajů

3.5. Zákon o ochraně osobních údajů

[9]Moderní informační a komunikační technologie umožňují různým subjektům získávat, uchovávat, zpracovávat a využívat údaje o svých zákaznících. Jedná-li se o osobní údaje, je nutné stanovit taková opatření, aby nedošlo jejich použitím k diskriminaci člověka. Informace o občanech jsou neoddělitelným a nezcizitelným vla-

---

[8] Čerpáno z literatury: ŠALAMOUN, Michal. Ochrana osobních údajů v teorii i praxi. *Ochrana osobních údajů* [online]. [cit. 2007-04-24]. Dostupný z WWW: <http://www.oou.cz/index.php?file=nastroje_k_ochrane_osobnich_dat_kniha>.

[9] Čerpáno z literatury: ŠMÍD, Vladimír. *Ochrání nový zákon naše osobní údaje?* [online]. [cit. 2007-05-06]. Dostupný z WWW: <http://www.fi.muni.cz/~smid/cw4.html>.

stnictvím každého člověka bez ohledu na jeho ekonomickou situaci a společenské postavení. Na základě negativních zkušeností a zneužívání osobních údajů v minulosti bylo nutné vytvořit zákon, který by upravoval podmínky zpracovávání a využívání těchto citlivých dat. Po několikaletém úsilí byl v roce 2000 Parlamentem ČR přijat **zákon č. 101/2000 Sb. o ochraně osobních údajů**[10] upravující ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů a stanovující podmínky, za nichž se uskutečňuje jejich předávání do jiných států. Nahradil tak **zákon č. 256/1992 Sb., o ochraně osobních údajů v informační systémech**[11]. Byl první svého druhu v našich podmínkách a vedle mnohých nesporných kladů trpěl zejména dvěma problémy:

- nedočkal se dostatečné „popularity“ (ať již mezi bočany, jejichž data byla zpracovávána, nebo u zpracovatelů těchto dat), aby byl alespoň dostatečně dodržován, resp. jeho dodržování bylo důsledně vyžadováno,
- předpokládal ustanovení orgánu, jehož posláním by byla ochrana osobních údajů jednotlivců, ovšem takový orgán nikdy nebyl zřízen.

Motivem pro přijetí nového zákona byla především snaha vyrovnat se s podmínkami Úmluvy Rady Evropy o ochraně osob s ohledem na automatizované zpracování osobních údajů a Směrnicí č. 95/46/ES o ochraně osob se zřetelem na zpracování osobních dat a o jejich volném pohybu.

Přijetí zákona, až vyvoláno děním v mezinárodním prostředí, je reakcí na skutečnost, že osobní údaje na straně jedné tvoří součást soukromé (osobnostní) sféry a současně na straně druhé mohou působit a dokonce i vznikat bez vůle a vědomí toho, o kom informují.

[12]Bez nějakých hlubších rozborů je zřejmé, že způsobilost informace samostatně vstupovat do rozmanitých vztahů je důvodem pro doplňování právního řádu demokratických států a mezinárodních uskupení o samostatné instituty ochrany osobních údajů.

---

[10] Viz Příloha č. 2

[11] Viz Příloha č. 3

Zákony o ochraně osobních údajů, jakož i mezinárodní předpisy o ochraně osobních údajů, vždy upravují pouze některé formy a způsoby používání osobních údajů. Obecný právní pojem v českém právním řádu, který „pokrývá“ prakticky všechny formy a způsoby používání osobních údajů, je **nakládání s osobními údaji**. Některé formy nakládání s osobními údaji podléhají zákonu o ochraně osobních údajů; tyto formy jsou **zpracováním osobních údajů**. Až na některé výjimky není zpracování osobních údajů zakázáno, jsou jen pro ně stanoveny podmínky. Společensky nepřijatelné formy a způsoby nakládání s osobními údaji jsou odpovídajícími právními předpisy považovány za správní delikty nebo dokonce za trestné činy. Postih neoprávněného nakládání s osobními údaji jako trestného činu podle ustanovení §178 **trestního zákona**[13] není již považován za součást ochrany osobních údajů.

Cílem takto pojaté ochrany je dosažení preventivní účinnosti. Dalo by se říci, že lze ochranu osobních údajů přirovnat třeba k požární ochraně. Taktéž vyžaduje od každého přijímání preventivních opatření spojených s určitými náklady a omezením volnosti při rozhodování. Shodné je dokonce i to, že přijímaná opatření chodí někdo kontrolovat. Nejdůležitější shoda je však v tom, že pokud je účinná, jeví se ochrana téměř jako zbytečná a obtěžující. Nikdo z nás však nedá přednost tomu, poznat na vlastní kůži skutečné závažné důsledky jejího porušení.

Zákon o ochraně osobních údajů upravuje ochranu osobních údajů o fyzických osobách, práva a povinnosti při zpracování těchto údajů a stanoví podmínky, za nichž se uskutečňuje jejich předávání do jiných států. Týká se každého z nás. Tento zákon je o tom, jak se zachází s našimi údaji, které díky rozvoji informačních technologií jsou přenosné na téměř libovolnou vzdálenost během několika sekund. Jako jeden z mála zákonů neukládá zákon č. 101/2000 Sb. fyzickým osobám povinnosti. Všem osobám, které na základě tohoto zákona mohou do styku s našimi osobními údaji přijít, je uložena obecná povinnost dbát, abychom jako subjekt údajů neutrpěli újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochra-

[11] Čerpáno z literatury: MATOUŠKOVÁ, Miroslava. *Ochrana osobních údajů: v otázkách a odpovědích*. ASPI Publishing, 2005. 157s. ISBN 80-7357-037-8.

[12] Viz Příloha č.5

nu před neoprávněným zasahováním do našeho soukromého a osobního života. Fyzická osoba, k níž se osobní údaje vztahují, je nazývána **subjektem údajů**. Subjektem údajů tedy nejsou právnické osoby.

3.6. Úřad pro ochranu osobních údajů

Jelikož je na těchto stránkách neustále řeč o ochraně osobních údajů, nemohu se nezmínit o orgánu, který se touto problematikou zaobírá, konkrétně o **Úřadu pro ochranu osobních údajů (ÚOOÚ)**. Úřad, se sídlem Pplk. Sochora 27, 170 00 Praha 7, se ve své činnosti řídí zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. [14]Je nezávislým orgánem, který:

- provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů,
- vede registr povolených zpracování osobních údajů,
- přijímá podněty a stížnosti občanů na porušení zákona a informuje o jejich vyřízení,
- zpracovává a veřejnosti zpřístupňuje výroční zprávu o své činnosti,
- vykonává další působnosti stanovené mu zákonem,
- projednává přestupky a jiné správní delikty a uděluje pokuty podle tohoto zákona,
- zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána,
- poskytuje konzultace v oblasti ochrany osobních údajů,
- spolupracuje s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů.

Jako jednotlivec může každý občan České republiky adresovat podání ÚOOÚ, jehož obsahem může být například stížnost na porušení zákona o ochraně osobních údajů. Úřad je povinen stížností zabývat a autora podání informovat o vyřízení podnětu.

---

[14] Čerpáno z literatury: MATOUŠKOVÁ, Miroslava. *Ochrana osobních údajů: v otázkách a odpovědích*. ASPI Publishing, 2005. 157s. ISBN 80-7357-037-8.

Pokud však nechce občan vstupovat do kontaktu s Úřadem s adresně projevenými podněty, může využít informace zveřejňované Úřadem na průběžně aktualizované vývěsce **www.uoou.cz** a ve Věstníku ÚOOÚ. Významným zdrojem informací je každoročně vydávaná výroční zpráva zveřejňovaná do roku 2004 jako součást Věstníku, nyní samostatně.

3.7. Obecně k informačním systémům

[15]V dnešní moderní době již určitě každý z nás snad alespoň jednou slyšel pojem **informační systém,** stejně tak se většina z nás domnívá, že přesně ví, co vlastně tento pojem znamená a s jakými typy informačních systémů se může v praxi setkat. Bohužel - skutečnost je přesně opačná. Obdobně jako v dalších oblastech, jsou i zde představy odborné veřejnosti velmi často odlišné od reality. A aby toho nebylo málo, mnohdy se mezi sebou dohadují také odborníci na slovo vzatí. „Co vlastně může být za informačním systémem schováno?“ „Jaké je jeho rozdělení podle hlediska, o kterém se dnes velmi často hovoří - podle vztahu k systému řízení?“. Odpovědi na tyto otázky budou v příštích řádcích zodpovězeny.

Pod informačním systémem si asi většina z nás nejčastěji představí nějaký "rozsáhlejší" program, například pro skladové hospodářství podniku. Daná představa sice směřuje správným směrem, avšak je naprosto nedostatečná. Pod informačním systémem musíme chápat celou řadu dalších zdrojů a prostředků. Asi nejvýstižnější definicí je ta, která pod informačním systémem rozumí široký komplex lidí, informací, vlastního systému řízení (tedy programového vybavení), technické prostředky (převážně pak hardwarové pozadí) a systém organizace práce uživatele v příslušné oblasti. Účelem celého komplexu je sběr, přenos, aktualizace, uchování a další zpracování dat za účelem tvorby a prezentace informací, které by měly zlepšit výkonnost uživatelů.

[15] Čerpáno z literatury: KOCAN, Marek. Co vlastně je informační systém a jak souvisí s řízením? *Živě.cz: Co vlastně je informační systém a jak souvisí s řízením?* [online]. Poslední aktualizace 08. 11. 1998. [cit. 2007-05-01]. Dostupný z WWW: <http://www.zive.cz/h/Programovani/AR.asp?ARI=3436>.

Některým se může zdát zmíněná definice poněkud složitější, pokud však chceme pochopit podstatu funkce informačního systému, nesmíme se na něj dívat odděleně od jeho okolí. Informace jsou v dnešní době mohutnou zbraní, a to nejen pro boj s případnou konkurencí, ale také v boji se svými vlastními nedokonalostmi a chybami. A kvalitní informační systém nám může pomoci tuto „bitvu“ vyhrát.

Když už tedy víme, co si máme pod informačním systémem přesně představit, můžeme se ještě pokusit o jeho klasifikaci. Hledisek, podle kterých můžeme jeho rozdělení provést, je hned několik - od *komplexnosti*, přes *účel* až po *vztah k systému řízení* uživatele (zpravidla pak organizace). Podle tohoto, v současnosti často zmiňovaného hlediska, můžeme hovořit o transakčních systémech (*operativní řízení*), o informačních systémech pro řízení a systémech pro podporu rozhodování (*taktické řízení*) a o informačních systémech pro vrcholové řízení (*strategické řízení*).

[16]Pro informační systém (IS) platí několik faktů:

- Může, ale nemusí být podporován počítačem, přičemž při návrhu IS zkoumáme optimální kombinaci automatizovaných a neautomatizovaných činností.
- Musí disponovat prostředky sběru, kontroly a uchování dat.
- Jsou vyjasněné vztahy mezi informacemi a daty i v rámci jednoho zaměření informačního systému. Informace jsou jen ta data, která dokážeme využít, přiřadit jim význam či smysl. Při návrhu IS nutno umožnit získávání odlišných informací pro různé zaměstnance – skladník, ředitel atd.
- Informační systém ovlivňují pracovní procesy i organizační struktura podniků.
- Informační systém je vždy společným dílem dodavatele a zákazníka.

Informační systémy v dnešní době tvoří podstatnou část naší existence. Jsou na mnoha místech, dokonce i tam, kde bychom je vůbec neočekávali. A s postupem času budou ještě důležitější.

Rozvoj informatiky přinesl potřebu koncentrace velkého množství různých údajů ze všech oblastí lidské činnosti. Tato data mají ve většině případů mnohem větší hodnotu, než samotné informační systémy určené k jejich zpracování. Informace jsou neustále zhodnocovány a upravovány tak, aby byly aktuální a co nejvíce užitečné.

Propojením často samostatně nevýznamných údajů z více databází může dojít k takové situaci, kdy by zneužití dané informace (její zveřejnění, zničení, poskytnutí někomu, kdo by z ní mohl mít prospěch) mohlo výrazně poškodit určitou osobu či organizaci. Proto musí být zajištěna důsledná ochrana dat, a to jak technická (hierarchické přístupy k datům pomocí hesel, kódování dat, fyzické zabezpečení pracoviště), tak i právní – formou přijetí příslušných zákonných norem.

S informačními systémy nějakým způsobem souvisí hlavně tyto obecné právní předpisy: občanský zákoník, trestní zákon, autorský zákon, zákon o ochraně osobních údajů, zákon o ochraně topografií polovodičových výrobků, obchodní zákoník, zákon o ochraně státního tajemství, zákon o telekomunikacích, zákoník práce a konečně i sama Listina základních práv a svobod, jež je součástí naší Ústavy.

Všechny tyto právní předpisy se týkají informačního systému organizace, a to především v oblastech:

a) prevence před porušováním zákonů (např. autorského zákona, zákona o ochraně státního tajemství) bez dopadu na organizaci (s výjimkou odpovědnostního postihu);
b) prevence před poškozením vlastní organizaceí, zaměstnanci nebo jinými osobami (např. porušování pracovních předpisů, obchodního tajemství, neoprávněné používání cizí věci, poškozování a zneužití záznamu na nosiči informací atd.)

[16] Čerpáno z literatury: POKORNÝ, Martin. Vyvíjíme databázový a informační systém I. *Databázový svět – informační portál ze světa databázových technologií* [online]. Poslední aktualizace 05. 05. 2004. [cit. 2007-05-02]. Dostupný z WWW: <http://www.dbsvet.cz/view.php?cisloclanku=2004050501>.

4. Analýza problému a současné situace ve společnosti

4.1. Základní údaje o společnosti

Ve své práci jsem analyzovala systém ochrany osobních údajů ve společnosti Synthon, s.r.o. Blansko. Jedná se o společnost, která byla založena v roce 2003. Až do roku 2000 v Blansku působil odštěpný závod brněnské Lachemy a v tomto roce se tehdejší její vlastníci rozhodli blanenský odštěpný závod odprodat, a to nizozemské farmaceutické společnosti Synthon, která byla založena v roce 1991, ale od svého vzniku s Lachemou spolupracovala, hlavně v oblasti výzkumu a vývoje. Synthon, s.r.o. Blansko je tedy dceřinnou společností zahraniční farmaceutické společnosti. Je to společnost malá, ale s celosvětovou působností. Společnost je certifikovaná Státním ústavem pro kontrolu léčiv (SÚKL).

Kromě České Republiky má společnost Synthon, s.r.o. zastoupení v Nizozemí, Španělsku, USA, Argentině a Austrálii.

Od roku 2004 vyrábí produkty pouze pro mateřskou společnost Synthon International Holding B. V. se sídlem v Nizozemsku a pro nikoho jiného. Možná proto není společnost v obecném povědomí u českého farmaceutického průmyslu, protože na český trh nic nedodává.

4.2. Informační systémy ve společnosti

4.2.1. Informační systém ERP (systém J.D.Edwards OneWorld)

[17]**Enterprise Resource Planning (ERP)** je software pro plánování podnikových zdrojů, který umožňuje řízení těchto zdrojů. Ty se orientují na optimalizaci procesů nejen v rámci podniku, ale stále více ve vazbě s jeho dodavateli, partnery a zejména pak

[17] Čerpáno z literatury: Synthon, s.r.o., Blansko. Standardní operační postupy (SOP) společnosti Synthon. 2006.

zákazníky – nákup, příjem a prodej (ne)skladované položky, založení dodavatele, založení odběratele, vystavování dobropisů a vrubopisů. Kvalitní ERP systém je sice nutnou podmínkou, sám o sobě však nestačí. Zároveň musí být v podniku a podotýkám že ve společnosti Synthon je vůle naplno jej využívat, uzpůsobit tomu v případě potřeby i zaběhnuté postupy a procesy.

Jak funguje J.D.Edwards OneWorld?

Každý podnik je do značné míry definován svými daty a jejich toky. Zákazník si objedná zboží. Údaje z jeho objednávky jdou do výroby a poslouží jako základní informace. Týmiž daty se aktualizují skladové údaje: je třeba zajistit dostupnost všech potřebných součástek, látek…, dodat je do výroby, popřípadě objednat nové zásoby. Až se bude výrobek expedovat, vystaví se faktura. Zároveň je možné evidovat, kdo na zakázce co odpracoval a předat tyto údaje mzdové účetní k výpočtu mezd, odměn, přesčasů, nároků na dovolenou.

4.2.2. Informační systém ANeT-Time

[18]**ANeT-Time** je moderní docházkový systém. Zavedením tohoto informačního systému dle mého názoru společnost Synthon učinila důležitý a dnes nutný krok na cestě k vyšší prosperitě a efektivitě podnikání. „Papírové píchačky“ jsou již v dnešní moderní době minulostí. Společnosti se díky systému rozprostřely obrovské možnosti, které s sebou přináší současné informační technologie.

Mzdové moduly stávajícího informačního systému společnosti získávaly informace o práci, nemoci, dovolených či náhradních volnech zaměstnanců prostým opisování přepočítaných „píchaček“ na klávesnici PC. S tím je ale naštěstí konec a celá tahle činnost byla přenechána výpočetní technice a systému ANeT-Time.

Docházkový systém má ve svém názvu slovo systém zcela právem. Není to jenom software, ale taky hardware – terminály, komunikační linky nebo čipové karty v rukou zaměstnanců společnosti – a to vše dohromady tvoří funkční a spolehlivý celek.

4.2.2.1. Identifikační čipy

Jedná se o čipové plastikové karty obsahující **identifikační čip** s jedinečným číslem. Pokud se čipová karta přiloží ke čtecí zóně terminálu, čip se aktivuje, vyšel svůj číselný kód a průchod je v terminálu zaznamenán. Čip je zataven uvnitř plastikové karty, která ho chrání při běžném zacházení. Dojde-li ale například k silnému ohýbání karty, čip může být zničen. Na čipové kartě mohou být vytištěny libovolné informace přesně dle přání zákazníka.

4.2.2.2. Terminál

Terminál slouží k registraci průchodů osob v docházkovém systému ANeT-Time. Terminál je připojen sériovou linkou přes převodník na komunikační server, nebo z převodníku přímo na COM port řídící stanice. Komunikace dále již probíhá po LAN (protokol TCP/IP). Informace o průchodech jsou ukládány do databáze na databázovém serveru.

Terminál má vlastní paměť, což znamená, že i v případech, kdy dojde k přerušení komunikace, bude terminál dál pracovat a sbírat informace o průchodech. Po obnovení komunikace jsou všechny informace správně přeneseny do systému a uloženy do sdílené databáze.

4.2.2.3. Klientská stanice

Klientskou stanicí docházkového systému je každé síťové PC vybavené potřebným klientským software ANeT-Time. Běžnému uživateli slouží tyto stanice k prohlížení,

[18] ANeT – Time = Advanced Network Technology – Time.

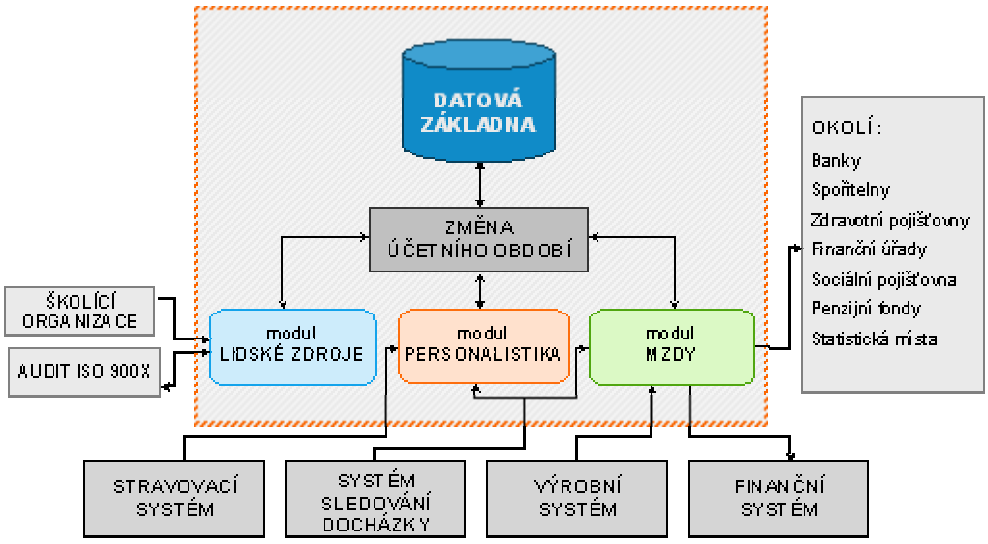
Čerpáno z literatury: FARSKÝ, Martin. *ANeT-Time: manuál k docházkovému systému*. Brno: ANet-Advanced Network Technology s.r.o., 2002. 153 s.

dále k opravám a zpracování dat uloženým na databázovém serveru. Vybraní uživatelé na nich mohou provádět konfigurace parametrů systému a definovat strukturu uživatelů.

4.2.3. Systém Nugget SW

[19]Jedná se o komplexní zpracování mzdové, personální agendy a řízení lidských zdrojů v architektuře Client/Server pod operačním systémem Windows NT (2000, XP). Datová základna je uchovávána na serveru, rovněž tak podstatná část programů funguje na serveru. Pracovní stanice jsou koncipovány jako „tenký klient“, tj. programy na nich zpracovávané zajišťují především grafickou prezentační vrstvu. Pomocí této architektury jsou docilovány okamžité odezvy a vysoká rychlost zpracování dávkových úloh.

Všechny moduly sdílí společnou datovou základnu .Z hlediska časové návaznosti programové vybavení umožňuje personalistovi zadávat a aktualizovat údaje, aniž by ovlivnil výsledky zpracování mezd. Speciální mechanismus zajišťuje, že veškeré změny údajů rozhodujících pro výpočet mezd se mzdové účetní aktivují až v okamžiku náběhu daného účetního období.



Obr. 1: Personální řízení – přehled

4.2.3.1. Modul MZDY/CS

Modul Mzdy/CS zajišťuje řadu činností, z nichž uvedu jen některé:

- snadné a úplné zadání údajů o zaměstnancích a jejich srážkách,
- možnost provádění hromadných změn,
- jednoduché zadávání nemocenské a mateřské dovolené,
- ošetření minimální mzdy,
- penzijní připojištění,
- kapitálové životní pojištění,
- možnost nastavení výše sazeb příplatků,
- výpočet daně z příjmu fyzických osob,
- automatické provádění srážek všech typů v zákonném pořadí,
- snižování pohledávek až do poslední splátky,
- tisk hromadných příkazů k úhradě nebo vytváření souboru pro elektronický přenos do banky nebo spořitelny,
- výpočet nároku na dovolenou a jeho krácení dle Zákoníku práce, atd.

4.2.3.2. Modul PERS/CS

Modul Personalistika je zaměřen především na detailní sledování a hodnocení osob z hlediska profesní zdatnosti, kvalifikačních předpokladů, jazykových znalostí, kurzů, školení a zdravotní způsobilosti.

- aktualizace personálních dat pracovníků,
- personální evidence,
- osobní karty,
- pracovní smlouvy,
- vzdělání a školení,
- výběrové a rozborové aktivity,
- personální statistiky, přehledy a analýzy,
- bezpečnost práce,
- podnikové byty,

- stravování zaměstnanců,
- stanovení uživatelských číselníků. Pevně nastavené číselníky jsou pouze u údajů, které vstupují do algoritmu zpracování dat a jejich nesprávné nastavení může způsobit chyby ve výpočtu mzdy.

4.2.3.3. Modul LZ/CS

Modul Lidské zdroje výrazným způsobem rozšiřuje řešení směrem do oblasti personálního řízení. Poskytuje další podporu pro činnosti plánovací a hodnotící. Komplexně a srozumitelně řeší zejména požadavky pro vzdělávání a hodnocení zaměstnanců, které ukládá norma ISO 9000 (týkající se systému řízení kvality).

- Jádrem řešení je tvorba a údržba organizačního schématu. Jeho základním stavebním prvkem je pozice, která má definovány určité vazby (propojení na katalog pracovních míst, příp. na databázi zaměstnanců) a atributy (pokud se jedná o atributy vztažené k pozici, tak se jednak přebírají z vazeb nebo se specifické požadavky mohou definovat přímo k dané pozici.
- Tato koncepce umožňuje kdykoli porovnávat plánované a skutečné kvalifikační předpoklady zaměstnance jak na funkci, na které je zařazen, tak na plánovanou funkci. S tím úzce souvisí plánování rezerv a postupů.
- V oblasti plánování vzdělávání je udržována databáze školících organizací včetně nabídky kurzů a školení zajímavých pro organizaci.
- Součástí řešení je i práce s databází uchazečů o zaměstnání v organizaci. V databázi lze dle zvolených kritérií vyhledávat vhodné kandidáty na pozice, vyhodnocovat jejich kvalifikaci a další předpoklady nutné pro výkon profese ve společnosti.
- Současně lze také evidovat náborové akce a následně je vyhodnocovat z hlediska účinností a nákladovosti.

[19] Čerpáno z literatury: Nugget SW spol. s r.o., Praha. *MZDY/CS, PERST/CS, LZ/CS*. Praha: Nugget SW spol. s r.o., 2003. 18 s.

4.3. Jak společnost chrání osobní údaje v IS?

4.3.1. Přístupová práva

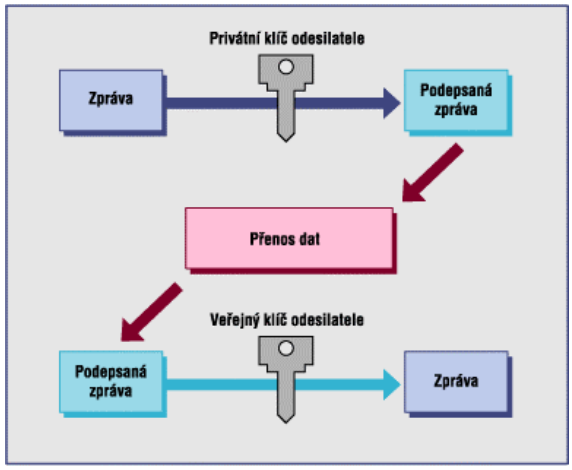
Jak si tedy společnost Synthon, s.r.o poradila s ochranou osobních údajů v informačním systému? Při průzkumu ve společnosti jsem zjistila, že v prvním případě jsou osobní údaje chráněny **přístupovými právy**.

Každý zaměstnanec při spuštění informačního systému zadá své uživatelské jméno a příjmení. Je vytvořen uživatelský účet. Zaměstnanec je také povinen zadat svoje heslo, kterým se umožní vstup do IS.

4.3.2. Kryptování

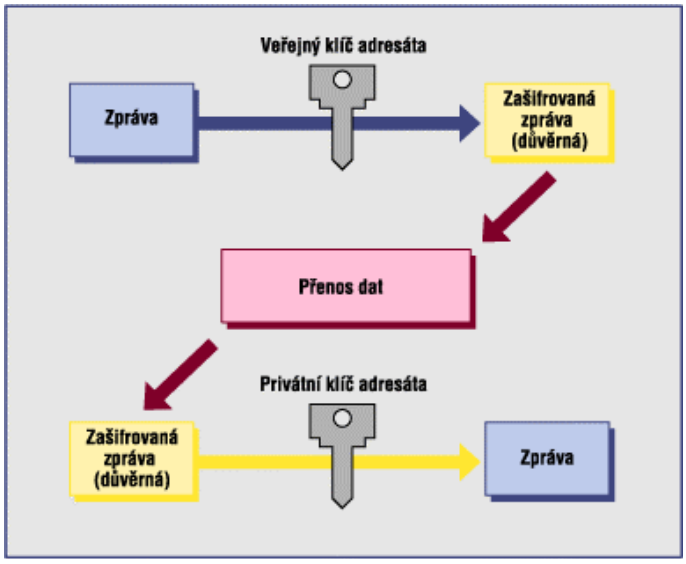
Dalším bezpečnostním prostředkem je **kryptování** neboli šifrování pro vyšší bezpečnost a ochranu osobních údajů. Kryptografie je členěna na dvě metody – symetrická a asymetrická. Ve společnosti Synthon, s.r.o. se využívá druhé zmiňované, tedy asymetrické.

[20]**Asymetrická kryptografie** se označuje z toho důvodu, že se zde užívá jiného klíče pro šifrování a jiného pro dešifrování (narozdíl od symetrické). Klíč pomocí, kterého se šifruje, se nazývá *veřejný klíč* a klíč, kterým se dešifruje, se nazývá *soukromý (privátní) klíč*. Tuto dvojici klíčů si vygeneruje uživatel pomocí některého z běžně dostupných SW produktů a stává se tak jejich jediným majitelem. Princip spočívá v tom, že data šifrovaná jedním z klíčů lze v rozumném čase dešifrovat pouze se znalostí druhého z dvojice klíčů a naopak. Privátní klíč je s maximální bezpečností ukrýván majitelem (čipové karty, disketa v trezoru, ...), zatímco veřejný klíč je – jak už z názvu vyplývá - zveřejněn. Známe-li tedy vlastníka veřejného klíče, kterým jsme zprávu dešifrovali, známe odesilatele. Protože je veřejný klíč obecně znám všem, nelze zprávu zašifrovanou podle výše popsaného postupu považovat za zašifrovanou v plném smyslu slova (důvěrnou), ale pouze za podepsanou.



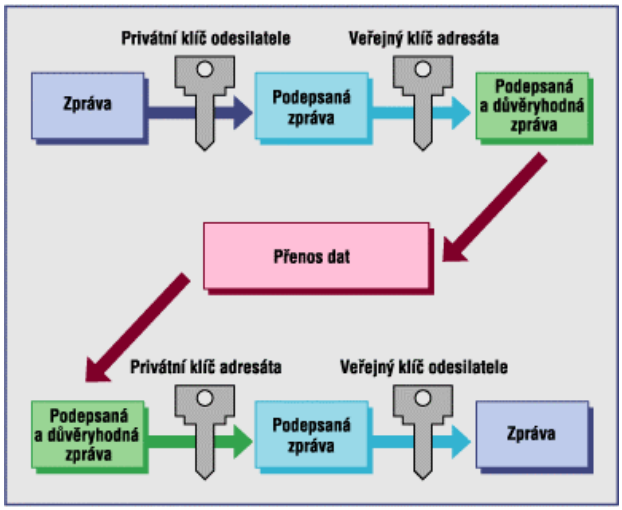
Obr.2: Přenos neadresované, nezašifrované (veřejné), ale podepsané (autorizované) zprávy.

Zmíněným způsobem lze za pomocí asymetrické kryptografie řešit integritu dat a neodmítnutelnost odpovědnosti na straně odesilatele. Jestliže příjemce pošle podepsané potvrzení o přijetí zprávy, je zajištěna neodmítnutelnost odpovědnosti i ze strany příjemce. Není tak ovšem vyřešena otázka důvěryhodnosti zpráv, tedy nečitelnosti pro neautorizované subjekty. K tomu lze využít šifrování zpráv pomocí veřejného klíče adresáta. Při zašifrování zprávy tímto klíčem máme jistotu, že ji přečte pouze adresát se svým privátním klíčem. Situace je znázorněna na obrázku 3.



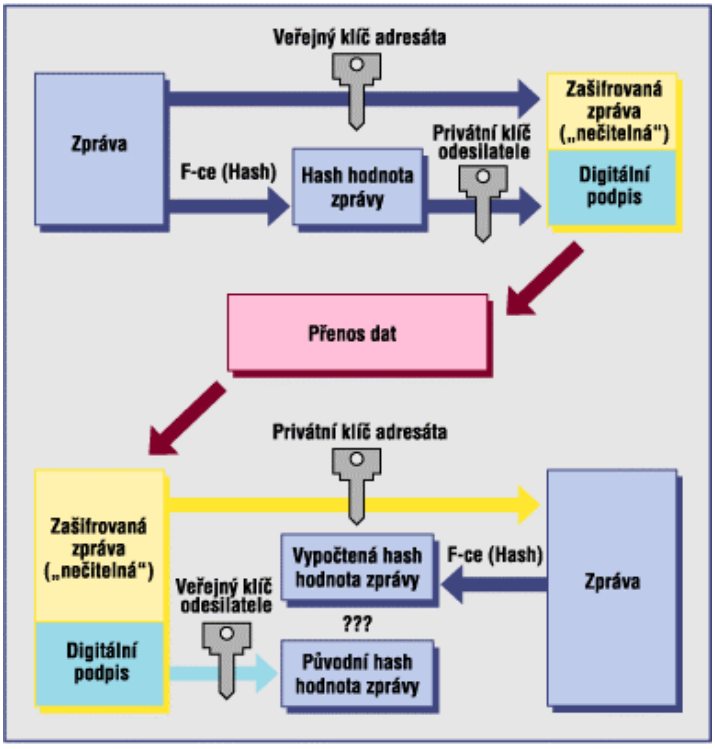
Obr. 3: Přenos adresované, zašifrované (důvěrné), ale nepodepsané (neautorizované) zprávy.

Celý systém pro šifrování a podepisování zpráv pomocí asymetrické kryptografie pracuje tedy následujícím způsobem. Zpráva je obvykle na straně odesilatele nejprve podepsána, podepsán je čitelný text zprávy, a potom šifrována. Na straně příjemce je zpráva nejprve dešifrována privátním klíčem příjemce, čímž je zajištěna adresnost zprávy a teprve potom je pomocí veřejného klíče ověřena identifikace odesilatele.



Obr.4: Přenos adresované, zašifrované (důvěrné) a podepsané (autorizované) zprávy.

Aplikace asymetrických algoritmů je výrazně pomalejší než užití algoritmů symetrických. Je to dáno matematickou podstatou asymetrických algoritmů. Proto se mnohdy při tvorbě podpisu nešifruje privátním klíčem odesilatele celá zpráva, ale nejprve se na data použije takzvaná **hashovací funkce**. Hashovací funkce je jednosměrná transformace, která z variabilních vstupních veličin vrací jednoznačnou hodnotu (textový řetězec) pevné délky, která se jmenuje hash hodnota. Hash hodnota představuje zhuštěnou hodnotu dlouhé zprávy ze které byla vypočtená, ve významu digitálního otisku prstu velkého dokumentu. Opačný proces je nemožný. Výpočet hash hodnoty zprávy je velmi rychlý. Nejprve se při podpisu zprávy vypočte hash hodnota zprávy, která bývá výrazně kratší než podepisovaná zpráva, a ta se zašifruje některým asymetrickým algoritmem (RSA) s použitím privátního klíče. Výsledkem je takzvaný digitální podpis, který je potom odeslán jako příloha zprávy.



Obr.5: Bezpečná komunikace s využitím digitálního podpisu

Odesílatel zprávy nejprve vypočte hash hodnotu zprávy a tu zašifruje svým privátním klíčem, čímž vznikne digitální podpis zprávy. Potom zprávu zašifruje veřejným klíčem adresáta (znečitelní pro neautorizované subjekty). Takto upravená zpráva je spolu s digitálním podpisem předána (zaslána po síti, předána na disketě, ...) adresátovi. Ten nejprve zprávu dešifruje za pomocí svého privátního klíče a tím se zpráva stane čitelná. Podpis ověří výpočtem hash hodnoty zprávy a jejím srovnáním s dešifrovanou hash hodnotou z digitálního podpisu.

[20] Čerpáno z literatury: Šifrovací metody. *I.CA – Teorie symetrické a asymetrické kryptografie*. [online]. [cit. 2007-05-03]. Dostupný z WWW: < http://www.ica.cz/home_cs/?acc=teorie_ symetricke_a_asymetricke_kryptografie >.

4.3.3. Zabezpečení datových struktur v systému Nugget

[21]Z hlediska přístupu z aplikačního programu jsou data v **systému Nugget** chráněna prostřednictvím systému autorizací na funkce, kmenová střediska a osobní čísla zaměstnanců a autorizací na klíčové údaje v základních souborech. Data jsou uložena v interní databázi a uživateli nejsou přístupná jiným prostředkem než aplikačním programem.

Před neoprávněným přístupem jsou data chráněna (kromě prostředků operačního systému, které zajišťuje IT uživatele) tímto způsobem:

- šifrováním klíčových „autorizačních" souborů (hesla, autorizace, pravidla pro práci s hesly),
- komprimací klíčových základních souborů,
- utajením datového modelu (uživateli není známa struktura dat).

4.3.4. Identifikace uživatele při přihlášení do systému Nugget

Pravidla pro práci s hesly může standardně nastavit pouze uživatel systému Nugget v servisním programu (nachází se zde samostatná složka *Autorizace → Pravidla práce s hesly*). Avšak pokud to umožní bezpečnostní standardy uživatele lze tuto pravomoc (po následné úpravě programu) delegovat na administrátora uživatele. Pro nastavení pravidel lze nastavit tyto parametry:

Jaká by měla být struktura hesla?:

Lze zadat následující pravidla pro strukturu hesla:

- vynucení použití písmen
- vynucení použití číslic
  - vynucení použití malých a velkých písmen současně
  - minimální délka hesla
  - maximální počet stejných po sobě jdoucích znaků
  - vynucení rozdílnosti hesla od jména uživatele

- vynucení rozdílnosti od posledních x použitých hesel (x = max. 44)

Jaká je platnost hesla?:

Lze zadat následující pravidla pro platnost hesla:

- vynucení změny hesla po prvním přihlášení
- počet dní platnosti hesla
- počet dní před vypršením platnosti hesla, kdy se má uživatel upozornit
- počet chybných pokusů přihlášení pro zablokování profilu

Parametry pro práci s hesly nemůže změnit ani uživatel, oprávněný nastavovat přístupová práva a zavádět nové uživatelské profily s prvotním heslem, rovněž také nemůže měnit heslo již zavedenému uživateli. Jestliže některý z uživatelů zapomene heslo, následně dojde k zablokování profilu. Nastavit nové heslo a tím znovu zpřístupnit profil může pouze uživatel systému Nugget (či delegovaný administrátor).

Po přihlášení zadá uživatel svůj profil (neboli účet) a heslo, které se kontroluje následujícím postupem: chybné heslo se odmítne a po opakovaném chybném zadání hesla (= počet chybných pokusů v parametrech) se profil znepřístupní. Pokud je avšak toto heslo správné, ale pozor „prošlé“, systém si vynutí okamžitě jeho změnu. Nové heslo se pro kontrolu zadává dvakrát a kontroluje se shodnost zadání, jakož i dodržení všech pravidel stanovených pro práci s hesly. Zda-li je zadané heslo platné, ale je třeba ho změnit po *x* dnech (x < početní dní na upozornění), napíše se uživateli upozornění.

Po správném přihlášení je heslo možno kdykoliv změnit pomocí tabulky, která se zobrazí po otevření položky *Změna hesla* umístěné ve složce *Funkce*.

[21] Čerpáno z literatury: Nugget SW spol. s r.o., Praha. *Provozní dokumentace: Popis základní konfigurace, nastavení a řešení nestandardních provozních situací*. Praha: Nugget SW spol. s r.o., 2003. 25 s.

4.3.5. Zákon o ochraně osobních údajů

Společnost Synthon, s.r.o. se při nakládání s osobními údaji řídí zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který je upraven vlastní směrnicí.

5. Vlastní návrhy řešení, efektivnost návrhů řešení

Dle provedené analýzy ochrany osobních údajů v informačních systémech ve společnosti Synthon jsem dospěla k názoru, že společnost chrání osobní údaje v souladu se zákonem a používá dostatečná bezpečnostní opatření. I přesto bych uvedla nějaká doporučení či takové malé shrnutí a zásady, které poslouží společnosti v orientování se v této problematice.

5.1. Návrhy, doporučení

Každý informační systém musí respektovat obecné principy ochrany soukromí každé fyzické osoby, jejíž osobní údaje jsou předmětem zpracování, a zajistit tak naplnění všech základních právních podmínek v oblasti ochrany osobních údajů.

1. Co se týče přístupových práv, zastavila bych se u **hesel**. Je důležité používat bezpečná hesla. Dle statistiky téměř polovina společností považuje právě hesla za největší hrozbu pro svou bezpečnost zaměstnance. Nejslabším článkem informačního sytému bývá totiž jeho uživatel. A proto důležitá rada: Heslo nikomu neprozrazovat a nenechávat je na viditelných místech! Může se to zdát jako banální věc, ale najdou se stále tací, kterým napsání hesla na papírek a jeho přilepení na monitor nedělá problém. Co se týče otázky, jak autentizačně zabezpečit informační systém, nejdůležitější dle mého názoru je stálé proškolování zaměstnanců o dodržování bezpečnostních pravidel při používání jakéhokoliv informačního systému. Je to základní předpoklad, jak nepřijít o osobní data. Pokud bych takové školení měla promítnout po finanční stránce, zdaleka to nepřijde tak drahé jako například investice do silných autentizačních mechanismů, jakými jsou různá biometrická zařízení, která rozpoznávají unikátní fyzické charakteristiky uživatele. Jistou možností je autentizace samotného uživatele na základě používání předmětů, které má ve vlastnictví pouze on. Těchto předmětů se již používá celá řada a jsou zaváděny ve většině západních firem. Napadá mě takové přirovnání. Dokud si uživatel bude myslet, že je rozdíl v přístupu k IS a přístupu k jeho kontu na bankovnímu účtu, nebude IS nikdy dokonale bezpečný.

2. Dále bych se věnovala **asymetrické kryptografii**, zda je vhodnější než symetrická. Nutno podotknout, že výhodou symetrické kryptografie je její rychlost. Dá

se dobře využít pro šifrování dat, která se nikam neposílají. Největší nevýhodou totiž je, že pokud chceme s někým tajně komunikovat, musíme si předem bezpečným kanálem předat klíč. Naopak hlavní výhoda asymetrické je to, že si lidé nemusí před zahájením vyměnit klíče neodposlouchávaným komunikačním kanálem, veřejný klíč mohou znát všichni a potřebují méně klíčů. Na druhou stranu je tento způsob asi tisíckrát pomalejší než symetrická kryptografie. Ale i tak bych se určitě přiklonila k asymetrické kryptografii.

3. Společnosti bych také doporučila, aby problematiku ochrany osobních údajů nebrala na lehkou váhu. Odborník ve společnosti na tuto oblast by měl být znalý a měl by mít zkušenosti, jelikož bezpečnost systému na něm právě stojí a padá. Zřejmě není pochyb o tom, že společnost Synthon svou úlohu v pracovněprávních vztazích nemůže plnit bez znalosti údajů o svých zaměstnancích, a to jak v průběhu doby trvání pracovněprávního vztahu, tak také před jeho vznikem i po jeho zániku. Vždyť osobní údaje se používají na dokladech, uchazeč o zaměstnání je vypisuje do životopisu apod.

4. Velmi kvituji, že mezi bezpečnostní opatření řadí Synthon Zákon č. 101/2000 Sb., o ochraně osobních údajů, který má upraven vlastní směrnicí.

5. Je důležité mít na paměti, že ochrana osobních údajů v informačních systémech je problém, u něhož nedodržení stanovené povinnosti, byť i zdánlivě velmi formálního rázu, může mít důsledky zcela zásadního významu. Proto také jakékoliv podcenění zpracovávání osobních údajů a jejich vedení nelze připustit.

5.2. Zásady, rady

5.2.1. Předmět ochrany údajů

Obecně lze problémy počítačové bezpečnosti rozdělit do sedmi klíčových oblastí:

1. Zajištění soukromí - každý jedinec nebo organizace musí mít možnost volby, kdy a s kým bude sdílet svá data.
2. Zajištění utajení - u velkých firem není prakticky možné definovat explicitně pro každého uživatele, ke které části dat má mít přístup. Místo toho se užívá klasifikace

dat do kategorií, nazývaných *stupně utajení*. Každému jedinci je pak přiřazena jistá míra jeho prověření, tzv. *oprávnění uživatele*, které uvádí, že daný jedinec je oprávněn pracovat s daty určitého stupně utajení.

3. Zajištění integrity - žádnému jedinci nesmí být zabráněno v použití osobního údaje proto, že někdo jiný osobní údaj zničil.
4. Zajištění přístupu ke službám - žádnému jedinci nesmí být zabráněno v použití osobního údaje proto, že někdo jiný poškodil prostředky, zajišťující k tomuto osobnímu údaji přístup.
5. Omezení možnosti zneužití - privilegovaným uživatelům nesmí být umožněno zneužít důvěry k získání neautorizovaného přístupu k datům a prostředkům nebo k oprávněnému udílení přístupu jiným osobám.
6. Identifikace problémů - administrátor musí být v případě prolomení bezpečnosti stanovit konkrétní příčinu a určit co nejpřesněji rozsah škody.
7. Zajištění bezpečnosti - uživatelé musí mít jistotu, že komunikují se skutečně důvěryhodným systémem

5.2.2. Rady týkající se hesel do IS

Často užívaná hesla bývají jméno uživatele, případně manželky, manžela, milenky, milence nebo psa, podle toho, koho má člověk nejraději. V jiných případech to může být název oblíbeného filmového hrdiny či jméno oblíbeného sportovce. To vše je ale dle mého názoru špatné. Proto zde uvedu rady, které by měly uživateli posloužit ke správnému zvolení hesla.

1. Za prvé bych doporučila při vstupu do nového informačního systému změnit heslo vytvořeného systémem nebo správcem sytému.

2. Doporučuji při přístupu k IS zadat delší heslo, které bude obsahovat velká i malá písmena, číslice, a nějaký speciální znak.

3. Častou chybou je též používání stejného hesla pro všechny používané aplikace. Může se stát, že si neoprávněný uživatel zjistí heslo z méně zabezpečeného sytému a pak se snadno dostane všech uživatelem používaných aplikací. Proto je i třeba téhle chyby se vyvarovat.

3. Řekněme speciálním případem jsou administrátorská hesla. Mají to být vůbec ta nejsložitější hesla. Ale opak je pravdou, protože tato hesla mezi sebou sdílí několik uživatelů, zná je většinou každý zaměstnanec ve společnosti.
4. Lidé nemají rádi změny, a z tohoto důvodu si dávají stále stejná hesla, proto pokud to systém umožňuje, je dobré zakázat používání stávajícího hesla po vypršení jeho platnosti na minimálně jeden měsíc. Proto si myslím, že v systému Nugget SW, který společnost používá, je velkou výhodou zmíněná pravidla pro práci s hesly (viz 4.3.3.5. Identifikace uživatele při přihlášení do systému Nugget)

5.2.3. Povinnosti správce

Základní myšlenkou ochrany osobních údajů, která je promítnuta do povinností správce, je, že osobní údaje se zpracovávají za určitým účelem. Když bych to měla shrnout, platí, že to, k čemu osobní údaje správce má, musí mít odraz v tom, kolik osobních údajů má a jak je používá. Většina povinností správce nějakým způsobem reaguje na tuto myšlenku.. A proto v Zákoně o ochraně osobních údajů speciální termíny jako je *účel zpracování, prostředky zpracování, způsob zpracování, kategorie osobních údajů, kategorie subjektů údajů* či *kategorie příjemců*. V těchto termínech je třeba nakládání s osobními údaji (zákon používá termín *zpracování*) popsat.

Zpravidla správce nezpracovává osobní údaje za jedním, ale několika účely. Je proto vhodné udělat si takový „přehled osobních údajů“ – tedy seznam o tom, jaké osobní údaje zpracovávám, proč to dělám a roztřídit si tyto údaje podle účelu (podle toho, na co je potřebuji). co jako správce mám a proč) a každý účel podrobně popsat v termínech, jež stanovuje zákon.

Dále bych navrhla, aby si ve společnosti odpovědné osoby v téhle problematice zorganizovali práci, tak aby byla, co nejeefiktivnější. Důležitou věcí, je zákaz zpracování citlivých údajů[22].

[22] Citlivý údaj - viz Příloha č.2

A v neposlední řadě bych doporučila vedení evidence zpracování osobních údajů. Myslím si, že se jedná o velmi užitečnou činnost.

5.2.4. Zásady zpracování osobních údajů

Nyní se dostanu k shrnutí zásad, jak zpracovávat osobní údaje. Tyto zásady musí každý odborník v této oblasti mít na zřeteli a řídit se jimi:

1. Při zpracovávání osobních údajů musí být chráněna osobní práva osob poskytujících údaje.
2. Osobní údaje mohou být zpracovány, pouze pokud to povoluje zákon nebo dohoda nebo pokud s tím osoba poskytující údaje souhlasila. Osobní údaje mohou být zpracovány pouze pro účely, pro které byly původně shromážděny, a pokud účel povoluje zákon nebo dohoda nebo pokud s tím osoba poskytující údaje souhlasila.
3. Uložené osobní údaje by měly být přesné a v případě potřeby aktualizovány. Případně musí být podniknuty kroky s cílem zajistit, aby byly nepřesné nebo neúplné údaje vymazány nebo opraveny.
4. K osobním údajům mají přístup pouze ty osoby, jejichž funkce a kompetence zahrnují manipulaci s nimi; právo přístupu je omezeno podle povahy a rozsahu jednotlivé funkce a kompetencí.
5. Vzhledem k případným právním závazkům uchovávat záznamy jsou údaje vymazány, pokud již nejsou pro obchodní účely, pro které byly původně shromážděny a uloženy, potřebné.
6. Zpracování údajů by mělo být určeno pouze k shromažďování, zpracovávání nebo používání údajů, které jsou potřebné, tj. mělo by pokud možno probíhat co nejméně. Musí být realizovány možnosti anonymního nebo pseudoanonymního zpracování údajů, pokud je to možné nebo se zdá, že to vzhledem k výdajům bude rozumné. Statistická hodnocení na základě anonymních nebo pseudoanonymních údajů nemusí splňovat požadavky ohledně ochrany údajů, pokud je již nelze spojit s osobou poskytující údaje.
7. Osoba poskytující údaje má právo rozhodnout se, že pro ni nebude platit rozhodnutí, v jehož důsledku vzniknou nevýhodné účinky, které se jí týkají nebo které ji

výrazně ovlivňují a které se opírají výhradně o automatické zpracování údajů, jehož cílem je hodnocení určitých osobních aspektů týkajících se jí, například její důvěryhodnosti. Informační technologie mohou sloužit jako rozhodovací nástroje, ale nemohou být jediným základem pro rozhodování. Jestliže by měla být v jednotlivých případech učiněna taková automatická rozhodnutí, musí osoba poskytující údaje dostat příležitost vyjádřit své stanovisko, pokud rozhodnutí není povoleno zákonem, který rovněž stanovuje opatření na ochranu legitimních zájmů takové osoby.

8. V případech, kdy je plánováno zpracování údajů, které by mohlo s sebou nést určitá rizika pro osobní práva osoby poskytující údaje, musí být od samého začátku před zahájením zpracování zapojeno oddělení na ochranu údajů.

5.2.5. Otázky

Každý zaměstnanec či uchazeč o zaměstnání ve společnosti by si měl položit následující otázky:

1. Jaké osobní údaje společnost sbírá? A pro koho?
2. Má společnost povolení shromažďovat osobní údaje?
3. Kde jsou ukládány osobní údaje?
4. Jak se lze domoci jejich odstranění z databází?
5. Jak jsou osobní údaje zabezpečeny?

6. Závěr

V další části práce bych se zastavila nad Zákonem č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. „Z jakého důvodu tak činím?“ Zákon o ochraně osobních údajů v informačních systémech předcházel Zákonu č. 101/2000 Sb., o ochraně osobních údajů a z tohoto důvodu si myslím, že by zde neměl chybět a i když již neexistuje, nesmím ho při rozebírání dané problematiky opomenout.

6.1. Porovnání Zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů a Zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

Zákon č. 256/1992[23] byl první ucelenou obecnou normou České republiky (přesněji České a Slovenské Federativní Republiky), která upravovala práva a povinnosti provozovatelů (respektive dalších zúčastněných osob) při provozování informačních systémů, které nakládají s osobními údaji, směřující k ochraně těchto informací (tedy českým „informačním zákonem“). Ideovým podnětem pro jeho znění byla Úmluva ETS č. 108 o ochraně osob s ohledem na automatizované zpracování osobních údajů, která v dané době byla doplněna celkem osmi dodatečnými speciálními doporučeními a to je jednoznačně patrné na jeho struktuře i obsahu.

Zmíněný zákon za prvé v našem zákonodárství poprvé právně definoval některé zásadní pojmy z informatiky, za druhé stanovil pravidla nakládání s informacemi. Pravidla byla stanovena obecně jako minimální požadavky pro veškeré informační systémy takového typu bez ohledu na to, kdo je jejich provozovatelem a týkala se i těch

[23] Čerpáno z literatury: ŠMÍD, Vladimír. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 227/2000 Sb., zákona č. 177/2001 Sb., zákona č. 450/2001 Sb., zákona č. 107/2002 Sb., zákona č. 310/2002 Sb., zákona č. 517/2002 Sb., zákona č. 439/2004 Sb., zákona č. 480/2004 Sb., zákona č. 626/2004 Sb., zákona č. 413/2005 Sb. a zákona č. 444/2005 Sb. – komentář.* Brno, 2005. Masarykova univerzita v Brně. 69s.

informačních systémů, které vznikly již dříve na základě jiných zákonů.

Dle mého názoru jsou hlavní částí tohoto zákona definice jednotlivých pojmů, který vyplňují téměř celou jeho první polovinu. Jsou zde tak definovány například pojmy dotčená osoba (tj. *subjekt údajů), provozovatel* (tj. správce osobních údajů), dále pojmy jako *osobní údaj, informační služba, zpracování informace, likvidace informace, účastník výměny informací, uživatel, zprostředkovatel, náležitý způsob sběru informací* a *zveřejněná informace*.

Jisté komplikace ovšem v praxi způsobovaly dvě z těchto definic – „*informační systém*“ (měl být ekvivalentní pojmu „automatizovaný soubor dat“) a „*provozování informačního systému*“ (měl být ekvivalentní pojmu „automatizované zpracování“). Z těchto uvedených definic nebylo zcela jasné, zda se informačním systémem rozumí pouze počítačový informační systém či nikoli. Faktem je, že v definicích v tomto zákoně se skutečně pojmy „počítačový“ či „elektronický“ výslovně nepoužívaly. Jenže žádné upřesnění, výklad ani alespoň soudní rozhodnutí za dobu účinnosti tohoto zákona nebyly vydány, mimo jiné i proto, že tato norma vlastně nebyla důsledně v praxi aplikována.

Povinnosti související s provozováním IS zákon rozšířil o údaje, které vypovídají o osobnosti a soukromí dotčené osoby (což nijak neupřesnil, ale ponechal v této velmi nejasné obecné poloze) a její národnosti, ochranu informací o politických postojích blíže specifikoval rovněž ve smyslu členství v politických stranách a navíc doplnil i ochranu údajů o majetkových poměrech. Údaje bylo možné zpracovávat pouze, stanoví-li tak zvláštní zákon, nebo se souhlasem žijící dotčené osoby, pokud je možné, aby tento projev vůle učinila. Jestliže nelze podmínku souhlasu splnit, bylo možno s informacemi nakládat jen za předpokladu, že bude zachována lidská důstojnost, osobní čest, dobrá pověst a chráněno dobré jméno dotčené osoby.

Je zde však nadmíru stručně pojat princip otevřenosti a princip účasti subjektu osobních údajů. Z požadavků dle Úmluvy ETS č. 108 se zde objevil pouze požadavek na poskytnutí zprávy o informacích o subjektu údajů uchovávaných v informačním systému a to jedenkrát do roka bezplatně, nebo za přiměřenou úplatu kdykoli, pokud zvláštní zákon nestanoví jinak. Ostatní požadavky jako zjištění existence takového

systému vůbec, respektive související opravné prostředky zde zcela chybí nebo jsou obecně chápány nikoliv jako přirozený požadavek, ale pouze jako sekundární povinnost při porušení primární povinnosti z tohoto zákona.

S ohledem na princip bezpečnosti jsou zde stanoveny povinnosti odpovídající Úmluvě ETS č. 108 doplněné, respektive upřesněné o:

- běžné odpovědnostní tituly korespondující s obdobnými kategoriemi chráněných informací v českém právu (například ochrana osobnosti nebo obchodní tajemství),
- zamezení přístupu k informacím v průběhu sporu, pokud orgán příslušný pro rozhodnutí sporu výjimečně nestanoví jinak (přičemž nárok se týká pouze sporem dotčených informací).

Zásadním problémem bylo, že zmiňované předpokládané návazné právní normy se nikdy nerealizovaly a předpokládaný státní orgán pověřený dohledem nad provozováním informačních systémů, které nakládají s citlivými osobními údaji, tedy nikdy nevznikl. Současně práva případně postižených osob tak nebyla dostatečně chráněna v souladu s Úmluvou ETS č. 108 (potažmo přirozeně i se Směrnicí č. 95/46/EC) a z toho mimo jiné plynulo, že státy Evropské unie by ani nebyly oprávněny povolit přenos dat do České republiky.

Zákon č. 256/1992 Sb. byl postaven pouze na aplikaci ochrany osobních údajů při automatizovaném zpracování údajů, a to pouze v rámci systematické činnosti, jíž je provozování informačního systému, přičemž u manuálního zpracování bylo zákon přiměřeně aplikovat. Mimo působnost zákona tak zůstalo nakládání s osobními údaji vně informačních systémů.

Dále za negativní věc bych považovala definici pojmu *osobní údaj*. Ten byl totiž pouze vymezen jako informace vztahující se k určité osobě.

Nový **zákon o ochraně osobních údajů** Vláda ČR schválila 22. 9. 1999 a Poslanecké sněmovně Parlamentu ČR jej předložila 28. 9. 1999. Jeho význam byl mimo jiné zdůrazněn i tím, že byl zahrnut mezi právní normy, které explicitně směřují k harmonizaci práva České republiky s právem Evropské unie. Když si každý porovná tyto dva zákony, může vidět, že ve stávajícím zákoně přibyly nové pojmy (*citlivý údaj,*

anonymní údaj, subjekt údajů apod.), stávající byly rozšířeny či změněny jejich názvy (*provozovatel – správce údajů, dotčená osoba – subjekt údajů, zprostředkovatel – zpracovatel* apod.). Dále přibyla část, která je věnovaná Úřadu pro ochranu osobních údajů, předání osobních údajů apod.

6.2. Postavení ČR v rámci právní normy zajišťující ochranu osobních údajů ve světě

[24]Organizace Privacy International vyhodnotila úroveň ochrany osobních údajů ve vybraných zemích světa a sestavila tabulku. Česká republika se zde řadí (koeficient 2,5) mezi státy, které mají formálně zabezpečenou ochranu osobních údajů v souladu s obecnou právní normou zajišťující ochranu osobních údajů, ovšem nedostatky vyplývají z nastavení ochrany osobních údajů ve speciálních zákonech. Předseda Úřadu pro ochranu osobních údajů Igor Němec ale průměrné umístění České republiky považuje za neuspokojivé. Na nedobrém výsledku se mj. podepsalo nadměrné množství odposlechů.

6.3. Závěr

Při zpracovávání mojí bakalářské práce jsem se snažila postupovat tak, aby konečný výsledek byl co nejlepší, analyzovat ochranu osobních údajů v právní úpravě i v praxi. Dle mého názoru se jedná o velmi složitý obor a nesmí se podceňovat. Při psaní práce jsem vycházela především ze Zákona o ochraně osobních údajů a z elektronických zdrojů publikovaných na Internetu.

Práce na tomto dokumentu byla pro mne velkým přínosem a v průběhu jeho zpracovávání jsem získala mnoho nových poznatků. Snažila jsem se nahlédnout na problematiku z právního i technického hlediska. Doufám, že tato práce byla alespoň minimálním přínosem k pochopení a řešení problematiky ochrany osobních údajů v informačním systému.

[24] Zdroj: Úřad pro ochranu osobních údajů. Dostupný z WWW: <http://www.uoou.cz>.

7. Literatura

7.1. Písemné zdroje publikované

7.1.1. Knihy

[1] BASL, Josef. *Podnikové informační systémy: Podnik v informační společnosti*. 144 s. ISBN 80-247-0424-2.

[2] BÉBR, Richard, DOUCEK, Petr. *Informační systémy pro podporu manažerské práce*. 1. vydání. Praha: Professional Publishing, 2005. 223 s.

[3] BOGUSZAK, Jiří, ČAPEK, Jiří a GERLOCH, Aleš. *Teorie práva*. 1. vydání. EUROLEX BOHEMIA, s. r. o., 2001. 323 s. ISBN: 80-86432-13-0.

[4] BOGUSZAK, Jiří, ČAPEK, Jiří a GERLOCH, Aleš. *Teorie práva*. 2. přeprac. vydání. ASPI Publishing, s. r. o, 2004. 324 s. ISBN: 80-86432-13-0.

[5] BUCHALCEVOVÁ, Alena. *Metodiky vývoje a údržby informačních systému*. 164 s. ISBN 80-247-1057-7.

[6] BRUCKNER, Tomáš, DOUCEK, Petr, SKLENÁK, Vilém. *Informační systémy v podniku: sylaby k přednáškám*. 1. vydání. Praha: Oeconomica, 2004. 74 s.

[7] CIBULKA, Karel, CIBULKOVÁ, Veronika. *Trestní právo*. 1. vydání. Institut vzdělávání SOKRATES, 2005. 182 s. ISBN 80-86572-21-8.

[8] D'AMBROSOVÁ, H. *Ochrana osobních údajů při vedení per. agend*. 1. vydání. PRAGOEDUCA, 2003. ISBN 80-7310-003-7.

[9] DOBDA, Luboš. *Ochrana dat v informačních systémech*. 1. vydání. Praha: Grada, 1998. 286 s.

[10] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. ISBN 80-25101-06-1.

[11] DOSEDĚL, Tomáš. *21 základních pravidel počítačové bezpečnosti*. Brno: Computer Press, 2005. 52 s. ISBN 80-251-0574-1.

[12] DVOŘÁK, Jiří, DVOŘÁK, Jiří. *Elektronický obchod: Studijní text pro kombinované studium*. 1. vydání. Brno: Ing. Zdeněk Novotný, CSc., 2004. 78 s. ISBN 80-214-2600-4.

[13] CHLAPEK, Dušan, ŘEPA, Václav a STANOVSKÁ, Iva. *Vývoj informačních systému: pracovní sešit ke cvičením*. 1. vydání. Praha: Oeconomica, 2005. 161 s.

[14] KASTL, Jan. *Informační a komunikační systémy*. 2. vydání. Praha: Oeconomica, 2005. 185 s.

[15] KNAPP, Viktor a kol. *Právo a informace*. 1. vydání. Praha: Academia, 1988. 289s.

[16] KRÁL, Mojmír. *Bezpečnost domácího počítače*. Grada. ISBN 80-247-1408-6.

[17] KUBÍK, Jaroslav, VACULÍK, Jan. *Informační systémy v ČSSR: Minimum pro práci s informacemi*. Praha: Novinář, 1988. 184 s.

[18] KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář.* 1. vydání. Praha : C.H. Beck, 2003. 388 s. ISBN 80-7179-762-6.

[19] LÁTAL, Ivo. *Ochrana informací dat v informačních systémech.* 1. vydání. Praha: Eurounion, 1996. 237 s.

[20] MATOUŠKOVÁ, Miroslava. *Ochrana osobních údajů: v otázkách a odpovědích*. ASPI Publishing, 2005. 157 s. ISBN 80-7357-037-8.

[21] MATOUŠKOVÁ, Miroslava, HEJLÍK, Ladislav. Osobní údaje a jejich ochrana. 1. vydání. ASPI Publishing, 2003. 416 s. ISBN 80-86395-50-2.

[22] MOLNÁR, Zdeněk. *Efektivnost informačních systému*.2. rozš. vydání. Praha: Grada, 2001. 179 s.

[23] NEJEDLÝ, Josef. *Ochrana osobních údajů*. 1. vydání. Vyškov: Irena Spirová, 2004. 155 s. ISBN 80-239-3896-7.

[24] POŽÁR, Josef. *Informační bezpečnost.* Vydavatelství a Nakladatelství Aleš Čeněk, s.r.o., 2005. 311 s. ISBN 80-86898-38-5.

[25] RODRYČOVÁ, Danuše, STAŠA, Pavel. *Bezpečnost informací: jako podmínka prosperity firmy*. GRADA Publishing, s.r.o. 144 s. SBN 80-7169-144-5.

[26] SOUKUP, Ladislav. *Prameny k dějinám práva v českých zemích*. Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2004. 36 s. ISBN 80-86898-04-0.

[27] ŠMÍD, Vladimír. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 227/2000 Sb., zákona č. 177/2001 Sb., zákona č. 450/2001 Sb., zákona č. 107/2002 Sb., zákona č. 310/2002 Sb., zákona č. 517/2002 Sb., zákona č. 439/2004 Sb., zákona č. 480/2004 Sb., zákona č. 626/2004 Sb., zákona č. 413/2005 Sb. a zákona č. 444/2005 Sb. – komentář.* Brno, 2005. Masarykova univerzita v Brně. 69 s.

[28] ŠMÍD, Vladimír. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů –komentář.* Brno, 2000. Masarykova univerzita v Brně. 30 s.

[29] VANÍČEK, Tomáš. *Informační systémy 22*. 1. vydání. Praha: Vydavatelství ČVUT, 2001. 133 s.

[30] VOŘÍŠEK, Jiří, Bankovní institut-vysoká škola. *Informační systémy a jejich řízení*. 1. vydání. Praha: Professional Publishing, 2005. 223 s.

[31] VRANA, Ivan, RICHTA, Karel. *Zásady a postupy zavádění podnikových informačních systémů*. 188 s. ISBN 80-247-1103-6.

7.1.2. Časopisy, noviny

[1] KARÁSEK, Petr. Ať je systém ERP propojen s kanceláří. *Hospodářské noviny: Komerční příloha deníku Hospodářské noviny*. 6.4.2006, s. 3.

[2] KOVÁŘ, Jaromír. Informační systémy a projektové řízení. *Hospodářské noviny: Komerční příloha deníku Hospodářské noviny*. 6.10.2006, s. 3.

[3] MATLIS, J. Ochrana vašeho soukromí. *Computerworld*, 2002, roč. 13, č. 43, s. 20. ISSN 1210-9924.

[4] ŠABATOVÁ, Ivana. Elektronický podpis / principy a použití. *Ekonom: Komerční příloha týdeníku Ekonom*. 2005, č. 45, s. 2-4.

[5] TAX, Martin. Znalostní nebo jen informační systém? *Komerční příloha deníku Hospodářské noviny*. 26.4.2006, s. 1-3.

[6] TILL, M. Ochrana osobních údajů na webu. *Computerworld*. 2002, roč. 13, č. 24, s. 23. ISSN 1210-9924.

[7] Stručná historie systémů ERP. *Hospodářské noviny: Komerční příloha deníku Hospodářské noviny*. 26.4.2006, s. 4.

[8] Variabilita výrobního systému v rámci ERP. *Hospodářské noviny: Komerční příloha deníku Hospodářské noviny*. 6.10.2006, s. 6.

7.1.3. Zákony a vyhlášky

[1] Zákon č. 101/2000/Sb., o ochraně osobních údajů a o změně některých zákonů

[2] Zákon č. 106/1999/Sb., o svobodném přístupu k informacím

[3] Zákon č. 140/1961/Sb., trestní zákon

[4] Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

7.1.4. Firemní materiály

[1] FARSKÝ, Martin. *Anet-Time: manuál k docházkovému systému.* Brno: Anet-Advanced Network Technology s.r.o., 2002. 153 s.

[2] Nugget SW spol. s r.o., Praha. *Provozní dokumentace: Popis základní konfigurace, nastavení a řešení nestandardních provozních situací*. Praha: Nugget SW spol. s r.o., 2003. 25 s.

[3] Nugget SW spol. s r.o., Praha. *MZDY/CS, PERST/CS, LZ/CS*. Praha: Nugget SW spol. s r.o., 2003. 18 s.

[4] Nugget SW spol. s r.o., Praha. Personalistika: Komplexní zpracování personální agendy. Praha: Nugget SW spol. s r.o., 2003. 104 s.

[5] Nugget SW spol. s r.o., Praha. MZDY/CS: Komplexní zpracování mezd pro WINDOWS NT. Praha: Nugget SW spol. s r.o., 2003. 170 s.

[6] Synthon, s.r.o., Blansko. *Standardní operační postupy (SOP) společnosti Synthon,* 2006.

7.2. Internetové adresy

[1] HUJER, Petr. Používáte bezpečná hesla?. *LUPA: Používáte bezpečná hesla?* [online]. Poslední aktualizace 01.06. 2000. Dostupný z WWW: <http://www.lupa.cz/clanky/pouzivate-bezpecna-hesla/>.

[2] JANKŮ, Anna. Jak přistupovat k implementaci ERP systému z pohledu zákazníka a z pohledu dodavatele. *Zpravodajský portál časopisu IT Systems* [online]. Poslední aktualizace 10.10.2002. Dostupný z WWW: <http:// www.systemonline.cz/site/prehledy_systemu/erp/implem2.htm>.

[3] KOCAN, Marek. Bezpečná data? *Databázový svět: informační portál ze světa databázových technologií* [online]. Poslední aktualizace 15.01.2004. Dostupný

z WWW: <http://www.dbsvet.cz/view.php?cisloclanku=2004011501>.

[4] KOCAN, Marek. Co vlastně je informační systém a jak souvisí s řízením?. *Živě.cz: Co vlastně je informační systém a jak souvisí s řízením?* [online]. [cit. 2007-05-01]. Dostupný z WWW: <http://www.zive.cz/h/Programovani/ARI=3436>.

[5] LUDVÍK, Jiří. Proč se zajímat o zákon o ochraně osobních údajů? *LUPA: Proč se zajímat o zákon o ochraně osobních údajů?*. Poslední aktualizace 20.6.2000. Dostupný z WWW: <http://www.lupa.cz/clanky/proc-se-zajimat-o-zakon-o-ochrane-osobnich-udaju-cast-1/>.

[6] LUDVÍK, Jiří. Proč se zajímat o zákon o ochraně osobních údajů? *LUPA: Proč se zajímat o zákon o ochraně osobních údajů?*. Poslední aktualizace 3.7.2000. Dostupný z WWW: <http://www.lupa.cz/clanky/proc-se-zajimat-o-zakon-o-ochrane-osobnich-udaju-cast-2/>.

[7] KUČEROVÁ, Helena. Ochrana osobních údajů. *Ochrana osobních údajů* [online]. Dostupný z WWW: <http://vydavatelstvi.vscht.cz/knihy/uid_es-005/hesla/ochrana_osobnIch_UdajV.html>.

[8] MARIANOVÁ, Lenka, HEJLOVÁ, Pavla. Osobní údaje - tajemství nebo přítěž? *iLIST.cz: Osobní údaje – tajemství nebo přítěž?* [online]. Poslední aktualizace 4.9.2006. Dostupný z WWW: <http://www.ilist.cz/clanky/osobni-udaje-tajemstvi-nebo-pritez>.

[9] RYBÁK, Jan. Tajemství kryptografie: referát do programování. *Referát do Programování – Kryptografie, hashování, RSA, soukromý a veřejný klíč, digitální podpis* [online]. Dostupný z WWW: <http://kryptografie.web-idea.net/index.php?id=uvod>.

[10] POKORNÝ, Martin. Vyvíjíme databázový a informační systém I. *Databázový svět: informační portál ze světa databázových technologií* [online]. Poslední aktualizace 05. 05. 2004. [cit. 2007-05-02]. Dostupný z WWW: <http://www.dbsvet.cz/view.php?cisloclanku=2004050501>.

[11] SKLENÁŘ, Pavel. Co znamená ERP?: (úvod do problematiky). *E-komerce.cz: business na internetu* [online]. Poslední aktualizace 12.3.2002. Dostupný z WWW: <http://www.e-komerce.cz/ec/ec.nsf/0/ BB3C13DB9522519AC1256B79003104F2>.

[12] ŠALAMOUN, Michal. Ochrana osobních údajů v teorii i praxi. *Ochrana osobních údajů* [online]. [cit. 2007-04-24]. Dostupný z WWW: <http://www.oou.cz/index.php?file=nastroje_k_ochrane_osobnich_dat_kniha>.

[13] TOŠNER, Daniel. Nad oprávněním zpracovávat osobní údaje. *IT právo : server o internetovém a počítačovém právu* [online]. Poslední aktualizace 28.10.2003. Dostupný z WWW: < http://www.itpravo.cz/index.shtml?x=142872>.

[14] VRŠEK, Petr, ČERMÁK, J. Moderní databázové systémy a ochrana osobních údajů. *IT právo : server o internetovém a počítačovém právu* [online]. Poslední aktualizace 11.2.2002. Dostupný z WWW: <http://www.itpravo.cz/index.shtml?x=63674>.

[15] Kryptografie. *Wikipedie: otevřená encyklopedie* [online]. Dostupný z WWW: < http://cs.wikipedia.org/wiki/Kryptografie#Z.C3.A1kladn.C3.AD_pojmy >.

[16] Ochrana dat za 1. republiky. *Právní ochrana osobních údajů za I. republiky* [online]. [cit. 2007-05-05]. Dostupný z WWW: <http://www.czso.cz/sldb/sldb.nsf/i/ochrana_dat_za_1_republiky>.

[16] Ochrana osobních údajů. *Wikimedia Foundation* [online]. Dostupný z WWW: <http://wikimediafoundation.org/wiki/Ochrana_osobn%C3%ADch_%C3%BAdaj%C5%AF>.

[17] Ochrana osobních údajů. *Proč se zabývat ochranou osobních údajů?*[online]. [cit. 2007-05-05]. Dostupný z WWW: <http://www.oou.cz/index.php?file=ochra--na_dat_proc_chranit_osobni_udaje>.

[18] Ochrana osobních údajů - v podmínkách malých a středních organizací. *Pro IT: ochrana_oo* [online]. Dostupný z WWW: <http://www.proit.cz/cz/ochranaoo.php >.

[19] Šifrování. *Web 4 company: Šifrování* [online]. Dostupný z WWW: <http://www.web4company.cz/bezpecnost/sifrovani/tabid/106/Default.aspx>.

[20] Úřad pro ochranu osobních údajů [online]. [cit. 2007-04-24]. Dostupný z WWW: <www.uoou.cz/zpravodaj/bulletin_2000_02.pdf>.

[21] Zákon o svobodném přístupu k informacím. *EPRAVO.CZ - zákony, judikatura, komentáře, právní předpisy, poradna* [online]. Poslední aktualizace 19.5.2004. Dostupný z WWW: <http://www.epravo.cz/v01/index.php3?s1=Y&s2=6&s3=1&s4=0&s5=0&s6=0&m=1&typ=predpisy&recid_zak=1547>.

[22] Šifrovací metody. *I.CA – Teorie symetrické a asymetrické kryptografie*. [online]. [cit. 2007-05-03]. Dostupný z WWW: < http://www.ica.cz/home_cs/?acc=teorie_symetricke_a_asymetricke_kryptografie >.

8. Seznam použitých obrázků

9. Seznam použitých zkratek

10. Seznam použitých cizích slov

11. Seznam příloh

Příloha č. 1: Grafy souvislostí do úrovně (obrázek)

Příloha č. 2: Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (text)

Příloha č. 3: Zákon o ochraně osobních údajů v informačních systémech (text)

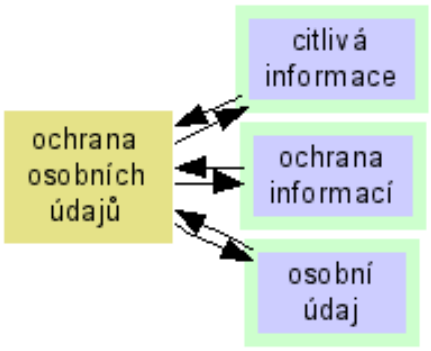
Příloha č. 4: Zákon o svobodném přístupu k informacím (text)

Příloha č. 5: Výňatek ze zákona č. 140/1961 Sb., trestní zákon (text)

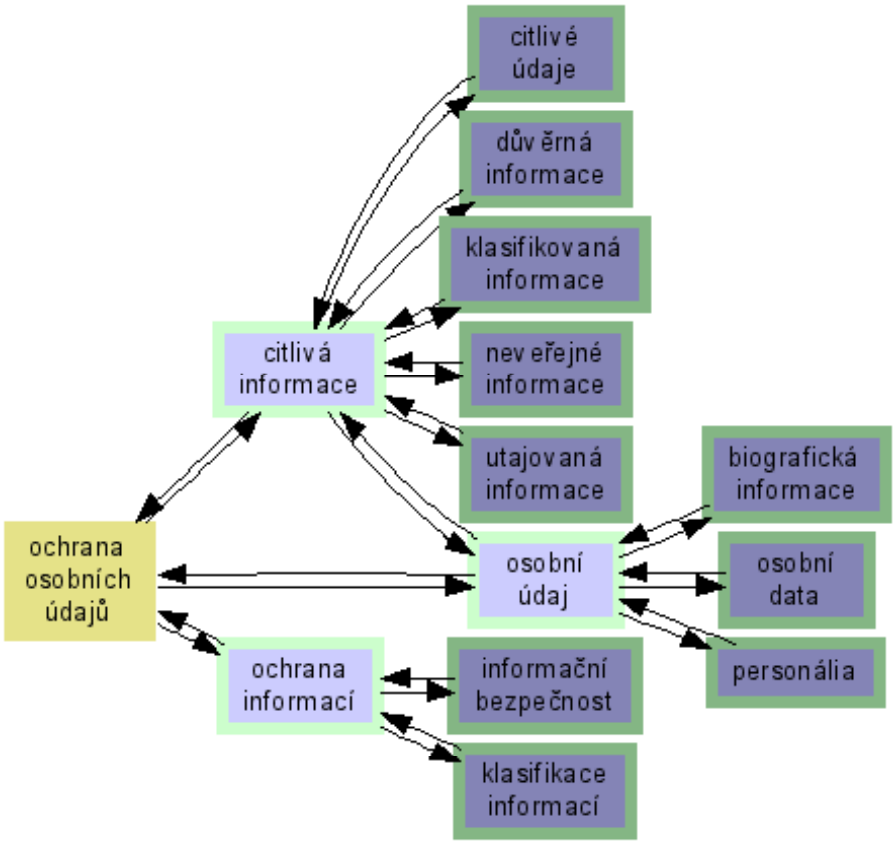
12. Přílohy

Příloha č. 1

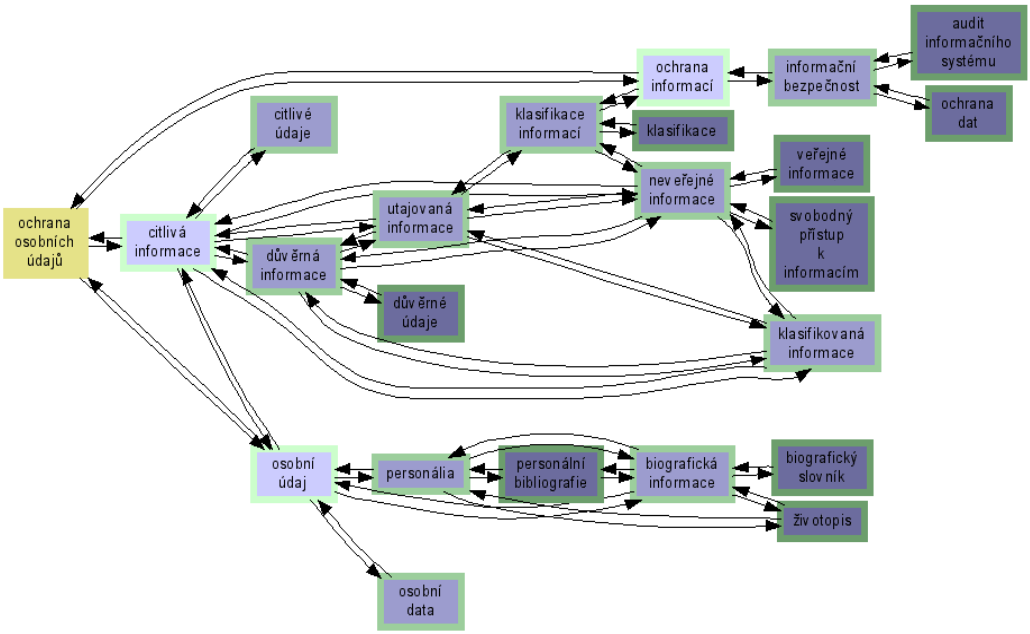
I. úroveň



II. úroveň



III. úroveň


audit informačního systému
ochrana informací
informační bezpečnost
ochrana dat
citlivé údaje
klasifikace informací
klasifikace
veřejné informace
neveřejné informace
ochrana osobních údajů
citlivá informace
utajovaná informace
svobodný přístup k informacím
důvěrná informace
důvěrné údaje
klasifikovaná informace
osobní údaj
personália
personální bibliografie
biografická informace
biografický slovník
životopis
osobní data

Příloha č. 2

101/2000 Sb.

ZÁKON

ze dne 4. dubna 2000

o ochraně osobních údajů a o změně některých zákonů

ve znění zákona č. 227/2000 Sb., zákona č. 177/2001 Sb., zákona č. 450/2001 Sb., zákona č. 107/2002 Sb., zákona č. 310/2002 Sb., zákona č. 517/2002 Sb., zákona č. 439/2004 Sb., zákona č. 480/2004 Sb., zákona č. 626/2004 Sb., zákona č. 413/2005 Sb., zákona č. 444/2005 Sb., zákona č. 109/2006 Sb., zákona č. 112/2006 Sb. a zákona č. 342/2006 Sb.

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

OCHRANA OSOBNÍCH ÚDAJŮ

HLAVA I

ÚVODNÍ USTANOVENÍ

§ 1

Předmět úpravy

Tento zákon v souladu s právem Evropských společenství, 1) mezinárodními smlouvami, kterými je Česká republika vázána, 1a) a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.

§ 2

(1) Zřizuje se Úřad pro ochranu osobních údajů se sídlem v Praze (dále jen „Úřad").

(2) Úřadu jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem a další kompetence stanovené zvláštním právním předpisem. 1)

§ 3

Působnost zákona

(1) Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.

(2) Tento zákon se vztahuje na veškeré zpracovávání osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky.

(3) Tento zákon se nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu.

(4) Tento zákon se nevztahuje na nahodilé shromažďování osobních údajů, pokud tyto údaje nejsou dále zpracovávány.

(5) Tento zákon se dále vztahuje na zpracování osobních údajů,
a) jestliže se právní řád České republiky použije přednostně na základě mezinárodního práva veřejného, i když správce není usazen na území České republiky,

b) jestliže správce, který je usazen mimo území Evropské unie, provádí zpracování na území České republiky a nejedná se pouze o předání osobních údajů přes území Evropské unie; v tomto případě je správce povinen zmocnit postupem podle § 6 na území České republiky zpracovatele.
Jestliže zpracování provádí správce prostřednictvím svých organizačních jednotek umístěných na území Evropské unie, musí zajistit, že tyto organizační jednotky budou zpracovávat osobní údaje v souladu s národním právem příslušného členského státu Evropské unie.

(6) Ustanovení § 5 odst. 1 a § 11 a 12 se nepoužijí pro zpracování osobních údajů nezbytných pro plnění povinností správce stanovených zvláštními zákony pro zajištění

a) bezpečnosti České republiky, 4)

b) obrany České republiky, 5)

c) veřejného pořádku a vnitřní bezpečnosti, 6)

d) předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů, 7)

e) významného hospodářského zájmu České republiky nebo Evropské unie, 8)

f) významného finančního zájmu České republiky nebo Evropské unie, kterým je zejména stabilita finančního trhu a měny, fungování peněžního oběhu a platebního styku, jakož i rozpočtová a daňová opatření, 9)

g) výkonu kontroly, dozoru, dohledu a regulace spojených s výkonem veřejné moci v případech uvedených v písmenech c), d), e) a f), 10) nebo

h) činností spojených se zpřístupňováním svazků bývalé Státní bezpečnosti. 10a)

§ 4

Vymezení pojmů

Pro účely tohoto zákona se rozumí

a) osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu,

b) citlivým údajem osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů,

c) anonymním údajem takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů,

d) subjektem údajů fyzická osoba, k níž se osobní údaje vztahují,

e) zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,

f) shromažďováním osobních údajů systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování,

g) uchováváním osobních údajů udržování údajů v takové podobě, která je umožňuje dále zpracovávat,

h) blokováním osobních údajů vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej jinak zpracovávat,

i) likvidací osobních údajů se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování,

j) správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak,

k) zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona,

l) zveřejněným osobním údajem osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu,

m) evidencí nebo datovým souborem osobních údajů (dále jen „datový soubor") jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií,

n) souhlasem subjektu údajů svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů,

o) příjemcem každý subjekt, kterému jsou osobní údaje zpřístupněny; za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g).

HLAVA II

PRÁVA A POVINNOSTI PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

§ 5

(1) Správce je povinen

a) stanovit účel, k němuž mají být osobní údaje zpracovány,

b) stanovit prostředky a způsob zpracování osobních údajů,

c) zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje. Nepřesné osobní údaje lze zpracovat pouze v mezích uvedených v § 3 odst. 6. 11) Nepřesné osobní údaje se musí označit. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem příjemcům,

d) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,

e) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické

služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné,

f) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6, nebo pokud k tomu dal subjekt údajů předem souhlas,

g) shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti,

h) nesdružovat osobní údaje, které byly získány k rozdílným účelům.

(2) Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce, 12)

b) jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,

c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,

d) jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem. 13) Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů,

e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,

f) pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení, nebo,

g) jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona.

(3) Provádí-li správce zpracování osobních údajů na základě zvláštního zákona, 12) je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů.

(4) Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování.

(5) Provádí-li správce nebo zpracovatel zpracování osobních údajů za účelem nabízení obchodu nebo služeb subjektu údajů, lze pro tento účel použít jméno, příjmení a adresu subjektu údajů, pokud tyto údaje byly získány z veřejného seznamu nebo v souvislosti se svojí činností jakožto správce nebo zpracovatele. Správce nebo zpracovatel však nesmí uvedené údaje dále zpracovávat, pokud s tím subjekt údajů vyslovil nesouhlas. Nesouhlas se zpracováním je nutné vyjádřit písemně. Bez souhlasu subjektu údajů nelze k uvedeným údajům přiřazovat další osobní údaje.

(6) Správce, který zpracovává osobní údaje podle odstavce 5, může tyto údaje předat jinému správci pouze za splnění těchto podmínek:
a) údaje subjektu údajů byly získány v souvislosti s činností správce nebo se jedná o zveřejněné osobní údaje,

b) údaje budou využívány pouze za účelem nabízení obchodu a služeb,

c) subjekt údajů byl o tomto postupu správce předem informován a nevyslovil s tímto postupem nesouhlas.

(7) Jiný správce, kterému byly předány údaje podle odstavce 6, nesmí tyto údaje předávat jiné osobě.

(8) Nesouhlas se zpracováním podle odstavce 6 písm. c) musí subjekt údajů učinit písemně. Správce je povinen informovat každého správce, kterému předal jméno, příjmení a adresu subjektu údajů, o tom, že subjekt údajů vyslovil nesouhlas se zpracováním.

(9) Za účelem vyloučení možnosti, že jméno, příjmení a adresa subjektu údajů budou opakovaně použity k nabídce obchodu a služeb, je správce oprávněn dále zpracovávat pro svoji vlastní potřebu jméno, příjmení a adresu subjektu údajů přesto, že subjekt údajů vyslovil nesouhlas podle odstavce 5.

§ 6

Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.

§ 7

Povinnosti stanovené v § 5 platí obdobně také pro zpracovatele.

§ 8

Jestliže zpracovatel zjistí, že správce porušuje povinnosti stanovené tímto zákonem, je povinen jej na to neprodleně upozornit a ukončit zpracování osobních údajů. Pokud tak neučiní, odpovídá za škodu, která subjektu údajů vznikla, společně a nerozdílně se správcem údajů. Tím není dotčena jeho odpovědnost podle tohoto zákona.

§ 9

Citlivé údaje

Citlivé údaje je možné zpracovávat, jen jestliže

a) subjekt údajů dal ke zpracování výslovný souhlas. Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Existenci souhlasu subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování. Správce je povinen předem subjekt údajů poučit o jeho právech podle § 12 a 21,

b) je to nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku, pokud není možno jeho souhlas získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je nezvěstný nebo z jiných podobných důvodů. Správce musí ukončit zpracování údajů, jakmile pominou uvedené důvody, a údaje musí zlikvidovat, ledaže by subjekt údajů dal k dalšímu zpracování souhlas,

c) se jedná o zpracování při zajišťování zdravotní péče, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví podle zvláštního zákona 15) nebo se jedná o posuzování zdravotního stavu v jiných případech stanovených zvláštním zákonem, 15a)

d) je zpracování nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem, 16)

e) jde o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti občanského sdružení, nadace nebo jiné právnické osoby nevýdělečné povahy (dále jen „sdružení"), a které se týká pouze členů sdružení nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů,

f) se jedná o údaje podle zvláštního zákona nezbytné pro provádění nemocenského pojištění, důchodového pojištění (zabezpečení), státní sociální podpory a dalších státních sociálních dávek, sociálních služeb, sociální péče, pomoci v hmotné nouzi a sociálně-právní ochrany dětí, a při zajištění ochrany těchto údajů v souladu se zákonem,

g) se zpracování týká osobních údajů zveřejněných subjektem údajů,

h) je zpracování nezbytné pro zajištění a uplatnění právních nároků, nebo

ch) jsou zpracovány výlučně pro účely archivnictví podle zvláštního zákona.

§ 10

Při zpracování osobních údajů správce a zpracovatel dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

§ 11

(1) Správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21.

(2) V případě, kdy správce zpracovává osobní údaje získané od subjektu údajů, musí subjekt údajů poučit o tom, zda je poskytnutí osobního údaje povinné či dobrovolné. Je-li subjekt údajů povinen podle zvláštního zákona osobní údaje pro zpracování poskytnout, poučí jej správce o této skutečnosti, jakož i o následcích odmítnutí poskytnutí osobních údajů.

(3) Informace a poučení podle odstavce 1 není povinen správce poskytovat v případech, kdy osobní údaje nezískal od subjektu údajů, pokud
a) zpracovává osobní údaje výlučně pro účely výkonu státní statistické služby, vědecké nebo archivní účely a poskytnutí takových informací by vyžadovalo neúměrné úsilí nebo nepřiměřeně vysoké náklady; nebo pokud ukládání na nosiče

informací nebo zpřístupnění je výslovně stanoveno zvláštním zákonem. V těchto případech je správce povinen přijmout potřebná opatření proti neoprávněnému zasahování do soukromého a osobního života subjektu údajů,

b) zpracování osobních údajů mu ukládá zvláštní zákon nebo je takových údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštních zákonů,

c) zpracovává výlučně oprávněně zveřejněné osobní údaje, nebo

d) zpracovává osobní údaje získané se souhlasem subjektu údajů.

(4) Předchozími ustanoveními nejsou dotčena práva subjektu údajů požadovat informace podle zvláštních zákonů. 18)

(5) Při zpracování osobních údajů podle § 5 odst. 2 písm. e) a § 9 písm. h) je správce povinen bez zbytečného odkladu subjekt údajů informovat o zpracování jeho osobních údajů.

(6) Žádné rozhodnutí správce nebo zpracovatele, jehož důsledkem je zásah do právních a právem chráněných zájmů subjektu údajů, nelze bez ověření vydat nebo učinit výlučně na základě automatizovaného zpracování osobních údajů. To neplatí v případě, že takové rozhodnutí bylo učiněno ve prospěch subjektu údajů a na jeho žádost.

(7) Informační povinnost upravenou v § 11 může za správce plnit zpracovatel.

§ 12

Přístup subjektu údajů k informacím

(1) Požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.

(2) Obsahem informace je vždy sdělení o
a) účelu zpracování osobních údajů,

b) osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování, včetně veškerých dostupných informací o jejich zdroji,

c) povaze automatizovaného zpracování v souvislosti s jeho využitím pro rozhodování, jestliže jsou na základě tohoto zpracování činěny úkony nebo rozhodnutí, jejichž obsahem je zásah do práva a oprávněných zájmů subjektu údajů,

d) příjemci, případně kategoriích příjemců.

(3) Správce má právo za poskytnutí informace požadovat přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace.

(4) Povinnost správce poskytnout informace subjektu údajů upravenou v § 12 může za správce plnit zpracovatel.

Povinnosti osob při zabezpečení osobních údajů

§ 13

(1) Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

(2) Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

§ 14

Zaměstnanci správce nebo zpracovatele a jiné osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném.

§ 15

(1) Zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.

(2) Ustanovením předchozího odstavce není dotčena povinnost zachovávat mlčenlivost podle zvláštních zákonů. 19)

(3) Povinnost zachovávat mlčenlivost se nevztahuje na informační povinnost podle zvláštních zákonů. 20)

§ 16

Oznamovací povinnost

(1) Ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle tohoto zákona, s výjimkou zpracování uvedených v § 18, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováváním osobních údajů.

(2) Oznámení musí obsahovat tyto informace:
a) identifikační údaje správce, u fyzické osoby, která není podnikatelem, jméno, popřípadě jména, příjmení, datum narození a adresu místa trvalého pobytu, u jiných subjektů obchodní firmu nebo název, sídlo a identifikační číslo, pokud bylo přiděleno, a jméno, popřípadě jména, a příjmení osob, které jsou jejich statutárními zástupci,

b) účel nebo účely zpracování,

c) kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají,

d) zdroje osobních údajů,

e) popis způsobu zpracování osobních údajů,

f) místo nebo místa zpracování osobních údajů,

g) příjemce nebo kategorie příjemců,

h) předpokládaná předání osobních údajů do jiných států,

i) popis opatření k zajištění ochrany osobních údajů podle § 13.

(3) Obsahuje-li oznámení všechny náležitosti podle odstavce 2 a není-li zahájeno řízení podle § 17 odst. 1, lze po uplynutí lhůty 30 dnů ode dne doručení oznámení zahájit zpracování osobních údajů. Úřad v takovém případě zapíše informace uvedené v oznámení do registru.

(4) Neobsahuje-li oznámení všechny náležitosti podle odstavce 2, Úřad neprodleně zašle oznamovateli výzvu, v níž upozorní na chybějící nebo nedostatečné informace a stanoví lhůtu k doplnění oznámení. V případě doplnění oznámení začíná běžet lhůta podle odstavce 3 dnem doručení doplnění oznámení. V případě, že Úřad neobdrží doplnění oznámení ve stanovené lhůtě, nahlíží na učiněné oznámení tak, jako by nebylo podáno.

(5) O provedení registrace vydá Úřad na žádost správce osvědčení, které obsahuje datum vyhotovení, číslo jednací, jméno, příjmení a podpis osoby, která osvědčení vydala, otisk úředního razítka, identifikační údaje správce a účel zpracování.

(6) Na postup Úřadu podle odstavců 1 až 5 se nevztahuje správní řád.

§ 17

(1) Vznikne-li z oznámení důvodná obava, že při zpracování osobních údajů by mohlo dojít k porušení tohoto zákona, zahájí Úřad z vlastního podnětu řízení.

(2) Zjistí-li Úřad, že oznámeným zpracováním neporušuje správce podmínky stanovené tímto zákonem, řízení zastaví a provede zápis podle § 16 odst. 3. Nejdříve dnem následujícím po provedení zápisu lze zahájit zpracování osobních údajů. V

případě, že oznámené zpracování nesplňuje podmínky stanovené tímto zákonem, zpracování osobních údajů Úřad nepovolí.

§ 17a

(1) Zjistí-li Úřad, že správce, jehož oznámení bylo zapsáno do registru, porušuje podmínky stanovené tímto zákonem, rozhodne o zrušení registrace.

(2) Pomine-li účel, pro který bylo zpracování zaregistrováno, Úřad z vlastního podnětu nebo na žádost správce rozhodne o zrušení registrace.

§ 18

(1) Oznamovací povinnost podle § 16 se nevztahuje na zpracování osobních údajů,
a) které jsou součástí datových souborů veřejně přístupných na základě zvláštního zákona,

b) které správci ukládá zvláštní zákon nebo je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona, nebo

c) jde-li o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti sdružení, a které se týká pouze členů sdružení, nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů.

(2) Správce, který provádí zpracování podle § 18 odst. 1 písm. b), je povinen zajistit, aby informace, týkající se zejména účelu zpracování, kategorií osobních údajů, kategorií subjektů údajů, kategorií příjemců a doby uchování, které by byly jinak přístupné prostřednictvím registru vedeného Úřadem podle § 35, byly zpřístupněny, a to i dálkovým přístupem nebo jinou vhodnou formou.

§ 19

Jestliže správce hodlá ukončit svoji činnost, je povinen Úřadu neprodleně oznámit, jak naložil s osobními

údaji, pokud se na jejich zpracování vztahuje oznamovací povinnost.

§ 20

Likvidace osobních údajů

(1) Správce nebo na základě jeho pokynu zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti subjektu údajů podle § 21.

(2) Zvláštní zákon stanoví výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.

Ochrana práv subjektů údajů

§ 21

(1) Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může
a) požádat správce nebo zpracovatele o vysvětlení,

b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.

(2) Je-li žádost subjektu údajů podle odstavce 1 shledána oprávněnou, správce nebo zpracovatel odstraní neprodleně závadný stav.

(3) Nevyhoví-li správce nebo zpracovatel žádosti subjektu údajů podle odstavce 1, má subjekt údajů právo obrátit se přímo na Úřad.

(4) Postup podle odstavce 1 nevylučuje, aby se subjekt údajů obrátil se svým podnětem na Úřad přímo.

(5) Pokud vznikla v důsledku zpracování osobních údajů subjektu údajů jiná než majetková újma, postupuje se při uplatňování jejího nároku podle zvláštního zákona. 22)

(6) Došlo-li při zpracování osobních údajů k porušení povinností uložených zákonem u správce nebo u zpracovatele, odpovídají za ně společně a nerozdílně.

(7) Správce je povinen bez zbytečného odkladu informovat příjemce o žádosti subjektu údajů podle odstavce 1 a o blokování, opravě, doplnění nebo likvidaci osobních údajů. To neplatí, pokud je informování příjemce nemožné nebo by vyžadovalo neúměrné úsilí.

§ 22

zrušen

§ 23

zrušen

§ 24

zrušen

§ 25

Náhrada škody

V otázkách neupravených tímto zákonem se použije obecná úprava odpovědnosti za škodu. 23) , 24)

§ 26

Povinnosti podle § 21 až 25 se obdobně vztahují i na osoby, které shromáždily osobní údaje neoprávněně.

HLAVA III

PŘEDÁNÍ OSOBNÍCH ÚDAJŮ DO JINÝCH STÁTŮ

§ 27

(1) Volný pohyb osobních údajů nemůže být omezován, pokud jsou údaje předány do členského státu Evropské unie.

(2) Do třetích zemí mohou být osobní údaje předány, pokud zákaz omezování volného pohybu osobních údajů vyplývá z mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas, a kterou je Česká republika vázána, 1a) nebo jsou osobní údaje předány na základě rozhodnutí orgánu Evropské unie. Informace o těchto rozhodnutích zveřejňuje Úřad ve Věstníku.

(3) Není-li podmínka podle odstavců 1 a 2 splněna, může být předání osobních údajů uskutečněno, jestliže správce prokáže, že
a) předání údajů se děje se souhlasem nebo na základě pokynu subjektu údajů,

b) jsou v třetí zemi, kde mají být osobní údaje zpracovány, vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, například prostřednictvím jiných právních nebo profesních předpisů a bezpečnostních opatření. Takové záruky mohou být upřesněny zejména smlouvou uzavřenou mezi správcem a příjemcem, pokud tato smlouva zajišťuje uplatnění těchto požadavků nebo pokud smlouva obsahuje smluvní doložky pro předání osobních údajů do třetích zemí zveřejněné ve Věstníku Úřadu,

c) jde o osobní údaje, které jsou na základě zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem; v takovém případě lze osobní údaje zpřístupnit jen v rozsahu a za podmínek stanovených zvláštním zákonem,

d) je předání nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo z mezinárodní smlouvy, kterou je Česká republika vázána,

e) je předání nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů,

f) je předání nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou, nebo pro

uplatnění jiných právních nároků, nebo

g) je předání nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů, zejména pro záchranu života nebo pro poskytnutí zdravotní péče.

(4) Před předáním osobních údajů do třetích zemí podle odstavce 3 je správce povinen požádat Úřad o povolení k předání, nestanoví-li zvláštní zákon jinak. 25) Při posuzování žádosti Úřad přezkoumá všechny okolnosti související s předáním osobních údajů, zejména zdroj, konečné určení a kategorie předávaných osobních údajů, účel a dobu zpracování, s přihlédnutím k dostupným informacím o právních nebo jiných předpisech upravujících zpracování osobních údajů ve třetí zemi. V povolení k předání Úřad stanoví dobu, po kterou může správce předání provádět. Pokud dojde ke změně podmínek, za kterých bylo povolení vydáno, zejména na základě rozhodnutí orgánu Evropské unie, Úřad toto povolení změní nebo zruší.

HLAVA IV

POSTAVENÍ A PŮSOBNOST ÚŘADU

§ 28

(1) Úřad je nezávislý orgán. Ve své činnosti postupuje nezávisle a řídí se pouze zákony a jinými právními předpisy.

(2) Do činnosti Úřadu lze zasahovat jen na základě zákona.

(3) Činnost Úřadu je hrazena ze samostatné kapitoly státního rozpočtu České republiky.

§ 29

(1) Úřad

a) provádí dozor nad dodržováním povinností stanovených tímto zákonem,

b) vede registr zpracování osobních údajů,

c) přijímá podněty a stížnosti na porušení tohoto zákona a informuje o jejich vyřízení,

d) zpracovává a veřejnosti zpřístupňuje výroční zprávu o své činnosti,

e) vykonává další působnosti stanovené mu zákonem,

f) projednává přestupky a jiné správní delikty a uděluje pokuty podle tohoto zákona,

g) zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána,

h) poskytuje konzultace v oblasti ochrany osobních údajů,

i) spolupracuje s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů. Úřad v souladu s právem Evropských společenství plní oznamovací povinnost vůči orgánům Evropské unie. 25a)

(2) Při výkonu dozoru ve formě kontroly se postupuje podle zvláštního právního předpisu. 26)

(3) Dozor nad zpracováním osobních údajů, které provádějí zpravodajské služby, stanoví zvláštní právní předpis. 27)

§ 29a

(1) Ministerstvo vnitra, krajské úřady a úřady obcí s rozšířenou působností poskytují Úřadu pro výkon působnosti stanovené tímto zákonem a dalšími právními předpisy na základě žádosti Úřadu z informačního systému evidence obyvatel údaje o obyvatelích; obyvatelem se rozumí fyzická osoba podle zvláštního právního předpisu 3) .

(2) Poskytovanými údaji podle odstavce 1 jsou údaje o

a) státních občanech České republiky 4)
1. jméno, popřípadě jména, příjmení, popřípadě rodné příjmení,

2. datum narození,
3. adresa místa trvalého pobytu, včetně předchozích adres místa trvalého pobytu,
4. počátek trvalého pobytu, popřípadě datum zrušení trvalého pobytu nebo datum ukončení trvalého pobytu na území České republiky,

b) cizincích, kteří jsou obyvateli
1. jméno, popřípadě jména, příjmení, popřípadě rodné příjmení,
2. datum narození,
3. druh a adresa místa pobytu,
4. číslo a platnost povolení k pobytu,
5. počátek pobytu, popřípadě datum ukončení pobytu.

(3) Z poskytovaných údajů lze v konkrétním případě použít vždy jen takové údaje, které jsou nezbytné ke splnění daného úkolu.

HLAVA V

ORGANIZACE ÚŘADU

§ 30

(1) Zaměstnanci Úřadu jsou předseda, inspektoři a další zaměstnanci.

(2) Kontrolní činnost Úřadu provádějí inspektoři a pověření zaměstnanci (dále jen „kontrolující").

(3) Na zaměstnance Úřadu se vztahují ustanovení zákoníku práce , pokud tento zákon nestanoví jinak.

(4) Předseda Úřadu má nárok na plat, náhradu výdajů a naturální plnění jako prezident Nejvyššího kontrolního úřadu podle zvláštního zákona. 26a)

(5) Inspektoři Úřadu mají nárok na plat, náhradu výdajů a naturální plnění jako členové Nejvyššího kontrolního úřadu podle zvláštního zákona. 26a)

(6) Platové poměry zaměstnanců Úřadu, s výjimkou

předsedy a inspektorů se řídí právními předpisy upravujícími platové poměry zaměstnanců orgánů státní správy. 28)

(7) Zaměstnancům Úřadu, s výjimkou předsedy a inspektorů přísluší náhrada cestovních výdajů podle zvláštního právního předpisu. 29)

§ 31

Kontrolní činnost Úřadu se provádí na základě kontrolního plánu nebo na základě podnětů a stížností.

§ 32

Předseda Úřadu

(1) Úřad řídí předseda, kterého jmenuje a odvolává prezident republiky na návrh Senátu Parlamentu České republiky.

(2) Předseda Úřadu je jmenován na dobu 5 let. Může být jmenován maximálně na 2 po sobě jdoucí období.

(3) Předsedou Úřadu může být jmenován pouze občan České republiky, který
a) je způsobilý k právním úkonům,

b) je bezúhonný, splňuje podmínky stanovené zvláštním právním předpisem 30) a jeho znalosti, zkušenosti a morální vlastnosti jsou předpokladem, že bude svoji funkci řádně zastávat,

c) má ukončené vysokoškolské vzdělání.

(4) Bezúhonnou je pro účel tohoto zákona fyzická osoba, která nebyla pravomocně odsouzena pro úmyslný trestný čin nebo i trestný čin spáchaný z nedbalosti v souvislosti se zpracováním osobních údajů.

(5) S výkonem funkce předsedy Úřadu je neslučitelná funkce poslance nebo senátora, soudce, státního zástupce, jakákoliv funkce ve veřejné správě, funkce člena orgánů územní samosprávy a členství v politických stranách a hnutích.

(6) Předseda Úřadu nesmí zastávat jinou placenou funkci, být v dalším pracovním poměru ani vykonávat výdělečnou činnost s výjimkou správy vlastního majetku a činnosti vědecké, pedagogické, literární, publicistické a umělecké, pokud tato činnost nenarušuje důstojnost nebo neohrožuje důvěru v nezávislost a nestrannost Úřadu.

(7) Z funkce je předseda Úřadu odvolán, přestal-li splňovat některou z podmínek pro jeho jmenování.

(8) Z funkce může být předseda odvolán také tehdy, jestliže nevykonává po dobu 6 měsíců svoji funkci.

Inspektoři Úřadu

§ 33

(1) Inspektora jmenuje a odvolává prezident republiky na návrh Senátu Parlamentu České republiky.

(2) Inspektor je jmenován na období 10 let. Může být jmenován opakovaně.

(3) Inspektor vykonává kontrolu, řídí kontrolu, vypracovává kontrolní protokol a provádí další úkony, jež souvisejí s úkoly Úřadu.

(4) Činnosti podle odstavce 3 vykonává 7 inspektorů Úřadu.

§ 34

(1) Inspektorem může být jmenován občan České republiky, který je způsobilý k právním úkonům, bezúhonný, splňuje podmínky stanovené zvláštním právním předpisem 30) a má ukončené odborné vysokoškolské vzdělání.

(2) S výkonem funkce inspektora je neslučitelná funkce poslance nebo senátora, soudce, státního zástupce, jakákoliv funkce ve veřejné správě, funkce člena orgánů územní samosprávy a členství v politických stranách a hnutích. Inspektor nesmí zastávat jinou placenou funkci, být v pracovním poměru ani vykonávat výdělečnou činnost s výjimkou

správy vlastního majetku a činnosti vědecké, pedagogické, literární, publicistické a umělecké, pokud tato činnost nenarušuje důstojnost nebo neohrožuje důvěru v nezávislost a nestrannost Úřadu.

(3) Z funkce je inspektor odvolán, přestal-li splňovat některou z podmínek pro jeho jmenování.

HLAVA VI

ČINNOST ÚŘADU

§ 35

Registr

(1) Do registru zpracování osobních údajů se k osobám správců zapisují informace z oznámení podle § 16 odst. 2 a datum provedení, případně zrušení registrace.

(2) Informace zapsané do registru, s výjimkou informací uvedených v § 16 odst. 2 písm. e) a i), jsou veřejně přístupné, zejména způsobem umožňujícím dálkový přístup.

(3) Zrušení registrace podle § 17a oznamuje Úřad ve Věstníku Úřadu.

§ 36

Výroční zpráva

(1) Výroční zpráva Úřadu obsahuje zejména informace o provedené kontrolní činnosti a její zhodnocení, informace a zhodnocení stavu v oblasti zpracovávání a ochrany osobních údajů v České republice a zhodnocení ostatní činnosti Úřadu.

(2) Výroční zprávu předkládá předseda Úřadu pro informaci Poslanecké sněmovně a Senátu Parlamentu České republiky a vládě České republiky do 2 měsíců po skončení rozpočtového roku a zveřejňuje ji.

§ 37

Oprávnění kontrolujících

Kontrolující jsou při provádění kontroly oprávněni
a) vstupovat do objektů, zařízení a provozů, na pozemky a do jiných prostor kontrolovaných správců a zpracovatelů nebo každého, kdo zpracovává osobní údaje, (dále jen „kontrolovaný"), pokud to souvisí s předmětem kontroly; do obydlí mohou vstupovat pouze v případě, že tato slouží také k provozování podnikatelské činnosti,

b) požadovat na kontrolovaných a na jiných osobách, aby ve stanovených lhůtách předložily originální doklady a další písemnosti, záznamy dat na paměťových médiích, výpisy a zdrojové kódy programů, pokud je vlastní, výpisy a opisy dat (dále jen „doklady"), pokud to souvisí s předmětem kontroly, a provádět vlastní dokumentaci,

c) seznamovat se s utajovanými informacemi za podmínek stanovených zvláštním právním předpisem, 31) jakož i dalšími skutečnostmi, které jsou chráněny povinností mlčenlivosti,

d) požadovat na fyzických i právnických osobách poskytnutí pravdivých a úplných informací o zjišťovaných a souvisejících skutečnostech,

e) zajišťovat v odůvodněných případech doklady; jejich převzetí musí kontrolovanému písemně potvrdit a na jeho žádost mu ponechat kopie převzatých dokladů,

f) pořídit kopie obsahu paměťových médií, obsahujících osobní údaje, nacházejících se u kontrolovaného,

g) požadovat, aby kontrolovaní podali ve stanovené lhůtě písemnou zprávu o odstranění zjištěných nedostatků,

h) používat telekomunikační zařízení kontrolovaných v případech, kdy je jejich použití nezbytné pro zabezpečení kontroly.

§ 38

Povinnosti kontrolujících

(1) Kontrolu nesmějí provádět ti kontrolující, u nichž

se zřetelem na jejich vztah ke kontrolovaným nebo k předmětu kontroly jsou důvodné pochybnosti o jejich nepodjatosti.

(2) Kontrolující je povinen bezprostředně po tom, co se dozví o skutečnostech nasvědčujících jeho podjatosti, oznámit to předsedovi Úřadu.

(3) O námitce podjatosti kontrolujícího rozhodne předseda Úřadu bez zbytečného odkladu. Do rozhodnutí o námitce podjatosti činí kontrolující pouze úkony, které nesnesou odkladu.

(4) Proti rozhodnutí o námitce podjatosti se nelze odvolat.

(5) Kontrolující jsou povinni
a) prokázat se kontrolovanému průkazem, jehož vzor upraví nařízení vlády,

b) oznámit kontrolovanému zahájení kontroly,

c) šetřit práva a právem chráněné zájmy kontrolovaných,

d) předat neprodleně převzaté doklady, jakož i kopie paměťových médií kontrolovanému, pominou-li důvody jejich převzetí,

e) řádně ochraňovat zajištěné doklady proti jejich ztrátě, zničení, poškození nebo zneužití,

f) pořizovat o výsledcích kontroly kontrolní protokol,

g) zachovávat mlčenlivost o skutečnostech zjištěných při výkonu kontroly a nezneužít znalosti těchto skutečností. Povinností mlčenlivosti není dotčena oznamovací povinnost podle zvláštních zákonů. Povinnost mlčenlivosti přetrvává i po skončení pracovněprávního vztahu k Úřadu. Povinnosti mlčenlivosti může kontrolujícího zbavit předseda Úřadu. Povinnost mlčenlivosti se nevztahuje na anonymizované a zobecněné informace.

(6) Kontrolní protokol obsahuje zejména popis zjištěných skutečností s uvedením nedostatků a označení ustanovení právních předpisů, které byly porušeny, a

opatření, která byla uložena k nápravě, a stanovení lhůt, do kdy je třeba je učinit. V kontrolním protokolu se uvádí označení Úřadu a jména kontrolujících na kontrole zúčastněných, označení kontrolovaného, místo a čas provedení kontroly, předmět kontroly, skutečný stav, označení dokladů a ostatních dokumentů a zjištění, o které se protokol opírá. Kontrolní protokol podepisují kontrolující, kteří se kontroly zúčastnili.

(7) Povinností kontrolujících je seznámit kontrolované s obsahem kontrolního protokolu a předat jim jeho stejnopis. Seznámení s kontrolním protokolem a jeho převzetí potvrzují kontrolovaní podpisem kontrolního protokolu. Odmítne-li kontrolovaný seznámit se s kontrolním protokolem nebo toto seznámení potvrdit, vyznačí se tyto skutečnosti v kontrolním protokolu.

§ 39

(1) Každý je povinen v souvislosti s výkonem kontroly poskytnout kontrolujícím při výkonu jejich činnosti potřebnou součinnost.

(2) Tomu, kdo neposkytne Úřadu při výkonu kontroly potřebnou součinnost, může být uložena pořádková pokuta do výše 25 000 Kč, a to i opakovaně. Za neposkytnutí součinnosti se považuje i nesplnění opatření uložených k nápravě zjištěného stavu ve stanovené lhůtě.

Opatření k nápravě

§ 40

(1) Zjistí-li kontrolující, že došlo k porušení povinností uložených tímto zákonem, uloží inspektor, jaká opatření je třeba učinit, aby byly zjištěné nedostatky odstraněny, a stanoví lhůtu pro jejich odstranění.

(2) Byla-li uložena likvidace osobních údajů, jsou osobní údaje do likvidace blokovány. Proti uložení likvidace může správce podat námitku k předsedovi Úřadu. Do doby, než bude o námitce rozhodnuto, musí být osobní údaje blokovány. Proti rozhodnutí předsedy lze podat žalobu podle předpisů o správním soudnictví. Do doby, než bude soudem rozhodnuto,

jsou údaje blokovány.

(3) Kontrolovaný je povinen ve stanovené lhůtě podat zprávu o přijatých opatřeních.

§ 41

V řízení ve věcech upravených tímto zákonem se postupuje podle správního řádu, 32) pokud ustanovení tohoto zákona nestanoví jinak.

§ 42

Provozováním informačních systémů nakládajících s osobními údaji podle dosavadních předpisů se rozumí zpracování osobních údajů.

§ 43

Oprávnění a povinnosti při dozoru

Oprávnění a povinnosti kontrolujících a kontrolovaných osob se řídí zvláštním právním předpisem, 26) pokud tento zákon nestanoví jinak.

HLAVA VII

SANKCE

§ 44

Přestupky

(1) Fyzická osoba, která
a) je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru,

b) vykonává pro správce nebo zpracovatele činnosti na základě dohody, nebo

c) v rámci plnění zvláštním zákonem uložených oprávnění a povinností přichází u správce nebo zpracovatele do styku s osobními údaji,

se dopustí přestupku tím, že poruší povinnost mlčenlivosti (§ 15).

(2) Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů
a) nestanoví účel, prostředky nebo způsob zpracování [§ 5 odst. 1 písm. a) a b)] nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona,

b) zpracovává nepřesné osobní údaje [§ 5 odst. 1 písm. c)],

c) shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu [§ 5 odst. 1 písm. d), f) až h)],

d) uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování [§ 5 odst. 1 písm. e)],

e) zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně (§ 5 odst. 2 a § 9),

f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§ 11),

g) odmítne subjektu údajů poskytnout požadované informace (§ 12 a 21),

h) nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů (§ 13),

i) nesplní oznamovací povinnost podle tohoto zákona (§ 16 a 27).

(3) Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů některým ze způsobů podle odstavce 2
a) ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života, nebo

b) poruší povinnosti pro zpracování citlivých údajů (§ 9).

(4) Za přestupek podle odstavce 1 lze uložit pokutu do

výše 100 000 Kč.

(5) Za přestupek podle odstavce 2 lze uložit pokutu do výše 1 000 000 Kč.

(6) Za přestupek podle odstavce 3 lze uložit pokutu do výše 5 000 000 Kč.

§ 45

Jiné správní delikty

(1) Právnická osoba nebo fyzická osoba podnikající podle zvláštních předpisů se jako správce nebo zpracovatel dopustí správního deliktu tím, že při zpracování osobních údajů

a) nestanoví účel, prostředky nebo způsob zpracování [§ 5 odst. 1 písm. a) a b)], nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona,

b) zpracovává nepřesné osobní údaje [§ 5 odst. 1 písm. c)],

c) shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu [§ 5 odst. 1 písm. d), f) až h)],

d) uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování [§ 5 odst. 1 písm. e)],

e) zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně (§ 5 odst. 2 a § 9),

f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem (§ 11),

g) odmítne subjektu údajů poskytnout požadované informace (§ 12 a 21),

h) nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů (§ 13),

i) nesplní oznamovací povinnost podle tohoto zákona (§ 16 a 27).

(2) Právnická osoba jako správce nebo zpracovatel se dopustí správního deliktu tím, že při zpracování osobních údajů některým ze způsobů podle odstavce 1
a) ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života, nebo

b) poruší povinnosti pro zpracování citlivých údajů (§ 9).

(3) Za správní delikt podle odstavce 1 se uloží pokuta do výše 5 000 000 Kč.

(4) Za správní delikt podle odstavce 2 se uloží pokuta do výše 10 000 000 Kč.

§ 46

nadpis vypuštěn

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Při rozhodování o výši pokuty se přihlíží zejména k závažnosti, způsobu, době trvání a následkům protiprávního jednání a k okolnostem, za nichž bylo protiprávní jednání spácháno.

(3) Odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán.

(4) Porušení povinností podle § 44 a 45 projednává Úřad.

(5) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby nebo v přímé souvislosti s ním, se použijí ustanovení o odpovědnosti a postihu právnické osoby.

(6) Pokuta je splatná do 30 dnů ode dne, kdy rozhodnutí o jejím uložení nabylo právní moci.

(7) Pokutu vybírá Úřad a vymáhá místně příslušný celní

úřad podle zvláštního zákona. 34) Výnos z pokut je příjmem státního rozpočtu.

HLAVA VIII

USTANOVENÍ SPOLEČNÁ, PŘECHODNÁ A ZÁVĚREČNÁ

§ 47

Opatření pro přechodné období

(1) Každý, kdo zpracovává ke dni nabytí účinnosti tohoto zákona osobní údaje a na něhož se vztahuje povinnost oznámení podle § 16, je povinen tak učinit nejpozději do 6 měsíců ode dne nabytí účinnosti tohoto zákona.

(2) Zpracování osobních údajů prováděné před účinností tohoto zákona je nutno uvést do souladu s tímto zákonem do 31. prosince 2001.

(3) V případě, že kontrolující zjistí porušení povinnosti podle odstavce 2, ustanovení § 46 odst. 1 a 2 se v takovém případě do 31. prosince 2002 nepoužijí.

§ 48

Zrušovací ustanovení

Zrušuje se zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.

ČÁST DRUHÁ

§ 49

Novela trestního zákona

Zákon č. 140/1961 Sb., trestní zákon, ve znění zákona č. 120/1962 Sb., zákona č. 53/1963 Sb., zákona č. 56/1966 Sb., zákona č. 148/1969 Sb., zákona č. 45/1973 Sb., zákona č. 43/1980 Sb., zákona č. 10/1989 Sb., zákona č. 159/1989 Sb., zákona č. 47/1990 Sb., zákona č. 84/1990 Sb., zákona č. 175/1990 Sb., zákona č. 457/1990 Sb., zákona č. 545/1990

Sb., zákona č. 490/1991 Sb., zákona č. 557/1991 Sb., nálezu Ústavního soudu ČSFR ze 4. 9. 1992, zákona č. 290/1993 Sb., zákona č. 38/1994 Sb., zákona č. 91/1994 Sb., zákona č. 152/1995 Sb., zákona č. 19/1997 Sb., zákona č. 103/1997 Sb., zákona č. 253/1997 Sb., zákona č. 92/1998 Sb., zákona č. 112/1998 Sb., zákona č. 148/1998 Sb., zákona č. 167/1998 Sb., zákona č. 96/1999 Sb., zákona č. 191/1999 Sb., zákona č. 210/1999 Sb., zákona č. 223/1999 Sb., zákona č. 238/1999 Sb., zákona č. 305/1999 Sb., zákona č. 327/1999 Sb., zákona č. 360/1999 Sb. a zákona č. 29/2000 Sb., se mění takto:

1. V § 178 odstavec 1 zní:

„(1) Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem.".

2. V § 178 odst. 2 se za slovo „kdo" vkládá slovo „osobní".

ČÁST TŘETÍ

§ 50

Novela zákona o svobodném přístupu k informacím

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, se mění takto:

1. V § 2 odstavec 3 včetně poznámky pod čarou č. 1) zní:

„(3) Zákon se nevztahuje na poskytování osobních údajů a informací podle zvláštního právního předpisu. 1)

1) Například zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a zákon č. 123/1998 Sb., o právu na informace o životním prostředí.".

2. V § 5 odst. 3 se věta druhá nahrazuje větou, která včetně poznámky pod čarou č. 3a) zní:

„Na tyto subjekty se pro tento účel nevztahuje

povinnost zamezit sdružování informací podle zvláštního právního předpisu. 3a)

3a) § 5 odst. 1 písm. h) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.".

3. V § 8 se odstavce 1 a 2 včetně nadpisu a poznámky pod čarou č. 5) zrušují.

ČÁST ČTVRTÁ

ÚČINNOST

§ 51

Tento zákon nabývá účinnosti dnem 1. června 2000, s výjimkou ustanovení § 16, 17 a 35, která nabývají účinnosti dnem 1. prosince 2000.

Klaus v. r.

Havel v. r.

Zeman v. r.

Vybraná ustanovení novel

Čl.II zákona č. 439/2004 Sb.

Přechodná ustanovení

1. Oznámení a rozhodnutí ve věci registrace zpracování osobních údajů podle § 16 , 17 a 17a zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění zákona č. 450/2001 Sb., podaná a vydaná přede dnem nabytí účinnosti tohoto zákona zůstávají v platnosti.

2. Povolení k předání nebo předávání osobních údajů do jiného státu vydané přede dnem nabytí účinnosti tohoto zákona pozbývá dnem nabytí účinnosti tohoto zákona platnosti, pokud státem, pro který bylo povolení určeno, je členský stát Evropské unie nebo stát, pro který zákaz omezování volného pohybu osobních údajů vyplývá z vyhlášené

mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas, a kterou je Česká republika vázána. Povolení k předání nebo předávání osobních údajů do státu, který není uveden v předchozí větě, vydané přede dnem nabytí účinnosti tohoto zákona zůstává v platnosti.

3. Řízení zahájené a neskončené přede dnem nabytí účinnosti tohoto zákona se dokončí podle dosavadních právních předpisů, s výjimkou řízení o povolení k předání nebo předávání osobních údajů do členského státu Evropské unie nebo státu, pro který zákaz omezování volného pohybu osobních údajů vyplývá z vyhlášené mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas, a kterou je Česká republika vázána, které se zastaví.

4. Správce provádějící zpracování osobních údajů, ke kterému podle dosavadních právních předpisů nebylo zapotřebí registrace, a které ode dne nabytí účinnosti tohoto zákona registraci podléhá, musí takové zpracování osobních údajů oznámit Úřadu pro ochranu osobních údajů do 6 měsíců ode dne nabytí účinnosti tohoto zákona.

---

1) § 10 odst. 1 písm. a) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

1) Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

1a) Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108, vyhlášená pod č. 115/2001 Sb.m. s.

3) § 1 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů.

4) Například ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění zákona č. 300/2000 Sb., zákon č. 219/1999 Sb., o ozbrojených silách České republiky, ve znění pozdějších předpisů, zákon č. 238/2000 Sb ., o Hasičském záchranném sboru České republiky a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění zákona č. 320/2002 Sb., zákon č. 153/1994 Sb., o

zpravodajských službách České republiky, ve znění pozdějších předpisů, zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů, a zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů.

4) Zákon č. 40/1993 Sb., o nabývání a pozbývání státního občanství České republiky, ve znění pozdějších předpisů.

5) Například zákon č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění zákona č. 320/2002 Sb., zákon č. 218/1999 Sb., o rozsahu branné povinnosti a o vojenských správních úřadech (branný zákon), ve znění pozdějších předpisů, zákon č. 219/1999 Sb., o ozbrojených silách České republiky, ve znění pozdějších předpisů, a zákon č. 124/1992 Sb., o Vojenské policii, ve znění pozdějších předpisů.

6) Například zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění zákona č. 320/2002 Sb., zákon č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, a zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů.

7) Například zákon č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů, ve znění pozdějších předpisů, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů.

8) Například zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění zákona č. 320/2002 Sb., a zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů.

9) Například zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů, zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění pozdějších předpisů, zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů, a zákon č. 212/1992 Sb., o soustavě daní, ve znění zákona č. 302/1993 Sb.

10) Například zákon č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, ve znění pozdějších předpisů, zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, a zákon č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.

10a) Zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činností bývalé Státní bezpečnosti, ve znění zákona č. 107/2002 Sb.

11) Například zákon č. 13/1993 Sb., celní zákon, ve znění pozdějších předpisů.

12) Například zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zákon č. 564/1990 Sb., o státní správě a samosprávě ve školství, ve znění pozdějších předpisů, zákon č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, zákon č. 154/2000 Sb., o šlechtění, plemenitbě a evidenci hospodářských zvířat a o změně některých souvisejících zákonů (plemenářský zákon), ve znění pozdějších předpisů, zákon č. 166/1999 Sb., o veterinární péči a o změně některých souvisejících zákonů (veterinární zákon), ve znění pozdějších předpisů, zákon č. 246/1992 Sb., na ochranu zvířat proti týrání, ve znění pozdějších předpisů, zákon č. 147/1996 Sb., o rostlinolékařské péči a změnách některých souvisejících zákonů, ve znění pozdějších předpisů, a zákon č. 219/2003 Sb., o uvádění do oběhu osiva a sadby pěstovaných rostlin a o změně některých zákonů (zákon o oběhu osiva a sadby).

13) Zákon č. 81/1966 Sb., o periodickém tisku a o ostatních hromadných informačních prostředcích, ve znění pozdějších předpisů.

15) Například zákon č. 20/1966 Sb., o péči o zdraví lidu, ve znění pozdějších předpisů, zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů, ve znění pozdějších předpisů, zákon č. 280/1992 Sb., o resortních, oborových, podnikových a dalších zdravotních pojišťovnách, ve znění pozdějších předpisů, zákon č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky, ve znění pozdějších předpisů, a zákon č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění, ve znění pozdějších předpisů.

15a) Například zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů.

16) Například zákon č. 65/1965 Sb., zákoník práce, ve znění pozdějších předpisů, zákon č. 1/1992 Sb., o mzdě, odměně za pracovní pohotovost a o průměrném výdělku, ve znění pozdějších předpisů, zákon č. 218/2002 Sb., o službě státních zaměstnanců ve správních úřadech a o odměňování těchto zaměstnanců a ostatních zaměstnanců ve správních úřadech (služební zákon), ve znění pozdějších předpisů, a zákon č. 1/1991 Sb., o zaměstnanosti, ve znění pozdějších předpisů.

18) Například zákon č. 123/1998 Sb., o právu na informace o životním prostředí, zákon č. 367/1990 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů, zákon č. 106/1999 Sb., o svobodném přístupu k informacím.

19) Například zákon č. 148/1998 Sb., ve znění pozdějších předpisů, zákon č. 89/1995 Sb., zákon č. 20/1966 Sb., ve znění pozdějších předpisů, zákon č. 15/1998 Sb., o Komisi pro cenné papíry a o změně a doplnění dalších zákonů.

20) Například § 167 a 168 zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, zákon č. 20/1966 Sb., ve znění pozdějších předpisů.

22) § 13 občanského zákoníku.

23) Zákon č. 40/1964 Sb., ve znění pozdějších předpisů.

24) Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů.

25) Například § 5c zákona č. 1/1991 Sb., o zaměstnanosti, ve znění zákona č. 167/1999 Sb., zákona č. 155/2000 Sb. a zákona č. 220/2002 Sb., § 71a zákona č. 325/1999 Sb., o azylu a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o azylu), ve znění zákona č. 2/2002 Sb., § 35 odst. 3 zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí, ve znění pozdějších předpisů, a § 4a odst. 3 zákona č. 13/1993 Sb., celní zákon, ve znění zákona č. 1/2002 Sb.

25a) Článek 8 odst. 6 a článek 26 odst. 3 Směrnice č. 95/46/ES.

26) Zákon č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.

26a) Zákon č. 236/1995 Sb., o platu a dalších náležitostech spojených s výkonem funkce představitelů státní moci a některých státních orgánů a soudců, ve znění pozdějších předpisů.

27) § 12 zákona č. 153/1994 Sb.

28) Zákon č. 143/1992 Sb., o platu a odměně za pracovní pohotovost v rozpočtových a některých dalších organizacích a orgánech, ve znění pozdějších předpisů.

Nařízení vlády č. 253/1992 Sb., o platových poměrech zaměstnanců orgánů státní správy, některých dalších orgánů a obcí, ve znění pozdějších předpisů.

29) Zákon č. 119/1992 Sb., o cestovních náhradách, ve znění pozdějších předpisů.

30) Zákon č. 451/1991 Sb.

31) Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

32) Zákon č. 71/1967 Sb., o správním řízení (správní řád), ve znění zákona č. 29/2000 Sb.

34) Zákon č. 337/1992 Sb., o správě daní a poplatků.

Příloha č. 3

256

ZÁKON

ze dne 29. dubna 1992

o ochraně osobních údajů v informačních systémech

Federální shromáždění České a Slovenské Federativní Republiky se usneslo na tomto zákoně:

ČÁST PRVNÍ

Rozsah působnosti

§ 1

Zákon upravuje ochranu osobních údajů, zejména povinnosti související s ochranou informací při provozování informačního systému, který nakládá s osobními údaji a odpovědnost provozovatele informačního systému a dalších fyzických a právnických osob, které se účastní provádění činností souvisejících s provozováním takového informačního systému.

§ 2

Tento zákon se vztahuje i na informační systémy založené zvláštním zákonem.[1])

ČÁST DRUHÁ

VYMEZENÍ NĚKTERÝCH POJMŮ PRO ÚČELY TOHOTO ZÁKONA

§ 3

Informace

Informace, které se vztahují k určité osobě, jsou osobními údaji.

§ 4

Informační systém

Informačním systémem se rozumí funkční celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Každý informační systém zahrnuje informační základnu, technické a programové prostředky, technologie a procedury a pracovníky.

§ 5

Provozování informačního systému

Provozováním informačního systému se rozumí provádění činností směřujících ke shromažďování (sběru) informací, jejich vstupnímu zpracování, ukládání informací do údajové základny, zpracování informací pro vnitřní potřeby systému nebo pro poskytování informační služby. Provozování zahrnuje všechny nebo jen některé z uvedených činností.

§ 6

Informační služba

Informační službou se rozumí provádění činností směřujících k poskytování informací z informačního systému, obvykle spojené se zpracováním informací uchovávaných v informačním systému.

§ 7

Zpracování informace

Zpracováním informace se rozumí

a) technická nebo obsahová úprava informace,
b) automatizované zpracování, zahrnující operace prováděné v úplnosti nebo částečně pomocí automatizačních prostředků, zejména uchovávání informací a dat, provádění logických nebo aritmetických operací s informacemi a daty, jejich úpravy a výmaz,
c) začlenění informace bez fyzické nebo obsahové změny do souboru informací nebo jiného sdělení, které může být určeno k jiným účelům, než je poskytnutí informační služby.

§ 8

Likvidace informace

Likvidací informace se rozumí její výmaz nebo fyzické rozložení takovým způsobem, aby informace nemohla být znovu sestavena, nebo fyzické zničení hmotného nosiče, na nějž je vázána.

---

[1]) Např. zákon č. 244/1991 Sb., o Federální bezpečnostní informační službě, zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), zákon č. 563/1991 Sb., o účetnictví, zákon č. 47/1990 Sb., o volbách do Federálního shromáždění, ve znění pozdějších předpisů.

§ 9

Účastníci výměny informací

Účastníky výměny informací se rozumí provozovatel informačního systému (dále jen „provozovatel"), uživatel informačních služeb (dále jen „uživatel") a zprostředkovatel informací (dále jen „zprostředkovatel").

§ 10

Dotčená osoba

Dotčenou osobou se rozumí jednotlivá fyzická osoba, o které informace vypovídá.

§ 11

Provozovatel

(1) Provozovatelem se rozumí fyzická nebo právnická osoba, která zabezpečuje zpracování informací nebo poskytování informačních služeb a vystupuje vůči ostatním fyzickým nebo právnickým osobám jako nositel práv a povinností spojených s provozováním informačního systému.

(2) Za provozovatele se nepovažují

a) fyzické osoby, které v rámci svého pracovního nebo obdobného poměru přicházejí do styku s informacemi, s nimiž nakládá příslušný informační systém,
b) právnické osoby, které vykonávají činnosti při provozování informačního systému na základě smlouvy uzavřené s provozovatelem.

§ 12

Uživatel

Uživatelem se rozumí fyzická nebo právnická osoba, která využívá informace získané z informačního systému nebo o tyto informace žádá v rámci informačních služeb poskytovaných informačním systémem.

§ 13

Zprostředkovatel

Zprostředkovatelem se rozumí fyzická nebo právnická osoba zjišťující, shromažďující, zpracovávající nebo poskytující informace pro provozovatele nebo uživatele.

§ 14

Náležitý způsob sběru informací

Náležitým způsobem sběru informací se rozumí jejich zjišťování, které není maskováno jiným účelem, kryto jinou činností a nenarušuje práva a svobody občanů.

§ 15

Zveřejněná informace

Za zveřejněnou informaci se považuje informace uvedená na veřejnost prostřednictvím hromadných sdělovacích prostředků nebo prostřednictvím elektronických veřejně přístupných informačních služeb.

ČÁST TŘETÍ

POVINNOSTI SOUVISEJÍCÍ S PROVOZOVÁNÍM INFORMAČNÍHO SYSTÉMU

§ 16

Provozovat informační systém, který nakládá s informacemi, které vypovídají o osobnosti a soukromí dotčené osoby, jejím rasovém původu, národnosti, politických postojích a členství v politických stranách a hnutích, vztahu k náboženství, o její trestné činnosti, zdraví, sexuálním životě a majetkových poměrech, lze pouze, stanoví-li tak zvláštní zákon, nebo se souhlasem žijící dotčetné osoby, pokud je možné, aby tento projev vůle učinila. Jestliže nelze podmínku souhlasu splnit, lze s informacemi nakládat jen za předpokladu, že bude zachována lidská důstojnost, osobní čest, dobrá pověst a chráněno dobré jméno dotčené osoby.

§ 17

Povinností provozovatele je

a) provozovat informační systém v souladu s účelem, pro který je systém zřízen,
b) získávat informace rozsahem přiměřené účelu, pro který je systém zřízen, zejména vystříhat se shromažďování nadbytečných údajů,
c) ověřovat, zda informace, s nimiž informační systém nakládá, jsou přesné, a podle potřeby je aktualizovat,
d) označit náležitým způsobem v informačním systému nepřesné nebo neověřené informace,
e) neuchovávat v informačním systému nepravdivé informace,
f) zamezit sdružování informací a informačních systémů sloužících k rozdílným účelům, pokud zvláštní zákon nestanoví jinak,
g) získávat informace pro informační systémy náležitým způsobem; získávat informace pod krytím jiným účelem nebo jinou činností lze pouze, pokud tak stanoví zvláštní zákon,

h) uchovávat informace, umožňující identifikaci dotčené osoby pouze po dobu přiměřenou účelům informačního systému, pokud zvláštní zákon nestanoví jinak,
i) zajistit ochranu informací i celého systému před náhodným nebo neoprávněným zničením, náhodným poškozením, jakož i před neoprávněným přístupem nebo zpracováním,
j) stanovit práva a povinnosti fyzických a právnických osob, které mají přístup k informačnímu systému,
k) učinit opatření, aby po skončení pracovního nebo obdobného poměru mezi fyzickou osobou a provozovatelem nemohly být informace, s nimiž nakládá příslušný informační systém, touto osobou využity; obdobná opatření je povinen učinit i vůči osobám, které při plnění svých úkolů u provozovatele přicházejí nebo mohou přicházet do styku s informacemi, s nimiž nakládá příslušný informační systém,
l) poskytnout jednou do roka bezplatně, nebo za přiměřenou úplatu kdykoli, každé dotčené osobě na požádání zprávu o informacích o ní uchovávaných v informačním systému, pokud zvláštní zákon nestanoví jinak.

§ 18

(1) Při ukončení provozu informačního systému je provozovatel povinen provést taková opatření, aby informace, s nimiž informační systém nakládal, nemohly být zneužity.

(2) V případě porušení povinnosti podle odstavce 1 má oprávněná osoba nárok na zadostiučinění, odstranění závadného stavu, vydání bezdůvodného obohacení od osoby, která jej získala, a dále nárok upravený v § 20 písm. d) a e).

§ 19

(1) Zprostředkovatel je povinen

a) ověřovat, zda informace, které zprostředkovává, jsou přesné,
b) nepřesné nebo neověřené informace náležitě označit, popřípadě, je-li to možné, tuto nepřesnost odstranit,
c) získávat informace pro informační systémy náležitým způsobem; získávat informace pod krytím jiným účelem nebo jinou činností lze pouze, pokud tak stanoví zvláštní zákon,
d) zajistit ochranu zprostředkovávaných informací před náhodným nebo neoprávněným zničením, náhodným poškozením, jakož i před neoprávněným přístupem nebo zpracováním.

(2) Při zprostředkování informací pro uživatele i provozovatele je zprostředkovatel povinen uchovávat informace získané v souvislosti s výkonem zprostředkovatelské činnosti pouze po dobu nezbytně nutnou a v rozsahu oprávnění provozovatele.

§ 20

V případě porušení povinností provozovatele uvedených v § 17 vzniká oprávněné fyzické osobě vůči provozovateli nárok na

a) zdržení se takového jednání, odstranění závadného stavu, vydání bezdůvodného obohacení tomu subjektu, na jehož úkor bylo toto obohacení získáno, a poskytnutí zadostiučinění (omluvy, opravy) tomu, jehož porušení povinností poškodilo, na náklady provozovatele. Nárok poskytnout zadostiučinění nevzniká, jedná-li s o porušení povinnosti podle § 17 písm. d) a e), pokud provozovatel neporušil svoji povinnost podle § 17 písm. c) nebo pokud prokáže, že s informací bylo nakládáno v mezích souhlasu dotčené osoby nebo jedná-li se o zveřejněnou informaci,
b) likvidaci informace; tento nárok vzniká, porušil-li provozovatel povinnosti uvedené v § 17 písm. a), b), d), e), g), h). Tento nárok též vzniká, jedná-li se o informační systém nakládající se zveřejněnými informacemi, pokud se ukáže, že tyto informace byly zveřejněny neoprávněně nebo pokud tyto informace byly opraveny,
c) doplnění informace, jedná-li se o informaci, která byla do informačního systému vložena se souhlasem dotčené osoby, nebo jestliže se jedná o zveřejněnou informaci,
d) zaplacení přiměřené peněžní úhrady, jestliže bylo porušeno její právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a na ochranu jejího jména, pokud není postižitelná stávajícími občanskoprávními a obchodněprávními instituty,
e) zamezení přístupu k informacím v průběhu sporu, pokud orgán příslušný pro rozhodnutí sporu výjimečně nestanoví jinak; nárok se týká pouze sporem dotčených informací.

§ 21

Zprostředkovatel odpovídá za činnosti, které vykonává pro provozovatele nebo uživatele v rozsahu odpovědnosti provozovatele.

§ 22

(1) Fyzické osoby v rámci svého pracovního nebo obdobného poměru nebo v rámci své veřejné či jiné funkce (např. funkce soudního znalce, auditora) anebo další osoby, které při plnění svých úkolů u provozovatele přicházejí do styku s informacemi, s nimiž nakládá příslušný informační systém (dále jen „povinné osoby“) mají povinnost mlčenlivosti o těchto informacích a nesmí je bez souhlasu provozovatele zpřístupnit jiným subjektům nebo je využít pro sebe, pokud zvláštní zákon nestanoví jinak.

(2) Povinnosti uvedné v odstavci 1 přetrvávají i po skončení pracovního nebo obdobného poměru mezi povinnou osobou a provozovatelem nebo po skončení výkonu funkce povinné osoby.

(3) V případě porušení povinností uvedených v odstavci 1 vzniká oprávněné osobě vůči povinné osobě nárok na

a) zdržení se takových jednání, odstranění závadného stavu, vydání bezdůvodného obohacení a poskytnutí zadostiučinění (omluvy, opravy) na náklady povinné osoby,
b) likvidaci informací, které byly neoprávněně zpřístupněny nebo využity,
c) zaplacení přiměřené peněžní úhrady, jestliže povinná osoba nesplněním těchto povinností způsobila újmu, především nemateriální povahy, která není postižitelná stávajícími občanskoprávními a obchodněprávními instituty a která není spojena s plněním ostatních nároků podle tohoto odstavce,
d) zamezení zpřístupnění informací v průběhu sporu, pokud orgán příslušný pro rozhodnutí výjimečně nestanovil jinak; tento nárok se týká pouze sporem dotčených informací.

(4) Jestliže jsou tyto povinnosti porušeny povinnou osobou, která je v pracovním nebo obdobném poměru k provozovateli, odpovídá provozovatel za poskytnutí peněžitého plnění podle odstavce 3 písm. c) a za poskytnutí zadostiučinění podle odstavce 3 písm. a).

(5) Získá-li někdo informace z informačního systému protiprávním jednáním, vztahují se na něj obdobně odstavce 1 a 3.

§ 23

Spory vyplývající z uplatňování práv a povinností podle tohoto zákona řeší soud.

ČÁST ČTVRTÁ

REGISTRACE INFORMAČNÍHO SYSTÉMU A DOZOR NAD PROVOZOVÁNÍM INFORMAČNÍHO SYSTÉMU

§ 24

K provedení registrace a provádění dozoru nad provozem informačních systémů jsou příslušné orgány, zřízené zvláštními zákony.

§ 25

Žádost o registraci

(1) Orgán uvedený v § 24 eviduje registrované informační systémy po dobu jejich provozu. Evidence je veřejně přístupná a úředně zveřejňována tímto orgánem vždy k 31. prosinci.

(2) Provozovatel je povinen bez zbytečného odkladu informovat orgán uvedený v § 24 o ukončení provozu informačního systému s uvedením data, ke kterému se provoz informačního systému ukončuje. Toto se netýká informačních systémů, na něž se nevztahuje povinnost registrace.

§ 26

Povinnosti registrovat se podléhají pouze informační systémy nakládající s informacemi uvedenými v § 16, pokud neslouží výhradně pro vnitřní potřebu provozovatele; výjimky z povinnosti registrace stanoví zvláštní zákon. Registraci nepodléhají informační systémy nakládající výhradně se zveřejněnými informacemi.

ČÁST PÁTÁ

PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

§ 27

Provozovat informační systém zřízený po dni účinnosti tohoto zákona lze pouze při splnění podmínek uvedených v tomto zákoně; jeho provozovatel je povinen požádat o registraci do tří měsíců po nabytí účinnosti zákona, kterým se zřizuje orgán uvedený v § 24.

§ 28

Vláda České a Slovenské Federativní Republiky může výjimečně stanovit podmínky provozování již fungujícího informačního systému, který není v souladu s tímto zákonem, na období ne delší tří let od nabytí účinnosti tohoto zákona. Tímto není dotčena povinnost provozovatele požádat orgán podle § 24 o registraci v období do tří měsíců po nabytí účinnosti zákona, kterým se tento orgán zřizuje.

§ 29

Tento zákon nabývá účinnosti dnem vyhlášení.

Havel. v. r.
Dubček v. r.
Čalfa v. r.

Příloha č. 4

106

ZÁKON

ze dne 11. května 1999

o svobodném přístupu k informacím

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

§ 1
Účel zákona

Zákon upravuje podmínky práva svobodného přístupu k informacím a stanoví základní podmínky, za nichž jsou informace poskytovány.

§ 2
Povinnost poskytovat informace

(1) Povinnými subjekty, které mají podle tohoto zákona povinnost poskytovat informace vztahující se k jejich působnosti, jsou státní orgány a orgány územní samosprávy

(2) Povinnými subjekty jsou dále ty subjekty, kterým zákon svěřil rozhodování o právech, právem chráněných zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy, a to pouze v rozsahu této jejich rozhodovací činnosti.

(3) Zákon se nevztahuje na postup při poskytování informací povinnými subjekty, který je upraven zvláštními předpisy.[1])

§ 3
Základní pojmy

(1) Žadatelem pro účel tohoto zákona je každá fyzická i právnická osoba, která žádá o informaci.

(2) Možností dálkového přístupu pro účel tohoto zákona je přístup k informaci neomezeného okruhu žadatelů pomocí telekomunikačního zařízení[2]) (například prostřednictvím sítě Internet).

(3) Zveřejněnou informací pro účel tohoto zákona je taková informace, která může být vždy znovu vyhledána a získána, zejména vydaná tiskem nebo na jiném nosiči dat

umožňujícím zápis a uchování informace, vystavená na úřední desce, s možností dálkového přístupu nebo umístěná ve veřejné knihovně.[3])

(4) Doprovodnou informací pro účel tohoto zákona je taková informace, která úzce souvisí s požadovanou informací (například údaj o její existenci, původu, počtu, důvodu odepření, době, po kterou důvod odepření trvá a kdy bude znovu přezkoumán, a dalších důležitých rysech).

§ 4
Poskytování informací

Povinné subjekty poskytují informace žadateli na základě žádosti nebo zveřejněním.

§ 5
Zveřejňování informací

(1) Každý povinný subjekt musí pro informování veřejnosti ve svém sídle a svých úřadovnách zveřejnit na místě, které je všeobecně přístupné, jakož i umožnit pořízení jejich kopie, tyto informace:

a) důvod a způsob založení povinného subjektu, včetně podmínek a principů, za kterých provozuje svoji činnost,

b) popis své organizační struktury, místo a způsob, jak získat příslušné informace, kde lze podat žádost či stížnost, předložit návrh, podnět či jiné dožádání anebo obdržet rozhodnutí,

c) místo, lhůtu a způsob, kde lze podat opravný prostředek proti rozhodnutí povinného subjektu, a to včetně výslovného uvedení požadavků, které jsou v této souvislosti kladeny na žadatele, jakož i popis postupů a pravidel, která je třeba dodržovat při těchto činnostech, a název příslušného formuláře a způsob a místo, kde lze takový formulář získat,

d) postup, který musí povinný subjekt dodržovat při vyřizování všech žádostí, návrhů i jiných dožádání občanů, a to včetně příslušných lhůt, které je třeba dodržovat,

e) přehled nejdůležitějších předpisů, podle nichž povinný subjekt zejména jedná a rozhoduje, které stanovují právo žádat informace a povinnost poskytovat informace a které upravují další práva občanů ve vztahu k povinnému subjektu, a to včetně informace, kde a kdy jsou tyto předpisy poskytnuty k nahlédnutí,

f) sazebník úhrad za poskytování informací,

g)
výroční zprávu za předcházející kalendářní rok o své činnosti v oblasti poskytování informací (§ 18).

(2) Povinné subjekty jsou povinny zveřejňovat informace uvedené v odstavci 1 též způsobem umož-ňujícím dálkový přístup. Tato povinnost se nevztahuje na povinné subjekty, které jsou pouze fyzickými osobami.

(3) Povinné subjekty, které vedou a spravují registry obsahující informace, které jsou na základě zvláštního zákona každému přístupné, jsou tyto údaje povinny zveřejňovat v přehledné formě způsobem umož-ňujícím i dálkový přístup. Na tyto subjekty se pro tento účel nevztahuje povinnost zamezit sdružování informací podle § 17 písm. f) zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.

(4) Povinný subjekt může informace podle odstavce 1 zveřejnit i dalšími způsoby a s výjimkami uvedenými v tomto zákoně může zveřejnit i další informace.

§ 6
Povinnost odkázat na zveřejněnou informaci

(1) Pokud žádost směřuje k poskytnutí zveřejněné informace, může povinný subjekt co nejdříve, nejpozději však do sedmi dnů, místo poskytnutí informace sdělit žadateli údaje umožňující vyhledání a získání zveřejněné informace.

(2) Pokud žadatel trvá na přímém poskytnutí zveřejněné informace, povinný subjekt mu ji poskytne.

§ 7
Ochrana utajovaných skutečností

Je-li požadovaná informace v souladu s právními předpisy[4]) označena za utajovanou skutečnost, k níž žadatel nemá oprávněný přístup, povinný subjekt ji neposkytne.

§ 8
Ochrana osobnosti a soukromí

(1) Informace, které vypovídají o osobnosti a soukromí fyzické osoby, zejména o jejím rasovém původu, národnosti, politických postojích a členství v politických stranách a hnutích, vztahu k náboženství, o její trestné činnosti, zdraví, sexuálním životě a majetkových poměrech, povinný subjekt poskytne pouze tehdy, stanoví-li tak zvláštní zákon, nebo s předchozím písemným souhlasem žijící dotčené osoby. Jestliže dotčená osoba nežije, lze informaci o ní poskytnout jen za předpokladu, že bude zachována její lidská důstojnost, osobní čest, dobrá pověst a chráněno její dobré jméno.

(2) Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy povinný subjekt

poskytne jen za podmínek stanovených zvláštním zákonem.[5])

§ 9
Ochrana obchodního tajemství

(1) Pokud je požadovaná informace označena za obchodní tajemství,[6]) povinný subjekt ji neposkytne.

(2) Při poskytování informace, která se týká používání prostředků státního rozpočtu, rozpočtu územního celku nebo fondu zřízeného zákonem[7]) anebo nakládání s majetkem těchto subjektů, se nepovažuje poskytnutí informace o rozsahu a příjemci těchto prostředků za porušení obchodního tajemství.

§ 10
Ochrana důvěrnosti majetkových poměrů

Informace o majetkových poměrech osoby, která není povinným subjektem, získané na základě zákonů o daních, poplatcích, penzijním nebo zdravotním po-jištění anebo sociálním zabezpečení[8]) povinný subjekt podle tohoto zákona neposkytne.

§ 11
Další omezení práva na informace

(1) Povinný subjekt může omezit poskytnutí informace, pokud:

a) se vztahuje výlučně k vnitřním pokynům a personálním předpisům povinného subjektu,

b) jde o novou informaci, která vznikla při přípravě rozhodnutí povinného subjektu, pokud zákon nestanoví jinak; to platí jen do doby, kdy se příprava ukončí rozhodnutím.

(2) Povinný subjekt informaci neposkytne, pokud:

a) byla předána osobou, jíž takovouto povinnost zákon neukládá, pokud nesdělila, že s poskytnutím informace souhlasí,

b) ji zveřejňuje na základě zvláštního zákona[9]) a v předem stanovených pravidelných obdobích až do nejbližšího následujícího období,

c)
by tím byla porušena ochrana duševního vlastnictví stanovená zvláštním předpisem.[10])

(3) Při poskytování informací, které získal povinný subjekt od třetí osoby k plnění úkolů na základě zvláštního zákona,[11]) podle kterého by se na ně vztahovala povinnost mlčenlivosti anebo jiný postup chránící je před zveřejněním nebo zneužitím, avšak které lze poskytnout podle tohoto zákona, poskytne povinný subjekt jen ty informace, které přímo souvisejí s plněním jeho úkolu.

(4) Povinné subjekty dále neposkytnou informace o

a)
probíhajícím trestním řízení,

b)
rozhodovací činnosti soudů,

c)
plnění úkolů zpravodajských služeb,[12])

d)
přípravě, průběhu a projednávání výsledků kontrol v orgánech Nejvyššího kontrolního úřadu.

Ustanovení zvláštních zákonů[13]) o poskytování informací v uvedených oblastech tím nejsou dotčena.

§ 12
Podmínky omezení

Všechna omezení práva na informace provede povinný subjekt tak, že poskytne požadované informace včetně doprovodných informací po vyloučení těch informací, u nichž to stanoví zákon. Právo odepřít informaci trvá pouze po dobu, po kterou trvá důvod odepření. V odůvodněných případech povinný subjekt ověří, zda důvod odepření trvá.

§ 13
Žádost o poskytnutí informace

(1) Žádost o poskytnutí informace se podává ústně nebo písemně, a to i prostřednictvím telekomunikačního zařízení.
(2) Není-li žadateli na ústně podanou žádost informace poskytnuta anebo nepovažuje-li žadatel informaci poskytnutou na ústně podanou žádost za dostačující, je třeba podat žádost písemně.
(3) Ustanovení § 14 až 16 a § 18 platí pouze pro žádosti podané písemně.

§ 14

Postup při podávání a vyřizování písemných žádostí o poskytnutí informace

(1) Žádost je podána dnem, kdy ji obdržel povinný subjekt. Sdělení žadatele, že trvá na poskytnutí informace podle § 6 odst. 2, se považuje za nové podání žádosti.

(2) Z podání musí být zřejmé, kterému povinnému subjektu je určeno a kdo jej činí. U podání prostřednictvím telekomunikačního zařízení[2]) musí být uvedena rovněž příslušná identifikace žadatele (například elektronická adresa). Neobsahuje-li žádost tyto údaje, není žádost podáním ve smyslu tohoto zákona a žádost se odloží.

(3) Povinný subjekt posoudí obsah žádosti a:

a)
v případě, že je žádost nesrozumitelná, není zřejmé, jaká informace je požadována, nebo je formulována příliš obecně, vyzve žadatele ve lhůtě do sedmi dnů od podání žádosti, aby žádost upřesnil, neupřesní-li žadatel žádost do 30 dnů, rozhodne o odmítnutí žádosti,

b)
v případě, že požadované informace se nevztahují k jeho působnosti, žádost odloží a tuto odůvodněnou skutečnost sdělí do tří dnů žadateli,

c)
poskytne požadovanou informaci ve lhůtě nejpozději do 15 dnů od přijetí podání nebo od upřesnění žádosti podle písmena a), a to písemně, nahlédnutím do spisu, včetně možnosti pořídit kopii, nebo na paměťových médiích.

(4) O postupu při poskytování informace se pořídí záznam.

(5) Lhůtu pro poskytnutí informace je možno prodloužit ze závažných důvodů, nejvýše však o deset dní. Závažnými důvody jsou:

a)
vyhledání a sběr požadovaných informací v jiných úřadovnách, které jsou oddělené od úřadovny vyřizující žádost,

b)
vyhledání a sběr objemného množství oddělených a odlišných informací požadovaných v jedné žádosti,

c)
konzultace s jiným povinným subjektem, který má závažný zájem na rozhodnutí o žádosti, nebo mezi dvěma nebo více složkami povinného subjektu, které mají závažný zájem na předmětu žádosti.

Žadatel musí být o prodloužení lhůty i o jeho důvodech vždy prokazatelně informován, a to včas před uplynutím lhůty pro poskytnutí informace.

§ 15
Rozhodnutí

(1) Pokud povinný subjekt žádosti, byť i jen zčásti, nevyhoví, vydá o tom ve lhůtě pro vyřízení žádosti rozhodnutí, s výjimkou případů, kdy se žádost odloží podle § 14 odst. 2 nebo podle § 14 odst. 3 písm. b). Je-li povinným subjektem obec, vydává rozhodnutí obecní úřad.

(2) Rozhodnutí musí obsahovat označení povinného subjektu, číslo jednací a datum vydání rozhodnutí, označení příjemce rozhodnutí, výrok s uvedením právních předpisů, podle nichž bylo rozhodováno, odůvodnění každého omezení práva na informace, poučení o místu, době a formě podání opravného prostředku, vlastnoruční podpis pověřeného pracovníka povinného subjektu s uvedením jména, příjmení a funkce.

(3) Rozhodnutí se doručuje do vlastních rukou žadatele.

(4) Jestliže orgán ve lhůtě pro vyřízení žádosti neposkytl informace či nevydal rozhodnutí podle § 15 odst. 1, má se za to, že vydal rozhodnutí, kterým informace odepřel. Proti tomuto rozhodnutí lze podat odvolání do 15 dnů ode dne, kdy uplynula lhůta pro vyřízení žádosti.

§ 16
Odvolání

(1) Proti rozhodnutí povinného subjektu o odmítnutí žádosti lze podat odvolání ve lhůtě do 15 dnů od doručení rozhodnutí nebo od marného uplynutí lhůty pro vyřízení žádosti v případě uvedeném v § 15 odst. 4. Odvolání se podává u povinného subjektu, který rozhodnutí vydal nebo měl vydat.

(2) O odvolání proti rozhodnutí povinného subjektu rozhoduje povinný subjekt nejblíže vyššího stup-ně nadřízený povinnému subjektu, který rozhodnutí vydal nebo měl vydat. Jde-li o rozhodnutí obecního úřadu, které se týká informací ve věcech samostatné působnosti obce, rozhoduje o odvolání obecní rada, pokud obecní zastupitelstvo nestanoví, že rozhoduje jiný orgán obce. V ostatních případech rozhoduje o odvolání ten, kdo stojí v čele povinného subjektu, který rozhodnutí vydal nebo měl vydat, a je oprávněn za něj jednat.

(3) Odvolací orgán rozhodne o odvolání do 15 dnů od předložení odvolání povinným subjektem. Jestliže v uvedené lhůtě o odvolání nerozhodl, má se za to, že vydal rozhodnutí, kterým odvolání zamítl a napadené rozhodnutí potvrdil; za den doručení tohoto rozhodnutí se považuje den následující po uplynutí lhůty pro vyřízení odvolání.

(4) Proti rozhodnutí o odvolání se nelze odvolat.

(5) Proti rozhodnutí ústředního orgánu státní správy o odmítnutí žádosti lze podat rozklad, o kterém rozhoduje vedoucí ústředního orgánu státní správy. Ustanovení odstavců 1, 3 a 4 platí pro rozklad obdobně.

(6) Rozhodnutí o odmítnutí žádosti je přezkoumatelné soudem podle zvláštního zákona.[14])

§ 17
Hrazení nákladů

(1) Povinné subjekty jsou v souvislosti s poskytováním informací oprávněny žádat úhradu ve výši, která nesmí přesáhnout náklady spojené s vyhledáváním informací, pořízením kopií, opatřením technických nosičů dat a s odesláním informací žadateli.

(2) Žadateli musí být na jeho žádost potvrzena předpokládaná výše úhrady nákladů.

(3) Povinný subjekt může podmínit vydání informací zaplacením úhrady nebo zálohy.

(4) Úhrada je příjmem povinného subjektu.

§ 18
Výroční zpráva

(1) Každý povinný subjekt musí vždy do 1. břez-na zveřejnit výroční zprávu za předcházející kalendářní rok o své činnosti v oblasti poskytování informací podle tohoto zákona obsahující následující údaje:

a)
počet podaných žádostí o informace,

b)
počet podaných odvolání proti rozhodnutí,

c)
opis podstatných částí každého rozsudku soudu,

d)
výsledky řízení o sankcích za nedodržování tohoto zákona bez uvádění osobních údajů,

e)
další informace vztahující se k uplatňování tohoto zákona.

(2) Pokud má povinný subjekt zvláštním zákonem uloženou povinnost předkládat veřejnou výroční zprávu, údaje podle odstavce 1 písm. a) až e) začleňuje do této výroční zprávy jako její samostatnou část s názvem „Poskytování informací podle zákona č. 106/ /1999 Sb., o svobodném přístupu k informacím".

§ 19

Umožnění přístupu k informacím nebo poskytnutí informací za podmínek a způsobem stanoveným tímto zákonem není porušení povinnosti zachovávat mlčenlivost uložené zvláštními zákony.[15])

ČÁST DRUHÁ
PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

§ 20

(1) Povinnost uvedená v § 5 odst. 2 nastává dnem 1. ledna 2001. Pro obce, které nejsou městy,[16]) povinnost podle § 5 odst. 2 nastává dnem 1. ledna 2002.

(2) Povinnost uvedená v § 5 odst. 3 nastává dnem 1. ledna 2002.

(3) Lhůta pro poskytnutí informace [§ 14 odst. 3 písm. c)] a prodloužení této lhůty (§ 14 odst. 5) se v prvních 12 měsících od účinnosti zákona prodlužují na dvojnásobek, a dalších 12 měsíců se prodlužují o polovinu.

(4) Pokud tento zákon nestanoví jinak, vztahuje se na počítání lhůt a na řízení podle § 15 a 16 správní řád,[17]) s výjimkou ustanovení o obnově řízení a o pře-zkoumávání rozhodnutí mimo odvolací řízení.

§ 21

Vláda vydá nařízení, kterým upraví součinnost orgánů státní správy s obcemi při zajišťování povinností obcí podle § 5 tohoto zákona.

§ 22

Účinnost

Tento zákon nabývá účinnosti dnem 1. ledna 2000.

Klaus v. r.

Havel v. r.

Zeman v. r.

---

[1]) Například zákon č. 123/1998 Sb., o právu na informace o životním prostředí.

[2]) § 1 odst. 4 písm. a) zákona č. 110/1964 Sb., o telekomunikacích, ve znění zákona č. 150/1992 Sb.

[3]) Zákon č. 53/1959 Sb., o jednotné soustavě knihoven (knihovnický zákon), ve znění zákona č. 425/1990 Sb.

[4])

Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů.

[5]) Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. § 11 zákona č. 40/1964 Sb., občanský zákoník, ve znění zákona č. 509/1991 Sb.

[6]) § 17 zákona č. 513/1991 Sb., obchodní zákoník.

[7]) Například zákon č. 388/1991 Sb., o Státním fondu životního prostředí České republiky, ve znění zákona č. 334/1992 Sb., zákon č. 171/1991 Sb., o působnosti orgánů České republiky ve věcech převodů majetku státu na jiné osoby a o Fondu národního majetku České republiky, ve znění pozdějších předpisů, zákon č. 472/1992 Sb., o Státním fondu tržní regulace v zemědělství, ve znění pozdějších předpisů.

[8]) Například § 24 zákona č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů, § 23 zákona č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění, ve znění pozdějších předpisů, § 14 zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů, § 24a zákona č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky, zákon č. 117/1995 Sb., o státní sociální podpoře, ve znění pozdějších předpisů.

[9]) Například zákon č. 89/1995 Sb., o státní statistické službě, zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.

[10]) Například zákon č. 35/1965 Sb., o dílech literárních, vědeckých a uměleckých (autorský zákon), ve znění pozdějších předpisů.

[11]) Například zákon č. 592/1992 Sb., ve znění pozdějších předpisů, zákon č. 222/1994 Sb., o podmínkách podnikání a výkonu státní správy v energetických odvětvích a o Státní energetické inspekci, ve znění zákona č. 83/1998 Sb., zákon č. 283/1993 Sb., o státním zastupitelství, ve znění pozdějších předpisů, zákon č. 166/1993 Sb., o Nejvyšším kontrolním úřadu, ve znění pozdějších předpisů, zákon č. 15/1998 Sb., o Komisi pro cenné papíry a o změně a doplnění dalších zákonů, zákon č. 77/ /1997 Sb., o státním podniku, zákon č. 273/1993 Sb., o některých podmínkách výroby, šíření a archivování audiovizuálních děl, o změně a doplnění některých zákonů a některých dalších předpisů, ve znění zákona č. 40/1995 Sb., zákon č. 13/1993 Sb., celní zákon, ve znění pozdějších předpisů, zákon č. 570/1991 Sb., o živnostenských úřadech, ve znění zákona č. 286/ /1995 Sb., zákon č. 389/1991 Sb., o státní správě ochrany ovzduší a poplatcích za jeho znečišťování, ve znění pozdějších předpisů, zákon č. 64/1986 Sb., o České obchodní inspekci, ve znění pozdějších předpisů, zákon č. 133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů.

[12]) § 5 a 8 zákona č. 153/1994 Sb., o zpravodajských službách, ve znění zákona č. 118/1995 Sb.

[13])

Například § 8a zákona č. 141/1961 Sb., trestní řád, ve znění zákona č. 292/1993 Sb., § 45 zákona č. 166/1993 Sb.

[14]) § 247 a násl. zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

[15]) Například zákon č. 15/1998 Sb., zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, zákon č. 199/1994 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, zákon č. 283/1993 Sb., ve znění pozdějších předpisů, zákon č. 6/1993 Sb., ve znění pozdějších předpisů.

[16]) Zákon č. 367/1990 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů.

[17]) Zákon č. 71/1967 Sb., o správním řízení (správní řád).

Příloha č. 5

Zákon č. 140/1961 Sb.,

trestní zákon

§ 178 Neoprávněné nakládání s osobními údaji

(1) Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem.

(2) Stejně bude potrestán, kdo osobní údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, byť i z nedbalosti, sdělí nebo zpřístupní, a tím poruší právním předpisem stanovenou povinnost mlčenlivosti.

(3) Odnětím svobody na jeden rok až pět let nebo zákazem činnosti nebo peněžitým trestem bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se údaj týká,

b) spáchá-li čin uvedený v odstavci 1 nebo 2 tiskem, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem, nebo

c) spáchá-li čin uvedený v odstavci 1 nebo 2 porušením povinností vyplývajících z jeho povolání, zaměstnání nebo funkce.