Technické a legislativní aspekty zabezpečení služeb externích datových úložišť

Výzkumná zpráva projektu FR CESNET

Jiří Bořík, Luboš Kejzlar, Jan Kolouch

2015

Obsah

1 Úvod do problematiky externích datových úložišť 4
2 Informace a její životní cyklus 6

2.1 Životní cyklus informace 6

3 Doporučená struktura bezpečnostní architektury ICT 7

3.2 Základní pojmy a předpoklady 7
3.3 Obecné požadavky na ICT infrastrukturu 8
3.4 Principy návrhu bezpečnostní infrastruktury 8
3.5 Aplikační členění bezpečnostní infrastruktury 8
3.6 Bezpečnostní bariéry 9
3.7 Přiřazení bezpečnostních zón 9

4 Bezpečnostní klasifikace informací 11

4.1 Základní pojmy a předpoklady 11
4.2 Stupně klasifikace 11
4.3 Způsob provedení klasifikace 12

5 Přehled relevantních norem a doporučení 14

5.1 Právně závazné normy ČR 14
5.2 Technické normy a doporučení 14

6 Rozbor vybraných právně závazných norem 16

6.1 Úvod do legislativní problematiky 16
6.2 Rozbor vybraných norem 18

6.2.1 Zákon č. 480/2004 Sb., o některých službách informační společnosti 18
6.2.2 Zákon na ochranu osobních údajů 24
6.2.3 Zákon č. 89/2012 Sb., občanský zákoník 28
6.2.4 Přestupky na úseku IT 30
6.2.5 Trestněprávní odpovědnost 32

7 ISMS a normy řady ISO 27000 33

7.1 Přehled norem řady ISO 27000 33
7.2 Obvyklý postup nasazování ISMS 34

7.2.1 Určení rozsahu nasazení 34
7.2.2 Ohodnocení informačních aktiv 34
7.2.3 Analýza rizik 34

7.2.4 Návrh bezpečnostních politik a další dokumentace ... *34*
7.2.5 Implementace bezpečnostních opatření ... *35*
7.2.6 Certifikační proces ... *35*
7.2.7 PDCA cyklus ... *35*

7.3 Shrnutí ... 35

8 Často kladené otázky (FAQ) ... 37
9 Vnitřní předpisy a EULA ... 47
10 Literatura a odkazy ... 51
Příloha 1: Příklad EULA ... 53
Příloha 2: Příklad smluvních podmínek ... 57
Příloha 3: Bezpečnostní provozní směrnice IS (metodický pokyn) ... 62
Příloha 4: ISO 27000: Information Classification Matrix ... 75
Příloha 5: Přehled norem řady ISO 27000 ... 76
Příloha 6: Výsledky průzkumu ... 81

1 Úvod do problematiky externích datových úložišť

Cílem tohoto dokumentu je pokusit se zmapovat vybrané technické, organizační a legislativní aspekty bezpečnostní problematiky využívání externích datových úložišť v akademickém prostředí. Diskutované závěry by měly být využitelné nejen pro koncové uživatele, ale i správce a poskytovatele takovéto služby.

Pojem *„externí datová úložiště“* je chápán v širším smyslu slova a dále pod ním rozumíme poskytování *služeb veřejných cloudů* (Google Drive, iCloud, OneDrive), *privátních cloudů* implementovaných v rámci organizace (ownCloud) nebo *vysokokapacitních datových úložišť* (např. poskytovaných sdružením CESNET nebo v rámci ICT služeb dané organizace)[1].

Veškerá opatření pro zabezpečení informací poskytovaných datovými úložišti a řízení přístupu k nim musí být integrální součástí širší bezpečnostní koncepce zahrnující všechny články řetězce *životního cyklu informace* (jak je stručně popsáno v kapitole 2.). Je podstatné si uvědomit, že ne všechny stavy, ve kterých se informace v průběhu svého životního cyklu nachází, lze pokrýt prostředky ICT. Samostatné oblasti problematiky bezpečnosti informací, kterými se tento dokument *nezabývá* tvoří např. fyzická bezpečnost či zabezpečení informací uchovaných mimo ICT systémy[2].

Hlavní těžiště práce sice spočívá ve zmapování administrativních, organizačních a legislativních opatření v oblasti bezpečnosti, ale je zřejmé, že pro správné pochopení principů a především následně úspěšnou aplikaci navržených doporučení v praxi je nezbytné *znát hodnotu* ukládaných nebo zpracovávaných informací. To jinými slovy znamená, že *klíčovým předpokladem* pro návrh a implementaci jakýchkoliv bezpečnostních opatření je *provedení analýzy rizik* a z ní vyplývající *klasifikace* důležitých informací. Popis doporučené praktické metodiky pro klasifikaci důležitých dat organizace je předmětem kapitoly 4.

Organizační a legislativní ukotvení bezpečnostní problematiky musí být neoddělitelně propojeno s odpovídajícím technickým řešení. Dokument se sice nezabývá detaily technického řešení, ale v kapitole 3. je popsán návrh ICT architektury umožňující relativně snadnou a efektivní implementaci požadovaných bezpečnostních pravidel.

Následující části dokumentu (kapitoly 5. až 7.) obsahují úvod do legislativní problematiky a podrobnější rozbor a komentáře vybraných právně závazných norem a technických doporučení. Dokument se podrobněji nezabývá provozními směrnicemi vzhledem k jejich velké specifičnosti pro konkrétní organizaci a typ poskytované služby[3].

---

[1] Není-li uvedeno jinak, jsou v dalším textu jednotlivé typy datových úložišť (a označující pojmy)

[2] Včetně problematiky vstupu informací do ICT systému a jejich následného výstupu (např. v papírové formě) a likvidace.

[3] Metodický pokyn NBÚ pro tvorbu provozních směrnic je uveden v příloze č. 3.

Závěrečná část dokumentu obsahuje shrnutí nejdůležitějších témat přehlednou formou „často kladených otázek“ (FAQ), jejichž formulace mapuje aktuální problémy uživatelů a vychází z dlouholetých praktických zkušeností řešitelů s danou problematikou.

V části příloh jsou pak uvedeny nekomentované konkrétní příklady jednotlivých typů smluvních ujednání a souhrnné výsledky provedeného průzkumu mezi uživateli.

Vzhledem k šíři řešené oblasti, různorodosti exitujících názorů[4] a jejich dynamickému vývoji si tento dokument (ani celý projekt) neklade za cíl poskytnout komplexní a ucelený pohled na danou problematiku či poskytnout jednoznačný názor nebo návod pro řešení konkrétní problémové situace.

Cílem dokumentu je pouze snaha zmapovat rozsáhlou problematiku administrativních a legislativních aspektů bezpečnosti poskytování služeb externích datových úložišť a poskytnout uživateli[5] základní opěrné body v tomto rozbouřeném moři...

Autoři projektu počítají s tím, že sepsáním závěrečné zprávy a odevzdáním projektu jejich práce nekončí a budou dále v rámci svých pracovních povinností průběžně monitorovat stav problematiky a poskytovat expertní konzultace uživatelům.

[4] Vyplývající z převažující právní podstaty problematiky.
[5] Resp. administrátorovi či poskytovateli služby.

2 Informace a její životní cyklus

Pojem *informace* (z lat. *in-formatio*, utváření, ztvárnění) je velmi široký, mnohoznačný a užívá se v různých oborech a významech. V nejobecnějším smyslu je informace chápána jako údaj o prostředí, jeho stavu a procesech v něm probíhajících. Informace snižuje nebo odstraňuje *neurčitost* (entropii) systému.

Pro naše potřeby budeme dále pod pojmem *informace* (resp. *data*) většinou rozumět (nebude-li uvedeno jinak): „Opakovaně interpretovatelnou, formalizovanou podobu informace vhodnou pro komunikaci, vyhodnocování nebo zpracování.“.

2.1 Životní cyklus informace

Pro správné pochopení popisované problematiky je podstatné si uvědomit, že informace v prostředí ICT procházejí určitým *životním cyklem*, který lze zjednodušeně popsat následujícími stavy:

1. *vznik* – nová myšlenka, pozorování apod.,
2. *vstup* – formalizace a zavedení do konkrétního ICT[6] prostředí ve formě dat,
3. *zpracování* – zpracování dat, jejich přenos, vyhodnocení apod.,
4. *výstup*[7] – data opouští (nebo se duplikují) ICT prostředí např. ve formě tištěného výstupu,
5. *zánik* – data jsou vymazána, skartována apod.

Následující text se zabývá převážně informacemi již *obsaženými v konkrétním ICT systému*, tj. nepokrývá komplexní problematiku *celého životního cyklu* informace.

Při návrhu a implementaci celkové bezpečnostní politiky organizace[8] je třeba chybějící články „skládačky“ řešit jinými (fyzickými, právními, organizačně-administrativními) prostředky.

Z tohoto pohledu je pro úspěšné řízení celého životního cyklu informace *zásadní* si uvědomit a *definovat pravidla* pro chování jednotlivých kategorií dat (viz dále) především ve stavech (2), (4) a (5), tj. definovat, zda a jaká data v těchto stavech *mohou*, *musí* či *nesmí* (a za jakých podmínek) opustit (resp. vstoupit do) konkrétní ICT prostředí. To je podstatné proto, že uvedené stavy představují *slabá místa*, kde potenciálně ztrácíme technickou kontrolu nad řízením přístupu dat (resp. předáváme kontrolu jiným nástrojům mimo ICT prostředí), což může vést ke znehodnocení předcházejících či následných bezpečnostních opatření.

---

[6] Konkretizace pojmu ICT v daném kontextu je uvedena v následující kapitole.

[7] Stavy (1) až (4) se mohou vzájemně kombinovat a opakovat.

[8] V praxi nelze úspěšně implementovat pouze bezpečnostní politiku ICT bez jejího zakotvení do širšího kontextu.

3 Doporučená struktura bezpečnostní architektury ICT

Cílem následující kapitoly je poskytnout jednoduché praktické „vodítko“ pro návrh a následnou implementaci takové ICT architektury organizace, která umožní dlouhodobě a koncepčně realizovat požadované zabezpečení klíčových dat a řízení přístupu k nim.

Je nezbytné si uvědomit, že vhodně zvolená architektura ICT infrastruktury umožňující využití dostupných technických prostředků pro efektivní oddělení a řízení jednotlivých bezpečnostních zón je *nutným (nikoliv však postačujícím) předpokladem* pro vlastní technické zabezpečení dat a následné prosazování organizačních a legislativních postupů v oblasti informační bezpečnosti.

V následujícím textu se mnohdy zdánlivě nesourodě prolínají předpoklady a požadavky jak z oblasti technologické, tak i legislativní a administrativně-organizační. Při důkladnějším pochopení problematiky však zjistíme, že obě tyto oblasti jsou navzájem velice silně propojeny a jedna bez druhé nemůže vytvořit požadovaný funkční celek.

Mohli bychom s úspěchem parafrázovat známý výrok: „...jsou plné (IT) hřbitovy těch, co chtěli bezpečnost řešit pouze technickými (administrativními) prostředky...“

Doporučení

Nebuďte jedním z nich! Snažte se vytvořit fungující „pracovní skupinu“ složenou ze zástupců vedení organizace, CIO a techniků (vizionářů), která bude mít vůli a schopnost (prostředky) připravované změny prosadit. Pamatujte, že technické řešení je vždy až na posledním místě...

3.2 Základní pojmy a předpoklady

Jak již bylo řečeno, vhodně členěná ICT infrastruktura je základním kamenem pro zajištění bezpečnosti důležitých informačních systémů (resp. jejich komponent) a jimi poskytovaných dat.

Pod pojmem *zabezpečení* (z technického hlediska) budeme dále rozumět především zajištění *důvěrnosti*, *integrity* a *dostupnosti* dat.

Nezbytným předpokladem odpovídajícího funkčního návrhu (a jeho následné technologické implementace) ICT infrastruktury je *existence bezpečnostní (informační) politiky*, která specifikuje globální cíle, postupy a priority organizace v dané oblasti, tj. de-facto specifikuje globální zadání pro bezpečnostní parametry ICT v širším kontextu bezpečnostní vize organizace.

3.3 Obecné požadavky na ICT infrastrukturu

Všechny součásti ICT infrastruktury organizace[9] musí z pohledu úspěšného návrhu a realizace bezpečnostních opatření splňovat základní požadavky:

- zajišťovat odpovídající ochranu *informačních aktiv*, která jsou definována na základě provedené *analýzy rizik* (risk assessment) a formálně kodifikována v *bezpečnostní politice organizace*. Problematika bezpečnosti obecně musí být zakotvena v interní legislativně a především *akceptována na úrovni vrcholového managementu*.
- klíčové komponenty infrastruktury musí být *trvale udržovány* v souladu s platnou bezpečnostní politikou organizace, přičemž zřetel musí být brán také na aktuální stav legislativy a relevantní směrnice a doporučení,
- celá infrastruktura musí mít trvale „odpovídající kvalitu“ a být budována (a v pravidelných cyklech inovována) s ohledem na požadovaný (resp. plánovaný) výkon, kapacitu a robustnost.

3.4 Principy návrhu bezpečnostní infrastruktury

Z technologického pohledu můžeme infrastrukturu zjednodušeně rozdělit na *síťovou* a *aplikační* část. Návrh síťové struktury by měl zohledňovat následující základní principy:

- Síťová infrastruktura musí umožňovat (logicky i technicky) členění na jednotlivé *zóny* a *bezpečnostní třídy.*
- Musí existovat jasné oddělení *serverové* a *klientské* části.
- Začlenění serverů a klientů do odpovídajících bezpečnostních zón musí být provedeno na základě analýzy rizik a klasifikace dat.
- Řízení přístupu k jednotlivým zdrojům (serverům, službám) je definováno tzv. *bezpečnostní bariérou*, která je realizována odpovídajícími (dostupnými) technickými prostředky.
- Virtuální komponenty (servery a klienti) musí být řízeny podle stejných pravidel jako ostatní prvky infrastruktury.
- Aplikační členění bezpečnostní infrastruktury

Aplikační část infrastruktury dělíme hlediska bezpečnosti do jednotlivých *zón*, *tříd* a *segmentů.* Členění by mělo respektovat následující základní principy:

- Členění musí vycházek z provedené analýzy rizik a klasifikace dat.

[9] A to nejen technologické, ale především legislativní a administrativně-organizační.

- *Vlastník systému vždy rozhoduje a je odpovědný* za klasifikaci daného IS (aplikace, komponenty) a jeho umístění do konkrétní zóny.
- Členění do jednotlivých *zón* je základním principem navrhované bezpečnostní architektury. Každá zóna definuje minimální garantovaný stupeň zabezpečení dat. Doporučujeme z počátku implementovat tři základní zóny: *otevřená (veřejná)*, *interní* a *bezpečná*. V případě potřeby je možno následně zjemnit toto členění a implementovat další zóny v souladu se specifickými potřebami organizace.
- Zóna na dané bezpečnostní úrovni nemá implicitně žádný přístup do zóny na úrovni vyšší.
- Zóna na dané bezpečnostní úrovni nemá nutně implicitní přístup do zóny na nižší úrovni.
- Bezpečnostní zóna je technicky realizována *jedním nebo více (síťovými) segmenty*.
- Síťové segmenty v rámci dané zóny mohou být provozovány s různými bezpečnostními konfiguracemi. Segmenty se stejným bezpečnostním nastavením mohou být sdružovány do tzv. *bezpečnostních tříd*.
- Síťové segmenty ve stejné zóně nebo bezpečnostní třídě nejsou nutně vzájemně přístupné.

3.5 Bezpečnostní bariéry

Bezpečnostní bariérou rozumíme sadu podmínek nebo opatření (logických i fyzických), které musí být splněny, aby byl uživateli poskytnut přístup ke specifikovanému zdroji (serveru, službě, aplikaci, komponentě) v rámci dané zóny nebo bezpečnostní třídy.

Bezpečnostní bariéra musí být realizována odpovídajícími (dostupnými) technickými prostředky na různých systémových úrovních jako např. firewall, packet filter, VPN, systém autentizace, autorizace a řízení přístupu, aplikační gateway apod.

3.6 Přiřazení bezpečnostních zón

Pro lepší představu uvedeme příklady přiřazení jednotlivých systémů do výše uvedených základních bezpečnostních zón:

- *bezpečná* – systémy kritické pro fungování organizace, tj. systémy obsahující citlivá osobní data a mission-critical data a aplikace,
- *interní* – vnitřní síť organizace sloužící pro zaměstnance a další spolupracovníky, tj. informační systémy pro podporu administrativy, vědy a výzkumu, výuky apod. Tyto systémy by neměly být přímo přístupné z veřejné zóny.

- *otevřená (veřejná)* – obsahuje „vše ostatní“ (dostupné v rámci sítě dané organizace), tj. studentský nebo hostovský přístup, veřejný portál organizace, připojení mobilních a personálních zařízení apod.

4 Bezpečnostní klasifikace informací

4.1 Základní pojmy a předpoklady

Cílem popisovaných doporučení je popsat neformální, prakticky realizovatelný postup pro klasifikaci klíčových informací v rámci organizace. Informace jsou posuzovány z hlediska bezpečnosti s ohledem na stupeň jejich citlivosti a významu (kritičnosti) pro organizaci. Součástí klasifikace musí být i definice způsobu a periody zálohování a následné archivace (resp. likvidace). Uvedená doporučení vycházejí ze zavedených postupů („best practices“) a umožňují v případě potřeby navázat následnou formalizací procesů např. ve formě certifikace ISO 27000.

Uvedená doporučení by měla také sloužit jako pomůcka pro *vlastníky informací* umožňující jim zajistit (specifikovat), že s obsahem, který je po danou skupinu uživatelů kritický bude nakládáno odpovídajícím způsobem (řízení přístupu, způsob zabezpečení, frekvence zálohování apod.) a v souladu s interní i externí legislativou.

Obdobný typ klasifikace informací je nezbytné provést také před plánovaným využitím externích datových úložišť (cloudových služeb) či zpřístupnění dat prostřednictvím mobilních zařízení.

4.2 Stupně klasifikace

Pro naše potřeby budeme v dalším textu uvažovat pouze tři základní stupně bezpečnostní klasifikace informací, které korespondují s navrženým členěním bezpečnostních zón:

- *Důvěrné* – systémy obsahující citlivá data, tj. jakákoliv data, jejichž kompromitace (porušením utajení, integrity nebo dostupnosti) může mít zásadní dopad na fungování (zájmy) organizace nebo soukromí jednotlivců. Citlivost dat je přímo úměrná škodám, které mohou vzniknout jejich kompromitací.
- Informace jsou přístupné pouze vyjmenovaným zaměstnancům (případně externím subjektům) v rámci *striktně definovaného systému řízení přístupu* (MAC, RBAC, ABAC apod.).
- *Interní* – systémy pro podporu hlavních činností organizace (vědy, výzkumu a výuky, administrativy apod.).
- Informace jsou přístupné zaměstnancům organizace, studentům i externím uživatelům v rámci definovaných pravidel řízení přístupu.
- *Otevřené* – ostatní data a informační zdroje veřejně poskytované danou organizací.
- Informace jsou veřejně přístupné zaměstnancům organizace, studentům i externím uživatelům bez specifických požadavků na řízení přístupu.

4.3 Způsob provedení klasifikace

Základní klasifikaci informací v dané organizaci lze provést přehledně prostřednictvím *matice aplikací*, kde jednotlivé *řádky* reprezentují logickou *množinu dat*, která se vztahují k dané oblasti činnosti organizace (skupině uživatelů apod.) a sdílejí stejné (obdobné) bezpečnostní charakteristiky, tj. patří do stejné bezpečnostní třídy. Jedná se např. specifický výzkumný projekt, data v systému pro personalistiku, HR, SIS apod.

Takto definovaná množina dat může ale nemusí (a typicky není) být umístěna v rámci jedné aplikace nebo fyzického systému.

Sloupce pak popisují hlavní charakteristiky umožňující zařazení množiny dat do odpovídající bezpečnostní zóny[10]. Význam jednotlivých sloupců matice je následující:

Vlastník: Organizační jednotka, funkční pozice nebo proces, který „vlastní" dané informace, tj. je zodpovědný za jejich pořizování, interpretaci a další využívání.

Obsah: Specifikuje typ (množinu) informací (nezávisle na konkrétním informačním systému, formátu či médiu), tj. k jaké oblasti činnosti se vztahují.

Legislativní rámec: Reference na legislativní dokumenty (interní i externí) vztahující se na danou množinu informací.

Umístění: Označení systému, aplikace (nebo její části) a/nebo fyzického média, kde se informace v rámci svého životního cyklu nacházejí. Součástí specifikace umístění je i odpovídající bezpečnostní zóna, ve které jsou všechny uvedené systémy umístěny.

Stupeň bezpečnostní klasifikace: Požadovaná úroveň zabezpečení informací podle výše uvedené klasifikace. Dané množině dat může obecně odpovídat více než jedna úroveň.

Požadavky na zabezpečení: Další specifické požadavky na zabezpečení (nad rámec obecných pravidel daných klasifikací) dat:

- **C** (confidential) – citlivá data, se kterými je třeba zacházet speciálním způsobem,
- **I** (integrity) – specifické požadavky na zajištění integrity,
- **A** (avaibility) – specifické požadavky na dostupnost.

Osobní údaje: Informace, zda aplikace může obsahovat osobní údaje (v legislativním smyslu):

- **P** (personal) – osobní údaje,

[10] Konkrétní výběr vhodných charakteristik se může lišit na základě speciálních požadavků, typu organizace nebo charakteru klasifikovaných dat.

- **S** (sensitive) – citlivé údaje.

Maximální doba výpadku: Maximální akceptovatelná doba výpadku (v rámci dané časové periody), po kterou mohou být data nedostupná. Pro různé systémy může být tato doba v průběhu roku variabilní. Akceptovatelná doba výpadku může být kratší např. pro SIS v rámci zkouškového období, FIS v období účetních závěrek či výplat apod.

Archivační hodnota: Kritérium specifikující relativní důležitost informací pro organizaci:

- **L** (legal) – legislativní význam,
- **K** (enterprise-critical) – klíčová data pro organizaci,
- **H** (historical) – dlouhodobě (historicky) významná data.

Doba archivace: Doba, po kterou mají být informace v rámci organizace archivovány. Úložná perioda začíná vytvořením „informačního objektu“ v archivu a udává se v letech:

- **P** (permanent) – trvalé uložení,
- **LT** (lifetime-related) – doba uložení je závislá na dalších objektech (počítačový systém, projekt, smluvní vztah apod.), např. doba archivace je stanovena na 5 let po ukončení projektu.
- **n-let** – organizací pevně stanovená doba v závislosti na dané činnosti nebo legislativní úpravě.

Likvidace dat: Specifikuje pravidla pro likvidaci (zneplatnění) dat na konci jejich životního cyklu. V praxi mohou existovat speciální pravidla pro data vlastněná skupinou uživatelů (projektem) nebo data jejichž uchování je zásadní z hlediska legislativy, jejich podstaty či významu pro organizaci. Doporučené kategorie jsou:

- **R** (review) – žádost o zaslání dat vlastníkovi k revizi jejich životního cyklu,
- **DST** (destroy) – data jsou smazána bezprostředně po konci jejich životního cyklu (citlivá nebo osobní data mohou vyžadovat speciální režim mazání),
- **DEP** (deposit) – uložení dat v archivní úložišti (státní archiv apod.),
- **K** (keep) – data budou uložena trvale.

5 Přehled relevantních norem a doporučení

5.1 Právně závazné normy ČR

K diskutované problematice se vztahují zejména následující právní normy:

- Zákon č. 89/2012 Sb., občanský zákoník (OZ).
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (ZOOÚ).
- Zákon č. 40/2009 Sb., trestní zákoník (TZK).
- Zákon č. 141/1961 Sb., o trestním řízení soudním.
- Zákon č. 121/2000 Sb., autorský zákon.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti (ZSIS).
- Zákon č. 127/2005 Sb., o elektronických komunikacích (ZeOK).
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví.
- Zákon č. 441/2003 Sb., o ochranných známkách.
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích.
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím.
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.

Praktický výklad a dopad vybraných legislativních norem je podrobněji uveden v následujících kapitolách.

5.2 Technické normy a doporučení

V oblasti nakládání s informacemi a jejich bezpečností jsou nejznámější dále uvedené standardy. Obvykle se jedná o skupinu norem nebo šířeji pojatý soubor pravidel a doporučení, který řeší celý proces zajišťování ICT služeb, nejen samotnou oblast nakládání s informacemi.

- **ISO/IEC TR 13335 1—5** je skupina norem pro řízení bezpečnosti IT, pokrývá jednotlivé kroky zavádění bezpečnosti ICT od návrhu, přes řízení až po konkrétní techniky.
- **ISO/IEC 27000** je řada norem pro nasazení a provozování ISMS (systému řízení informační bezpečnosti). Jednotlivé normy v této řadě se věnují všem etapám procesu, od definice systému informační bezpečnosti, přes implementaci procesů i technických opatření až po konkrétní technická doporučení v různých oblastech nasazení.

- **BS 7799** byla publikována v Británii jako soubor „best practices“ pro řízení rizik ICT s důrazem na politiky, lidské zdroje a legislativu. V roce 2000 byla převedena na ISO/IEC 17799 a následně v roce 2005 do ISO 27001 a 27002.
- **ISO/IEC 15408** (též známá jako Common Criteria for Information Technology Security Evaluation, CC) je standard pro posuzování bezpečnosti komponent ICT.
- **ISA/IEC-62443** (původně ANSI/ISA-99) je soubor norem a postupů pro návrh, výrobu a provoz průmyslových automatizačních a řídících systémů. Standard vytvořila International Society for Automation a následně byl publikován jako ANSI dokument.
- **ISO/IEC 20000** (Information Technology Infrastructure Library, ITIL) je soubor praxí osvědčených přístupů („best practices“) k provozování ICT služeb. Knihovnu řešení spravuje organizace Office of Government Commerce.
- **COBIT** (Control Objectives for Information and Related) Technology je soubor manažerských nástrojů a postupů pro řízení ICT. Systém byl vytvořen organizací Information Systems Audit and Control Association.
- **Standard of Good Practice** je soubor postupů pro řízení informační bezpečnosti. Standard spravuje nezávislá nezisková organizace Information Security Forum.

Výše uvedené normy vznikaly průběžně a odděleně v různém prostředí (bankovnictví, průmysl apod.). Postupným vývojem se začaly obsahově potkávat a překrývat a docházelo k jejich slučování a sjednocování do společného znění (např. BS7799 – ISO/IEC17799 – ISO 27002).

V samostatné kapitole dále bude probrán Systém řízení bezpečnosti informací (ISMS) dle norem řady ISO 27000.

6 Rozbor vybraných právně závazných norem

V následující části budou diskutovány výše uvedené vybrané *právní normy ČR*, které se úzce vztahují k problematice externích datových (cloudových) úložišť a to jak z hlediska poskytovatele tak i zákazníka.

Pro správné pochopení a vyhodnocení konkrétního případu je vždy podstatné uvědomit si, jaký typ činnosti či zpracování dat je konkrétním subjektem vykonáván.

6.1 Úvod do legislativní problematiky

Z hlediska aplikovatelnosti práva na problematiku externích datových úložišť (dále také cloudové služby či datová úložiště) obecně, budeme v dalším textu vycházet z dělení práva v ČR na:

- *veřejnoprávní úpravu*, kdy je jeden ze subjektů v nadřazeném postavení a převažují zde tzv. *kogentní* právní normy (blíže viz. dělení právních norem),
- *soukromoprávní úpravu*, kdy mají právní subjekty navzájem rovné postavení a stát do těchto vztahů zasahuje minimálně, tzv. *dispoziční zásada*.

Obecně je možné konstatovat, že v případě souhlasu s využíváním cloudových a datových úložišť dojde primárně k aplikaci soukromoprávních právních norem, typicky *End Users Licence Agreement (EULA)* uzavíraná mezi poskytovatelem a uživatelem služby.

Právní normou se rozumí *vyjádření toho, co má být*. Jde o normu, která je *právně závazná*. Právní norma je označením pro obecný příkaz, zákaz nebo dovolení vyplývající z právního řádu. Zároveň jsou stanoveny (určeny) nástroje a zmocnění k jeho dosažení nebo vymáhání.

Struktura právní normy je založena na následujících složkách:

- *hypotéza* (vymezení),
- *dispozice* (podstata),
- *sankce* (důsledek).

Jestliže je splněna hypotéza, vzniká tím závazek nebo oprávnění uvedené v dispozici a jestliže nebyla splněna hypotéza a nebyl splněn závazek v dispozici, pak vzniká sankční oprávnění nebo závazek.

Jedno z dalších možných členění dělí právní normy podle:

1. Způsobu vymezení pravidel chování:
   - *přikazující* – určují jak se chovat,
   - *zakazující* – zakazují určitý druh chování,
   - *opravňující* – dovolují určitý druh chování,

- *doporučující* – stanovují doporučení (v právním řádu nejsou příliš časté),
- *teleologické (finální)* – vyjadřují účel nebo cíl, kterého má být dosaženo, ale nestanovují, jak jej dosáhnout, tj. volba prostředků je zpravidla ponechaná adresátovi.

2. Stupně závaznosti:

- *kogentní (kategorické)* – jsou formulovány natolik imperativně, že nedávají žádný prostor pro vůli adresáta normy. Adresát musí přesně ustanovení normy naplnit. Kogentní normy jsou typické pro veřejné a procesní právo.
- *dispozitivní* – buď vůbec nestanoví pravidlo chování, nebo ho stanoví podpůrně. Subjekty právního vztahu si vlastní dohodou stanovily (určily) pravidlo chování; pokud si ho nestanovily, nastupuje podpůrné ustanovení příslušné podpůrné právní normy. Dispozitivní normy jsou typické pro soukromé právo.

Právní normou je tedy dle výše uvedeného také:

- *vnitřní právní předpis*, který stanoví podmínky a pravidla užívání cloudových služeb a datových úložišť,
- *EULA* uzavřená mezi poskytovatelem a uživatelem cloudových služeb a datových úložišť.

Obě výše uvedené právní normy by v sobě měly obsahovat *pravidla chování*, která přikazují, zakazují a opravňují k výkonu určitého druhu činnosti. Tato pravidla by měla být stanovena relativně vyváženě, avšak měla by umožňovat poskytovateli služeb autoritativním způsobem řešit incidenty, jakož i případy ohrožení služeb nebo porušení právních norem.

Vlastní právní normy by pak měly jasně seznámit všechny uživatele (jak správce, tak i koncové uživatele) s jejich právy a povinnostmi. Vzhledem k zaměření projektu bude větší pozornost věnována *dispozitivní* právní normě a nastavení pravidel a mechanismů pro její zajištění.

Dojde-li k porušení této právní normy, mohou být uplatněny jak sankce uvedené v této dispozitivní normě, tak bude následně možné užít odpovídající normy kogentní. Příkladem užití kogentních norem je např. vznik trestně či správně právní odpovědnosti za protiprávní jednání.

V této souvislosti je třeba definovat také *právní úkon*, což je projev vůle spočívající ve vzniku, změně nebo zániku právního vztahu. Právní úkon je jednáním (jak ve formě konání, tak opomenutí) vyvolávajícím *právní následky*.

Pro platnost právního jednání se vyžaduje:

- *subjekt* (právnická nebo fyzická osoba),

- *projev* (tj. forma písemná, ústní, konkludentní)[11],
- vůle,
- předmět.

6.2 Rozbor vybraných norem

V následujícím textu se budeme zabývat rozborem konkrétních právně závazných norem. Je zřejmé, že s ohledem na rozsah a komplexnost řešené problematiky nelze provést vyčerpávající rozbor. Zaměříme se na klíčové oblasti a postupy, které umožní pochopit danou problematiku a snadněji prakticky aplikovat základní principy.

6.2.1 Zákon č. 480/2004 Sb., o některých službách informační společnosti

Zákon č. 480/2004 Sb., o některých službách informační společnosti (ZSIS) je stěžejní právní normou, která obecně charakterizuje a vymezuje základní *práva a povinnosti poskytovatelů služeb informační společnosti* (ISP, Internet Service Provider).

Dle 2 písm. a) ZSIS se: „službou informační společnosti rozumí *jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky*, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky[12], pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat“.

Poskytovatelem služby (tedy ISP) je pak každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti. Uživatelem služby je fyzická nebo právnická osoba, která využívá službu informační společnosti.[13]

Zákon rozlišuje poskytovatele služeb spočívajících v:

- přenosu informací poskytnutých uživatelem (Mere Conduit, Access Provider). De-facto se jedná o operátory:
- elektronických komunikací,
- ostatních fyzických linek,
- logických linek,
- automatickém meziukládání (Caching[14]) informací poskytnutých uživatelem,

---

[11] § 561 OZ stanoví, že k: „Platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé.“ Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat.

[12] Viz § 2 písm. c) ZSIS: „Elektronickými prostředky se rozumí zejména síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy, telekomunikační koncová zařízení a elektronická pošta.“

[13] Viz § 2 písm. d) a e) ZSIS.

[14] Blíže viz např.: http://business.center.cz/business/pojmy/p2090-automaticke-docasne-meziukladani.aspx.

- ukládání informací poskytnutých uživatelem (storage nebo hosting).

Dále budou stručně vymezena práva a povinnosti všech uvedených typů ISP, přičemž z pohledu projektu je nejvýznamnější typ poskytovatele ukládání informací.

Poskytovatel služeb spočívajících v přenosu informací poskytnutých uživatelem

Takovéhoto poskytovatele nelze činit odpovědného za kvalitu informace (kterou mu nelze přičíst) a to i v případě, že si je vědom protiprávnosti přenášené informace. Operátoři *elektronických komunikací* mají specifické povinnosti dle zákona č. 127/2005 Sb., o elektronických komunikacích (dále jen ZoEK). Takovýto poskytovatel může být odpovědný pokud:

- přenos sám iniciuje,
- zvolí uživatele přenášené informace, nebo
- zvolí nebo změní obsah přenášené informace.

Dle čl. 12 směrnice č. 2000/31/ES je dána možnost členským státům nařídit poskytovateli ISP, aby přerušil poskytování služeb skrze něž dochází ke komunikaci protiprávních informací.

Dle § 6 ZSIS není takovýto ISP povinen:

- dohlížet na obsah přenášených informací,
- aktivně zjišťovat protiprávnost informace.

Vlastní činnost těchto poskytovatelů je výrazně ovlivněna implementací směrnice evropského parlamentu a rady 2006/24/ES, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (též nazývána směrnice o *„Data Retention“*).

V této směrnici byla stanovena povinnost ISP *preventivně uchovávat provozní a lokalizační údaje* o uskutečněné elektronické komunikaci.

Účelem směrnice bylo harmonizovat předpisy členských států týkající se povinnosti poskytovatelů veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí, pokud jde o uchovávání provozních a lokalizačních údajů tak, aby se daly poskytnout příslušným orgánům členských států pro:

- prevenci, vyšetřování, odhalování a stíhání závažné trestné činnosti, jako je terorismus a organizovaný zločin,
- oblast provozních a lokalizačních údajů o právnických i fyzických osobách a související údaje, které jsou nezbytné k identifikaci účastníka nebo registrovaného uživatele.

Tato směrnice se *nevztahuje* na obsah elektronických sdělení ani na informace vyžadované při použití sítě elektronických komunikací.

Členské státy byly dle této směrnice povinny zajistit, aby se telekomunikační údaje uchovávaly po dobu *nejméně šesti měsíců a nejvýše dvou let* ode dne uskutečnění komunikace.

Vlastní směrnice byla v ČR implementována do ZoEK[15] od 1.5.2005, přičemž EU vydala směrnici k 15. březnu 2006 a požadovala transpozici (zapracování do národních legislativ) do 15. září 2007.

Plošné uchovávání provozních a lokalizačních údajů je kontroverzním tématem, neboť v rámci této činnosti dochází k zásahu do práva na osobní svobodu. O konkrétní osobě jsou plošně zjišťovány údaje, které mohou víceméně jednoznačně určit její denní zvyklosti či informace o jejích kontaktech, činnosti apod.

Z uvedeného důvodu byla následně směrnice podrobena *testu proporcionality*, který je standardním právním nástrojem jak soudů mezinárodních, tak soudů ústavních (národních), posuzuje-li se konflikt ustanovení právního řádu sledující ochranu ústavně zaručeného práva či veřejného zájmu s jiným základním právem či svobodou.

Tato obecná zásada zahrnuje tři kritéria posuzování přípustnosti zásahu:

1. *princip vhodnosti* (způsobilosti naplnění účelu), dle něhož musí být příslušné opatření vůbec schopno dosáhnout zamýšleného cíle, jímž je ochrana jiného základního práva nebo veřejného statku,
2. *princip potřebnosti*, dle něhož je povoleno použití pouze nejšetrnějšího (ve vztahu k dotčeným základním právům a svobodám) z více možných prostředků,
3. *princip přiměřenosti* (v užším smyslu), dle kterého újma na základním právu nesmí být nepřiměřená ve vztahu k zamýšlenému cíli, tj. opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky přesahovat pozitiva, která představuje veřejný zájem na těchto opatřeních.

Soudní dvůr EU po předchozím stanovisku svého generálního advokáta Pedra Cruze Villalóna vynesl dne 8.4.2014 verdikt v jedné konkrétní kauze a v rámci tohoto verdiktu *zneplatnil směrnici o „Data Retention“*:

[15] Konkrétně do § 97 odst. 3.

„Dnešním rozsudkem prohlašuje Soudní dvůr směrnici za neplatnou s dovětkem, že: vzhledem k tomu, že Soudní dvůr neomezil časové účinky rozsudku, je prohlášení neplatnosti účinné ode dne, kdy směrnice vstoupila v platnost“.

Soudní dvůr EU dále konstatoval, že rozhodnutí „ponechat či zrušit“ je plně na příslušných národních orgánech a samotná EU jim nehodlá ani doporučovat či dávat nějaké vodítko ohledně toho, jak se mají zachovat.

V ČR je nadále platná povinnost uchovávat provozní a lokalizační údaje pro veřejné ISP, kteří poskytují „konektivitu“. Podmínky uchovávání a předávání provozních a lokalizačních údajů jsou upraveny zejména v § 88a a § 97 ZoEK:

§ 88a

1) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna zajistit, aby provozní a lokalizační údaje uchovávané podle § 97 odst. 3 měly stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně před neoprávněným přístupem, změnou, zničením, ztrátou anebo odcizením nebo jiným neoprávněným zpracováním nebo využitím, jako údaje podle § 88; tímto nejsou dotčeny povinnosti stanovené zvláštním právním předpisem.
2) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je *povinna zpracovat pro zajištění ochrany údajů podle odstavce 1 vnitřní technicko-organizační předpis*; ochranu údajů zajistí s ohledem na stávající technické možnosti a na náklady potřebné k zajištění ochrany na úrovni odpovídající existujícímu riziku porušení ochrany. Pro ochranu údajů podle tohoto ustanovení se ustanovení § 88 odst. 2 až 7 použijí obdobně.

§ 97

1) Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu *6 měsíců provozní a lokalizační údaje*.
2) Povinnost zajistit, aby při plnění uvedené povinnosti nebyl uchováván obsah zpráv a takto uchovávaný dále předáván.
3) Povinnost poskytovat informace:
   a) orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem,
   b) Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem,

c) Bezpečnostní informační službě pro účely a při splnění podmínek stanovených zvláštním právním předpisem,
d) Vojenskému zpravodajství pro účely a při splnění podmínek stanovených zvláštním právním předpisem,
e) České národní bance pro účely a při splnění podmínek stanovených zvláštním právním předpisem.

4) Po uplynutí doby podle věty první je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu nebo pokud tento zákon nestanoví jinak (§ 90).
5) Provozními a lokalizačními údaji jsou zejména:
   a) údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace,
   b) údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace.

Doporučení

Byť se vlastní směrnice o „Data Retention" týká výhradně ISP, kteří poskytují konektivitu a nařizuje plošné uchovávání provozních a lokalizačních údajů o připojovaných osobách, domníváme se, že *lze její rámec aplikovat i na jiné služby ISP*.

Toto tvrzení lze opřít o potřebu regulace jak činnosti poskytovatele služby,[16] tak činnosti uživatele při poskytování jakékoli služby. Vlastní uchovávání provozních a lokalizačních údajů by pak mělo být explicitně specifikováno v EULA (aby měl uživatel možnost využívání takové služby případně odmítnout) a mělo by respektovat především test proporcionality.

Ve vztahu k poskytování služeb externích datových úložišť je třeba poznamenat, že nejde o plošné uchovávání provozních a lokalizačních údajů. Uchovávány jsou pouze údaje, které se bezprostředně týkají dané služby či úložiště.

Při vlastní implementaci uchovávání provozních a lokalizačních údajů by měl být respektován *princip odděleného uchovávání* těchto údajů od údajů obsahových.[17]

Uchovávány mohou být provozní a lokalizační údaje v rozsahu stanoveném ZoEK, tedy:

- údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace,
- údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace.

Lhůtu pro uchování provozních a lokalizačních údajů doporučujeme stanovit obdobně jako v § 97 ZoEK, tedy *6 měsíců*.

---

[16] Který nemůže být neomezeným a je svrchovaným „vládcem" nad daty a uživatelskými účty. I poskytovatel služby se musí řídit pravidly a principy, které jsou pro jeho činnost definovány.

[17] Viz směrnice o „Data Retention" a § 97 ZoEK.

Dále doporučujeme *zpracovat vnitřní technicko-organizační předpis* pro zajištění ochrany provozních a lokalizačních, jakož i dalších ukládaných údajů a stanovit jasné podmínky, za kterých bude možné uvedená data předávat třetím stranám.

Poskytovatel služeb spočívajících v automatickém meziukládání dat poskytnutých uživatelem

Poskytovatelé cachingu nejsou zbaveni odpovědnosti za kvalitu informací, pokud dojde z jejich strany k porušení standardních či smluvených technických podmínek. Poskytovatel cachingu je odpovědný (dle § 4 ZSIS) v případě, že:

- změní obsah informace,
- nedodrží obecně uznávaná pravidla aktualizace informace,
- nevyhoví podmínkám přístupu k informaci,
- překročí povolené užívání technologie obecně uznávané v příslušném odvětví s cílem získat údaje o užívání informace,
- neodstraní nebo nezakáže přístup k informaci poté, co zjistí, že informace byla na místě původu odstraněna nebo k ní byl znemožněn přístup nebo soud nařídil stažení či znemožnění přístupu k této informaci.

Poskytovatel cachingu nemá povinnost aktivně prověřovat obsah meziukládaných informací, vyjma výše uvedeného případu.

Poskytovatel služeb spočívajících v ukládání informací poskytnutých uživatelem

V případě poskytovatele hostingu, což je typický příklad služeb externích datových úložišť, je situace nejsložitější (viz § 5 ZSIS).

V ustanovení daného paragrafu je dána podmínka alespoň nevědomé nedbalosti poskytovatele ve vztahu k protiprávnímu obsahu informace u něj uložené.

Poskytovatel hostingu je odpovědný tehdy:

- mohl-li vzhledem k předmětu své činnosti, okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní,
- dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré požadované kroky k odstranění nebo znepřístupnění takovýchto informací.

Poskytovatel hostingu odpovídá vždy, pokud vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.

Zákon však ani v tomto případě *neukládá* poskytovateli hostingu *povinnost aktivně vyhledávat* protiprávní informace uživatelů (neboť by v mnohých případech šlo de-facto o zásah do základních práv a svobod zaručených ústavním zákonem č. 2/1993 Sb., listina základních práv a svobod).

Doporučení

- Stanovit Access Policy.
- Smluvně (EULA) ošetřit povahu a účel ukládaných dat.
- Transparentně seznámit uživatele s podmínkami užívání poskytované služby.
- Vlastní potvrzení o seznámení se s podmínkami EULA uchovávat společně s údaji, které opravňují uživatele k užívání poskytovaných služeb.
- Vykonávat správu nad poskytovanými službami či úložištěm a v případě, že správce vzhledem k předmětu své činnosti, okolnostem a povaze případu mohl vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, postupovat dle vnitřního právního předpisu, který je vytvořen pro správu a dozor.[18]
- Informovat uživatele o kompromitaci či možnosti kompromitace dat. Vydávat upozornění v případě zjištění hrozby či incidentu, vztahujícímu se k dané službě či úložišti.

6.2.2 Zákon na ochranu osobních údajů

Prameny práva na ochranu soukromí vychází v EU zejména z Evropské úmluvy o ochraně lidských práv a základních svobod, kde je explicitně v čl. 8 uvedeno: „právo na respektování soukromého a rodinného života, obydlí a korespondence“.

Směrnice 95/46/EC zavedla *standard ochrany osobních údajů v rámci Evropské unie* s tím, že národní legislativa na ochranu osobních údajů může zavést přísnější pravidla než ta, která jsou uvedena v této směrnici.

Do práva ČR byla uvedená směrnice transponována zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (ZOOÚ). Za činnost podléhající tomuto zákonu je považována jakákoliv operace nebo soustava operací, kterou správce nebo zpracovatel systematicky provádí s osobními údaji, např. jejich shromažďování, zpřístupňování, zveřejňování či třídění, ale také ukládání na nosiče informací, uchovávání a předávání.

Zákon o ochraně osobních údajů se vztahuje na *jakékoli zpracování osobních údajů*, vyjma:

- zpracování osobních údajů fyzickou osobou pro osobní potřebu (§ 3 odst. 3 ZOOÚ),
- nahodilé shromažďování, pokud nejsou osobní údaje dále zpracovány (§ 3 odst. 4 ZOOÚ).

Dále podrobněji rozebereme základní pojmy definované tímto zákonem.

[18] Typicky učinit následující kroky: zaznamenat incident, znepřístupnit data, vytvořit zálohu dat, zajistit provozní a lokalizační údaje, kontaktovat právní oddělení.

Osobní údaj

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

Určeným nebo určitelným subjektem může být *výlučně fyzická osoba* a to ta, k níž se osobní údaje vztahují. K určení subjektu údajů může někdy postačit jeden znak (například fotografie), obvykle je však zapotřebí těchto znaků více, přičemž je třeba, aby jejich prostřednictvím byla osoba určena nebo alespoň určitelná a to případně i nepřímo.

Citlivý údaj

Citlivým údajem se rozumí: „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.“[19]

K tomu, aby byl údaj označen jako citlivý, musí splňovat nejenom znaky požadované pro osobní údaje obecně, ale současně je třeba, aby na jeho základě bylo možno určit národnost, rasový původ, členství v politické straně apod. subjektu údajů. Výčet citlivých údajů je *taxativní* a jiné údaje povahu citlivých údajů nemají. Bude-li údaj obsahovat jak citlivé, tak i ostatní osobní údaje, je třeba při jeho zpracování postupovat podle ustanovení o citlivých osobních údajích.

Příkladem osobních údajů je:

- příjmení a křestní jméno,
- poštovní adresa, e-mailová adresa,
- číslo bankovního účtu, číslo kreditní karty,
- telefonní číslo, číslo občanského nebo řidičského průkazu,
- fotografie.

Zpracování osobních údajů

Zpracováním se rozumí jakákoli operace nebo soubor operací s osobními údaji, které:

- jsou prováděny automatizovaně nebo jinými prostředky,

[19] § 4 písm. b) ZOOÚ.

- správce nebo zpracovatel systematicky provádějí s osobními údaji a to automatizovaně nebo jinými prostředky.

Příkladem zpracování je:

- shromažďování, ukládání na nosiče informací,
- uchovávání,
- úprava nebo pozměňování,
- používání,
- předávání, šíření, zpřístupňování nebo zveřejňování,
- blokování, výměna nebo likvidace.

Správce osobních údajů je fyzická nebo právnická osoba, která určuje účel a prostředky zpracování osobních údajů.

Správce provádí zpracování, odpovídá za něj a může zpracovávat osobní údaje pouze *se souhlasem subjektu údajů*[20]. *Bez* tohoto *souhlasu* je může zpracovávat pouze v *konkrétně stanovených případech* (např. statistické nebo vědecké účely).

Souhlasem subjektu údajů se rozumí svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.

Ze souhlasu musí být zřejmé, jaké osobní údaje smějí být zpracovány a musí z něj být patrno, kterému správci je dáván souhlas ke zpracování a vymezen jeho konkrétní účel. Souhlas musí také zahrnovat určení období, na které je dáván.

Povinností správce je *stanovit účel*, k němuž mají být osobní údaje zpracovány. Pokud je tato povinnost stanovena zákonem, nepřichází logicky v úvahu stanovení jiného účelu resp. tento účel není třeba vůbec stanovit.

Shromažďovat lze osobní údaje pouze ke stanovenému účelu a v rozsahu nezbytném k jeho naplnění. Dále musí být stanoveny prostředky a způsob zpracování údajů.

Shromažďovat lze údaje pouze otevřeně a je vyloučeno činit tak pod záminkou jiného účelu nebo činnosti. Zakázáno je sdružovat osobní údaje k rozdílným účelům.[21]

Zpracovatel osobních údajů je osoba, která zpracovává osobní údaje pro správce osobních údajů.

Zpracovatel je povinen, zjistí-li porušování povinností správcem, jej na to upozornit a ukončit zpracování údajů. Jestliže tak neučiní, nese s ním solidární odpovědnost za případnou škodu a mimo to může být postižen za správní delikt podle § 46 zákona o přestupcích.

Subjekt údajů musí být předně včas a řádně informován o tom, že jsou o něm vůbec údaje shromažďovány[22]. Subjekt musí informaci dostat natolik včas a v takové podobě, aby mohl účinně hájit svá práva.

---

[20] Osoba, jejíž osobní údaje mají být zpracovány.
[21] Výjimku připouští zákon.

Subjekt údajů musí být poučen o tom, je-li podle zákona povinen údaje poskytovat a jaké důsledky nastanou, jestliže tak neučiní, za jakých podmínek může informaci odmítnout nebo zda poskytuje údaje dobrovolně a také o právu na přístup k osobním údajům a možnosti chránit svoje práva, poruší-li správce či zpracovatel povinnosti stanovené tímto zákonem.

Doporučení

- Vlastní seznámení uživatele (subjektu údajů) o povaze uchovávaných dat vložit do EULA.
- Uchovávat potvrzení o seznámení se s povahou ukládaných dat společně s údaji, které opravňují uživatele k užívání cloudových služeb či datových úložišť.
- Stanovit období, na které je souhlas s uchováváním údajů dán. Po uplynutí této lhůty vyžádat souhlas nový.
- Stanovit účel uchovávání a zpracování osobních údajů.

Obecné podmínky pro zpracování osobních údajů

Zpracování osobních údajů je vázáno na předchozí oznámení o zpracování Úřadu pro ochranu osobních údajů (ÚOOÚ). Je vyžadována písemná smlouva mezi správcem a zpracovatelem osobních údajů.

Osobní údaje musí být:

- zpracovány zákonným způsobem,
- zpracovány pro stanovené účely,
- přiměřené, nezbytné pro naplnění stanoveného účelu,
- přesné,
- uchovávány pouze po nezbytně nutnou dobu,
- zpracovány v souladu s právy subjektů údajů,
- zpracovávány bezpečně.

Zpracování je povoleno, pokud:

- subjekt údajů nezpochybnitelně udělil souhlas,
- je nezbytné pro splnění právní povinnosti,
- je nezbytné pro ochranu práv a právem chráněných zájmů správce.

[22] V jakém rozsahu, pro jaký účel apod.

6.2.3 Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 89/2012 Sb., občanský zákoník (OZ) je stěžejní soukromoprávní normou, která zakotvuje práva a povinnosti jak ISP, tak i koncových uživatelů. V následujícím textu se budeme věnovat pouze vybraným ustanovením, která se bezprostředně vztahují k problematice cloudových služeb a externích datových úložišť.

Podoba a soukromí

Ustanovení § 84 OZ stanoví, že: „Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením."

V návaznosti na toto ustanovení pak § 86 stanoví, že: „Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy."

Věci a jejich rozdělení

Ustanovení § 489 OZ stanoví, že: „Věcí je vše, co je rozdílné od osoby a slouží potřebě lidí". Z tohoto pohledu je možné vyvodit, že *data a informace jsou věci*, neboť jsou rozdílné od osoby. Věci se dle § 496 OZ dělí na věci *hmotné* a *nehmotné*, přičemž hmotnou věcí se rozumí ovladatelná část vnějšího světa, která má povahu samostatného předmětu a nehmotnými věcmi jsou práva, jejichž povaha to připouští, a jiné věci bez hmotné podstaty.

Doporučení:

- Vzhledem k poskytovaným službám je nutné stanovit podmínky šíření dat mezi uživateli.
- Při šíření je vhodné nastavit pravidla tak, aby bylo jasné, že uživatel dává souhlas (a v jakém rozsahu) s šířením jeho dat.

Soukromoprávní aspekty poskytování služeb externích datových úložišť

V rovině soukromoprávní je třeba největší pozornost věnovat *vymezení licenční smlouvy* k využívání služeb datových úložišť (EULA). Licenční smlouva je alfou a omegou práv a povinností jak uživatele, tak poskytovatele těchto služeb.

Pokud se jedná například o společnost, která v prostředí cloudu provozuje aplikaci důležitou pro její chod, je více než na místě upravit smluvní podmínky mezi uživatelem a poskytovatelem služby písemně.[23]

Doporučení:

- *Jasně vymezit* práva a povinnosti jednotlivých stran (poskytovatel a uživatel) ve smlouvě.[24]
- Z hlediska bezpečnosti je naprosto nezbytné stanovit jasné a předem vymezené *procesy a pravidla*, které definují jak poskytování služeb a jejich případnou změnu (Change resp. Demand Management), tak proces přidělování uživatelských práv a řízení přístupu k informacím.
- Kritickým bezpečnostním aspektem v případě využívání služeb externích datových úložišť je minimální či *nulová schopnost uživatele kontrolovat fyzické umístění dat*.[25] Podle povahy dat a poskytované služby je vhodné do smlouvy EULA začlenit alespoň některá z následujících ustanovení:
- právo být neprodleně informován o výpadcích služby,
- právo mít přístup k systémovým informacím a logům, ze kterých je možné zjistit aktuální lokaci vlastních dat a přístupů k nim,
- právo provést (resp. opakovaně provádět) penetrační test za účelem ověření zabezpečení infrastruktury ICT poskytovatele,
- právo žádat provedení bezpečnostního auditu ICT poskytovatele služby nebo právo obdržet kopii jeho zprávy,

---

[23] § 561 OZ stanoví, že: „K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé. Jiný právní předpis stanoví, jak lze při právním jednání učiněném elektronickými prostředky písemnost elektronicky podepsat."

[24] Je nezbytné dbát na správné a jasné formulování smluvních práv a závazků, protože je značný rozdíl mezi povinností a snahou.

Porovnejme např. formulaci: *„Poskytovatel je povinen zajistit, že aplikace bude zákazníkovi dostupná 95% provozní doby poskytování služby."* a její (zdánlivě vhodnější) alternativu: *„Poskytovatel vyvine maximální úsilí k tomu, aby zákazník mohl aplikaci užívat 99,95% provozní doby poskytování služby"*. Ve druhém případě sice poskytovatel deklaruje vyšší dostupnost, ale zákazník se svého práva na takovou dostupnost nemusí vždy domoci, protože poskytovatel sice vyvinul maximální úsilí, ale ono to zkrátka nestačilo.

Obdobný příklad se týká samotného parametru *„dostupnost služby"*, kdy může být lákavé mít smluvní závazek dostupnosti 99,95%, ale pokud je dostupnost služby měřena za období jednoho roku, může být výpadek znatelně delší než v případě, kdy je dostupnost měřena na obvyklejší měsíční bázi.

[25] Což v sobě nese i aspekt určité omezenosti ochrany těchto dat před neoprávněným přístupem ze strany poskytovatele.

- vyžadovat certifikaci ISO (např. 27001 či 22307) poskytovatele.[26]

Občanskoprávní odpovědnost za incident

Na závěr je třeba připomenout občanskoprávní odpovědnost jak uživatele, tak poskytovatele za případný incident.

OZ stanoví že: „Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného."

V ustanoveních § 2909 a násl. OZ je pak vymezena odpovědnost za způsobenou škodu, kterou (vzhledem k povaze újmy a jejímu původci) je možné vymáhat jak po poskytovateli, tak po uživateli samotném.

§ 2909 a násl. OZ uvádí: „Pokud škůdce, způsobí poškozenému újmu, úmyslným porušením dobrých mravů, je povinen ji nahradit; vykonává-li však své právo, je škůdce povinen škodu nahradit, jen sledoval-li jako hlavní účel poškození jiného."

§ 2912 odst. 1 OZ dále uvádí: „Nejedná-li škůdce, jak lze od osoby průměrných vlastností v soukromém styku důvodně očekávat, má se za to, že jedná nedbale."

V této souvislosti je třeba připomenout, že ten kdo škodu způsobil (škůdce), je povinen škodu nahradit a to bez ohledu na své zavinění v případech stanovených zvlášť zákonem.

Veřejnoprávní odpovědnost

Za případný incident či újmu způsobenou při vlastním poskytování služeb externích datových úložišť je možné vyvodit i trestněprávní či správněprávní odpovědnost. Vlastní veřejnoprávní odpovědnost je podmíněna definováním protiprávního jednání v některé z veřejnoprávních norem.

Doporučení

V rámci EULA uzavírané mezi poskytovatelem a uživatelem je vhodné upozornit na možnost předání dat o případném incidentu třetí straně (typicky orgánům činným v trestním řízení, zpravodajským službám, subjektům podílejícím se na ochraně práv autorských apod.) v případě, že dojde ke spáchání trestného činu, přestupku, či jiného protiprávního jednání.

6.2.4 Přestupky na úseku IT

Přestupky na úseku IT jsou zakotveny v zákoně č. 200/1990 Sb., o přestupcích. Demonstrativně uvádíme některé z nich.

---

[26] Blíže viz *Právní aspekty cloud computingu*, http://www.systemonline.cz/clanky/pravni-aspekty-cloud-computingu.htm.

§ 33: Přestupky na úseku porušování průmyslových práv a porušování práv k obchodní firmě

1) Přestupku se dopustí ten, kdo:
   a) neoprávněně vykonával práva, která jsou zákony na ochranu průmyslového vlastnictví vyhrazena majitelům těchto práv,
   b) neoprávněně užíval obchodní firmu nebo jakékoliv značení zaměnitelné s obchodní firmou nebo označením příznačným pro jiného podnikatele.
2) Za přestupky podle odst. 1 lze uložit pokutu do 15 000 Kč.

§ 47a: Přestupky křivého vysvětlení

1) Přestupku se dopustí ten, kdo jako osoba podávající vysvětlení o trestném činu spáchaném jiným před orgánem činným v trestním řízení úmyslně:
   a) uvede nepravdu o okolnosti, která má podstatný význam pro rozhodnutí, nebo
   b) takovou okolnost zamlčí.
2) Za přestupek podle odst. 1 lze uložit pokutu do výše 50 000 Kč.

§ 49: Přestupky proti občanskému soužití

1) Přestupku se dopustí ten, kdo:
   a) jinému ublíží na cti tím, že ho urazí nebo vydá v posměch,
   b) jinému z nedbalosti ublíží na zdraví,
   c) úmyslně naruší občanské soužití vyhrožováním újmou na zdraví, drobným ublížením na zdraví, nepravdivým obviněním z přestupku, schválnostmi nebo jiným hrubým jednáním,
   d) omezuje nebo znemožňuje příslušníku národnostní menšiny výkon práv příslušníků národnostních menšin,
   e) působí jinému újmu pro jeho příslušnost k národnostní menšině nebo pro jeho etnický původ, pro jeho rasu, barvu pleti, pohlaví, sexuální orientaci, jazyk, víru nebo náboženství, pro jeho politické nebo jiné smýšlení, členství nebo činnost v politických stranách nebo politických hnutích, odborových organizacích nebo jiných sdruženích, pro jeho sociální původ, majetek, rod, zdravotní stav anebo pro jeho stav manželský nebo rodinný.
2) Za přestupek podle odstavce 1 písm. a) lze uložit pokutu do 5 000 Kč a za přestupek podle odstavce 1 písm. b) až e) pokutu do 20 000 Kč a za přestupek podle odstavce 1 písm. c) lze spolu s pokutou uložit zákaz pobytu.

6.2.5 Trestněprávní odpovědnost

Zákon č. 40/2009 Sb., trestní zákoník (TZK) stanoví a definuje trestné činy, přičemž uvádí, že trestným činem je protiprávní čin, který trestní zákon označuje za trestný čin a který vykazuje znaky uvedené v zákoně.

Mezi trestné činy spáchané v souvislosti s IT je možné zařadit:

- § 180 neoprávněné nakládání s osobními údaji,
- § 182 porušení tajemství dopravovaných zpráv,
- § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí,
- § 184 pomluva,
- § 191 šíření pornografie,
- § 192 výroba a jiné nakládání s dětskou pornografií,
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací,
- § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,
- § 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti,
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku,
- § 236 výroba a držení padělatelského náčiní,
- § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi,
- § 287 šíření toxikomanie,
- § 311 teroristický útok,
- § 345 křivé obvinění,
- § 348 padělání a pozměnění veřejné listiny,
- § 354 nebezpečné pronásledování,
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob,
- § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod,
- § 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka,
- § 407 podněcování útočné války.

7 ISMS a normy řady ISO 27000

Smyslem ISMS (Information Security Management System, Systém řízení bezpečnosti informací) je zabezpečit veškeré informace potřebné pro hlavní činnost organizace proti ztrátě nebo zneužití a tím zajistit kontinuitu činnosti organizace.

ISMS se zbývá ochranou informací v celém životním cyklu od jejich vzniku až po řízenou likvidaci. Pokrývá všechny formy záznamu, přenosu a sdílení informace, tedy nejen elektronickou, ale i papírovou nebo mluvenou. Ve všech formách má být informace odpovídajícím způsobem chráněna.

ISMS pro tento účel poskytuje komplexní řadu nástrojů a technik, od stanovení základních parametrů (rozsahu) ISMS, přes definici politik, pravidel a procesů až po konkrétní technické nástroje a postupy (bezpečnost IT systémů, fyzická bezpečnost na pracovišti apod.).

Výsledkem nasazení ISMS je:

- určení konkrétních informačních aktiv, která mají být chráněna,
- identifikace a klasifikace rizik ohrožujících tato informační aktiva,
- nasazení konkrétní technických i administrativních opatření, která známá rizika eliminují,
- pravidelná kontrola a vyhodnocení všech opatření, výsledky pak slouží k trvalému zlepšování procesu ochrany informačních aktiv.

7.1 Přehled norem řady ISO 27000

Základním kamenem jsou dvě normy této řady:

- ISO 27001 (Information security management systems — Requirements) specifikuje formální požadavky na zavedení ISMS.
- ISO 27002 (Code of practice for information security controls) je soubor (katalog) možných bezpečnostních opatření, ve kterém lze vyhledat vhodná řešení pro konkrétní potřeby organizace.

Další normy v této řadě se pak podrobněji věnují jak samotnému procesu přípravy a nasazení ISMS (průvodce nasazením včetně průběhu auditu), tak i technickým hlediskům v oblastech jako je bezpečnost služeb (samostatné normy pro jednotlivé vrstvy od síťové po aplikační úroveň), řešení incidentů, forenzní audit a podobně. V oblasti úložišť dat a cloudových technologií stojí za zmínku normy:

- ISO/IEC 27010 (Information security management for inter-sector and inter-organisational communications).
- ISO/IEC 27017 (Information security controls for cloud computing).
- ISO/IEC 27018 (Privacy controls for cloud computing).

- ISO/IEC 27036 (Information security aspects of ICT outsourcing and services).
- ISO/IEC 27040 (Storage security).

Kompletní seznam norem řady ISO 27000 je uveden v příloze 4.

7.2 Obvyklý postup nasazování ISMS

7.2.1 Určení rozsahu nasazení

Prvotním krokem je určení rozsahu nasazení ISMS, tedy oblastí činnosti organizace, které bude. Jde o klíčovou parametr celého procesu, protože příliš široký rozsah vede na obtížně řešitelnou úlohu, zatímco příliš úzký rozsah nemusí splnit záměr ochrany hlavní činnosti organizace.

7.2.2 Ohodnocení informačních aktiv

Následujícím krokem je identifikace a ohodnocení informačních aktiv. Cílem je v daném rozsahu vybrat všechna důležitá informační aktiva (data, se kterými se v dané oblasti činnosti pracuje) a ohodnotit jejich důležitost pro hlavní činnost organizace. Hodnocení se provádí obvykle formou klasifikační tabulky, zařazením konkrétního aktiva do jedné z kategorií (přinejmenším na stupnici veřejná, interní, důvěrná). Příklad klasifikační matice je uveden v příloze. Jednotlivé kategorie mají určený způsob nakládání s daty a to ve všech formách (elektronické, tištěné, mluvené apod.).

7.2.3 Analýza rizik

Známe-li informační aktiva a víme, která jsou pro organizaci důležitá, můžeme pro každé aktivum provést analýzu rizik. Analýza popisuje rizika hrozící ztrátou aktiva. Jednotlivá rizika jsou ohodnocena z hlediska pravděpodobnosti výskytu a míry dopadu. Pro každé riziko je pak definován návrh opatření. Opatření může být technického nebo organizačního charakteru (zavedení nebo změna technologie nebo procesu), přenesením rizika na jiný subjekt (pojištění) nebo i prostá akceptace rizika (např. pokud náklady na odstranění rizika převyšují možnou škodu).

7.2.4 Návrh bezpečnostních politik a další dokumentace

Tato etapa specifikuje konkrétní požadavky na ochranu informací formou bezpečnostních politik, provozních řádů a směrnic. Výsledkem by měla být hierarchická struktura dokumentace, která v nejnižší (provozní) úrovni zachycuje způsob práce pracovníků a konkrétní použité technologie a postupy.

7.2.5 Implementace bezpečnostních opatření

V této etapě dochází k praktické realizaci opatření podle bezpečnostního plánu a plánu implementace ISMS. Součástí této etapy je obvykle také zavedení kontrolních mechanizmů, školení pracovníků a další doplňkové činnosti potřebné k udržení kvality celého procesu. Výsledkem této etapy by měl být funkční stav organizace, který zároveň podle možností splňuje požadavky normy.

7.2.6 Certifikační proces

Certifikační proces provádí vždy externí auditor. Nejprve se v rámci předcertifikačního auditu ověřuje existence potřebné dokumentace a technických i organizačních opatření (testy procesů, techniky, penetrační testy apod).

Vlastní audit ověřuje na místě jednak formální záležitosti (dokumentaci, vnitřní legislativu), ale také znalosti pracovníků a praktické dodržování postupů popsaných v dokumentaci. V rámci auditu se neověřuje veškerá dokumentace a procesy (to není reálné z hlediska času), auditor namátkou vybírá vzorky, které prověřuje a hodnotí soulad s normou.

Výsledky auditu jsou zpracovány ve formě zprávy pro management organizace. Zpráva kromě jiného obsahuje seznam výhrad auditora. Běžná výhrada (v kategorii doporučení nebo neshoda) ještě není překážkou v certifikaci, organizace následně sama zajistí v přiměřené době nápravu kritizovaných jevů. Pokud však jde o zásadní (systémovou) neshodu, je certifikační proces přerušen až do odstranění závady.

7.2.7 PDCA cyklus

Nasazení ISMS není jednorázovou akcí nebo krátkodobým projektem. Jedná se o trvalý proces, který neustále zlepšuje parametry ochrany informací. Pro tento postup se používá zkratka PDCA cyklus (Plan-Do-Check-Act). Organizace by měla trvale pracovat na zlepšení. Pokroky oproti předchozímu stavu jsou pak ověřovány auditorem pravidelnou recertifikací v cyklu několika let.

7.3 Shrnutí

Normy této řady tvoří zcela jistě ucelený a funkční koncept zajištění informační bezpečnosti. Instituce jako banka či podobná komerční organizace může (respektive musí) jasně definovat hlavní předmět svého podnikání a tomuto cíli podřídit vlastní strukturu organizace i pravidla pro pracovníky.

Pro použití v akademickém prostředí může být problémem důsledné pokrytí všech důležitých oblastí činnosti organizace, právě s ohledem na rozmanitost činností a širokou spolupráci vědeckých týmů napříč hranicemi organizací. Je otázkou, zda dosažení certifikace v plném rozsahu všech aktivit by u akademické instituce bylo adekvátním vynaložením prostředků.

Jako rozumný kompromis se spíše jeví výběr a implementace konkrétních technických opatření, která jsou přínosná i pro oblast R&E. Striktní pravidla požadovaná normou mohou být dobrou inspirací, nikoliv dogmatem.

8 Často kladené otázky (FAQ)

Tato kapitola obsahuje nejčastější dotazy sebrané a vyhodnocené v průzkumu prováděném v rámci řešení projektu. Dotazy tak podle našeho názoru dobře reprezentují obecnou úroveň povědomí o právních otázkách cílové skupiny uživatelů.

Odpovědi jsou dále prezentovány ve zjednodušené a přehledné formě tak, aby byly dobře srozumitelné i právním laikům. Z tohoto důvodu mohou v některých případech odpovědi duplikovat již dříve uvedené podrobnější rozbory a argumenty.

Obecné otázky

Jaká je odpovědnost pracovníka za ochranu dat v případě, že organizace nemá interní předpis o nakládání dat? Z čeho se pravidla nakládání s daty v takovém případě odvozují?

I v případě, že nemá organizace stanoveny vnitřní předpisy pro nakládání s daty, je každý povinen chovat se tak, aby svým jednáním nezasáhl do práv jiného. A v případě, že to vyplývá např. z pracovní náplně, smlouvy, či jiného závazného předpisu organizace, pak se musí pracovník řídit těmito dokumenty.

Dále pro pracovníka vyplývá povinnost řídit se platnými zákony a ratifikovanými mezinárodními smlouvami. Ve vztahu k těmto předpisům platí zásada: „*ignorantia iuris non excusat*“ (neznalost zákona neomlouvá).

Jaká je právní odpovědnost provozovatele za data v Dropboxu, iCloudu a dalších veřejných cloudových úložištích?

Pokud má uživatel v datovém úložišti provozovatele „prolink“ na jiné datové úložiště, pak nese odpovědnost za data uložená v tomto jiném datovém úložišti uživatel, který tam data nahrál, případně jiný subjekt (viz EULA uzavřená mezi uživatelem a provozovatelem Dropboxu, iCloudu aj.).

Pokud má datové úložiště nastaveno striktní politiku zakazující „prolink“ na jiná datová úložiště, pak je v případě porušení smluvních podmínek (EULA) odpovědný uživatel, který tyto podmínky porušil.

Osobní údaje

Považuje se uložení osobních údajů do úložiště jiného provozovatele za zpracování osobních údajů?

Za činnost podléhající ZOOÚ je považována jakákoliv operace nebo soustava operací, kterou správce nebo zpracovatel systematicky provádí s osobními údaji, např. jejich shromažďování, zpřístupňování, zveřejňování či třídění, ale *také ukládání na nosiče informací, uchovávání a předávání.*

Dle této dikce je uložení osobních údajů do úložiště jiného provozovatele zpracováním osobních údajů.

Stává se tím (viz výše) provozovatel úložiště správcem a musí být pro tento účel registrován jako zpracovatel?

Pokud provozovatel začne zpracovávat osobní údaje, pak se stává správcem osobních údajů a je jeho povinností *stanovit účel, k němuž mají být osobní údaje zpracovány.*

Pokud je tato povinnost stanovena zákonem, nepřichází logicky v úvahu stanovení jiného účelu, resp. tento účel není třeba vůbec stanovit. Shromažďovat lze osobní údaje pouze ke stanovenému účelu (např. poskytování právní pomoci) a v rozsahu nezbytném k jeho naplnění. Dále musí být stanoveny prostředky a způsob zpracování údajů.

Zpracovatelem osobních údajů je osoba, která zpracovává osobní údaje pro správce osobních údajů (typicky tedy osoba pověřená správou nad úložištěm, aplikacemi apod.).

Pokud provozovatel úložiště manipuluje provozně s uloženými cizími daty (zálohy, migrace, obnova) a tato data mají charakter osobních (citlivých) údajů, nemůže se jednat o nepovolené shromažďování osobních údajů za strany provozovatele?

V tomto případě je třeba jasně určit, kdo nese odpovědnost za jakou činnost.

Pokud poskytovatel provozuje pouze hardwarovou část datového úložiště a zajišťuje jen základní softwarovou platformu, pak nenese odpovědnost za nakládání s osobními údaji.

Toto tvrzení je podmíněno skutečností, že nijak nezasahuje do chodu datového úložiště, tj. data nezálohuje, nepřesouvá apod. Jinak řečeno, poskytovatel prostě jen „zajišťuje přívod elektřiny, datových linek a hardware pro práci jiných“.

Na druhou stranu, pokud provozovatel ví, že jsou v datovém úložišti zpracovávány osobní údaje a provádí např. migraci nebo zálohování dat, může se stát zpracovatelem osobních údajů.

Co když provozovatel nic neví o povaze dat, která si zákazník nebo uživatel ukládá? Může mít i tak odpovědnost v případě, že se jedná o osobní nebo citlivá data?

Odpověď je částečně uvedena v předchozím bodě. Máme zato, že by měl být jasně vymezen vztah provozovatel datového úložiště vs. zákazník (uživatel). Z tohoto vymezení by mělo být jasné, jaká data (jejich povaha) budou na předmětné úložiště ukládána a kdo bude zastávat jakou roli ve vztahu k těmto datům. Touto jasnou deklarací práv a povinností lze předejít případným sporům.

Je vhodné, aby byly jasně definovány skupiny údajů a pro každou z nich:

- co se s nimi má/může dělat,
- kdo je oprávněn k nim přistupovat a za jakých podmínek,
- kdo a za jakých podmínek je oprávněn provádět „technickou údržbu“ (zálohování, přesuny apod.).

Pokud provozovatel aplikace, která zpracovává osobní data, začne používat místo lokálního externí úložiště, musí si vyžádat od všech subjektů souhlas s touto změnou i když předchozí souhlas se zpracováním údajů má?

Subjekt údajů musí být předně včas a řádně informován o tom, že jsou o něm vůbec údaje shromažďovány[27]. Obecně je tato technická změna kryta prvním souhlasem subjektu údajů.

V případě, že jsou data přenášena jinam, měla by být tato skutečnost nahlášena ÚOOÚ, neboť dochází ke změně způsobu zpracování osobních údajů.

Pokud jsou data předávána třetí straně či do zahraničí a subjekt na tuto možnost nebyl dostatečně řádně upozorněn při podpisu prvního souhlasu znamená to, že musí být vystaven souhlas nový. Subjekt údajů nemusí souhlasit s touto změnou.

Územní platnost legislativy

Jak je to s místní působností práva ve vztahu k datovým úložištím?

Z pohledu trestního práva je čin spáchán na území ČR (a tudíž se na něj vztahuje české trestní právo), pokud došlo k jednání (či části jednání) nebo následku (či části následku) na území ČR (viz *zásada teritoriality*). Z pohledu využívání datových úložišť je třeba vyzdvihnout i *zásadu personality*. Pro úplnost dále uvádíme všechny principy místní příslušnosti:

Zákon	Místo činu	Pachatelé	Trestné činy	Další podmínky
Zásada teritoriality (§ 4 odst. 1 TZK)	spáchán v ČR spáchán z části v ČR (jednání/následek)	všichni	veškeré trestné činy uvedené v TZK	
Zásada registrace (§ 5 TZK)	letadla, lodě aj.	všichni	veškeré trestné činy uvedené v TZK	
Zásada personality (§ 6 TZK)	v cizině	občan ČR	veškeré trestné činy uvedené v TZK	
Zásada ochrany (§ 7 odst. 1TZK)	v cizině	cizinec	vyjmenované trestné činy (proti republice, státním	

[27] V jakém rozsahu, pro jaký účel atd.

			orgánům aj.)	
Zásad univerzality (§ 7 odst. 2 TZK)	v cizině	cizinec	oboustranná trestnost	Proti občanu ČR.
Subsidiární zásada univerzality (§ 8 TZK)	v cizině	cizinec		Zadržen na území ČR. Nedošlo k vydání ani předání.

Kdo je zodpovědný za porušení práva, pokud data uložená v jiné zemi porušují místní legislativu? Provozovatel úložiště nebo uživatel, který je tam uložil?

Trestní právo je postaveno na principu individuální odpovědnosti za spáchaný trestný čin (i když je třeba podotknout, že tato individuální odpovědnost je modifikována možností trestněprávního postihu právnické osoby za podmínek daných zákonem č. 418/2011Sb., zejména § 8 tohoto zákona).

Tímto tvrzením nicméně není vyloučena odpovědnost správněprávní (viz zákon č. 480/2004 Sb., kdy může být odpovědný i ISP provozující datové úložiště) či občanskoprávní.

Jak snížit odpovědnost provozovatele za následky činnosti uživatele, který nedodrží např. smluvní podmínky?

Poskytovatel datového úložiště by měl učinit následující kroky, aby tak co možná nejvíce přenesl odpovědnost na uživatele, který způsobil konkrétní porušení práva:

- Jasně definovat smluvní podmínky užívání datového úložiště (včetně uvedení práv a povinností smluvních stran).
- Upozornit zákazníky na logování provozu a možnost předání informací třetím stranám, případně předání informací orgánům činným v trestním řízení.
- Nastavit procesy a pravidla, která jasně definují jednotlivé pozice (role) a jejich oprávnění, tj. např. definovat správce systému, správce aplikací, správce osobních údajů, zpracovatele osobních údajů, uživatele apod. (při definování rolí a jejich oprávnění vždy záleží na konkrétním typu datového úložiště a poskytovaných služeb).

Co když uživatel neví, že porušil zákon v zemi, kde sice jeho data leží, ale on nezná místní legislativu, protože tam nežije?

Každý uživatel by se měl seznámit s právem té které země, ve které se pohybuje a je zcela jedno, zda se v zemi nachází fakticky či digitálně. I v tomto případě tedy platí, že neznalost zákona neomlouvá.

Šifrování dat v úložišti

Pokud jsou data ukládaná do externího úložiště šifrovaná, je to dostačující opatření ze strany zákazníka pro uložení citlivých dat?

Citlivými daty se rozumí data, která nejsou osobními ani osobními citlivými daty. Jedná se např. o know-how společnosti, bezpečnostní standardy, přístupy a oprávnění, logy apod.

Je vždy na uživateli, který data ukládá, aby stanovil podmínky a pravidla (resp. správně aplikoval platná pravidla specifikovaná bezpečnostní politikou organizace pro danou kategorii dat), za jakých je možné tato data „transportovat" vně chráněné zóny (organizace), případně je předat dalším stranám ke zpracování, uskladnění apod.

Kvalitní šifrování (algoritmus i klíč odpovídající kvality) je základním, nikoliv však postačujícím předpokladem pro přenos nebo uchovávání jakýchkoliv citlivých dat.

Může být pro provozovatele nějak problematické, že má v úložišti cizí zašifrovaná data?

Ne. Pokud umožňuje ukládání šifrovaných dat (což je standardní), pak odpovědnost za obsah těchto dat nese uživatel, který je do datového úložiště nahrál.

Je však vhodné upozornit uživatele na výše uvedené, tedy na skutečnost, že nese odpovědnost za svá zašifrovaná data.

Odpovědnost provozovatele za obsah

Může na provozovatele dopadnout nějaká nepředpokládaná povinnost, pokud si tam uživatel uloží data zvláštního charakteru (např. klasifikace tajné)?

Pokud nemůže provozovatel předpokládat určitou okolnost, pak nebude odpovědný za úmyslné jednání. To však nevylučuje odpovědnost za nedbalostní jednání viz § 2912 odst. 1 OZ: „Nejedná-li škůdce, jak lze od osoby průměrných vlastností v soukromém styku důvodně očekávat, má se za to, že jedná nedbale." V této souvislosti je třeba připomenout, že ten kdo škodu způsobil (škůdce), je povinen škodu nahradit a to bez ohledu na své zavinění v případech stanovených zvlášť zákonem, jakož i při porušení smluvní povinnosti.

Provozovatel tedy může být odpovědný i za škodu způsobenou z nedbalosti.

Uživatel, který předmětná data do datového úložiště uložil a tím porušil povinnost vyplývající z jiné právní normy je zcela odpovědný za své (úmyslné či nedbalostní) jednání dle platné legislativy.

Z tohoto důvodu doporučujeme jasně stanovit účel využívání datového úložiště a povahu ukládaných dat v EULA. V případě porušení těchto podmínek je pak odpovědný uživatel, který tyto podmínky porušil.

Kdo a v jaké míře zodpovídá za obsah úložiště?

V případě poskytovatele hostingu velmi záleží na tom, jaké služby provozovatel poskytuje. Pokud se jedná pouze infrastrukturu (hardware a nic víc), pak je prostor zcela ve vlastnictví toho, kdo tam data ukládá. V tomto případě nese za obsah dat odpovědnost uživatel.

Je však vhodné uživatele upozornit na skutečnost, že nese odpovědnost za svá „zvláštní data". Případně je možné deklarovat, že tato data se do daného datového úložiště nesmí ukládat.

Obecně neexistuje univerzální řešení. Vždy záleží na konkrétním typu datového úložiště a poskytovaných služeb. Za služby datového úložiště je poskytovatel ze zákona odpovědný tehdy:

- Mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní.
- Dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.
- Poskytovatel hostingu odpovídá za obsah vždy, pokud vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.
- Zákon však ani v tomto případě neukládá provozovateli povinnost aktivně vyhledávat uložená protiprávní data uživatelů.
- Za protiprávní jednání nese vždy odpovědnost uživatel, který se protiprávně choval.

Jaký je správný postup provozovatele úložiště v prevenci i v reakci na nelegální obsah?

Je vhodné aplikovat doporučení uvedené na konci kap. 7.2.1.

Může nebo musí provozovatel nelegální obsah odstranit z úložiště i proti vůli nebo bez vědomí uživatele?

Může (respektive musí) zamezit přístup k těmto datům a následně např. informovat orgány činné v trestním řízení či nadřízené daného uživatele (v závislosti na nastavených procesech), pokud mohl vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.

Kdo všechno má právo požadovat odstranění nelegálního obsahu? A jak je to v situaci, kdy data leží fyzicky v jiném právním prostředí, než kam spadá uživatel?

Typicky mohou odstranění dat požadovat ti, do jejichž zájmů bylo zasaženo a jejich právní zástupci. Tito zpravidla informují poskytovatele datového úložiště o protiprávním obsahu zde uloženém. Poskytovatel by tento podnět měl prověřit a pokud bude založen na pravdě, je povinen zamezit přístup k takovým datům. Dále se doporučuje postupovat dle vnitřních směrnic a procesů organizace.

Stejně tak mohou požadovat odstranění dat i orgány činné v trestním řízení či další bezpečnostní složky.

Jsou nějaké nástroje a služby, které by provozovatel neměl poskytovat? Např. indexování veřejného obsahu uživatelů a vyhledávání v něm jako poskytuje uloz.to?

Indexace obsahu (vyhledávání apod.) může být poskytována, pokud je to účelem služeb datového úložiště a uživatelé jsou s tímto seznámeni. Pokud jde o datové úložiště kde jsou ukládány citlivé údaje nebo dokumenty, které nechtějí uživatelé veřejně zpřístupňovat), je plošná indexace a vyhledávání nežádoucí.

Obecně nesmí být poskytovány služby, které porušují smluvní podmínky (EULA) či platné právní normy.

Shromažďování provozních dat a logování přístupových operací

Existuje povinnost provozovatele zaznamenávat (logovat) informace o tom kdo, kdy a co uložil nebo zpřístupnil?

V rámci hostingové služby tato povinnost není dána. Nicméně doporučujeme respektovat doporučení uvedená v kap. 7.2.1, neboť vlastní logy mohou sloužit k identifikaci osoby, která jednala protiprávně či v rozporu s přijatou EULA.

Platí povinnost logovat i přístup (čtení) dat z úložiště?

Viz předchozí odpověď. Tato povinnost není zákonem dána, avšak je vhodné z výše uvedených důvodů uchovávat i záznamy tohoto typu.

Kdo má právo žádat tyto informace (logy)?

Orgány činné v trestním řízení a další bezpečnostní složky. Dále pak subjekt provozující datové úložiště, aby zjistil, zda došlo např. k porušení smluvních podmínek, vnitřních předpisů apod. V tomto případě je však vhodné mít nastaveny vnitřní procesy, které budou jasně deklarovat, kdo a za jakých podmínek má k takovým datům přístup.

Naopak, může „nadměrným“ logováním dojít k porušení práv uživatele na soukromí?

Pokud jsou logovány údaje uvedené v kap. 7.2.1 a jsou respektována zde uvedená doporučení a uživatel je s procesem logování prokazatelně seznámen, pak by nemělo dojít k porušení jeho práv.

Mohou se logovací údaje použít pro optimalizaci služeb, případně nabídku nových vhodnějších služeb uživateli, nebo je nutné mít k těmto účelům vždy souhlas uživatele?

Odosobněné údaje získané z logu provozu je možné využít k optimalizaci služeb. Pokud bude v EULA obsaženo, že je možné využívat logy a další identifikátory (např. cookies) k cílení reklamy či jiných služeb a uživatel s tím souhlasí, pak lze tyto údaje využívat i tímto způsobem.

Je určena nějaká minimální a maximální lhůta, po kterou mají být logy uschovány?

S odkazem na informace uvedené v kap. 7.2.1 doporučujeme uchovávat takové údaje po dobu 6 měsíců.

Smluvní ujednání a obecná odpovědnost

Vztah mezi uživatelem a poskytovatelem je určen smlouvou nebo EULA. Existují ale nějaká další práva a povinnosti, kterých se nelze smluvně vzdát?

EULA je de-facto smlouvou mezi uživatelem a provozovatelem. Mimoto existuje řada dalších práv, kterých se nelze vzdát. Typicky se není možné vzdát přirozených osobnostních práv, např. osobnostní právo autora, právo na změnu rozhodnutí, sociální práva, právo na zdraví a život apod.

Jak silně jsou závazné elektronicky odsouhlasené podmínky bez papírové smlouvy?

Elektronicky odsouhlasené podmínky není třeba znovu sepisovat v papírové podobě. Písemnou formu vyžadují konkrétní typy smluv uvedené v zákoně nebo smlouvy, kde se na tom účastníci vzájemně dohodli (blíže viz § 560 OZ a násl.).

Podle aktuální právní úpravy nelze např. uzavřít elektronicky kupní smlouvu, jíž se převádí vlastnické právo k nemovitosti, která podléhá evidenci v katastru nemovitostí nebo smlouvu o zřízení věcného břemene k nemovitosti. Z možnosti uzavření smlouvy v elektronické podobě jsou rovněž vyloučeny ty smlouvy, které musí být učiněny ve formě notářského zápisu, kupříkladu společenská smlouva společnosti s ručením omezeným nebo dohody o modifikaci společného jmění manželů. Taktéž nebude možné uzavřít elektronicky písemnou smlouvu osobami, které nemohou číst a psát. Je tedy vhodné do EULA začlenit i „zaškrtávací políčko“, kde osoba potvrzuje, že umí číst a psát.

Ostatní

Jak se na poskytovatele úložiště vztahuje autorský zákon?

Trestněprávní odpovědnost za porušení práv autorských je popsána v kap. 7.2.5 (viz § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi).

Autorský zákon definuje co je to dílo, kdo je autorem, co je to zaměstnanecké dílo apod. Vlastní rozbor autorských práv by byl nad rámec tohoto dokumentu.

Jak se na poskytovatele úložiště vztahuje zákon o svobodném přístupu k informacím?

Záleží na tom o jaký subjekt poskytovatele se jedná. Tento zákon se vztahuje na subjekty uvedené v § 2 Povinnost poskytovat informace:

- Povinnými subjekty, které mají podle tohoto zákona povinnost poskytovat informace vztahující se k jejich působnosti jsou státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce.
- 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.
- Zákon se nevztahuje na poskytování informací, které jsou předmětem průmyslového vlastnictví a dalších informací, pokud zvláštní zákon upravuje jejich poskytování, zejména vyřízení žádosti včetně náležitostí a způsobu podání žádosti, lhůt, opravných prostředků a způsobu poskytnutí informací.
- Povinnost poskytovat informace se netýká dotazů na názory, budoucí rozhodnutí a vytváření nových informací.

Jak se na poskytovatele úložiště nebo jeho uživatele vztahuje zákon o kybernetické bezpečnosti?

Záleží o jaký subjekt poskytovatele se jedná. Velmi zjednodušeně lze konstatovat, že pokud se nejedná o subjekt, který je definován jako kritická informační či komunikační infrastruktura, pak se ho tento zákon netýká. Zákon o kybernetické bezpečnosti však funguje i preventivně a to tak, že informuje uživatele (prostřednictvím NBÚ resp. NCKB) o incidentech a hrozbách, které se se v kyberprostoru odehrávají.

9 Vnitřní předpisy a EULA

V této kapitole se pokusíme shrnout jak právní, tak technické náležitosti obou výše uvedených typů dokumentů. Podrobnější popis jednotlivých typů dokumentů a základní právní rámec lze nalézt v předchozích kapitolách, v příloze jsou pak uvedeny konkrétní příklady obou typů norem.

Každodenní praxe ukazuje, že při vlastní tvorbě jak vnitřního předpisu, tak smluvních podmínek (EULA) je třeba *vzít v potaz všechny okolnosti*, které se k vlastnímu provozu datových úložišť mohou vztahovat (např. povaha ukládaných dat, potřeba dostupnosti, replikace dat, počet uživatelů přistupujících k datům apod.). Z tohoto důvodu není možné vytvořit obecné a plošně aplikovatelné pravidla či smluvní podmínky. Lze pouze upozornit na podstatné náležitosti těchto dokumentů.

Vlastní prováděcí předpis či smlouvu je vhodné vždy modifikovat a dotvořit na základě *vzájemné spolupráce správce systému* (který by měl definovat zejména technické náležitosti, včetně definování požadavků ze strany provozovatele datového úložiště) s *právním oddělením* (které by předložené požadavky mělo zaštítit legislativním rámcem, případně by mělo upozornit na možný rozpor s právem ČR či EU).

Doporučujeme vytvořit smlouvu (resp. smluvní podmínky), která bude definovat pouze základní práva a povinnosti. Tento dokument by měl být pokud možno stručný a přehledný a neměl by odradit uživatele od seznámení se s ním. V rámci tohoto dokumentu pak doporučujeme uvést odkaz na plné znění (obdobně jak to známe z běžné praxe) smluvních podmínek či pravidel užívání poskytovaných služeb. V tomto plném znění by pak měly být dopodrobna rozebrány jednotlivé pojmy, práva, povinnosti a možnosti interakce třetích stran apod.

- Z hlediska práva jde v případě EULA především o deklaraci základních pojmů,
- definování rolí, tj. vymezení jednotlivých subjektů právního vztahu (typicky správce, vlastník, auditor),
- vymezení práv a povinností těchto subjektů,
- přechodná a závěrečná ustanovení.

Z hlediska vnitřního předpisu pak jde především o definici rolí a vymezení jejich práv a povinností (viz výše).

Zopakujme, že EULA je soukromoprávní normou (smlouvou) typicky uzavíranou mezi poskytovatelem a uživatelem služby.

Vnitřní předpis je právní normou, kterou na základě zákona vytváří vlastník či provozovatel určité služby za účelem stanovení podmínek a pravidel jejího užívání (typicky v rámci organizace se jedná o vztah správce a vlastníka systému).

Obě výše uvedené právní normy by v sobě měly obsahovat pravidla chování, která přikazují, zakazují a opravňují k výkonu určitého druhu činnosti. Tato pravidla by měla být stanovena relativně vyváženě, avšak měla by umožňovat správci služeb autoritativním způsobem řešit incidenty, jakož i ohrožení služeb či porušení právních norem.

Dále uvedeme některá doporučení pro jednotlivé kategorie poskytovaných služeb, která je vhodné při tvorbě těchto norem respektovat.

Uchovávání provozních a lokalizačních údajů

EULA

- Upozornit uživatele na skutečnost, že dochází k uchovávání provozních a lokalizačních údajů a dalších identifikátorů (např. MAC adresa) ve vztahu k veškeré jeho činnosti spojené s datovým úložištěm.
- Ponechat možnost pro uživatele odmítnout využívání takové služby za těchto podmínek.

Vnitřní předpis

- Uchovávat pouze údaje, které se bezprostředně týkají dané služby či úložiště.
- Vlastní uchovávání provozních a lokalizačních údajů mělo respektovat princip odděleného uchovávání těchto údajů od údajů obsahových.
- Uchovávat provozní a lokalizační údaje v rozsahu stanoveném ZoEK, tedy zajišťovat:
    - údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace,
    - údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace.
- Uvedené údaje uchovávat po dobu 6 měsíců. Pak je mazat, vyjma případů uvedených v § 97 ZoEK.
- Zpracovat vnitřní technicko-organizační předpis pro zajištění ochrany provozních a lokalizačních, jakož i dalších ukládaných údajů.
- Stanovit podmínky, za kterých bude možné uvedená data předávat třetím stranám.

Provoz datového úložiště

Obecné zásady

- Stanovit pravidla řízení přístupu.
- Ošetřit povahu a účel ukládaných dat (vzhledem k povaze a účelu poskytované služby).

EULA

- Transparentně seznámit uživatele s podmínkami užívání služeb externího datového úložiště.

Vnitřní předpis

- Vlastní potvrzení o seznámení se s podmínkami EULA uchovávat společně s údaji, které opravňují uživatele k užívání poskytovaných služeb.
- Vykonávat správu nad poskytovanými službami a v případě, že se správce vzhledem k předmětu své činnosti, okolnostem a povaze případu mohl vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, postupovat dle vnitřního právního předpisu, který je vytvořen pro správu a dozor (tj. zejména: zaznamenat incident, znepřístupnit data, vytvořit zálohu dat, zajistit provozní a lokalizační údaje a kontaktovat právní oddělení).
- Informovat uživatele o kompromitaci, či možnosti kompromitace dat.
- Vydávat upozornění v případě zjištění hrozby či incidentu, vztahujícímu se k provozované službě či úložišti.

Osobní údaje

EULA

- Seznámit uživatele (subjektu údajů) s povahou uchovávaných údajů.
- Stanovit období, na které je souhlas s uchováváním údajů dán.
- Stanovit účel uchovávání a zpracování osobních údajů.
- Vložit souhlas uživatele s výše uvedeným do EULA.

Vnitřní předpis

- Definice osobních údajů a citlivých dat.
- Stanovit účel uchovávání a zpracování osobních údajů.
- Stanovení procesů při kompromitaci či zásahu do osobních údajů nebo citlivých dat.
- Uchovávat potvrzení o seznámení se s povahou ukládaných dat společně s údaji, které opravňují uživatele k užívání poskytovaných služeb.
- Stanovit období, na které je souhlas s uchováváním údajů dán.
- Po uplynutí této lhůty vyžádat souhlas nový.

Uložená data

Obecné zásady

- Stanovit jasné a předem vymezené procesy a pravidla, které definují jak poskytování služeb (resp. jejich změnu), tak proces přidělování uživatelských práv (včetně přístupu k informacím).

- Upozornit na možnost předání dat o případném incidentu třetí straně (orgánům činným v trestním řízení, zpravodajským službám, subjektům podílejícím se na ochraně práv autorských apod.) v případě, že dojde ke spáchání trestného činu, přestupku či jiného protiprávního jednání.

EULA

- Seznámit uživatele s podmínkami šíření dat mezi uživateli.
- Jasně vymezit práva a povinnosti jednotlivých stran (poskytovatel a uživatel).
- Upozornit uživatele na občanskoprávní odpovědnost za škodu.
- Upozornit uživatele na trestněprávní odpovědnost.

Vnitřní předpis

- Vzhledem k poskytovaným službám je nutné stanovit podmínky šíření dat mezi uživateli.
- Při šíření dat je vhodné nastavit pravidla tak, aby bylo jasné, že uživatel dává souhlas (a v jakém rozsahu) s šířením jeho dat.
- Upozornit správce na občanskoprávní odpovědnost za škodu.
- Upozornit správce na trestněprávní odpovědnost.

10 Literatura a odkazy

[1] BITPIPE. *Data Classification Reports.* Dostupné z: http://www.bitpipe.com/tlist/Data-Classification.html

[2] ČESKO. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Dostupný z: http://www.zakonyprolidi.cz/cs/2000-101

[3] ČESKO. Zákon č. 121/2000 Sb., autorský zákon. Dostupný z: http://www.zakonyprolidi.cz/cs/2000-121

[4] ČESKO. Zákon č. 480/2004 Sb., o některých službách informační společnosti. Dostupný z: http://www.zakonyprolidi.cz/cs/2004-480

[5] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. Dostupný z: http://www.zakonyprolidi.cz/cs/2009-40

[6] ČESKO. Zákon č. 89/2012 Sb., občanský zákoník. Dostupný z: http://www.zakonyprolidi.cz/cs/2012-89

[7] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Dostupný z: http://www.zakonyprolidi.cz/cs/2014-181

[8] DONÁT, Josef. *Právní aspekty cloud computingu*. Dostupné z: http://www.systemonline.cz/clanky/pravni-aspekty-cloud-computingu.htm

[9] FEDERAL INFORMATION PROCESSING STANDARDS. *Standards for Security Categorization of Federal Information and Information Systems*. Publication 199. Dostupné z: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[10] HØIEM, Øivind. *Guidelines for Classification of Information*. © Terena 2013. Dostupné z: http://services.geant.net/cbp/Knowledge_Base/Security/Documents/gn3-na3-t4-ufs136.pdf

[11] ISO ORGANIZATION. *The ISO27k FAQ*. Dostupné z: http://www.iso27001security.com/html/faq.html

[12] JANSA, Lukáš. *Interní předpisy firmy ve vztahu k užívání IT*. Dostupné z: http://www.pravoit.cz/article/interni-predpisy-firmy-ve-vztahu-k-uzivani-it

[13] JANSA, Lukáš. *Odpovědnost za škodu v IT*. Dostupné z: http://www.pravoit.cz/article/odpovednost-za-skodu-v-it

[14] JANSA, Lukáš. *Odpovědnost za ztrátu dat poskytovatele hostingu či cloudů*. Dostupé z: http://www.pravoit.cz/article/odpovednost-za-ztratu-dat-poskytovatele-hostingu-ci-cloudu

[15] MALIŠ, Petr. *Právní aspekty přijetí zákona o kybernetické bezpečnosti*. Dostupné z: http://www.pravoit.cz/article/pravni-aspekty-prijeti-zakona-o-kyberneticke-bezpecnosti

[16] MARKIEWICZ, Doug. *Guidelines for Data Classification.* Dostupné z: http://www.cmu.edu/iso/governance/guidelines/data-classification.html

[17] NBÚ. *Bezpečnostní provozní směrnice informačního systému*. Dostupné z: http://www.nbu.cz/download/nodeid-875/

[18] NBÚ. *Minimální obsah bezpečnostní dokumentace pro malé informační systémy pro zpracování utajovaných informací*. Dostupné z: http://www.nbu.cz/download/nodeid-782/

[19] OTEVŘEL, Petr. *Několik postřehů ze sjednávání smlouvy o IaaS*. Dostupné z: http://www.pravoit.cz/article/nekolik-postrehu-ze-sjednavani-smlouvy-o-iaas

[20] OTEVŘEL, Petr. *Sjednávání smluv v IT podle nového občanského zákoníku*. Dostupné z: http://www.systemonline.cz/it-pravo/sjednavani-smluv-v-it-podle-noveho-obcanskeho-zakoniku.htm

[21] RUEGGER, Cody. *Legal Issues in Cloud Computing*. Dostupné z: http://stlr.org/2013/11/18/legal-issues-in-cloud-computing/

[22] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb*. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002

Příloha 1: Příklad EULA

Pravidla využití služeb datových úložišť CESNET

1. Uživatelem (odběratelem služeb) datových úložišť (DÚ) sdružení CESNET se může stát na základě smluvního vztahu mezi sdružením CESNET a organizací fyzická osoba, která je buď v platném pracovněprávním vztahu (zaměstnanci) nebo v platném studijním vztahu (studenti) k právnické osobě (organizaci), která splňuje „Zásady pro přístup do Velké infrastruktury CESNET (Access Policy, AP)“ sdružení CESNET (viz http://www.cesnet.cz/doc/podminky.html).
2. Uživatel smí DÚ využívat pouze pro přenos a ukládání dat, která souvisejí s činnostmi ve vědě, výzkumu, vývoji, šíření vzdělanosti, kultury a prosperity, detailně viz „Zásady přijatelného užití Velké infrastruktury CESNET (Acceptable Use Policy, AUP)“, které jsou přílohou AP viz výše.
3. Správcem DÚ je sdružení CESNET, http://www.cesnet.cz/.
4. Uživatelé služeb DÚ jsou organizováni v tzv. virtuálních organizacích (VO). VO má správce a členy. Správce VO je partnerem správce DÚ pro dojednání podmínek využití služeb a způsobů přístupu uživatelů k DÚ. Portfolio a úroveň služeb poskytovaných konkrétnímu uživateli závisí na jeho členství ve VO. Uživatel může být členem více VO.
5. Pro účely těchto pravidel jsou uživatelé služeb přístupných primárně prostřednictvím federace identit (tj. zejména FileSender a ownCloud) považováni za členy specifických VO, jejichž správcem je správce DÚ.
6. Úroveň a základní vlastnosti poskytovaných datových služeb jsou provozovatelem DÚ vyjádřeny v technické dokumentaci na webu http://du.cesnet.cz, která tak slouží jako Deklarace úrovně služeb (Service Level Declaration, SLD).
7. Požadavky na nestandardní konfigurace DÚ řeší správce DÚ se správcem VO. Takové požadavky mohou zahrnovat poskytnutí specifických přístupových protokolů, speciální zacházení s uloženými daty (např. postačuje pouze jedna kopie na páskách, nebo je naopak vyžadována vyšší úroveň zabezpečení větším počtem geograficky oddělených páskových replik) a další. Správce DÚ je oprávněn požadovat zdůvodnění potřebnosti a účelnosti takové konfigurace a o poskytnutí takové služby rozhoduje dle vlastního uvážení na základě účelu požadovaného prostoru, požadované kapacity, volných kapacit na úložišti, požadovaného typu přístupu k datům a požadované kvalitě ochrany dat.
8. DÚ je technicky realizováno jako hierarchické. To znamená, že obsahuje vrstvu (tier) rychlých diskových polí a pomalejší páskovou knihovnu či vypínatelné disky (MAID), data jsou automaticky dle nastavených pravidel přesouvána (migrována) mezi disky a páskami. Pro uživatele jsou přesuny dat transparentní, všechna data se mu jeví, jako by byla na discích. Pokud ale přistoupí k datům, která jsou odsunuta do pomalejších tierů úložiště, jejich přesun zpět

na disky nějakou dobu trvá. Důvody pro toto řešení jsou ekonomické, uchovávání dat na páskách nebo vypnutých discích je provozně výrazně levnější.

9. Politiky přesunů dat mezi vrstvami úložiště jsou nastaveny na základě dohody mezi správcem úložiště a správcem VO, aby byly naplněny potřeby uživatelů s ohledem na technické a ekonomické požadavky provozu. Je vhodné, aby uživatel bral při své práci v úvahu fakt, že vybavovací doba delší dobu nepoužívaných dat je delší.
10. Způsoby přístupu uživatele k DÚ jsou popsány v samostatném přehledu na webu datových úložišť https://du.cesnet.cz/. Návody také obsahují popisy autentizačních mechanismů pro přístup uživatele.
11. Správce úložiště je po uživateli oprávněn požadovat potvrzení, že uživatel je oprávněn k úložišti přistupovat ve smyslu bodu 1. Toto potvrzení se vyžaduje zpravidla jedenkrát ročně formou prodloužení členství uživatele ve VO. K prodloužení členství je uživatel vyzván automatizovaně prostřednictvím systému správy uživatelů na uvedenou administrativní emailovou adresu, který k prodloužení členství opakovaně uživatele vyzývá. Výzva je doplněna instrukcemi, jak prodloužení provést. Obvyklou formou je přihlášení do systému pomocí federace eduID.cz, alternativní postupy jsou popsány v dokumentaci služby Hostel.
12. Zaniklo-li členství uživatele ve VO, správce úložiště zpravidla data tohoto uživatele znepřístupní (nastavením přístupových práv). Správce VO může se správcem úložiště dohodnout jinou formu nakládání s daty takového uživatele, přitom jsou vázáni pravidly použití úložiště a účelem příslušné VO. Po uplynutí šesti měsíců po zániku členství uživatele ve VO je správce úložiště oprávněn data tohoto uživatele v příslušné VO smazat. Obvykle se mazání provádí po výrazně delší době, umožňuje-li to provozní stav úložiště.
13. Správce úložiště v odůvodněných případech a dle technických možností jednorázově vydá uživateli se zaniklým členstvím jeho data z příslušné VO ke stažení po síti. Správce úložiště bude přitom po uživateli požadovat doklad, že je původcem těchto dat (např. prokázání identity a doložení předchozí příslušnosti k organizaci, kterou měl uživatel vedenou v systému správy uživatelů a podobně).
14. Uživatel je povinen užívat služeb DÚ s ohledem na ostatní uživatele.
15. Uživatel je povinen chránit přístup ke svým účtům pomocí netriviálního hesla. Netriviálním heslem je myšleno takové heslo, které není možno odvodit (i po jednoduchých mutacích) z údajů známých o majiteli účtu, a které není jménem osoby, zvířete nebo věci (i po jednoduchých mutacích).
16. Správci DÚ jsou oprávněni provádět testy na výskyt triviálních hesel; v případě pozitivního výsledku uvědomí bezpečným kanálem majitele účtu, který je tímto povinen neprodleně heslo změnit (do doby změny hesla může být původní účet uzavřen).
17. Uživatel je povinen bez zbytečného odkladu oznámit na adresu du-support(zavináč)cesnet.cz, pokud se dozví nebo pokud se domnívá, že došlo ke

zneužití infrastruktury, vyzrazení osobních přístupových údajů, nebo jinému jevu, který může indikovat bezpečnostní incident, jako například podivné chování účtu, objevování nebo mizení souborů a podobně.

18. Uživatel bere na vědomí, že informace o uživateli a jeho činnosti na úložišti jsou ukládány pro účely administrativy, provozu, statistik, monitoringu a bezpečnosti.
19. Správce DÚ je oprávněn regulovat nebo zablokovat přístup uživatele z důvodů administrativních, provozních nebo bezpečnostních. V případě zvlášť hrubého porušování provozních a bezpečnostních pravidel je správce DÚ oprávněn uživateli odepřít přístup k úložišti i trvale.
20. Uživatel nesmí ke svému účtu povolit přístup jiné osobě sdělením svých přístupových údajů (hesla, soukromého klíče a podobně). Uživatel je povinen soukromé přístupové údaje udržovat v tajnosti.
21. Uživatel nesmí užívat DÚ způsobem porušujícím platné zákony (zejména autorský zákon a zákon o ochraně osobních údajů), obcházet administrativní a bezpečnostní opatření pro přístup k DÚ, nebo se o takové obcházení pokoušet.
22. Uživatel by neměl vynucovat přesun dat z pomalejších (archivních) vrstev úložiště na disky, pokud tato data nehodlá bezprostředně využívat. Přesuny neobvykle velkého množství dat je vhodné předem dohodnout se správcem DÚ.
23. Na DÚ jsou nastaveny kvóty, které omezují množství dat, která uživatel může na DÚ uložit. Kvóty slouží zejména pro ochranu uživatelů před chybou. Nastavení kvóty neznamená, že taková kapacita je skutečně na úložišti dostupná. Garantované rezervace prostoru pro data nejsou individuálním uživatelům poskytovány. Využití úložiště uživatelem je z technických důvodů sledováno systémem accountingu.
24. Datové úložiště je provozováno v „best effort“ režimu. Provozovatel vyvíjí veškeré úsilí k zaručení dostupnosti a bezpečnosti datových služeb a k uchování a bezpečnosti dat uložených uživateli na datových úložištích. Provozovatel pro tento účel zajišťuje, že ochrana uložených dat a přístup k nim odpovídají standardům špičkových technologií vyvinutých pro provoz datových úložišť. Provozovatel také deklaruje vysokou odbornou a morální úroveň osob obslužného technického personálu. Vysoká dostupnost a bezpečnost datových služeb je dána redundancí hardwarových komponent, bezpečnostními politikami HSM systému, zálohováním požadovaných dat pro jednotlivé uživatele či VO a v neposlední řadě parametry technické a systémové podpory, kterou v režimu 7×24 smluvně zajišťuje dodavatel DÚ. Architektura úložišť byla navržena pro špičkové zajištění před ztrátou dat (až 99,99999999%). Provozovatel neposkytuje další záruky nad ty, které vyplývají z režimu „best effort“ popsaného výše.
25. Správce DÚ deklaruje, že zařízení sloužící k provozu služeb DÚ se nacházejí na území České republiky.

26. Správce DÚ je oprávněn tyto podmínky změnit. Nová verze pravidel je zveřejněna vždy nejméně jeden měsíc před jejich platností na webu sdružení CESNET.
27. Tato pravidla jsou dostupná v české a anglické verzi. Dojde-li k rozporu mezi těmito verzemi, přednost má verze česká.

Příloha 2: Příklad smluvních podmínek

Následující text je příkladem konkrétního (pro potřeby dokumentu zjednodušeného) *smluvního ujednání*, jehož odsouhlasením se uživatel níže uvedené služby zavazuje dodržovat pravidla v něm stanovená. V případě porušení smluvních ujednání kterýmkoli uživatelem, může poskytovatel uvedené služby uplatnit opatření obsažená v tomto smluvním ujednání, případně jiná opatření dle platných zákonů ČR nebo mezinárodních smluv, jimiž je ČR vázána.

Všeobecné smluvní podmínky využívání služeb datových úložišť CESNET

1. Obecné pojmy
   1.1. Datové úložiště
   1.2. Poskytovatel služby (**Poskytovatel**)
   1.3. Uživatel služby (**Uživatel**)
   1.4. **Služba** představuje soubor služeb poskytovaných **Poskytovatelem Uživateli** spočívajících zejména v ukládání obsahu informací poskytnutých **Uživatelem** ve smyslu ustanovení § 5 zákona č. 480/2004 Sb., o některých službách informační společnosti, v účinném znění.
   1.5. Strany uzavírají smlouvu podle občanského zákoníku a dalších relevantních právních předpisů České republiky. Smlouva je uzavřena okamžikem, kdy uživatel vysloví souhlas s těmito smluvními podmínkami a jeho projev vůle je doručen poskytovateli služeb.
   1.6. Data poskytnutá **Uživatelem** a jím k tomuto účelu zaslaná prostřednictvím služby jsou **Poskytovatelem** uložena v jeho úložném prostoru, který je přístupný **Uživateli**, jež data nahrál (nebo k nim jiným uživatelům umožnil přístup) a **Poskytovateli**.
2. Základní vlastnosti **Služby**
   2.1. **Služby** poskytované **Uživatelům** spočívají v následujících činnostech:
      a) poskytnutí datového prostoru v rámci služby tak, aby si **Uživatel** mohl ukládat, mazat, případně poskytovat jím vložená data jiným osobám.
   2.2. **Služby** uvedené v čl. 2.1. jsou poskytovány **Uživatelům** bezplatně na základě odsouhlasení těchto podmínek.
3. Práva a povinnosti **Uživatele**
   3.1. **Uživatel** je oprávněn využívat **Službu** v plném rozsahu.
   3.2. Plný rozsah **Služeb**:
      a) oprávnění nahrávání a stahování dat v rámci přiděleného prostoru (xGB),
      b) mazání uživatelem uložených dat,
      c) oprávnění zasílat komentáře k uloženým datům,
      d) sdělování informací o uložených datech jiným uživatelům,
      e) oprávnění poskytnout URL uložených dat jiným uživatelům k jejich stažení,

f) oprávnění stažení dat z obdržených URL,
g) oprávnění stanovit expiraci dat uložených prostřednictvím služby.

3.3. **Uživatel** je oprávněn zvolit si název uložených dat. Název uložených dat nesmí obsahovat vulgarizmy nebo výrazy, které odporují čl. 3.4. těchto **Podmínek**. Nebude-li takový název odpovídat podmínkám uvedeným v předchozí větě nebo bude-li jinak obsahově či graficky nevhodný, vyhrazuje si **Poskytovatel** právo na změnu jeho znění či grafické podoby.

3.4. Uložená data (soubory nebo jejich části/pasáže) nesmí být v rozporu s právním řádem České republiky.[28] Výslovně je v rámci **Služby** zakázáno umisťovat a šířit soubory a jiné informace, které zejména:

a) porušují práva duševního vlastnictví[29], zejména autorská práva, práva související s právem autorským, práva k ochranné známce, práva k chráněnému označení původu nebo jiná průmyslová práva[30] třetích osob,
b) obsahují neoprávněně užité ochranné známky, obchodní jména a chráněná označení původu, k nimž přísluší výhradní právo jinému, nebo jakékoliv označení s ním zaměnitelné,
c) vedou k nekale-soutěžnímu jednání, které je v rozporu s předpisy upravujícími soutěž v hospodářském styku nebo se zvyklostmi soutěže, přičemž poškodí dobrou pověst nebo ohrozí chod nebo rozvoj podniku soutěžitele nebo je způsobilé tak učinit,
d) obsahují pasáže, jež podněcují k trestnému činu nebo schvalují zločin nebo veřejně vychvalují pro zločin jeho pachatele,
e) obsahují pasáže, jež svádí jiné ke zneužívání návykové látky nebo je v tom podporují anebo zneužívání takové látky jinak podněcují,
f) obsahují pasáže, jež vyhrožují jiným osobám nebo skupině obyvatelů usmrcením, ublížením na zdraví nebo způsobením škody velkého rozsahu,
g) obsahují pasáže, jež hanobí některý národ, jeho jazyk, některou etnickou skupinu nebo rasu, nebo skupinu obyvatelů republiky pro jejich politické přesvědčení, vyznání nebo proto, že jsou bez vyznání,
h) obsahují pasáže, jež podněcují k nenávisti k některému národu, etnické skupině, rase, náboženství, třídě nebo jiné skupině osob nebo k omezování práv a svobod jejich příslušníků,
i) obsahují poplašnou zprávu, která je nepravdivá,
j) obsahují pornografická díla, mající sexuální či erotický obsah, jež jsou v rozporu s právním řádem ČR či obecně uznávanými etickými a morálními

---

[28] Zejména nesmí obsahovat pasáže, jež jsou protiprávní, zejména porušují ustanovení zákona č. 40/2009 Sb., Trestní zákoník; zákona č. 200/1990 Sb., o přestupcích apod.

[29] Zejména zákon č. 121/2000 Sb., Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů.

[30] Vyplývající zejména ze zákonů č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích, č. 206/2000 Sb., o ochraně biotechnologických vynálezů, č. 478/1992 Sb., o užitných vzorech, č. 207/2000 S., o ochraně průmyslových vzorů, č. 529/1991 Sb., o ochraně topografií polovodičových výrobků, vše ve znění pozdějších předpisů.

principy (zejména obsahují pornografická díla zobrazující dítě, styk se zvířetem nebo v nichž se projevuje násilí či neúcta k člověku),

k) zobrazující kruté či nelidské zacházení s lidmi (např. týrání, či mučení),

l) zobrazující týrání zvířete,

m) obsahují nepravdivý údaj o jiném, který je způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo mu způsobit jinou vážnou újmu,

n) podporují nebo propagují hnutí, které prokazatelně směřuje k potlačení práv a svobod člověka nebo hlásá národnostní, rasovou, náboženskou či třídní zášť nebo zášť vůči jiné skupině osob, nebo veřejně projevují sympatie k těmto hnutím,

o) popírají, zpochybňují, schvalují nebo se snaží ospravedlnit nacistické nebo komunistické genocidium nebo jiné zločiny nacistů nebo komunistů proti lidskosti,

p) porušují zákonem stanovenou nebo uznanou povinnost mlčenlivosti či porušují nebo ohrožují obchodní tajemství třetí osoby.

3.5. **Uživatel** odpovídá za data jím uložená. V případě, že **Uživatel** umožní třetí osobě přístup ke službě prostřednictvím svých přístupových údajů (heslo, soukromý klíč, apod.), nese plnou odpovědnost za případné následky jednání takovéto osoby, včetně odpovědnosti za škodu.

3.6. **Uživatelé** nesmějí do svých souborů a jiných informací vkládat jakoukoliv placenou reklamu. Placenou reklamou se rozumí také reklama, za níž uživatel získá jakékoliv jiné plnění nebo protislužbu. Za reklamu se nepovažují odkazy na jiné servery.

3.7. Prostor poskytnutý **Uživatelům** je určen zejména pro ukládání dat k vědecko-výzkumným, studijním, pedagogickým, kulturním a jiným obdobným účelům.

3.8. **Uživatel** se nesmí žádným způsobem pokoušet prolomit zabezpečení služby, obcházet administrativní a bezpečnostní opatření pro přístup ke službě nebo se o takové obcházení pokoušet, ohrozit provoz služby nebo získávat osobní údaje o jiných **Uživatelích**.

3.9. Je zakázáno prostřednictvím **Služby** zasílat nevyžádaná obchodní sdělení (spam).

3.10. **Uživatel** je povinen bez zbytečného odkladu upozornit **Poskytovatele** (na e-mailové adrese) na porušení těchto **Podmínek**, zejména pokud se domnívá, že došlo či dochází ke zneužívání **Služby**, vyzrazení osobních přístupových údajů nebo k jinému jevu, který může indikovat bezpečnostní incident.

3.11. **Uživatelé** jsou si vědomi toho, že za jejich projev, či uveřejnění materiálů jim nepřísluší žádná finanční či nefinanční náhrada. Veškeré jednání je zcela dobrovolné.

3.12. **Uživatel** je povinen užívat **Službu** s ohledem na ostatní **Uživatele**, zejména nesmí zahlcovat servery nadměrnými a neopodstatněnými datovými přenosy.

4. Práva a povinnosti **Poskytovatele**
   4.1. **Poskytovatel** služeb podle čl. 2.1., které spočívajících v ukládání informací (souborů) poskytnutých **Uživatelem**, odpovídá podle ustanovení § 5 zákona o některých službách informační společnosti, ve znění pozdějších předpisů, za obsah informací uložených na žádost uživatele, jen:
      a) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání **Uživatele** jsou protiprávní, nebo
      b) dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání **Uživatele** a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.
   4.2. Podle ustanovení § 6 zákona o některých službách informační společnosti, **Poskytovatel** služeb uvedený v čl. 2.1. není povinen dohlížet na obsah **Uživateli** přenášených nebo ukládaných informací, ani aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace.
   4.3. Za účelem zajištění povinností **Poskytovatele** stanovených zákonem o některých službách informační společnosti je **Poskytovatel** v případě, že se dozví o existenci souborů nebo jejich částí nebo jiných informací **Uživatelů**, které porušují tyto **Podmínky**, oprávněn je neprodleně smazat, učinit veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací, či zajistit tyto informace pro účely případného trestního řízení. **Uživatel** bere na vědomí a souhlasí s tím, že **Poskytovatel** služeb neodpovídá za jakoukoliv přímo či nepřímo způsobenou škodu nebo jinou újmu, která by tímto postupem **Uživateli** vznikla nebo vzniknout mohla.
   4.4. V případě, že se **Uživatel** dopustí jednání, které je v rozporu s článkem 3. těchto **Podmínek**, je **Poskytovatel** oprávněn zamezit uživateli **Službu** využívat.
   4.5. **Poskytovatel** služeb neposkytuje uživatelům žádnou záruku za nepřetržitý provoz služeb či jejich dostupnost a rychlost připojení.
   4.6. **Poskytovatel** služeb neprovádí žádné zálohy dat na serveru umístěných a nenese žádnou odpovědnost za jakoukoliv přímo či nepřímo způsobenou škodu nebo jinou újmu, způsobenou jejich poškozením, zničením nebo smazáním. Zálohu obsahu umístěného na serveru si provádí uživatel vlastními prostředky.
   4.7. **Poskytovatel** služeb se zavazuje veškeré informace získané při registraci uživatele chránit ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. **Poskytovatel** je oprávněn údaje uvedené **Uživatelem** poskytnout orgánům činným v trestním řízení pro účely jejich užití v souladu s platnými právními předpisy.
   4.8. **Poskytovatel** si vyhrazuje právo na změnu poskytování **Služby** a to i bez předchozího upozornění. **Poskytovatel** si dále vyhrazuje právo na změnu

těchto **Podmínek**, na změnu je však **Poskytovatel** povinen vhodným způsobem **Uživatele** upozornit nejpozději 30 dní předem.

4.9. V případě porušení těchto **Podmínek** kterýmkoliv **Uživatelem** může **Poskytovatel** vyjma uvedených oprávnění přijmout i jiná opatření dle v ČR platných právních předpisů a mezinárodních smluv, jimiž je ČR vázána.

4.10. **Poskytovatel** je oprávněn vyzvat **Uživatele** k vysvětlení nadměrných a neobvyklých datových toků probíhajících prostřednictvím jeho uživatelského účtu (viz čl. 3.12. těchto podmínek).

4.11. **Poskytovatel** je oprávněn ukládat informace o **Uživatelích** a jejich činnosti ve **Službě** pro účely administrativy, provozu, statistik, monitoringu a bezpečnosti.

5. Závěrečná ustanovení

5.1. Tyto **Podmínky** se stávají pro **Uživatele** závaznými okamžikem, kdy **Uživatel** odsouhlasí podmínky využití Služby na (URL). **Podmínky** jsou pro **Uživatele** závazné po celou dobu využívání **Služby**.

5.2. Tyto Podmínky navazují na „Zásady pro přístup do sítě národního výzkumu a vzdělávání nové generace (Access Policy, AP)“ viz URL.

5.3. **Uživatel** odsouhlasením **Podmínek Služby** souhlasí, ve smyslu ustanovení § 7 odst. 2 zákona o některých službách informační společnosti, s tím že **Poskytovatel** bude oprávněn zasílat **Uživateli** e-mailové zprávy, které budou obchodními sděleními ve smyslu ustanovení § 2 písm. f) zákona o některých službách informační společnosti., obsahujícími zejména, nikoli však pouze, informace o **Službě** a o jejím obsahu.

5.4. Smlouva uzavřená podle těchto smluvních podmínek se řídí právním řádem České republiky.

5.5. Tuto smlouvu je možno také ukončit výpovědí, učiněnou formou odhlášení ze strany **Uživatele**. Smlouva je ukončena okamžikem, kdy je projev vůle **Uživatele** je doručen **Poskytovateli**.

5.6. Komunikace mezi **Uživatelem** a **Poskytovatelem** probíhá především formou elektronické pošty či zveřejněním zpráv ze strany **Poskytovatele** na URL.

5.7. Stisknutí tlačítka „Souhlasím“ umístěného pod tímto Smluvním ujednáním, stvrzuje **Uživatel**, že si uvedené licenční ujednání přečetl, veškerým v něm uvedeným informacím rozumí a naprosto s nimi souhlasí. Dále stvrzuje, že nebyl k odsouhlasení uvedených smluvních podmínek donucen (ať fyzicky, či psychicky), a že se jedná o projev jeho svobodné vůle.

5.8. **Poskytovatel** není zodpovědný za žádné následky, které vzniknou **Uživateli** v průběhu využití **Služby**. U **Uživatele**, který svým jednáním při využití **Služby** způsobil protiprávní následky, není vyloučena občanskoprávní, správněprávní či trestněprávní odpovědnost za takovéto jednání.

5.9. Tyto podmínky nabývají účinnosti dne (datum).

Příloha 3: Bezpečnostní provozní směrnice IS (metodický pokyn)

Bezpečnostní provozní směrnice[31] musí být zpracovány pro každý informační systém (IS) uchovávající, zpracovávající nebo přenášející utajované informace, od velkých systémů se složitými sítěmi až po samostatné malé systémy, jako jsou osobní počítače. Jejich účelem je pokrýt veškeré předvídatelné aspekty vztahující se k bezpečnosti IS ve fázi jeho provozování.

Bezpečnostní provozní směrnice musí být odvozeny z bezpečnostní politiky IS a jsou konečným, konkrétním vyjádřením jejích požadavků. Popisují zejména bezpečnostní provozní procedury, které mají být dodržovány, organizační opatření, odpovědnost osob působících v IS, předepisují korektní chování jednotlivým subjektům IS. Rozsah a obsah bezpečnostních provozních směrnic jsou ovlivněny typem systému i prostředím, ve kterém pracuje.

Bezpečnostní provozní směrnice mají obsahovat vše, co vyžaduje bezpečnostní politika a návrh bezpečnosti (bezpečnostní projekt) od uživatelů a správy systému. Jde o realizaci některých „netechnických“ opatření zejména organizační a administrativní povahy, o různé procedury v oblasti fyzické a personální bezpečnosti a práce s dokumenty, tak jak jsou potřebné pro zajištění bezpečnosti během provozu IS.

Kromě toho řada bezpečnostních funkcí realizovaných počítačovými prostředky vyžaduje určitou interakci s uživatelem nebo správci systému. Jde např. o identifikaci a autentizaci (akce uživatele, pravidla pro hesla, uzamykání stanic, akce správy – prvotní přidělení hesla, seznamy uživatelů), audit (akce správce – kontrola a uchovávání auditních záznamů, ošetřování incidentů), řízení přístupu (akce správce i uživatelů v oblasti nastavování přístupových práv, pravidla pro vlastnická práva), akce uživatele a správce vyžadované v oblasti zálohování, akce uživatele a správce v oblasti komunikační bezpečnosti apod.

Pečlivý popis je vyžadován i pro způsob realizace některých bezpečnostních funkcí z oblasti počítačové bezpečnosti náhradními opatřeními.

Existují také speciální požadavky týkající se jen bezpečnosti provozu IS, zejména v oblasti dostupnosti informace a služeb, oblasti integrity SW a HW, v oblasti servisní činnosti, řešení bezpečnostních incidentů, řešení krizových situací.

[31] Metodický pokyn NBÚ, verze 2.1, 2006.

Bezpečnostní směrnice má být rozčleněna tak, aby činnost bezpečnostního správce, činnost správce IS (administrátora) a činnost uživatelů byly popsány odděleně, a běžným uživatelům se tak nedostával zbytečně do ruky nástroj, ulehčující jim nelegální využívání systému. Podle této zásady je třeba členit směrnice i do dalších částí (pro různé typy uživatelů, pro obsluhu kryptografických prostředků apod.). Kromě uplatňování zásady „need-to-know" je nutno vzít v úvahu i potřebu utajovat bezpečnostní provozní směrnici určenou pro bezpečnostního správce nebo pro oblast správy kryptografického zařízení.

Pokud jde o distribuovaný IS, je často vhodné a efektivní zpracovat jednu generickou bezpečnostní směrnici zastřešující celý systém a na jejím základě pak lokální směrnice pro jednotlivá konkrétní místa.

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, vyžaduje pro každý IS nakládající s utajovanými informacemi jako výchozí specifikaci v oblasti bezpečnosti bezpečnostní politiku (podporovanou analýzou rizik), na jejím základě pak návrh celkové bezpečnosti IS, obsahující zejména:

- HW a SW architekturu (včetně popisu komunikačních sítí) a bezpečnostní funkce, které zajišťuje (včetně komunikační bezpečnosti),
- popis náhradních opatření za určité bezpečnostní funkce vyžadované v rámci minimálních bezpečnostních požadavků v oblasti počítačové bezpečnosti, pokud jsou použita,
- návrh, jak mají být realizována opatření z oblasti fyzické, administrativní a personální bezpečnosti a organizační opatření, tak aby to odpovídalo zvolenému bezpečnostnímu provoznímu módu a výsledkům analýzy rizik a posléze bezpečnostní provozní směrnice IS.

Příklady

Pro oblast zálohování se uvede v:

- *bezpečnostní politice*: co se má zálohovat a jak často, jak dlouho zálohy uchovávat, jaký systém zálohování používat, jak zálohy chránit aj.,
- *návrhu bezpečnosti*: jaké prostředky pro zálohování, které umožňují tuto politiku splnit, se budou používat,
- *bezpečnostní provozní směrnici*: kdo provádí zálohování, jakým systémem, jak často, konkrétní místo uložení záloh atd.

Pro oblast fyzické bezpečnosti se uvede v:

- *bezpečnostní politice*: např. požadavek kontrolovaného vstupu do určité počítačové místnosti,
- *návrhu bezpečnosti:* přesně, jakých prostředků fyzické bezpečnosti má být použito,
- *bezpečnostní provozní směrnici*: procedury pro legitimní dosažení vstupu do místnosti.

K tvorbě bezpečnostních provozních směrnic je správné přistoupit tak, že se analyzuje návrh bezpečnosti IS a pro všechny elementy návrhu, které vyžadují během provozu IS určitou činnost správy systému a/nebo uživatelů se specifikuje příslušná procedura, organizační opatření, pravidlo, které musí uživatel dodržet apod.

Kromě toho je třeba také ověřit, zda bezpečnostní politika neobsahuje některé požadavky nepokryté návrhem IS, z toho důvodu, že se týkají až provozu IS vzniklého realizací návrhu.

Některé požadavky specifické pro bezpečnost provozu IS jsou přímo určeny vyhláškou č. 523/2005 Sb., podobně jako dříve vyhláškou č.56/1999 Sb. Jde zejména o:

- zavedení role bezpečnostního správce IS, případně celé struktury bezpečnostních správců,
- zajištění školení uživatelů v oblasti bezpečného využívání IS,
- ošetření autorizace uživatele a včasné změny této autorizace,
- vedení seznamu uživatelů,
- zajištění ochrany integrity programového vybavení i utajovaných informací před působením škodlivého kódu (antivirová ochrana),
- provádění správy konfigurace, aby bylo používáno pouze programové vybavení dodané provozovatelem informačního systému a schválené v rámci certifikačního procesu,
- zajištění zálohování programového vybavení a utajovaných informací a bezpečného ukládání záloh,
- zajištění bezpečnosti při instalaci informačního systému,
- zajištění bezpečnosti při servisní činnost v informačním systému tak, aby nebyla ohrožena jeho bezpečnost, zejména důvěrnost utajovaných informací a integrita HW i SW,
- pravidelné vyhodnocování auditních záznamů s uvedením odpovědnosti, neprodlené provedení vyhodnocení auditních záznamů při vzniku krizové situace, stanovení pravidel pro jejich zálohování a uchovávání,
- zajištění bezpečnosti provozních datových nosičů utajovaných informací,
- stanovení pravidel pro řešení krizových situací provozovaného informačního systému a opatření zaměřených na jeho uvedení do známého bezpečného stavu,
- stanovení způsobu zabezpečení utajované informace před likvidací informačního systému (vyjmutí, vymazání nebo zničení utajovaných informací, se kterými informační systém nakládal).

Pokud se bezpečnostní směrnice píše podle jednotné šablony, je často velmi formální, špatně navázaná na bezpečnostní politiku a návrh konkrétního informačního systému, v podstatě se pak nepozná, když se směrnice pro dva různé systémy navzájem vymění. V provozu informačního systému se pak mohou projevit bezpečnostní mezery.

Následující text je proto třeba chápat pouze jako pomůcku pro přehledné strukturování bezpečnostní směrnice a pro uvědomění si oblastí, které mají být obecně pokryty. Poskytuje kontrolní seznam relevantních aspektů.

Obsah provozních bezpečnostních směrnic

- Stručný popis IS, jeho rozsahu, umístění, napojení na externí systémy, jeho funkčnosti.
- Údaj, v jakém bezpečnostním provozním módu IS pracuje a jaký je nejvyšší stupeň utajení zpracovávaných informací.
- Funkce (role) zavedené v IS pro výkon správy bezpečnosti IS a činnosti, které zajišťují. Vždy půjde o bezpečnostního správce IS, správce IS (administrátora), podle okolností o správce kryptografického zařízení aj. V malých systémech je možné (a někdy nevyhnutelné) tyto funkce přidělit třeba jednomu z uživatelů nebo je kumulovat s funkcí správce systému, v některých rozsáhlých systémech naopak půjde o samostatná tabulková místa, případně bude potřebné ustavit i funkci správce síťové bezpečnosti. Uvádí se postup pro jmenování osob do těchto funkcí, požadavky na jejich bezpečnostní prověření.
- Postup pro zařazení osoby do seznamu oprávněných uživatelů IS a pro její vyřazení, požadavky na bezpečnostní prověření uživatelů, kdo o zařazení/vyřazení rozhoduje, kdo vede seznam uživatelů.
- Jmenný seznam uživatelů IS, s uvedením stupně utajení, pro který je daná osoba prověřena a doby platnosti osvědčení (z praktických důvodů v příloze). V seznamu lze vyznačit i skupiny osob se stejnými přístupovými právy (pokud byly vytvořeny).
- Bezpečnostní školení uživatelů IS, absolvované před zavedením do IS a poté periodicky, kdo za ně zodpovídá, zajištění podepsaného prohlášení uživatele o absolvovaném školení a znalosti bezpečnostních směrnic, dostupnost směrnic pro uživatele.
- Schválená základní konfigurace HW a SW, umístění jednotlivých komponent IS, odpovědnost za dodržování konfigurace HW a SW, systém řízení konfigurace (schvalování změn, aktualizace).
- Specifikace přístupových práv konkrétních uživatelů (skupin uživatelů) k objektům IS. Podrobnost závisí na definování přístupových práv v bezpečnostní politice informačního systému (např. zda daný subjekt má právo daný soubor číst, zapisovat do něj, měnit jej, zrušit a podobně). Pracuje-li IS v bezpečnostním provozním módu vyhrazeném, mají všichni uživatelé přístup ke všem informacím a službám IS. Pracuje-li v bezpečnostním provozním mó-

du s nejvyšší úrovní nebo víceúrovňovém, jsou již přístupová práva diferencována. Ve víceúrovňovém módu je navíc nutno uživatele rozdělit i podle stupně utajení, pro který jsou prověřeni.
    - Uvést, kdo je oprávněn stanovit přístupová práva uživatelů k objektům IS a odpovídá za jejich správnou aktualizaci, jak je přidělení zdokumentováno.
    - Uvést mechanismy pro řízení přístupu – procedury pro implementaci volitelného a/nebo povinného řízení přístupu k informaci/službám/zařízením, procedury pro ustavení uživatelských práv a povolení pro užívání služeb a zdrojů IS, údaje o odpovědných autoritách a udržovaných kontrolních záznamech. Může se jednat nejen o logické řízení přístupu, ale i o řízení přístupu do počítačové oblasti, prováděné prostředky objektové a technické bezpečnosti.
- V oblasti identifikace a autentizace se uvádí, kdo odpovídá za správu identifikačních a autentizačních mechanismů, kdo je oprávněn a odpovědný za přidělování a změny přístupových hesel, čipových karet nebo jiných pomůcek, postup pro přidělování a změny přístupových hesel, čipových karet nebo jiných pomůcek, pravidla pro tvorbu hesel a nakládání s nimi, pravidla pro nakládání s čipovými kartami nebo jinými pomůckami,
    - pojetí identifikace (user ID) – procedury pro ustavení uživatelského účtu, uživatelských skupin, přidělení uživatelského jména (identifikátoru), procedury pro vymazání uživatelského účtu po jeho odchodu z dané pozice nebo když byl účet kompromitován,
    - pojetí autentizace – ochrana autentizační informace (hesla, tokeny, biometrické metody), procedury pro kontrolu hesel a jejich změnu, vydávající je autorita, udržování kontrolních záznamů a kým, procedura pro frekvenci změny , procedura pro užívání autentizačních mechanismů.
- Procedury pro zavedení uživatelského účtu, uživatelských skupin, přidělování ID a prvotního hesla, rušení účtů.
- Určit případné uplatnění pravidla dvou osob a kde se to jeví jako nezbytné, pak v příloze určit i jména určitých osob.
- Fyzické zabezpečení
    - popis počítačové oblasti (oblastí) a jejího fyzického zabezpečení, umístění a druh všech zařízení IS, pro vzdálené pracovní stanice/terminály minimální fyzické zabezpečení vyžadované pro připojení k hlavnímu systému,
    - kdo je oprávněn povolit přístup na pracoviště, jakým způsobem je řízen přístup osob na pracoviště, seznam osob, které mají přístup na pracoviště (v pracovní době, mimo ni),
    - postupy které musí uživatel dodržovat, jak nakládat s klíči, čipovými kartami, přístupovými hesly,
    - audit EKV apod., systém propustek,

- kontroly fyzického zabezpečení kabeláže LAN, aktivních prvků sítě (huby, switche apod.), bezpečnostních rozhraní do jiných sítí, kryptografických zařízení, odpovědnost, příslušná síťová schémata umožňující kontroly,
- údaje o klíčích a/nebo kombinacích zámků – jaké jsou používány, kde jsou uloženy, jaké evidence jsou o nich vedeny, kdo má povoleno je vyzvedávat a/nebo používat,
- časová omezení fyzického přístupu, procedury pro zajištění fyzické bezpečnosti počítačové oblasti (oblastí) po pracovní době,
- řízení fyzického přístupu dalších osob (a vybavení):
  - procedury a záznamy udržované pro kontrolu návštěvníků včetně opatření pro zabránění neautorizovanému prohlížení klasifikovaných výstupů nebo displeje,
  - propustky – používané a požadavky na jejich nošení nebo ukazování, kdo odpovídá za jejich autorizaci a/nebo vydání,
  - místní procedury pro kontrolu vnášení, ukládání, provozování a odnášení různého vybavení,
- alarmy na proniknutí a na rizika prostředí - kde jsou umístěny, režim testování, frekvence testů, procedury pro nastavení alarmů a pro reakce na alarmy.

- Povinnosti při zajišťování integrity HW a SW – např. kontrola pečetí na HW, neporušenosti kabeláže (kdy, kým), antivirová ochrana a příslušné procedury.
- V oblasti správy auditních a provozních záznamů IS se stanoví
  - metodika vyhodnocování auditních záznamů (oprávněnost ke kontrolní činnosti, způsob hlášení výsledků kontrol, charakteristické jevy, které se musí při zjištění v auditních záznamech hlásit, popis opatření, která musí kontrolní orgán uskutečnit),
  - metodika vyhodnocování manuálně vedených provozních záznamů (kniha vstupu na pracoviště, evidenční knihy apod.), přičemž obsah metodiky je obdobný jako u auditních záznamů,
  - předepsaná doba, místo a forma uchování auditních záznamů a provozních záznamů pro zpětné zkoumání,
  - procedury pro spouštění a provoz automatizovaných nástrojů/programů pro správu bezpečnosti a údaje o auditních rysech.
- Pokud jsou používány zvláštní bezpečnostních prostředky, např. kryptografické prostředky, je nutno je specifikovat, uvést
  - jejich umístění,
  - osoby oprávněné osoby pro práci s těmito prostředky,
  - povinnosti a odpovědnost oprávněných osob vzhledem k těmto prostředkům a
  - odkaz na příslušné směrnice pro práci s těmito prostředky.

- Povinnost dodržovat instalační podmínky z hlediska TEMPEST, pokud jsou používány stíněné místnosti nebo stínicí komory (proti jakémukoliv typu odposlechu) uvést organizaci práce v nich, odpovědnost za kontrolu.
- Způsob evidence utajovaných dokumentů na daném pracovišti, případně seznam evidenčních pomůcek, jaká počítačová média se používají, způsob označování médií, možnost snížení stupně utajení, způsob ničení médií, způsob ukládání a výdeje médií (zajištění nepřetržité odpovědnosti za přenosná sdílená média), úschovné objekty, nakládání s tiskovými výstupy apod.
- Případné bezpečnosti se týkající procedury pro start systému.
- Procedury pro zahájení denní práce se systémem (uživatel, správa systému).
- Případná pravidla pro odpojení některých zařízení během provozu nebo po jeho ukončení.
- Procedury pro ukončení denní práce (uživatel, správa systému), pro ponechání pracovní stanice bez autorizované obsluhy během pracovní doby apod.
- Procedury vztahující se k provádění údržby HW a SW zajišťující integritu HW a SW a ochranu utajovaných skutečností zpracovávaných v IS, co se má předem odstranit, odpovědnost správy IS a uživatelů, záznamy o úpravách – jak mají být vedeny a kým, kde a jak dlouho se uchovávají.
- Seznam bezpečnostních incidentů a mimořádných událostí a deklarace povinnosti uživatelů hlásit je bezpečnostnímu správci IS, komu je dále hlásí bezpečnostní správce, že musí být zpracována zpráva, kam se zaznamenává výskyt, jak dlouho se záznamy uchovávají a kde. Nezapomenout na kompromitaci hesla, napadení viry nebo jiným zlomyslným SW.
- Pro jednotlivé incidenty a mimořádné situace postup řešení a kdo za řešení odpovídá.
    - Konstatování, že každý incident, který znamená narušení personální, HW, SW, komunikační bezpečnosti, bezpečnosti dokumentů nebo i fyzické bezpečnosti musí být bezprostředně hlášen bezpečnostnímu správci IS,
    - Postup při haváriích: Pro případ havárie (způsobené například chybou obsluhy, teroristickým útokem, poruchou techniky nebo živelní pohromou), musí být, zejména pro větší systémy, stručně a jasně popsán sled činností pracovníka při dané události. V bezpečnostních směrnicích má být uvedena:
        - činnost následující ihned po havárii, vedoucí k minimalizaci škod,
        - činnost, která vede k likvidaci následků havárie a která obsahuje konkrétní pracovní postup se jmény a způsobem vyrozumění a dosažení pracovníků povolávaných na pracoviště,
        - způsob zálohování informačního systému,
        - způsob zajištění servisní činnosti,
        - způsob zajištění nouzového provozu informačního systému s vyjmenováním minimálních funkcí, které musí být zachovány.

- Pro provoz prostředků technické bezpečnosti tj. elektrické zabezpečovací signalizace, elektrické požární signalizace apod., odkaz na příslušné směrnice.
- Procedury pro kontrolu personálu údržby a jiného podpůrného personálu, který může potřebovat přístup do oblasti, v níž je umístěn IS nebo vzdálené pracovní stanice a terminály.
- Kde hledat radu týkající se bezpečnosti nebo provozuschopnosti IS.

Členění provozních bezpečnostních směrnic

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, podobně jako vyhláška č. 56/1999 Sb. o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátů, ukládá zpracování provozní bezpečnostní směrnice popisující činnost bezpečnostního správce a provozní bezpečnostní směrnice pro jednotlivé typy uživatelů IS.

Při zpracování bezpečnostních provozních směrnic je možný různý přístup:

- zpracovat celkovou bezpečnostní směrnici (v úplnosti dostupnou jen pro bezpečnostního správce a případně administrátora) a z ní pak příslušný výtah pro uživatele a pro další role (funkce) v IS,
- od počátku rozdělit směrnice na části podle toho, komu jsou určeny,
- vytvořit základní směrnici obsahující všeobecně platné povinnosti a doplnit ji speciálními směrnicemi pro jednotlivé role.

Přitom je nutno vycházet z toho, že musí být pokryty všechny aspekty bezpečnosti, dodrženo pravidlo „need-to-know“ a princip minimálních privilegií a že je vhodné oddělit méně a více citlivé informace (směrnice pro bezpečnostního správce a administrátora bude většinou klasifikována výše, nežli směrnice pro koncového uživatele).

Obvykle je třeba zpracovat bezpečnostní provozní směrnici bezpečnostního správce IS, bezpečnostní provozní směrnici správce IS a bezpečnostní provozní směrnici pro uživatele IS, podle potřeby pak bezpečnostní provozní směrnice pro další role ustanovené v oblasti správy bezpečnosti IS.

V případě, že výkon některých rolí v IS je na základě bezpečnostní politiky prováděn jedinou osobou (např. role bezpečnostního správce a správce IS v malých systémech), může odpovídající bezpečnostní směrnice obsahovat povinnosti vyplývající z obou rolí.

V případě, že je v IS využívána kryptografická ochrana utajovaných informací, je součástí provozní bezpečnostní dokumentace i provozní dokumentace kryptografického prostředku. V ní jsou stanoveny podmínky provozu a povinnosti pracovníků speciální kryptografické obsluhy i provozní obsluhy.

Typické povinnosti bezpečnostního správce IS, správce IS a uživatele IS.

Pozn. 1: Toto *není* univerzální a úplný seznam povinností osob působících v IS. Vybrat je třeba povinnosti adekvátní pro konkrétní IS, další povinnosti je třeba naopak doplnit podle okolností.
Pozn. 2: Pokud je bezpečnostní politikou a/nebo v návrhu bezpečnosti zavedena další funkce (role) v IS, je třeba vytvořit také pro ni příslušnou bezpečnostní směrnici.
Pozn. 3: Bezpečnostní správce i správce informačního systému musí být prověřen na nejvyšší stupeň utajení informací, s nimiž IS nakládá.
Pozn. 4: Některé z povinností bezpečnostního správce IS lze udělit správci IS.

Bezpečnostní správce IS zpravidla

- udržuje aktuální seznam oprávněných uživatelů, s čímž souvisí také postup pro zařazení osoby do seznamu oprávněných uživatelů IS a pro její vyřazení, požadavky na bezpečnostní prověření uživatelů, kdo o zařazení/vyřazení rozhoduje,
- zajišťuje, aby přístup do počítačových místností, k výměnným pevným diskům apod. mohli získat jen autorizovaní uživatelé IS (jde i o klíče a kódy zámků, magnetické karty, zavedení do databáze EZS a audit přístupů a podobné problémy podle konkrétní situace),
- vytváří uživatelské účty, přiděluje uživatelské jméno (ID) a počáteční heslo, spravuje účty ve shodě s bezpečnostní politikou, v této činnosti mu technickou podporu může poskytovat správce IS,
- vede seznamy HW, SW, lokalit apod., odpovídá za trvalé dodržování schválené konfigurace HW i SW informačního systému,
- odpovídá za správné nastavení bezpečnostních charakteristik operačního systému, aplikačního SW, bezpečnostního rozhraní do jiných systémů,
- odpovídá za dodržování schváleného rozmístění komponent IS a dodržování instalačních podmínek,
- zkoumá pravidelně auditní záznamy, vytváří jejich záložní kopie, ukládá je po stanovenou dobu pro zpětné zkoumání, kontroluje zavedené manuální evidence,
- zkoumá auditní záznamy a manuální evidence po bezpečnostním incidentu,
- zkoumá a řeší bezpečnostní incidenty, hlásí je bezpečnostnímu řediteli, řediteli organizace (nebo jiné odpovědné osobě),
- zajišťuje školení uživatelů v oblasti bezpečnosti IS,
- kontroluje dodržování bezpečnostních směrnic,
- zajišťuje v předepsaném rozsahu bezpečnost počítačových médií, zejména vyřazování a ničení médií (uvést proceduru pro ničení médií a jak se zničení eviduje),

- vede potřebné evidence podle bezpečnostní politiky a návrhu systému (uvést které),
- zajišťuje kontrolu vstupu návštěv (popsat jak),
- provádí zálohování systémového programového vybavení, zajišťuje ochranu záložních dat (konkretizovat jak často, kde zálohy ukládá apod.),
- provádí správu dokumentace bezpečnosti IS (kde je uložena apod.),
- v některých systémech vydává uživatelům výměnné pevné disky, přenosný počítač (popsat jak, pokud je ovšem tento postup použit),
- zajišťuje bezpečnost utajovaných informací v případě oprav počítače, prováděných osobou bez oprávnění pro přístup k utajovaným informacím uloženým v IS (avšak schválenou odpovědnou osobou), kdy hlavní zásadou je, že
    - před započetím oprav HW musí být odstraněny klasifikované tiskové výstupy a paměťová média a odpojeno napájení všech zařízení, aby byly vymazány vyrovnávací paměti,
    - opravy musí být prováděny pod dohledem bezpečnostního správce a případně dalšího uživatele IS s dostatečným technickým vzděláním, aby byla vyloučena možnost modifikovat HW nepovoleným způsobem (vložení neschválené komponenty),
    - porouchané výměnné pevné disky použité v IS nesmí být opravovány nebo připojovány k jinému systému, mohou být pouze nahrazeny novými, uloženy jako utajovaná skutečnost a posléze zničeny (ke zničení je možno je předat na NBÚ).
- dojde-li k havárii operačního systému nebo aplikačního SW, zajistí ve spolupráci se správcem IS uvedení IS do zabezpečeného stavu odpovídajícího schválené bezpečnostní dokumentaci IS,
- odpovídá za řešení základních krizových situací ve stanoveném rozsahu.

Správce IS (oblastí činnosti jsou počítače a připojená zařízení, počítačová síť) zpravidla:

- provádí činnost administrátora operačního systému (lokální i síťová úroveň), spravuje aplikační SW, spravuje bezpečnostní rozhraní do jiných systémů, zabezpečuje denní provoz IS po technické stránce,
- instaluje operační systém, aplikační SW a další schválené SW vybavení,
- zajišťuje antivirovou ochranu IS,
- spolupracuje s bezpečnostním správcem IS při nastavení bezpečnostních charakteristik operačního systému, aplikačního SW a bezpečnostních rozhraní do jiných systémů podle schválené bezpečnostní dokumentace IS a odpovídá za udržování tohoto nastavení,
- spravuje uživatelské účty ve spolupráci s bezpečnostním správcem IS,
- spolupracuje s bezpečnostním správcem při vyčištění a zotavení systému po napadení viry,

- spolupracuje s bezpečnostním správcem při uvedení systému do stavu odpovídajícího schválené bezpečnostní dokumentaci IS po ostatních bezpečnostních incidentech nebo mimořádných událostech,
- nemá možnost modifikovat auditní záznamy operačního systému,
- v oblasti údržby HW zajišťuje některé činnosti vlastními silami, na provedení jiných dohlíží, spolupracuje při tom s bezpečnostním správcem IS,
- vede předepsané provozní evidence, např. provozní deník IS.

Podle potřeby (zejména ve větších systémech) se ustavují další role, jako např. správce určitého aplikačního programu, správce databáze, správce určitého bezpečnostního rozhraní, lokální správci v jednotlivých lokalitách, pracovník údržby a oprav HW apod. Může také dojít k přesunu některých povinností bezpečnostního správce (zejména v oblasti výkonu) na správce IS, zde záleží i na lidských zdrojích, kterými provozovatel bude disponovat.

Pracovníci správy IS musí mít v přílohách k bezpečnostním směrnicím k dispozici všechny potřebné informace, jako je rozmístění komponent IS nebo nastavení bezpečnostních charakteristik.

Bezpečnostní provozní směrnice uživatele

Účelem je shrnout srozumitelnou formou informace, které popisují korektní chování uživatele při využívání IS, od způsobu zahájení činnosti v IS, přes práci v něm až po způsob ukončení činnosti v IS. Tomu pak slouží uvedení následujících údajů:

- jaká zařízení IS může uživatel používat a kde jsou umístěna, případně v jakém časovém rozpětí během dne jsou mu přístupná,
- standardní postup pro zahájení práce s informačním systémem, včetně způsobu vstupu do místnosti, získání potřebného HW (výměnný pevný disk, přenosný počítač), získání potřebných počítačových médií, přihlášení do systému atd.,
- jak má zacházet s disketami a dalšími počítačovými médii používanými v tomto IS – jakmile je mu jednou vydána, nesmí ji použít mimo tento IS a musí s ní nakládat jako s utajovanou písemností, kam ji má ukládat,
- jakým způsobem získá výměnný disk nebo přenosný počítač nebo jiný HW systému před započetím práce, jak ho opět ukládá , s tím spjaté povinnosti, evidence,
- zálohování uživatelských dat na diskety nebo jiná média a jejich ochraně,
- jak se chovat k návštěvě, jak k úklidu (aby to vyhovovalo bezpečnostní politice a návrhu bezpečnosti),
- že musí hlásit poruchy HW i SW, výskyt bezpečnostního incidentu nebo podezření na možnost kompromitace utajovaných informací bezpečnostnímu správci, pokud to typ události vyžaduje, předepsat bezprostřední reakci uživatele před kontaktem s bezpečnostním správcem,

- jaké jsou podmínky a pravidla pro předání informací z IS jinému subjektu pro různé stupně utajení,
- jak má nakládat s tiskovými výstupy (označení stupněm utajení a dalšími náležitostmi podle požadavků administrativní bezpečnosti, po vytvoření musí být ihned zaevidovány v knize utajovaných písemností, ničení a skartace podle pravidel administrativní bezpečnosti),
- jak se postupuje v případě potřeby zničit disketu a/nebo jiná počítačová média,
- jaké má povinnosti v případě potřeby opustit počítače v průběhu práce s IS,
- procedura pro standardní bezpečné ukončení práce v IS – veškeré povinnosti týkající se počítače, periférií, místnosti, klíčů, EZS atd.,
- pravidla pro používání hesla, jak ho tvořit, že ho nesmí sdílet, prozradit atd.,
- jak má používat klíč od místnosti,
- jak se smí manipulovat s výměnnými pevnými disky,
- jak se má chovat v případě výskytu základních krizových situací a o jaké situace se jedná,
- co je považováno za bezpečnostní incident a jak se má chovat, pokud k němu dojde.

Některé aspekty řešení krizových situací a bezpečnostních incidentů

Jde-li o situaci, která přímo nesouvisí s funkcí HW a SW je základem, pokud možno ukončit činnost systému, vyjmout veškerá počítačová média z počítače, vypnout počítač a připojená zařízení (vyprázdnění volatilních pamětí) a uložit počítačová média, dokumenty s utajovanými informacemi i dokumentaci IS do příslušného úschovného objektu. Není-li to v době výskytu mimořádné události možné, uchovat veškeré nosiče utajovaných informací v osobní péči oprávněného uživatele IS, oprávněné osoby nebo bezpečnostního správce IS, do doby kdy je možno je uložit podle zásad ochrany utajovaných skutečností.

Pokud situace vyžaduje zásah nepovolaných osob, musí být zamezeno neoprávněnému přístupu k utajovaným informacím a zařízením IS, zásahu (hasičů, instalatérů, příslušníků bezpečnostní služby zajišťujících fyzickou ostrahu apod.) musí být přítomen bezpečnostní správce nebo oprávněný uživatel IS nebo statutární zástupce, bezpečnostní tajemník apod.

Pokud jde o poruchu HW, SW nebo výskyt počítačového viru, přeruší uživatel práci se systémem a přivolá bezpečnostního správce, který tuto situaci vyřeší.

Opravy HW se musí provádět pod dohledem bezpečnostního správce IS a tak, aby se technik provádějící opravu nemohl seznámit s utajovanými informacemi a zároveň, aby nemohlo dojít k narušení schválené konfigurace IS. Bez svolení bezpečnostního správce nesmí přinést ani odnést žádnou komponentu IS ani počítačové médium.

Údržba SW, řešení selhání operačního systému nebo aplikačního SW a řešení virového incidentu musí být prováděno buďto administrátorem prověřeným pro nejvyšší stupeň utajení nebo bezpečnostním správcem IS. Výjimečně může tuto správu provádět osoba prověřená pouze pro stupeň utajení Vyhrazené, avšak pod stálým dohledem bezpečnostního správce, obnovení systému a aplikačního SW pak musí provádět z instalačních médií uložených u bezpečnostního správce, neodnáší žádné médium. Výsledkem činnosti musí být uvedení IS do zabezpečeného stavu podle bezpečnostní dokumentace IS.

O každé z mimořádných situací nebo z bezpečnostních incidentů musí být bezpečnostním správcem pořízen zápis, s uvedením dne a doby výskytu, způsobem řešení, jmen zúčastněných osob, podepsaný zúčastněnými osobami. Zápis je dán na vědomí i statutárnímu orgánu, který z něj vyvodí akce, vyžadované případně zákonem.

Základní pokyny pro práci s hesly

- heslo je kombinací velkých a malých písmen a nejméně jedné číslice a oddělovacích symbolů (včetně mezery), nesmí být použito slovo některého běžného jazyka, musí začínat písmenem,
- heslem nebo jeho součástí nesmí být jméno uživatele nebo jeho blízkých, číslo některého z jeho průkazu apod.,
- heslo musí uživatel chránit jako utajovanou skutečnost nejvyššího stupně utajení, jaký je v IS zpracováván,
- dočasné opuštění pracovní stanice během pracovní doby je možné pouze po uzamčení stanice (např. CTRL-ALT-DEL a volba „Uzamknout stanici“),
- heslo nesmí uživatel sdílet s jiným uživatelem,
- v systému pro zpracování utajovaných informací nesmí být používáno stejné heslo, jako v jiných systémech,
- heslo administrátora pro účet Administrator (přejmenovaný) je uloženo v zalepené obálce v bezpečnostní schránce,
- administrátor používá účet Administrator (přejmenovaný) jen pro správu W NT, pro své uživatelské aktivity užívá jiného účtu, podle principu nejmenších privilegií.

Příloha 4: ISO 27000: Information Classification Matrix

ISO 27001 security

INFORMATION CLASSIFICATION MATRIX AND HANDLING GUIDE

CATEGORY	DESCRIPTION	Sample Documents/Records	MARKING	PHYS & ADMIN CONTROLS	REPRODUCTION	DISTRIBUTION	DESTRUCTION/ DISPOSAL
PUBLIC or open	Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders. The [PR Office/Marketing Dept/Information Security Management dept/etc.] must pre-approve the use of this classification. These documents may be disclosed or passed to persons outside the organization.	Marketing materials authorized for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices	None	None	Unlimited	No restrictions	Recycling/trash
INTERNAL or proprietary	Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient. Disclosure to anyone outside of [Company name] requires management authorization.	Most corporate information falls into this category. Departmental memos, information on internal bulletin boards, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing or promotional information (prior to authorized release), investment options. transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, internal vacancy notices, intranet Web pages	"**INTERNAL USE ONLY**" Apply to bottom left corner of each page.	**Author:** responsible for proper markings. **User:** responsible for proper storage and document control.	Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement.	**Internal**: use an internal mail envelope. **External**: use a sealed envelope. **Electronic**: use internal email system. Encryption is required for transmission to external email addresses. **FAXing**: take care over the FAX number!	**Paper documents:** shred. **Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to **IT** for appropriate disposal
CONFIDENTIAL or restricted	Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organization without the explicit permission of a Director-level senior manager.	Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal information (such as employee HR records, Social Security Numbers), most accounting data, other highly sensitive or valuable proprietary information	"**CONFIDENTIAL**" Apply to bottom left corner of each page.	**Originator:** responsible for ensuring that confidential information is distributed on a strict need-to-know basis. **Recipient:** responsible for ensuring that confidential information is encrypted and/or kept under lock & key when not in use.	Limited copies may be made only by permission of originator or his/her designates. A signed authorization slip will be presented.	**Internal:** use a sealed envelop inside an internal mail envelope. Hand deliver if possible. **External:** use a plain sealed envelope. Hand deliver or send by registered mail, courier *etc*. **Electronic:** use internal email system only. Encyrpt data. **FAXing:** requires phone confirmation of receipt of a test page immediately prior to sending the FAX, and phone confirmation of full receipt.	**Paper documents:** shred using an approved cross-cut shredder. **Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to **IT** for appropriate disposal.

This work is copyright © 2009, **Richard O. Regalado and ISO27k implementers' forum**, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.

Note: this classification scheme only relates to the confidentiality of the information. Similar schemes are feasible for integrity and availability requirements.

Příloha 5: Přehled norem řady ISO 27000

The ISO27k Standards

Contributed to the ISO27k Forum
by Gary Hinson
Last updated in March 2014

The following ISO/IEC 27000-series information security standards ("ISO27k") are either published or currently being developed:

Standard	Published	Title	Notes
ISO/IEC 27000	2014	Information security management systems - Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus the specialist vocabulary; FREE!
ISO/IEC 27001	2013	Information security management systems — Requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant
ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
ISO/IEC 27003	2010	Information security management system implementation guidance	Basic advice on implementing ISO27k
ISO/IEC 27004	2009	Information security management — Measurement	Basic (and frankly rather poor) advice on information security metrics
ISO/IEC 27005	2011	Information security risk management	Discusses risk management principles; does not specify particular methods for risk analysis *etc.*
ISO/IEC 27006	2011	Requirements for bodies providing audit and certification of information security management systems	Formal guidance for the certification bodies
ISO/IEC	2011	Guidelines for information security management systems	Auditing the *management system*

Copyright © 2014 ISO27k Forum

Standard	Published	Title	Notes
27007		auditing	elements of the ISMS
ISO/IEC TR 27008	2011	Guidelines for auditors on information security management systems controls	Auditing the *information security* elements of the ISMS
ISO/IEC 27009	DRAFT	Application of ISO/IEC 27001 - requirements	Sector- or service-specific certifications (possibly)
ISO/IEC 27010	2012	Information security management for inter-sector and inter-organisational communications	Sharing information on information security between industry sectors and/or nations, particularly those affecting "critical infrastructure"
ISO/IEC 27011	2008	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called "ITU-T Recommendation x.1051"
ISO/IEC 27013	2012	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Combining ISO27k/ISMS with IT Service Management/ITIL
ISO/IEC 27014	2013	Governance of information security	Governance in the context of information security; will also be called "ITU-T Recommendation X.1054"
ISO/IEC 27015	2012	Information security management guidelines for financial services	Applying ISO27k in the finance industry
ISO/IEC TR 27016	2014	Information security management – Organizational economics	Economics applied to information security
ISO/IEC 27017	DRAFT	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Information security controls for cloud computing
ISO/IEC 27018	DRAFT	Code of practice for controls to protect personally identifiable information processed in public cloud computing services	Privacy controls for cloud computing

Copyright © 2014 ISO27k Forum

Standard	Published	Title	Notes
ISO/IEC TR 27019	2013	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Information security for ICS/SCADA/embedded systems (not just used in the energy industry!)
ISO/IEC 27031	2011	Guidelines for information and communications technology readiness for business continuity	Continuity (*i.e.* resilience, incident management and disaster recovery) for ICT, supporting general business continuity
ISO/IEC 27032	2012	Guidelines for cybersecurity	Despite the curious title, it is actually about Internet security
ISO/IEC 27033	-1 2009	Network security overview and concepts	Various aspects of network security; gradually updating and replacing ISO/IEC 18028
	-2 2012	Guidelines for the design and implementation of network security	
	-3 2010	Reference networking scenarios - threats, design techniques and control issues	
	-4 2014	Securing communications between networks using security gateways	
	-5 2013	Securing communications across networks using Virtual Private Networks (VPNs)	
	-6 DRAFT	Securing IP network access using wireless	
ISO/IEC 27034	-1 2011	Application security — Overview and concepts	Multi-part application security standard
	-2 DRAFT	Organization normative framework	
	-3 DRAFT	Application security management process	
	-4 DRAFT	Application security validation	

Copyright © 2014 ISO27k Forum

Standard	Published	Title	Notes
	-5 DRAFT	Protocols and application security control data structure	
	-6 DRAFT	Security guidance for specific applications	
	-7 DRAFT	Application security control attribute predictability	
	-8 DRAFT	Protocols and application security controls data structure – XML schemas	
ISO/IEC 27035	2011	Information security incident management	Replaced ISO TR 18044; now being split into three parts
ISO/IEC 27036	-1 DRAFT	Information security for supplier relationships – Overview and concepts	Information security aspects of ICT outsourcing and services
	-2 DRAFT	Information security for supplier relationships – Common requirements	
	-3 2013	Information security for supplier relationships – Guidelines for ICT supply chain security	
	-4 DRAFT	Information security for supplier relationships – Guidelines for security of cloud services	
ISO/IEC 27037	2012	Guidelines for identification, collection, acquisition, and preservation of digital evidence	First of several IT forensics standards
ISO/IEC 27038	2014	Specification for digital redaction	Redaction of digital documents
ISO/IEC 27039	DRAFT	Selection, deployment and operations of Intrusion Detection [and Prevention] Systems (IDPS)	IDS/IPS
ISO/IEC 27040	DRAFT	Storage security	IT security for stored data

Copyright © 2014 ISO27k Forum

Standard	Published	Title	Notes
ISO/IEC 27041	DRAFT	Guidelines for assurance for digital evidence investigation methods	Assurance is critically important for all forms of forensics: the courts demand it
ISO/IEC 27042	DRAFT	Guidelines for the analysis and interpretation of digital evidence	IT forensics analytical methods
ISO/IEC 27043	DRAFT	Digital evidence investigation principles and processes	The basic principles of IT forensics investigations
ISO/IEC 27044	DRAFT	Guidelines for security information and event management (SIEM)	SIEM
ISO 27799	2008	Health informatics — Information security management in health using ISO/IEC 27002	Developed by a different committee; tailored advice for the healthcare industry

Note

The official titles of all the ISO27k standards (except ISO 27799) start with "Information technology — Security techniques —" which is derived from the name of ISO/IEC JTC1/SC27, the committee responsible for the standards. However this is a misnomer since, in reality, the ISO27k standards concern *information security* rather than *IT security*. There's much more to it than securing computer data!

Copyright

This work is copyright © 2014, ISO27k Forum, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this *provided* that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Forum at www.ISO27001security.com, and (c) if shared, derivative works are shared under the same terms as this.

Copyright © 2014 ISO27k Forum

Příloha 6: Výsledky průzkumu

V rámci řešení projektu proběhl anonymní průzkum informovanosti mezi aktuálními či potenciálními uživateli externích datových úložišť či cloudových služeb. Snahou bylo získat co nejširší průřezový vzorek názorů a zkušeností od zástupců managementu, vedoucích ICT oddělení, správců služeb i běžných koncových uživatelů (a to jak z technických tak i netechnických oblastí).

V časovém horizontu vymezeném elektronickému průzkumu se nám podařilo získat reprezentativní vzorek cca. 60 respondentů působících na různých pozicích v rámci státní správy, vědeckovýzkumných a akademických institucí, středního školství i komerčních firem. Kromě výstupů z elektronického průzkumu byly využity i konkrétní znalosti dané problematiky řešitelů projektu a jejich osobní konzultace.

Pro vytváření elektronických formulářů, vlastní sběr dat i jejich následné zpracování byly použity nástroje Google Forms (souhrnné výsledky elektronického průzkumu jsou uvedeny dále v příloze).

Výsledky průzkumu potvrdily obecně známá fakta, která byla mj. motivací ke vzniku tohoto projektu:

- Externí datová nebo cloudová úložiště aktuálně v nějaké formě vyžívají všichni respondenti.
- Primární využití je pro zálohovací nebo „doplňkové“ služby.
- Většina respondentů subjektivně vnímá bezpečnost (zabezpečení) uložených dat jako jeden z klíčových problémů[32].
- Stále citelně převažuje potřeba *vlastnictví dat*, tj. většina respondentů preferuje „lokální“[33] úložné kapacity[34] před komerčním cloudovým řešením.
- Obdobně jako v jiných případech, uživatelé hledají vyváženou polohu mezi přínosem nových vlastností a jednoduchostí používání (přetrvává „rezistence“ k učení něčeho nového) nabízených služeb.
- Legislativní problematika (především oblast bezpečnosti osobních, citlivých či jinak kategorizovaných dat) je většinou pro koncové uživatele i správce (a mnohdy také právníky organizace) nejasná (nebo alespoň nejednoznačná) a těžko uchopitelná.

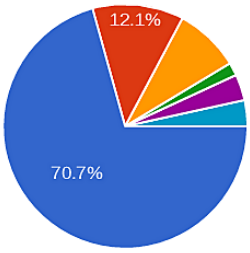
[32] Překvapivě na rozdíl od relativně běžného „laxního“ přístupu uživatelů k bezpečnosti jejich „lokálních“ dat.

[33] „Lokální“ ve smyslu, že vím, kde jsou data *fyzicky* uložena.

[34] A to většinou bez ohledu na kvalitu legislativního i technického zajištění poskytované služby.

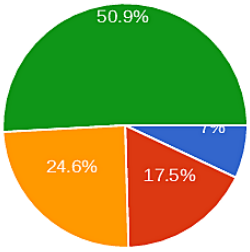
Respondent a jeho domovská organizace

Kategorie domovské organizace respondenta



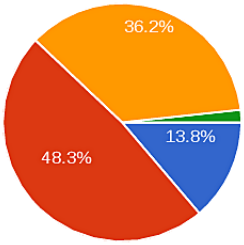
univerzita nebo vysoká škola	**41**	70.7 %
výzkumné pracoviště	**7**	12.1 %
střední škola	**5**	8.6 %
státní úřad nebo veřejná správa	**1**	1.7 %
komerční organizace	**2**	3.4 %
ostatní	**2**	3.4 %

Přibližný počet uživatelů ICT služeb organizace



do 100	**4**	7 %
1001,000	**10**	17.5 %
1,00010,000	**14**	24.6 %
nad 10,000	**29**	50.9 %

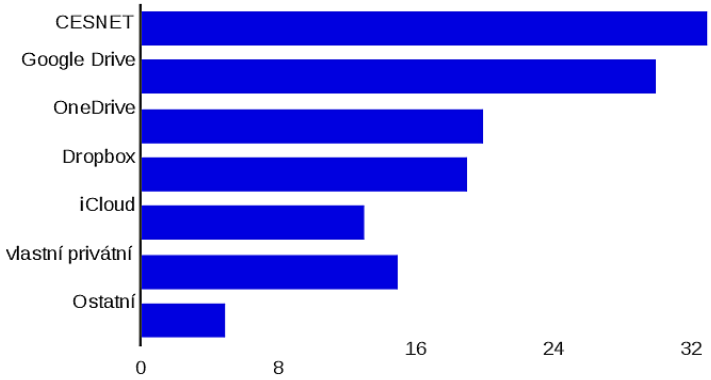
Pozice respondenta v organizaci



běžný uživatel ICT služeb	**8**	13.8 %
ICT správce	**28**	48.3 %
manažerská pozice	**21**	36.2 %
ostatní	**1**	1.7 %

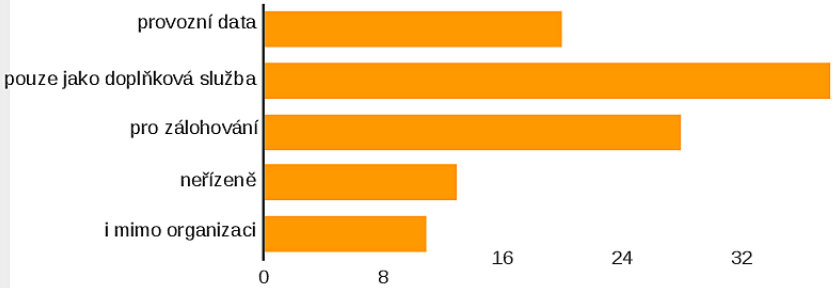
Využívání cloudových úložišť

Používáme cloudová úložiště



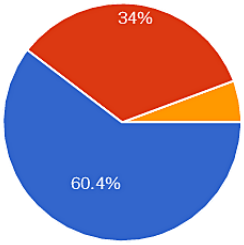
CESNET (owncloud...)	**33**	62.3 %
Google Drive	**30**	56.6 %
OneDrive	**20**	37.7 %
Dropbox	**19**	35.8 %
iCloud	**13**	24.5 %
vlastní privátní cloud	**15**	28.3 %
Ostatní	**5**	9.4 %

Způsob používání úložiště



provozní data, hlavní činnost	**20**	37 %
pouze jako doplňková služba pro některé činnosti	**38**	70.4 %
pro zálohování nebo archivaci	**28**	51.9 %
neřízeně nebo bez vědomí zaměstnavatele	**13**	24.1 %
do úložiště přistupují i osoby mimo organizaci	**11**	20.4 %

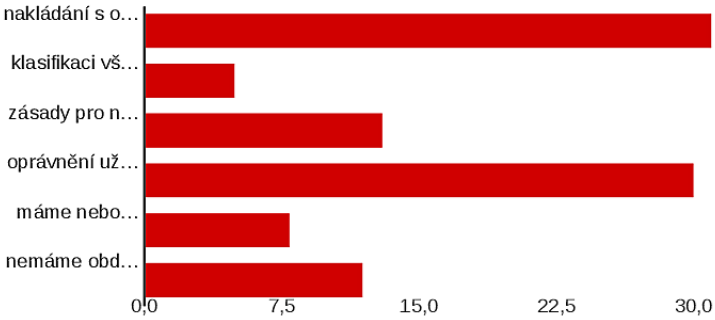
Ochrana ukládaných dat



Ukládáme data v otevřené podobě.	**32**	59.3 %
Některá data šifrujeme.	**18**	33.3 %
Všechna data před uložením do úložiště šifrujeme.	**3**	5.6 %

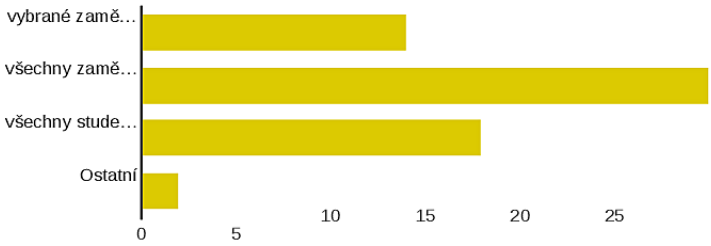
Interní legislativa a postupy

Máme interní předpisy, které určují



nakládání s osobními údaji	**31**	58.5 %
klasifikaci všech nebo většiny dat z hlediska důležitosti pro organizaci	**5**	9.4 %
zásady pro nakládání s různými kategoriemi dat	**13**	24.5 %
oprávnění uživatelů k přístupu k datům	**30**	56.6 %
máme nebo uvažujeme o certifikaci těchto procesů (ISO 27000 nebo podobně)	**8**	15.1 %
nemáme obdobné předpisy	**12**	22.6 %

Předpisy se vztahují na kategorie osob:



vybrané zaměstnance dle jejich pozice nebo organizační příslušnosti	**14**	32.6 %
všechny zaměstnance	**30**	69.8 %
všechny studenty	**18**	41.9 %
Ostatní	**2**	4.7 %

Osobní vnímání problematiky respondentem

Možnost pracovat s daty z různých platforem [Důležitost vlastností a rizik cloudových úložišť]

málo důležité	**4**	6.9 %
středně důležité	**16**	27.6 %
hodně důležité	**38**	65.5 %

Zjednodušení přístupu k datům [Důležitost vlastností a rizik cloudových úložišť]

málo důležité	**2**	3.4 %
středně důležité	**23**	39.7 %
hodně důležité	**33**	56.9 %

Ztráta dostupnosti dat při výpadku cloudu nebo ztrátě konektivity [Důležitost vlastností a rizik cloudových úložišť]

málo důležité	**3**	5.2 %
středně důležité	**24**	41.4 %
hodně důležité	**31**	53.4 %

Únik dat do nepovolaných rukou [Důležitost vlastností a rizik cloudových úložišť]

málo důležité	**2**	3.4 %
středně důležité	**11**	19 %
hodně důležité	**45**	77.6 %

Image „moderní technologie“ [Důležitost vlastností a rizik úložišť]

málo důležité	**42**	75 %
středně důležité	**12**	21.4 %
hodně důležité	**2**	3.6 %

Interní předpisy pro práci s daty jsou srozumitelné. [Subjektivní hodnocení respondentem]

vůbec	**6**	13 %
částečně	**25**	54.3 %
zcela	**15**	32.6 %

Jsem si jistý(á) v právní odpovědnosti při běžné práci s daty v úložišti. [Subjektivní hodnocení respondentem]

vůbec	**8**	14 %
částečně	**34**	59.6 %
zcela	**15**	26.3 %

Preferuji funkčnost a dostupnost před bezpečností. [Subjektivní hodnocení respondentem]

vůbec	**25**	45.5 %
částečně	**27**	49.1 %
zcela	**3**	5.5 %

Preferuji lokální (uvnitř organizace) uložení dat před externím úložištěm. [Subjektivní hodnocení respondentem]

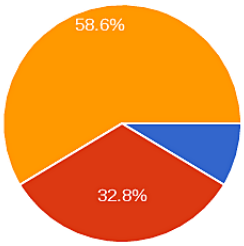
vůbec	**9**	15.8 %
částečně	**26**	45.6 %
zcela	**22**	38.6 %

Preferuji akademické úložiště před komerčním. [Subjektivní hodnocení respondentem]

vůbec	**18**	32.1 %
částečně	**20**	35.7 %
zcela	**18**	32.1 %

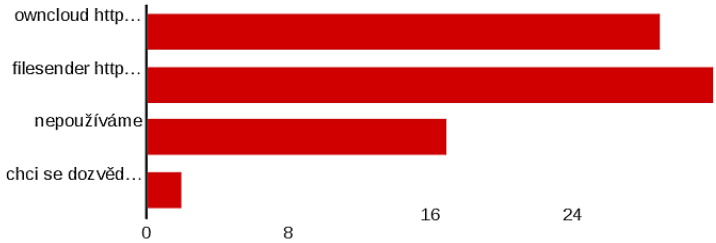
Služby CESNET z.s.p.o.

Vím co je CESNET z.s.p.o.



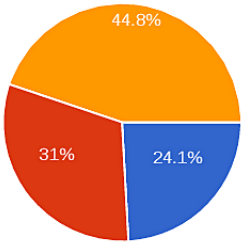
Ne, nevím.	**5**	8.6 %
Ano, CESNET znám.	**19**	32.8 %
Jsme členem nebo zákazníkem CESNET z.s.p.o.	**34**	58.6 %

Používáme služby datových úložišť CESNET



owncloud https://du.cesnet.cz/cs/navody/owncloud/start	**29**	52.7 %
filesender https://du.cesnet.cz/cs/navody/filesender/start	**32**	58.2 %
nepoužíváme	**17**	30.9 %
chci se dozvědět více	**2**	3.6 %

Vím co je Fond Rozvoje CESNET



Ne, nevím	**14**	24.1 %
Ano, vím.	**18**	31 %
Ano, byl nebo jsem řešitelem projektu FR CESNET.	**26**	44.8 %