# ZÁSADY PROVOZOVÁNÍ KAMEROVÉHO SYSTÉMU Z HLEDISKA ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ

*Miroslav Veselý, Vodní ráj Jihlava*

## 1. Kamerový systém

Jedním z fenoménů současné doby je snaha zabezpečit ochranu své osoby, rodiny, majetku, zdraví apod. prostřednictvím maximálního využití technologií umožňujících monitorovat pohyb kolem nás. Účinným způsobem takovéto prevence je nepochybně **instalace kamerového systému**, doplněného záznamovým zařízením. Tuto problematiku řeší **Zákon č. 101/2000 Sb.** o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. ledna 2010.

Na tomto místě si proto ze všeho nejdříve řekněme, že kamerový systém pro účely tohoto textu budeme chápat jako „automaticky provozovaný stálý technický systém umožňující pořizovat a uchovávat zvukové, obrazové nebo jiné záznamy ze sledovaných míst“, a to např. formou pasivního monitorování prostoru nebo pořizování cílených záběrů (zachycování pohybu) anebo reportážním způsobem. Používané kamerové systémy určitě umožňují řadu způsobů uchovávání záznamů od zastaralejší formy v podobě videokazet až po moderní formy digitalizace a zálohování dat zpracovávaných počítačovými technologiemi.

Nicméně zároveň s výběrem nejvhodnější technologie si každý, kdo hodlá instalovat kamerový systém, je-li jeho záměrem snímat a uchovávat záznamy sledovaných míst, kde se pohybují další fyzické osoby, musí určit účel a prostředky zpracování dat. Právě v této fázi rozhodování by měl mít každý provozovatel kamerového systému vyjasněny i základní otázky, zda jeho záměr je legitimní a zda a jaké povinnosti ve vztahu k jiným subjektům musí zajistit a dodržovat. Zároveň musí zvážit, zda nasazení kamerového systému je opravdu nezbytné a zda by tedy k dosažení předmětného cíle nepostačovalo jiné řešení. Takováto rozvaha, jak si ostatně ukážeme dále, nemusí přinést pouze momentální finanční úsporu, ale i eliminaci možných budoucích střetů s právem.

Z druhé strany je třeba přiznat, že problematika možné kolize užití kamerového systému s principy ochrany osobních údajů je v současné době často a hlasitě diskutovaným námětem.

Základní otázky, na něž je v této souvislosti nezbytné hledat odpověď, jsou nepochybně tyto:

kdy je kamerový systém považován za systém zpracovávající osobní údaje, a kdy tomu tak není;

kdy je zpracovávaná informace osobním údajem ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., případně citlivým údajem ve smyslu § 4 písm. b) tohoto zákona, a kdy tomu tak není.

Na první z výše nastíněných problémů se odpověď zdá být poněkud jednodušší. Zákon o ochraně osobních údajů se bude na provozovatele kamerového systému vztahovat za podmínky, že tento subjekt systematicky

zpracovává získávané informace, a to ve smyslu ustanovení § 4 písm. e) zákona č. 101/2000 Sb. Podle názoru Úřadu pro ochranu osobních údajů tomu bude vždy, pokud bude kamerový systém vybaven záznamovým zařízením zaměřeným na monitorování fyzických osob. V tomto případě dochází k systematickému shromažďování snímků osob v prostoru a časovém úseku korespondujícím s nastavením zařízení. V uvedených souvislostech lze nadto vyslovit i jistou presumpci dalšího využívání těchto záběrů. Je totiž nepochybné, že pokud by tyto záběry neměly být nijak využívány celé záznamové zařízení by postrádalo jakýkoli smysl.

Naopak za situace, kdy bude při provozování kamerového systému docházet k „pouhému“ monitorování sledovaných míst, se zákon o ochraně osobních údajů aplikovat nebude, což ovšem nevylučuje aplikaci jiných právních předpisů, zabývajících se ochranou soukromí fyzických osob, jako například článku 8 odst. 1 Úmluvy o ochraně lidských práv a základních svobod, garantující právo na respektování rodinného a soukromého života, obdobně také článku 7 odst. 1 a článku 10 odst. 2 Listiny základních práv a svobod, nebo dále § 12 odst. 1 občanského zákoníku, podle kterého smějí být obrazové a zvukové záznamy týkající se osoby pořizovány jen s jejím souhlasem a podobně. Na tomto místě je ovšem třeba pro úplnost zmínit i ustanovení § 1 odst. 2 občanského zákoníku, podle něhož se občanským zákoníkem upravují i práva na ochranu osob, pokud tyto občanskoprávní vztahy neupravují jiné zákony. Za takovýto jiný zákon je nepochybně nutno považovat i zákon č. 101/2000 Sb. Znamená to tedy, že pokud v souvislosti s provozem kamerového systému bude posledně citovaný předpis aplikovatelný, je zároveň nutno vyloučit účinky příslušných ustanovení občanského zákoníku upravujících ochranu osobnosti.

Na druhou z otázek je však již odpověď mnohem obtížnější, a to mimo jiné proto, že panuje jistá neshoda mezi dosud publikovanými názory (např. prostřednictvím systému ASPI) o tom, kdy je zpracovávaná informace osobním údajem, a kdy tomu tak není. V této souvislosti je třeba konstatovat, že pokud ze zvláštních okolností při pořízení záznamu nebude možné jednotlivé osoby identifikovat, lze v obecné rovině uvést, že informace obsažené v záznamech z kamerových systémů nedosahují kvality osobního údaje, neboť z pouhého obrazového záznamu fyzické osoby nelze tuto osobu bez použití dalších doprovodných údajů, v záznamu neobsažených, obecně ztotožnit. **Pokud tedy nebude záznam z kamerového systému možno doplnit dalšími informacemi o zaznamenané osobě, nelze údaje takto získané v obecné rovině vztáhnout k určitému nebo určitelnému subjektu údajů.**

Z tohoto náhledu by pak bylo možno uvést, že prvotní záznamy osob uchovávané v rámci provozovaného kamerového systému samy o osobě jen velmi těžko umožní jednoznačně a bez dalších údajů identifikovat určitý nebo určitelný subjekt údajů, a o aplikaci zákona č. 101/2000 Sb. lze hovořit jen ve zprostředkovaných souvislostech.

Nicméně z druhé strany je nepochybné, že každý záběr zachycující znaky umožňující odlišení fyzické osoby od jiné (zejména obličej) vytváří ze

záběru minimálně potenciální osobní údaj a jako s takovým by s ním mělo být nakládáno. Disponujeme-li totiž se snímkem uvedených kvalit, těžko můžeme vyloučit, že by nemohlo k identifikaci příslušné osoby kdykoli v budoucnu dojít, a takováto identifikace je nadto zcela evidentně hlavním důvodem toho, proč k pořizování záznamů snímků vůbec dochází (viz ostatně definice osobního údaje podle § 4 písm. a) zákona č. 101/2000 Sb.). Na okraj je možno poznamenat, že pokud by kamerový systém byl napojený na již existující databázi operující s osobními údaji jednalo by se o již z prvního pohledu zřejmé zpracování osobních údajů.

**Za uvedených okolností tak lze jedině doporučit, aby na kamerový systém umožňující sledování osob a vybavený záznamovým zařízením bylo pohlíženo jako na zařízení realizující zpracování osobních údajů. Rozhodně však bude třeba ke každému nasazení kamerového systému přistupovat individuálně.**

Pokud tedy budeme dále sledovat logiku zákona č. 101/2000 Sb., bude nezbytné i stanovení **účelu uchování záznamů** z kamerových systémů. Bezpochyby se odvozuje od využitelnosti těchto záběrů, kterou je pak třeba posuzovat podle skutečností, jež by předmětné záznamy mohly zachycovat a k jakému účelu by mohly být využity. Na prvém místě ve využití záznamů z kamerových systémů lze uvést jejich předložení jako důkazy o trestné činnosti anebo o způsobení škody ve sledované lokalitě. Dále je jejich použití možné jako důkaz v řízení o správních deliktech. V tomto případě se bude jednat zejména o využití záznamů z kamerových systémů provozovaných Policií ČR podle zákona č. 283/1991 Sb., ve znění pozdějších předpisů, nebo obecními policiemi v souladu se zákonem č. 553/1991 Sb., ve znění pozdějších předpisů. Správní úřady si přitom mohou vyžádat záznamy z kamerových systémů kdykoliv v průběhu celého správního řízení. Z těchto příkladů vyplývá nutnost při uchovávání záznamů z kamerových systémů počítat s během objektivních lhůt pro zánik trestnosti správních deliktů, které až na výjimky jako například v krizovém řízení, nepřekračují ve své většině délku tří let.

V návaznosti na shora uvedené názory na aplikaci zákona o ochraně osobních údajů se v souvislosti s tvrzením, že při zpracování informací zaznamenávaných a uchovávaných pomocí kamerových systémů nejde o osobní údaje, a tedy lze zákon o ochraně osobních údajů vztáhnout na nakládání se záznamy z kamerových systémů jen velmi okrajově, objevují názory, že není nezbytné omezovat lhůtu, po jejímž uplynutí by bylo nutno záznamy z kamerových systémů ničit, a tedy že lze uchovat tyto záznamy trvale po celou dobu existence systému popř. tak dlouho, pokud mu to kapacitní možnosti dovolí. Takovýto názor je nezbytné, až na výjimky shora uvedené, tedy výjimky, kdy monitorování a uchovávání zaznamenaných údajů vychází z veřejného zájmu, jehož účelem je především prevence a odhalování protiprávních jednání, jednoznačně odmítnout. Zejména v případech, kdy jsou kamerové systémy instalovány soukromými subjekty, jako například bankami či obchodními domy, jako především kamerové dohlížecí systémy, hrozí při dlouhodobém uchovávání těchto informací

vysoké riziko jejich možného zneužití při sledování klientů bank nebo nakupujících osob a jejich zvyklostí.

Vedle toho je nezbytné upozornit, že kromě neidentifikovatelných resp. neidentifikovaných osob, které do těchto veřejnosti přístupných prostor vstupují pro uspokojení svých požadavků a potřeb, jsou monitorováni kamerovým systémem také zaměstnanci vykonávající ve sledovaných prostorách své běžné pracovní povinnosti.

Na tomto místě pak nutno ještě předestřít otázku do jaké míry se v souvislosti se záznamy kamerových systémů jedná o citlivé údaje. Připomeneme-li si jejich výčet uvedený v § 4 písm. b) zákona č. 101/2000 Sb. je zřejmé, že ve skutečnosti přichází do úvahy více méně pouze kategorie údajů pojednávajících o národnostním, rasovém nebo etnickém původu. Nicméně i v tomto případě vzniká otázka do jaké míry takovéto snímky, často ostatně černobílé, umožní spolehlivé zjištění uvedeného. Pokud bychom si i přesto na tuto otázku odpověděli kladně, bylo by nutno zkoumat účel zpracování osobních údajů. V případě, že by byl účel stanovený tak, aby při jeho naplňování docházelo k systematickému zpracování předmětných informací, nepochybně by se jednalo o zpracování citlivých osobních údajů. Mluvíme-li tedy o odhalování pachatelů krádeží, jednalo by se o zpracování citlivých údajů pouze v případě, kdy by systém měl odhalovat pouze pachatele předem určeného etnického původu. Takovéto zpracování by ovšem muselo být, zřejmě s poukazem na ustanovení § 10 zákona č. 101/2000 Sb., označeno za nezákonné. Naopak ovšem, jedná-li se o odhalování všech pachatelů bez ohledu na rasový původ, ke zpracování citlivých údajů nedochází.

Z hlediska aplikace zákona č. 101/2000 Sb. je dále velmi důležité nalezení právního titulu pro předmětné zpracování osobních údajů. Nepochybně lze monitorovací systém použít k plnění úkolů uložených zákonem, takovéto nasazení však je umožněno velmi úzkému rozsahu subjektů (viz např. výše připomenutý zákon č. 283/1991 Sb., o Policii České republiky). Kamerový systém však je možno provozovat i na základě řádného souhlasu monitorovaných osob a zejména také na základě použití § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

Vyhovět však bude třeba i ostatním povinnostem stanoveným zákonem č. 101/2000 Sb. Především bude nezbytné záběry chránit před jakýmkoli jiným, byť náhodným, zpřístupněním, a to v souladu s ustanovením § 13 zákona č. 101/2000 Sb., a to již ve fázi pořizování záběrů a jejich přenosu ze snímacího zařízení k záznamu na datový nosič, plnit informační povinnosti vůči subjektu údajů a také předmětné zpracování registrovat u Úřadu pro ochranu osobních údajů.

Pokusím se předchozí náčrt teoreticky formulovaných požadavků promítnout do konkrétní modelové situace.

Z obecného pohledu je vcelku nepochybné, že v rámci provozu veřejně přístupného plaveckého bazénu dochází k odkládání oděvů a jiných osobních věcí do k tomu určených skříněk. Zde uzamčené předměty jsou po dobu několika hodin ponechány bez dozoru majitele a jako takové se často

stávají i objektem krádeží. Toto riziko nemůže zcela odstranit ani fyzická ostraha prováděná personálem bazénu. Nadto předmětná vloupání bývají zjišťována až s určitým časovým odstupem.

Tyto okolnosti tak zcela evidentně svědčí záměru instalovat kamerový systém, a to včetně záznamového zařízení za účelem identifikace pachatelů těchto krádeží.

V této souvislosti možno připomenout, že provozovatel bazénu žádným zákonným zmocněním k užití kamerového systému nedisponuje. Teoreticky by samozřejmě bylo možné, aby od každého z návštěvníků bazénu při vstupu požadoval souhlas s monitorováním. Z praktického hlediska by toto však vyvolávalo značné průtahy a tato varianta se tak jeví jako velmi obtížně realizovatelná. Celé zařízení tak zprovozní i bez souhlasu subjektů údajů (návštěvníků), a to na základě výše již připomenutého ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. Je totiž zjevné, že takovéto monitorování by bylo přínosem k ochraně práv a právem chráněných zájmů jak správce tak dotčené osoby, tedy návštěvníka bazénu.

Z pohledu ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. však vzniká určitý problém. Toto ustanovení totiž zakazuje porušovat práva subjektu údajů na ochranu jeho soukromého a osobního života. Pokud si uvědomíme, že v uvedených prostorách dochází k odkládání vlastně veškerých oděvních součástí, je kolize vcelku evidentní. **Té však lze velmi jednoduše zabránit, a to vytvořením speciálního prostoru určeného k převlékání, v němž by kamerové sledování neprobíhalo.**

O tomto však je třeba návštěvníky uvědomit viditelným nápisem, stejně tak je třeba návštěvníky uvědomit o vlastním nasazení monitorovacího zařízení (viz ustanovení § 11 odst. 5 zákona č. 101/2000 Sb.). Pokud by se pak i přes uvedená upozornění návštěvník převlékal v dosahu kamer, rozhodně toto nelze přičítat k tíži provozovatele bazénu.

**Příklad:**

UPOZORNĚNÍ pro návštěvníky bazénu

Z prostoru šaten je za účelem ochrany majetku návštěvníků koupaliště a provozovatele koupaliště trvale pořizován kamerovým systémem obrazový záznam.

**K převlékání proto prosím používejte převlékací boxy, které stejně jako sprchy, ani ostatní areál koupaliště není střežen kamerovým systémem.**

Pořízený obrazový záznam bude použit pouze v případě, že v tomto prostoru dojde ke ztrátě, odcizení či poškození majetku návštěvníků koupaliště nebo provozovatele koupaliště či k jiné obdobné události. V takovém případě bude pořízený obrazový záznam předám příslušným státním orgánům, zejména Policii ČR.

Ve smyslu ust.§11 zák. č. 101/2000 Sb., o ochraně osobních údajů, správce tímto informuje subjekty údajů o jejich právu přístupu k osobním údajům, jakož i o dalších právech stanovených v ust.§21 zákona.

V tomto rámci by pak byly využívány pouze záznamy vztahující se k předmětné škodní události. Ostatní záběry pak bude třeba v přiměřené lhůtě smazat. S ohledem na modelový případ lze předpokládat, že způsobená škoda by měla vyjít najevo maximálně do druhého dne po události a v těchto intencích je třeba postupovat v souvislosti se stanovením likvidační lhůty pořízených záznamů.

## 2. Na co je potřeba myslet!

**Na koho se vztahuje registrační povinnost?**

*Oznamovací povinnost se podle* § 16 odst. 1 *zákona vztahuje výlučně na správce osobních údajů. Oznamovací povinnosti nepodléhají zpracovatelé, ani jiné osoby, které se na zpracování podílejí. Oznámení o zpracování musí správce učinit ještě před zahájením samotného zpracování. Definice správce a zpracovatele osobních údajů můžete najít v* § 4 písm. j)*,resp.* k) *zákona č. 101/2000 Sb.*

**Jakým způsobem se lze zaregistrovat?**

*Od 27. listopadu 2006 bylo zavedeno elektronické přijímání registračních formulářů. Od tohoto data mohou správci podávat registrační oznámení elektronicky prostřednictvím registračního formuláře umístěného na webových stránkách Úřadu* ***www.uoou.cz*** *v rubrice „Registr". Součástí elektronického formuláře jsou rovněž podrobné pokyny k jeho vyplnění. Po vyplnění všech požadovaných bodů, oznamovatel formulář elektronicky odešle a systém jej informuje formou stručného sdělení o úspěšném odeslání . Podat oznámení o zpracování je rovněž možné učinit prostřednictvím vytištění formuláře a jeho vyplnění zaslat poštou nebo oznámení podat bez použití formuláře.. V tomto případě je nutné dbát na to, aby podání obsahovalo všechny zákonem požadované informace.*

*Registrační oznámení musí obsahovat všechny zákonem požadované informace podle § 16 odst. 2 písm. a) – i) zákona*

**Kde je možné získat nový registrační formulář?**

*Nový registrační formulář není k dispozici v tištěné podobě, jako tomu bylo dříve. Je však možné si ho vytisknout z webových stránek Úřadu a zaslat jej poštou, nebo jej vyplnit on-line a zaslat elektronicky.*

**Je vyžadován při elektronickém podávání registračního oznámení zaručený elektronický podpis?**

*Ne. Zaručený elektronický podpis není vyžadován.*

**Kdy je možné zahájit zpracování osobních údajů?**

*Správce je oprávněn zahájit zpracování osobních údajů dnem zápisu do registru nebo po uplynutí zákonné lhůty, tj. po 30 dnech ode dne, kdy bylo oznámení o tomto zpracování doručeno Úřadu, pokud nebyl vyzván k doplnění oznámení a ani nebylo zahájeno správní řízení o prověření zákonnosti oznámeného zpracování osobních údajů podle § 17 zákona.*

**Jaké jsou poplatky za registraci?**

*Žádné. Úkony spojené se zápisem informací z podaného oznámení do registru, případně vydání osvědčení o provedení registrace nejsou zpoplatněny.¨*

**Lze získat informace o zaregistrovaných zpracování?**

*Ano. Informace zapsané do registru, s výjimkou informací uvedených v § 16 odst. 2 písm. e) a i), jsou ze zákona veřejně přístupné. Veřejný registr zpracování osobních údajů je k dispozici na* ***www.uoou.cz*** *v rubrice „Veřejný registr zpracování“.*

## 3. Veřejný registr zpracování

Zákon o ochraně osobních údajů ukládá Úřadu povinnost vést registr zpracování osobních údajů [§ 29 odst. 1 písm. b) zákona], a rovněž povinnost učinit registr veřejně přístupným (§ 35 odst. 2 zákona), s výjimkou informací uvedených v § 16 odst. 2 písm. e) a i) zákona. Oznámené zpracování zapsané do registru obsahuje: identifikační údaje správce, účel nebo účely zpracování, kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají, zdroje osobních údajů, místo nebo místa zpracování osobních údajů, příjemce nebo kategorie příjemců a předpokládaná předání osobních údajů do jiných států. Do registru nejsou zapisována taková zpracování, jejichž vedení správci ukládá zvláštní zákon, a o jejich existenci je tedy subjekt údajů informován jejich prostřednictvím (jedná se o veřejně přístupné evidence, např. obchodní rejstřík apod.) nebo alespoň může jejich existenci předpokládat (zpracování osobních údajů, jichž je třeba k uplatnění práv a povinností vyplývajících ze zvláštních zákonů např. zpracování osobních údajů zaměstnanců pro vedení personální a mzdové agendy apod.)

Registr mj. umožňuje přesvědčit se, zda určitá právnická nebo fyzická osoba zpracovává osobní údaje, a zda splnila svou zákonnou povinnost takové zpracování oznámit Úřadu postupem podle § 16 zákona (pokud se na ni oznamovací povinnost vztahuje). V registru je možné vyhledávat podle názvu subjektu, přiděleného registračního čísla nebo IČ.

# 4. Slovníček nejdůležitějších pojmů

**Osobní údaj** - 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.

**Citlivý údaj** - 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.

**Anonymní údaj** - takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů, subjekt údajů fyzická osoba, k níž se osobní údaje vztahují.

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

**Shromažďování osobních údajů** - systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování.

**Uchovávání osobních údajů** - udržování údajů v takové podobě, která je umožňuje dále zpracovávat.

**Blokování osobních údajů** - vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej jinak zpracovávat.

**Likvidace osobních údajů** - fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.

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

**Zpracovatel** - každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.

**Zveřejněný osobní údaj** - osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.

**Evidence nebo datový soubor osobních údajů** - jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií.

**Souhlas subjektu údajů** - svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.

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

**Whistleblowing** – interní systém kontroly společnosti (podniku), jehož prostřednictvím mohou zejména zaměstnanci oznamovat škodlivé jednání (resp. podezření na takové jednání), kterého se dopustil jejich spolupracovník, nadřízený nebo obchodní partner. Zaměstnancům jsou zpravidla k dispozici call centra či webové aplikace, kde mohou toto jednání nahlásit. Termín whistleblowing vychází ze slovního spojení anglického whistle blower, což v překladu znamená oznamovatel, informátor, případně udavač, nebo dokonce „ten, kdo hvízdá na policejní píšťalku“. Při provozování whistleblowingu zpravidla dochází ke zpracování osobních údajů. (Více v rubrice Publikace/Bulletin č. 4/2009, str. 6–7.)

**Opt out pravidlo** – znamená, že nevyjádřím-li výslovný nesouhlas (např. s využitím svých údajů k marketingovým účelům), platí automaticky můj souhlas, tj. „od čeho se neodhlásím, to dostávám“.

**Opt in pravidlo** – znamená, že nevyjádřím-li svůj výslovný souhlas, platí automaticky můj nesouhlas, tj. „k čemu se nepřihlásím, to nedostávám“.