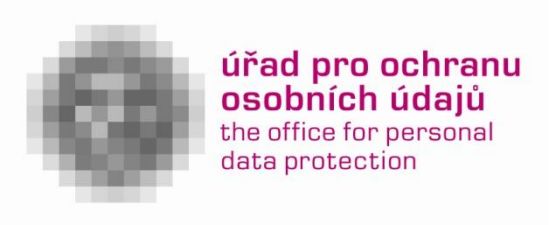
ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

PROVOZOVÁNÍ INTERNETOVÝCH OBCHODŮ (E-SHOPŮ)

Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů



OBSAH

Úvod

Zpracování osobních údajů při provozování internetových obchodů v souvislosti s ochranou osobních údajů přináší určité problémy a nejasnosti, které se projevují zvýšeným počtem dotazů jejich provozovatelů na Úřadu pro ochranu osobních údajů a také vyšší chybovostí v rámci oznámení o zpracování osobních údajů. Jedná se zejména o podávání oznámení v případech, kdy se na zpracování osobních údajů oznamovací povinnost nevztahuje, o problémy při definování účelu zpracování osobních údajů, o chybějící souhlas subjektu údajů při podání oznámení o zpracování osobních údajů a způsob jeho získávání, o nejasnosti v rozsahu podávaných informací subjektu údajů o zpracování jeho osobních údajů a některé další problémy.

Předkládaná metodika má subjektům provozujícím internetové obchody usnadnit jejich přípravu a nasazení tak, aby byly v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a to s využitím některých definovaných postupů a vzorů. Jde o návod orientační, případné řešení nejasností nebo problémů je možno konzultovat na Úřadě pro ochranu osobních údajů.

I. Provozování internetových obchodů

Elektronické obchodování lze definovat jako opakované řešení obchodních případů s využitím informačních a komunikačních technologií. Pokud se provádí v prostředí internetu, jedná se o internetové obchodování. Internetové obchodování bývá realizováno prostřednictvím provozování webových aplikací – internetového obchodu (dále také „e-shop“), který zahrnuje nabídku obchodníka, možnost vyhledávání a objednání výrobků, zboží nebo služeb zákazníkem, zprostředkování a evidenci plateb, řešení reklamací, případně i nabídku některých dalších souvisejících služeb (informace o pohybu zakoupeného výrobku nebo zboží na cestě k zákazníkovi, poskytovaní slev apod.).

V praxi existují různé způsoby řešení internetových obchodů:

1. Individuálně (na zakázku) vytvořené a realizované aplikace;
2. „Krabicově“ připravené aplikace, někdy s úpravou dle požadavků provozovatele e-shopu a s podporou jejich poskytovatele;
3. Využití volně šiřitelných připravených aplikací většinou bez podpory poskytovatele.

Způsob řešení a provozování internetového obchodu v kombinaci s umístěním dat a aplikací (vlastní zařízení a prostory, využití služeb typu housing, hosting, cloud computing apod.) a případnými smluvními podmínkami má, mimo jiné, výrazný vliv na bezpečnost osobních údajů. Volbě varianty řešení by tedy měla předcházet analýza vedoucí k nalezení ekonomicky a provozně nejvhodnějšího řešení spojeného se zajištěním odpovídající úrovně bezpečnosti.

Pozice provozovatele internetového obchodu z hlediska zpracování osobních údajů není z podaných oznámení o zpracování osobních údajů zřejmá. Obecně však lze uvést následující možnosti:

1. Provozovatel e-shopu je ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“) správcem osobních údajů, který určuje účel a prostředky zpracování, provádí jej a je za ně odpovědný.[1]
2. Provozovatel e-shopu je společně s dalšími provozovateli v postavení zpracovatele osobních údajů, ale správcem je jiná společnost (např. mateřská společnost, která zřizuje několik e-shopů).[2]

Za zpracování osobních údajů je primárně odpovědný správce. Odpovědnost případného zpracovatele osobních údajů najetého správcem vyplývá z některých ustanovení zákona o ochraně osobních údajů (§ 5, § 7, § 8, §10, § 13, § 14). Z hlediska osobních údajů je

[1] Definice správce viz § 4 písm. j) zákona o ochraně osobních údajů.

[2] Typickým příkladem může být právnická osoba v pozici mateřské společnosti (např. s.r.o.), která provozuje obchod, tj. zajišťuje zboží, které dodává napojeným osobám (většinou fyzickým osobám). K této mateřské společnosti přímo směřují všechny osobní údaje a objednávky, které zákazníci obchodu učiní, tj. veškeré údaje, které zákazníci zadají do registračních formulářů apod. Mateřská společnost rovněž vede databáze zákazníků a jejich osobních údajů. Napojená osoba („provozovatel e-shopu“) se tedy bude nacházet v pozici zpracovatele, jestliže bude poskytovat zákaznický servis a vytvářet pro správce databázi, kterou by jinak vytvářel správce, který ve smlouvě s napojenou osobou určuje napojené osobě takovouto databázi vytvářet ať již přímo, nebo nepřímo tím, že jí ukládá zákazníkům poskytovat servis. Rovněž není výjimkou, že ze strany správce bude poskytnut napojené osobě i software pro tvorbu této databáze. V tomto případě není na místě, aby se napojená osoba, jenž se nalézá v pozici zpracovatele, jelikož prostředky a účel zpracování bude určovat matka (správce), u Úřadu registrovala.

v rámci provozovaní internetového obchodu důležité definovat odpovědnost zpracovatele a také působnost zpracovatele vůči zákazníkům/subjektům údajů, a to v závislosti na podílu operací s osobními údaji, které zpracovatel namísto správce vykonává.

Situace může být rozdílná například u modelu, kdy zpracovatel poskytuje výpočetní techniku a programové vybavení a veškeré další činnosti zůstávají v rukou správce, a modelu, kdy v rukou správce zůstávají jen některé operace s daty, které jsou nezbytné pro vyřízení obchodního případu a veškerou výpočetní techniku včetně úložišť dat a počítačové programy poskytuje zpracovatel a také provádí většinu operací při zpracování osobních údajů.

V případě, že správce má na provádění některých operací najatého zpracovatele (nejedná se o zaměstnance nebo jiné osoby[3] zpracovávající údaje na základě smlouvy se správcem), musí mít ve smyslu § 6 zákona o ochraně osobních údajů uzavřenu se zpracovatelem smlouvu o zpracování osobních údajů.

[3] Jinými osobami se rozumí především zaměstnanci v pracovním poměru na základě pracovní smlouvy nebo na základě dohody o provedení práce nebo dohody o pracovní činnosti. Dále to mohou být např. fyzické osoby nebo fyzické osoby podnikající, případně i právnické osoby, pokud údaje zpracovávají na základě jiné smlouvy než smlouvy o zpracování osobních údajů podle § 6 zákona o ochraně osobních údajů, tedy na základě smlouvy dle občanského nebo obchodního zákoníku.

II. Zpracování osobních údajů – povinnost oznamovací

V rámci provozování internetových obchodů nezbytně dochází ke zpracování osobních údajů jeho zákazníků. Je přitom nutno zpracovávat osobní údaje v souladu se zákonem o ochraně osobních údajů. Jednou z povinností správce je oznámit Úřadu zpracování osobních údajů ještě před jeho zahájením postupem podle § 16 tohoto zákona[4].

Oznamovací povinnost se vztahuje na všechna zpracování prováděná nad rámec činností uložených správci zákonem nebo nezbytných pro uzavření či plnění smlouvy. Tato zpracování lze popsat:

- účely zpracování – tvorba databáze zákazníků, marketingové účely (mohou být i účely zasílání obchodních sdělení nebo nabízení obchodu a služeb, ale podmínkou je například širší rozsah zpracovaných údajů);
- doba uchování - nad rámec smluvních vztahů;
- informovanost subjektu údajů – zajištěna v souladu § 5 odst. 4, § 11, § 12 a § 21 zákona o ochraně osobních údajů (viz Příloha 1);
- získání souhlasu subjektu údajů se zpracováním osobních údajů – zajištěna ve smyslu § 4 písm. n) a § 5 odst. 4 zákona o ochraně osobních údajů (viz část IV.).

Při zpracování osobních údajů v rámci provozování internetových obchodů přichází v některých případech v úvahu rovněž výjimka podle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů, podle které se oznamovací povinnost nevztahuje na zpracování, které správci ukládá zvláštní zákon nebo je takových údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona. V případě internetových obchodů jde o následující možnosti:

- **uzavírání smluvních vztahů** - zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů; zákon č. 40/1964 Sb., občanský zákoník ve znění pozdějších předpisů; (od 1. ledna 2014 zákon č. 89/2012, nový občanský zákoník)

Podmínky:

- zpracovávat nezbytný rozsah údajů (v zákonech není přesně specifikován - přiměřený rozsah údajů je jméno, příjmení, /titul/, adresa, doručovací adresa, telefon nebo elektronická adresa, objednané zboží, číslo účtu, číslo objednávky, datum objednávky, cena zboží, informace o provedené platbě, případně i údaje o provedených oznámeních – potvrzení objednávky, informace o pohybu zboží);
- účelem je uzavírání a plnění smluvních vztahů, reklamace či jiná ochrana spotřebitele uložená provozovateli e-shopu zvláštní právní úpravou;
- zajistit informování subjektů údajů v souladu s § 11 odst. 1 a § 18 odst. 2 zákona o ochraně osobních údajů (viz Příloha 3);
- omezená doba uchování (po dobu trvání smluvního vztahu[5]);
- není potřeba souhlas subjektu údajů, neboť se ve smyslu § 5 odst. 2 písm. b) zákona o ochraně osobních údajů - jedná o zpracování osobních údajů, které je nezbytné

[4] Elektronický webový formulář včetně informace k jeho vyplnění je k dispozici na webových stránkách Úřadu v rubrice „Registr“.

[5] Tato doba zahrnuje interval od okamžiku objednání zboží do okamžiku projití záruční doby.

pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo se jedná o uzavření smlouvy uskutečněné na návrh subjektu údajů.

Kromě toho mohou být některé osobní údaje zákazníků získané v souvislosti s činností provozovatele internetového obchodu využity i k dalším účelům, které umožňují uplatnit výjimku z oznamovací povinnosti a bývají často součástí společného oznámení o zpracování osobních údajů. Jsou jimi:

- **šíření obchodních sdělení** - zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů (dále jen zákon o některých službách informační společnosti); jde o zasílání obchodních sdělení dle § 7 odst. 3 zákona o některých službách informační společnosti ve vztahu k uživatelům, kteří nedali předchozí souhlas, tj. majitel internetového obchodu získá elektronický kontakt v souvislosti s předchozím prodejem výrobků nebo služeb;

Podmínky:

- nezbytný rozsah údajů (elektronický kontakt např. e-mail, číslo mobilního telefonu apod.);
- účelem je zasílání obchodních sdělení;
- zajistit informování subjektu údajů v souladu s § 11 odst. 1 a § 18 odst. 2 zákona o ochraně osobních údajů (viz Příloha 3);
- doba uchování překračuje dobu trvání smluvního vztahu;
- subjektu údajů je umožněno při zaslání každého obchodního sdělení jednoduchým způsobem a zdarma odmítnout zasílání dalších nabídek (nejčastěji prostřednictvím e-mailu);
- součástí každého takového obchodního sdělení musí být:
  - označení, že jde o obchodní sdělení,
  - adresa provozovatele internetového obchodu,
  - adresa, na které může subjekt údajů odmítnout zasílání dalších obchodních nabídek.

- **nabízení ochodu a služeb subjektu údajů, jehož údaje byly získány v souvislosti s činností správce nebo zpracovatele** - § 5 odst. 5 zákona o ochraně osobních údajů

Podmínky:

- týká se rozesílání nabídek obchodu a služeb v klasické formě, nikoliv elektronicky;
- omezený/nezbytný rozsah údajů (jméno, příjmení, adresa bydliště, případně dodací adresa;
- účelem je nabízení obchodu a služeb;
- použité údaje jsou z veřejného seznamu nebo jde o údaje, které správce získal v souvislosti s výkonem své činnosti (bez souhlasu subjektu údajů k nim nelze přiřadit údaje další, ani např. údaje o již zakoupených výrobcích či službách);
- subjekt údajů nevyslovil nesouhlas se zpracováním osobních údajů za tímto účelem,
- informovanost subjektu údajů v souladu § 5 odst. 4, § 12 a § 21 (viz Příloha 3.);

- subjektu údajů je umožněno zaslání písemného nesouhlasu se zpracováním osobních údajů.

***Příklad**: Získá-li majitel internetového obchodu adresní a identifikační údaje zákazníka v rámci jeho objednávky zboží, může některé údaje použít k určitým činnostem i po ukončení smluvního vztahu, a to bez souhlasu subjektu údajů s takovýmto zpracováním osobních údajů a bez potřeby podávat oznámení o zpracování osobních údajů Úřadu. Jedná se o tyto údaje:*

- *jméno, příjmení a adresa, které lze použít k nabízení obchodu a služeb (nikoli prostřednictvím služeb elektronických komunikací), a to do doby, dokud subjekt údajů nevysloví písemný nesouhlas se zasíláním těchto informací (tedy lze zasílat i opakovaně); tyto údaje může vést v samostatné databázi a v případě, že subjekt vysloví písemný nesouhlas se zasíláním nabídky obchodu a služeb, je nutno údaje vymazat resp. přesunout do databáze subjektů, kterým se nemají zasílat nabídky obchodu a služeb[6];*
- *elektronický kontakt (např. e-mail) může použít k zasílání obchodních sdělení, dokud subjekt neodmítne zasílání obchodních sdělení (tedy lze zasílat i opakovaně). K tomuto účelu může vést i databázi elektronických kontaktů, a to do doby, než subjekt vysloví nesouhlas se zasíláním obchodních sdělení;*
- *výše uvedené databáze nelze slučovat;*
- *je třeba zajistit informovanost subjektu údajů o zpracování v souladu s § 11 odst. 1 zákona o ochraně osobních údajů.*

[6] Blíže viz § 5 odst. 9 zákona o ochraně osobních údajů.

III. Poznámky a doporučení k vyplňování oznámení o zpracování osobních údajů

Účelem následující části je usnadnit vyplňování formuláře Oznámení o zpracování (změně zpracování) osobních údajů podle § 16 zákona č. 101/2000 Sb., které se týká zpracování osobních údajů v souvislosti s provozováním internetového obchodu (viz též Příloha 1 - vzorové podání oznámení o zpracování a Příloha 1a – vzorové podání oznámení o změně zpracování).

Základní formulář

bod **1**. **Informace o povaze oznámení**

V případě, že dochází ke změně oznámení o zpracování osobních údajů:

- změna údajů v základním formuláři – vyplňuje se bod 1. (a to s uvedením pořadového čísla registrace, která se mění), 2., 12. a dále jen bod, který se mění (údaje v měněném bodě se vyplňují znovu za celé zpracování, nikoliv přírůstkovým způsobem, protože se údaje v příslušném bodě oznámení o změně v registru přepíší);

***Příklad**: Pokud se oznamovatel rozhodne najmout společnost Jindřich Kovář s.r.o. pro tisk štítků s adresami na poštovní zásilky, potom v rámci oznámení o změně zpracování osobních údajů je nutno v bodě 7 zaškrtnout kromě původního „automatizované - vlastními zaměstnanci“ ještě např. „automatizované – zpracovatelem“, v bodě 8 doplnit místo zpracování (pokud je odlišné od dříve uvedeného) a v bodě 9 uvést „dodavatelé zásilek (Česká pošta apod.), Jindřich Kovář s.r.o. (zpracovatel)“ viz Příloha 1a.*

bod **2. Informace o správci**

- S vyplňováním nebývají problémy.

bod **3. Účel(y) zpracování a kategorie osobních údajů**

***Účely zpracování*:**

- bezproblémové účely: *tvorba databáze zákazníků, marketing, věrnostní programy;*
- problematické účely: *zasílání zboží, plnění smluvních vztahů,* (jsou-li vyplněny tyto účely, obvykle Úřad odesílá výzvu k doplnění oznámení, která se týká aplikace výjimky z oznamovací povinnosti dle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů);

Kategorie osobních údajů:

- možné kategorie: adresní a identifikační údaje, popisné údaje a jiné údaje (např. údaje o realizovaných obchodech, zákaznických zvyklostech atd.);
- problematické kategorie: „citlivé údaje“ (viz poznámka pod čarou k bodu 5.);

***Rozsah zpracovávaných osobních údajů*:**

- *jméno, příjmení, adresa bydliště, dodací adresa, e-mail, telefonní číslo, objednané zboží či v minulosti dodané zboží, nároky na slevy apod.*

Osobní údaje budou zpracovávány se souhlasem subjektu údajů:

- Souhlas subjektu údajů je vždy nutný (v případě, že nutný není, jedná se u internetového obchodu o výjimku dle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů a zpracování není třeba oznamovat).

bod **4. Kategorie subjektů údajů**

- Zde většinou nebývá problém, označí se „*zákazníci (klienti) oznamovatele*".

bod **5. Citlivé údaje**

- V případě e-shopů by ke zpracování citlivých údajů nemělo docházet[7].

bod **6. Zdroje osobních údajů**

- Nejčastěji označit „přímo od subjektů údajů".

bod **7. Popis způsobu zpracování osobních údajů**

- S vyplňováním nebývají problémy.

bod **8. Adresa místa (míst) zpracování osobních údajů, je-li odlišná od adresy sídla (bydliště) oznamovatele**

- Doplňují se místa zpracování osobních údajů. Pokud všechno probíhá přímo v sídle oznamovatele, nemusí se bod 8. vyplňovat; pokud by formulář nepostačoval na zápis všech míst zpracování, je možno jejich seznam přiložit v rámci samostatné přílohy.

bod **9. Příjemce nebo kategorie příjemců, kterým jsou údaje zpřístupněny či sdělovány**

- Pokud zpracovává osobní údaje sám správce, jednou z nejčastěji využívaných možností je označení položky „jiní příjemci" a vepsat - *subjekty provádějící doručování zásilek.*
- Pokud se na zpracování osobních údajů podílí zpracovatel, je nejvhodnější označit položku „jiní příjemci" a vepsat - *subjekty provádějící doručování zásilek* a dále identifikaci (název) zpracovatele/zpracovatelů.

bod **10. Předpokládané předání osobních údajů do jiných států**

[7] I když v některých případech (erotické obchody, lékárny) by z objednávek bylo zřejmě možno některé citlivé údaje odvodit, nevyplňuje se ani tady kategorie citlivé údaje, pouze se u těchto typů obchodů doporučuje vyšší míra ochrany osobních údajů.

- Ve většině případů zpracování osobních údajů internetovými obchody by k předání do jiných států nemělo docházet (zasílání zásilek do ciziny není považováno za předávání údajů do zahraničí, přístup subjektů ze zahraničí k nabídce e-shopu a jejich objednávka zboží nebo registrace zákazníka rovněž není předáním údajů).

bod **11. Popis opatření k zajištění požadované ochrany osobních údajů podle §13 zákona č. 101/2000 Sb.**

- Označí se dle skutečně provedených opatření (je důležité vědět, že odpovědnost za zpracování osobních údajů nese správce, a tedy on musí analyzovat rizika a provést adekvátní opatření k ochraně osobních údajů).

bod **12. Prohlášení**

- S vyplněním nebývá problém.

K formuláři je třeba vložit/přiložit následující přílohy (pokud existují):

- ✓ kopie plné moci (není třeba, aby byla notářsky ověřena), pokud oznamovatele zastupuje jiný subjekt; a
- ✓ seznamy míst zpracování, pokud se nevešly do bodu 8. základního formuláře.

IV. Souhlas se zpracováním osobních údajů

Pokud správce hodlá při provozování internetového obchodu zpracovávat osobní údaje na základě souhlasu, tedy nad rámec zpracování uloženého mu zákonem nebo nezbytného pro plnění smluvních závazků, lze doporučit následující řešení:

1. **Varianta 1** (v Příloze 2)

   Zákazníkovi je nabídnuta jedna možnost – vyplnění registračního formuláře (potom je třeba dát zákazníkovi možnost vyjádřit souhlas nebo nesouhlas se zpracováním osobních údajů nad rámec upravený zákony tj. nad rámec nabízení obchodu a služeb podle § 5 odst. 5 zákona o ochraně osobních údajů, zasílání obchodních sdělení podle § 7 odst. 3 zákona o některých službách informační společnosti a plnění smlouvy), zde nejčastěji prostřednictvím zaškrtávacího políčka[8] s textem souhlasu v rámci registračního formuláře.

2. **Varianta 2** (v Příloze 2)

   Zákazníkovi jsou nabídnuty dvě možnosti využití služeb internetového obchodu. Jednak provedení prosté objednávky zboží, při které je informován o účelech zpracování s tím spojených, pro které není třeba souhlasu subjektu údajů[9] (tj. plnění smlouvy, nabízení obchodu a služeb podle § 5 odst. 5 zákona o ochraně osobních údajů a zasílání obchodních sdělení podle § 7 odst. 3 zákona o některých službách informační společnosti), a jednak registraci pro zpracování k zajištění dalších účelů (databáze stálých zákazníků využívaná nad rámec upravený zákony – například pro průzkumy trhu, pro nabízení slev/slevových karet, poskytnutí údajů dalším subjektům apod.). Každá možnost je uskutečňována prostřednictvím odlišného/samostatného formuláře. Jedná se jednak o jednorázovou objednávku, kdy není potřeba souhlas subjektu údajů/zákazníka se zpracováním osobních údajů, jednak o zařazení potenciálního zákazníka do zpracování, nad rámec upravený zákony, kdy je potřeba text informovaného souhlasu zákazníka se zpracováním osobních údajů uvést s tím, že souhlas vyjadřuje zákazník prostým odesláním formuláře.

Následující část řeší pouze problematiku náležitostí souhlasu se zpracováním osobních údajů, pokud mají být osobní údaje zpracovány na jeho základě (k právní úpravě více též § 4 písm. n) a § 5 odst. 4 zákona o ochraně osobních údajů):

- Před udělením souhlasu nebo nejpozději při udělení souhlasu (vzory k Variantě 1 a 2 v Příloze 2) musí být zákazník o zpracování podrobně informován v souladu se zákonem.
- Úřad doporučuje informace o zpracování poskytovat jedním dokumentem v rozsahu společném pro informování jak v případech, kdy je požadován souhlas subjektu údajů, tak i v případech, kdy není požadován souhlas subjektu údajů a také uvedeným dokumentem zajistit zpřístupnění informací dle § 18 odst. 2 zákona o ochraně osobních údajů (viz Příloha 3).

[8] Políčko nesmí být zaškrtnuto předem; pokud zákazník políčko souhlasu nezaškrtne, lze osobní údaje použít pouze pro vyřízení konkrétní objednávky v rámci smluvních vztahů a další účely uvedené v kapitole II, a poté je nutno osobní údaje likvidovat.

[9] Podrobněji viz kapitola II.

- V případě informování na webových stránkách Úřad doporučuje poskytnout zákazníkovi veškeré informace týkající se zpracování osobních údajů pokud možno na jednom místě nebo maximálně na dvou úrovních (systém provázaných odkazů, kdy musí subjekt údajů otevírat odkazy postupně na několika úrovních nebo otevírat řadu odkazů, není přehledným a žádoucím řešením).
- V případě zásadních změn (týká se změny účelu zpracování, změny rozsahu zpracovávaných údajů, zpřístupnění osobních údajů) je třeba subjekty údajů informovat a získat jejich souhlas s takto změněným zpracováním osobních údajů.
- Pokud provozovatel internetového obchodu předpokládá masivnější nákup ze zahraničí, Úřad doporučuje zpřístupnit text souhlasu (i ostatní texty) ve vícejazyčné verzi.
- Pokud se předpokládá přístup zrakově postiženým do internetového obchodu, Úřad doporučuje zpřístupnit text souhlasu (i ostatní texty) ve verzi čitelné i těmto osobám.

V. Internetový obchod z hlediska technicko-organizačních opatření

V případě provozování internetového obchodu Úřad doporučuje analyzovat potenciální hrozby, které zpracování osobních údajů mohou zasáhnout, a navrhnout a realizovat technicko-organizační opatření, která hrozby eliminují nebo maximálně omezují.

Zákon o ochraně osobních údajů v § 13 ukládá správci nebo zpracovateli zdokumentovat přijatá a provedená technicko-organizační opatření.

Obsah dokumentace přijatých technicko-organizačních opatření (může být součástí i jiného dokumentu).

1. Identifikace a popis internetového obchodu

- ✓ kdo je jeho správce,
- ✓ kdo je správcem pověřený zpracovatel/provozovatel (pokud existuje),
- ✓ kdo je projektant a dodavatel řešení,
- ✓ krátký popis technického a organizačního řešení internetového obchodu;

2. Popis technicko-organizačních opatření

Lze konstatovat, že zpracování osobních údajů v rámci internetového obchodu ohrožují čtyři druhy hrozeb (u jednotlivých opatření doplnit podrobnější technický popis realizovaných opatření):

- **Zničení nebo zneužití technických prostředků**
  - ✓ omezení přístupu k technickým prostředkům (zámky, mříže, přístupové karty apod.),
  - ✓ kamerový systém na místech možného průniku, využití pohybových čidel,
  - ✓ stálý dozor (recepce, bezpečnostní služba, centrální pult ochrany),
  - ✓ a jiné;

- **Přístup neoprávněných osob**
  - ✓ řízení přístupu k datům (hesla a role),
  - ✓ plná kontrola nad daty,
  - ✓ oddělení identifikačních a dalších dat zákazníků, pseudonymizace uživatelů,
  - ✓ programy ochraňující proti neoprávněnému průniku, programy ochraňující proti škodlivým kódům, šifrování dat, využití bezpečnějších komunikačních protokolů apod.,
  - ✓ zálohování dat,
  - ✓ bezpečnostní audit,

- ✓ a jiné;

- **Zneužití záznamů oprávněnými osobami**
  - ✓ identifikace přistupujících osob (hesla a role),
  - ✓ evidence činnosti při práci s daty (zápis dat, změna dat, kopírování dat, mazání dat),
  - ✓ zamezení kopírování dat na přenosná paměťová média, případně zamezení zasílání souborů s daty,
  - ✓ oddělení identifikačních a dalších dat zákazníků,
  - ✓ bezpečnostní audit,
  - ✓ pravidelná školení zaměstnanců/uživatelů systému,
  - ✓ a jiné;

- **Živelní událost**
  - ✓ zabezpečovací zařízení oznamující ohrožení, umístění mimo prostor ohrožených vodou,
  - ✓ zálohování dat,
  - ✓ záložní infrastruktura (hw i napájecí),
  - ✓ a jiné;

3. Ověřování funkčnosti technicko-organizačních opatření

Popis kontrol funkčnosti technicko-organizačních opatření (periodicita, kdo a jakým způsobem bude provádět, způsob zohlednění výsledků a doporučení kontroly).

Seznam dokumentů

(k dispozici na webových stránkách Úřadu – www.uoou.cz)

Mezinárodní dokumenty

- Směrnice evropského parlamentu a rady 2009/136/ES, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele
- Opinion 04/2012 on Cookie Consent Exemption

Stanoviska Úřadu pro ochranu osobních údajů

- Stanovisko č. 8/2012 – Možnost použití osobních údajů z veřejných telefonních seznamů
- Stanovisko č. 5/2012 – Poskytnutí informací a získání souhlasu subjektu údajů v elektronické komunikaci
- Stanovisko č. 1/2012 – Nepřípustné propojování databází pro marketingové účely
- Stanovisko č. 2/2011 – Zpracování osobních údajů na základě souhlasu ve smlouvě nebo Všeobecných obchodních podmínkách a s tím související problémy

Často kladené otázky

- Jsem povinen/povinna poskytnout kopii občanského průkazu doručovateli přepravní společnosti, který mi doručuje objednané zboží přes e-shop nebo od mobilního operátora?
- V jakých případech lze požadovat, aby ve smlouvě bylo uvedeno rodné číslo účastníka smluvního vztahu?
- Může správce ve smyslu § 5 odst. 5 nabízet také cizí obchody a služby (jiných osob než jeho samého)?
- Elektronický souhlas v souvislosti s § 40 OZ – znamená to, že jediný platný souhlas je s elektronickým podpisem? A co např. „klik“ na formulář na internetové stránce?

Kontroly Úřadu v předcházejících letech

- Předávání osobních údajů obchodními společnostmi za účelem nabízení obchodu nebo služeb
- Řetězení předávání osobních údajů za účelem nabízení obchodu nebo služeb
- Zpracování osobních údajů pro nabízení obchodu a služeb

Nevyžádaná obchodní sdělení

- Informace v rámci celé rubriky

Příloha 1- vzorové podání oznámení o zpracování

(číslice 9 v příslušném políčku nahrazují skutečné číslo např. IČO, telefonní a faxové číslo)

Oznámení o zpracování (změně zpracování) osobních údajů podle § 16 zákona č. 101/2000 Sb.

1. Informace o povaze oznámení

☑ nové oznámení o zpracování osobních údajů

registrační číslo oznamovatele (pokud již bylo Úřadem přiděleno):

☐ oznámení o změně zpracování osobních údajů

pořadové číslo registrace (pokud již bylo Úřadem přiděleno):

2. Informace o správci

Identifikace právnické osoby nebo fyzické osoby podnikající:

99999999 identifikační číslo (IČ)

Sportovní oděvy s.r.o. obchodní firma nebo název

Nováková 188/1 adresa sídla (ulice,číslo popisné a orientační)

Praha 6 obec PSČ

Identifikace fyzické osoby nepodnikající:

příjmení jméno

datum narození

místo trvalého pobytu (ulice,číslo popisné a orientační)

obec PSČ

Kontaktní osoba

Novák příjmení Petr jméno

Nováková 188/1 kontaktní adresa (ulice, číslo popisné a orientační)

Praha 6 obec PSČ

999999999 telefonní číslo 99999999 faxové číslo

novak@sportovniodevy.cz elektronická adresa

3. Účel(y) zpracování a kategorie osobních údajů

ÚČEL(Y) ZPRACOVÁNÍ (max. 2000 znaků)	Zasílaní informačních materiálů, marketing, vytváření databází registrovaných klientů e-shopu
KATEGORIE OSOBNÍCH ÚDAJŮ	☑ adresní a identifikační údaje ☐ citlivé údaje ☐ popisné údaje ☐ údaje o jiné osobě ☑ jiné
ROZSAH ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ (max. 2000 znaků)	Jméno, příjmení, dodávací adresa, telefon, objednané zboží, platební informace
OSOBNÍ ÚDAJE BUDOU ZPRACOVÁVÁNY SE SOUHLASEM SUBJEKTU ÚDAJŮ	☑ ANO ☐ NE

4. Kategorie subjektů údajů

☑ zákazníci (klienti) oznamovatele ☐ zaměstnanci oznamovatele ☐ členové oznamovatele

☐ osoby s jiným vztahem k oznamovateli - specifikujte:

5. Citlivé údaje

Citlivé údaje vypovídající o:

☐ národnostním rasovém nebo etnickém původu
☐ členství v odborových organizacích
☐ odsouzení za trestný čin
☐ sexuálním životě
☐ genetickém údaji
☐ politických postojích
☐ náboženství a filosofickém přesvědčení
☐ zdravotním stavu
☐ biometrickém údaji

6. Zdroje osobních údajů

☑ přímo od subjektů údajů
☐ z veřejných zdrojů - specifikujte:

☐ jiné zdroje - specifikujte:

7. Popis způsobu zpracování osobních údajů

- ☐ manuální - vlastními zaměstnanci
- ☐ manuální - zpracovatelem
- ☐ kamerovými systémy - zpracovatelem
- ☐ jiný způsob zpracování - specifikujte:
- ☑ automatizované - vlastními zaměstnanci
- ☐ automatizované - zpracovatelem
- ☐ kamerovými systémy - vlastními zaměstnanci

8. Adresa místa (míst) zpracování osobních údajů, je-li odlišná od adresy sídla (bydliště) oznamovatele

Kovářova 654 — ulice číslo popisné a orientační

Praha 8 — obec — 18600 — PSČ

9. Příjemce nebo kategorie příjemců, kterým jsou osobní údaje zpřístupněny či sdělovány

- ☐ nebudou jiní příjemci
- ☑ jiní příjemci - specifikujte:

dodavatelé zásilek (Česká pošta apod.),

10. Předpokládané předání osobních údajů do jiných států

- ☑ nebude docházet k předání osobních údajů do jiných států
- ☐ osobní údaje budou předány do členských zemí EU
- ☐ předání se uskuteční na základě smlouvy, jejíž součástí budou standardní smluvní doložky podle Rozhodnutí Komise
- ☐ osobní údaje budou předány do třetích zemí - specifikujte kterých:

11. Popis opatření k zajištění požadované ochrany osobních údajů podle § 13 zákona č. 101/2000 Sb.

(komentář: nutno vyplnit dle skutečnosti, zde jde jen o příklady)

Manuální i automatizované zpracování:

- ☑ zámky, mříže apod.
- ☐ centrální pult ochrany
- ☑ dokumentace k přijatým technicko-organizačním opatřením
- ☐ elektronické zabezpečení
- ☐ bezpečnostní směrnice

Automatizované zpracování:

- ☑ přístupová práva
- ☐ bezpečnostní zálohy
- ☑ kryptování
- ☐ jiné - specifikujte:
- ☑ antivirová ochrana
- ☐ bezpečnostní směrnice

12. Prohlášení:

☑ **Prohlašuji, že uvedené údaje jsou pravdivé a přesné a jsou vyplněné osobou oprávněnou jednat jménem oznamovatele**

Příjmení a jméno osoby oprávněné jednat jménem oznamovatele

Novák Petr

Místo vyplnění

Praha

Datum vyplnění 18.03.2013

Doplněk:

Poznámka:

Příloha 1a - vzorové podání oznámení o změně zpracování

(změna se týká bodů 7., 8. a 9. oznámení)

Oznámení o zpracování (změně zpracování) osobních údajů podle § 16 zákona č. 101/2000 Sb.

1. Informace o povaze oznámení

☐ nové oznámení o zpracování osobních údajů

registrační číslo oznamovatele (pokud již bylo Úřadem přiděleno): 00047494

☑ oznámení o změně zpracování osobních údajů

pořadové číslo registrace (pokud již bylo Úřadem přiděleno): 001

2. Informace o správci

Identifikace právnické osoby nebo fyzické osoby podnikající:

99999999 identifikační číslo (IČ)

Sportovní oděvy s.r.o. obchodní firma nebo název

Novákova 188/1 adresa sídla (ulice, číslo popisné a orientační)

Praha 6 obec PSČ

Identifikace fyzické osoby nepodnikající:

příjmení jméno

datum narození

místo trvalého pobytu (ulice,číslo popisné a orientační)

obec PSČ

Kontaktní osoba

Novák příjmení Petr jméno

Novákova 188/1 kontaktní adresa (ulice,číslo popisné a orientační)

Praha 6 obec PSČ

999999999 telefonní číslo 999999999 faxové číslo

novak@sportovniodevy.cz elektronická adresa

3. Účel(y) zpracování a kategorie osobních údajů

ÚČEL(Y) ZPRACOVÁNÍ (max. 2000 znaků)	
KATEGORIE OSOBNÍCH ÚDAJŮ	☐ adresní a identifikační údaje ☐ citlivé údaje ☐ popisné údaje ☐ údaje o jiné osobě ☐ jiné
ROZSAH ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ (max. 2000 znaků)	
OSOBNÍ ÚDAJE BUDOU ZPRACOVÁVÁNY SE SOUHLASEM SUBJEKTU ÚDAJŮ	☐ ANO ☐ NE

4. Kategorie subjektů údajů

☐ zákazníci (klienti) oznamovatele ☐ zaměstnanci oznamovatele ☐ členové oznamovatele

☐ osoby s jiným vztahem k oznamovateli - specifikujte:

5. Citlivé údaje

Citlivé údaje vypovídající o:

☐ národnostním, rasovém nebo etnickém původu
☐ členství v odborových organizacích
☐ odsouzení za trestný čin
☐ sexuálním životě
☐ genetickém údaji
☐ politických postojích
☐ náboženství a filosofickém přesvědčení
☐ zdravotním stavu
☐ biometrickém údaji

6. Zdroje osobních údajů

☐ přímo od subjektů údajů

☐ z veřejných zdrojů - specifikujte:

☐ jiné zdroje - specifikujte:

7. Popis způsobu zpracování osobních údajů

- ☐ manuální - vlastními zaměstnanci
- ☐ manuální - zpracovatelem
- ☐ kamerovými systémy - zpracovatelem
- ☐ jiný způsob zpracování - specifikujte:
- ☑ automatizované - vlastními zaměstnanci
- ☑ automatizované - zpracovatelem
- ☐ kamerovými systémy - vlastními zaměstnanci

8. Adresa místa (míst) zpracování osobních údajů, je-li odlišná od adresy sídla (bydliště) oznamovatele (doplněna adresa zpracovatele)

Kovářova 654	ulice číslo popisné a orientační		
Praha 8	obec	18600	PSČ
Sokolovská 142	ulice číslo popisné a orientační		
Praha 8	obec	18600	PSČ

9. Příjemce nebo kategorie příjemců, kterým jsou osobní údaje zpřístupněny či sdělovány

- ☐ nebudou jiní příjemci
- ☑ jiní příjemci - specifikujte:

dodavatelé zásilek (Česká pošta apod.), Jindřich Kovář s.r.o. (zpracovatel)

10. Předpokládané předání osobních údajů do jiných států

- ☐ nebude docházet k předání osobních údajů do jiných států
- ☐ osobní údaje budou předány do členských zemí EU
- ☐ předání se uskuteční na základě smlouvy, jejíž součástí budou standardní smluvní doložky podle Rozhodnutí Komise
- ☐ osobní údaje budou předány do třetích zemí - specifikujte kterých:

11. Popis opatření k zajištění požadované ochrany osobních údajů podle § 13 zákona č. 101/2000 Sb.

Manuální i automatizované zpracování:

- ☐ zámky, mříže apod.
- ☐ centrální pult ochrany
- ☐ dokumentace k přijatým technicko-organizačním opatřením
- ☐ elektronické zabezpečení
- ☐ bezpečnostní směrnice

Automatizované zpracování:

- ☐ přístupová práva
- ☐ bezpečnostní zálohy
- ☐ kryptování
- ☐ jiné - specifikujte:
- ☐ antivirová ochrana
- ☐ bezpečnostní směrnice

12. Prohlášení:

☑ **Prohlašuji, že uvedené údaje jsou pravdivé a přesné a jsou vyplněné osobou oprávněnou jednat jménem oznamovatele**

Příjmení a jméno osoby oprávněné jednat jménem oznamovatele

Novák Petr

Místo vyplnění

Praha

Datum vyplnění 18.10.2013

Doplněk:

Poznámka:

Příloha 2

Vzorové znění souhlasu:

Varianta 1

Před odesláním formuláře si pozorně přečtěte informace o zpracování osobních údajů, které jsou dostupné *zde*. V případě, že souhlasíte se zpracováním osobních údajů, potvrďte zaškrtnutím políčka před textem souhlasu. V případě, že nesouhlasíte se zpracováním osobních údajů, budou vaše údaje využity pouze pro vyřízení objednávky a související úkony, případně další účely, pro které se souhlas zákazníka nevyžaduje.

Údaje o zákazníkovi

Jméno*

Příjmení*

Adresa bydliště*

Dodací adresa (pokud se liší od adresy bydliště)*

Telefon nebo e-mail*

Přihlašovací jméno

Přihlašovací heslo

*Poznámka: Údaje označené * jsou nezbytné pro vyřízení Vaší objednávky; všechny uvedené údaje jsou nezbytné pro využívání služeb registrovaného zákazníka.*

☐ Uděluji *(název, IČO, adresa sídla správce)* souhlas se zpracováním svých osobních údajů uvedených na registračním formuláři pro účely (*marketing, evidence nároků na slevy, zasílání informačních materiálů a další),* a to na dobu .... měsíců/let do odvolání souhlasu. Před udělením souhlasu jsem byl/byla informován/informována o zpracování v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Varianta 2

1) formulář pro vyřízení prosté objednávky zboží:

Před odesláním objednávkového formuláře si pozorně přečtěte informace o zpracování osobních údajů, které jsou dostupné *zde*.

Jméno

Příjmení

Adresa bydliště

Dodací adresa (pokud se liší od adresy bydliště)

Telefon nebo e-mail

2) formuláře pro objednávku zboží a využívání služeb registrovaného zákazníka

Před odesláním registračního a objednávkového formuláře si pozorně přečtěte informace o zpracování osobních údajů, které jsou dostupné *zde*. Souhlas se zpracováním potvrdíte odesláním registračního formuláře.

Jméno

Příjmení

Adresa bydliště

Dodací adresa (pokud se liší od adresy bydliště):

Telefon nebo e-mail

Přihlašovací jméno

Přihlašovací heslo

Uděluji *(název, IČO, adresa sídla správce)* souhlas se zpracováním svých osobních údajů uvedených na registračním formuláři pro účely (*marketing, evidence nároků na slevy, zasílání informačních materiálů a další)*, a to na dobu … měsíců/let do odvolání souhlasu. Před udělením souhlasu jsem byl/byla informován/informována o zpracování v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Příloha 3

Informace o zpracování osobních údajů

Obsah informace:

- o správci osobních údajů (*jméno/název, IČO, adresa sídla/místa podnikání*);
- o zpracování osobních údajů pro účely *zasílání objednaného zboží/vyřizování objednávek, nabízení obchodu a služeb, zasílání obchodních sdělení,* které nevyžaduje souhlas subjektů údajů;
- o zpracování osobních údajů pro účely *tvorby databáze stálých a potenciálních zákazníků, marketing a podobně.*, které vyžaduje souhlas subjektů údajů;
- o kategoriích zpracování osobních údajů (nejčastěji *adresní a identifikační, údaje o jiné osobě, jiné údaje*);
- o rozsahu zpracování osobních údajů (*uvést výčet zpracovávaných údajů jako jméno, příjmení, adresa, doručovací adresa* apod; *uvést i informace o používání cookies*[10]*, pixel tags*, *action tags*, *web beacons*, *gif tags a dalších podobných nástrojích, pokud jsou využity*);
- o kategoriích subjektů údajů (*zákazníci internetového obchodu*);
- o době uchování osobních údajů;
- o tom, kdo a jakým způsobem bude osobní údaje zpracovávat (*jméno/název, IČO, adresa sídla/místa podnikání*);
- o tom, komu mohou být osobní údaje zpřístupněny (např*. dodavatelé zboží – v rozsahu jméno/název, IČO, adresa sídla/místa podnikání*) a za jakým účelem;
- o právu na přístup k informacím o zpracování svých osobních údajů (viz § 12 zákona o ochraně osobních údajů);
- o právu žádat správce nebo zpracovatele o vysvětlení zpracování osobních údajů, které je v rozporu s ochranou soukromého a osobního života nebo v rozporu se zákonem o ochraně osobních údajů (viz § 21 zákona o ochraně osobních údajů);
- o právu žádat správce nebo zpracovatele o odstranění stavu vzniklého zpracováním osobních údajů, které je v rozporu s ochranou soukromého a osobního života nebo v rozporu se zákonem o ochraně osobních údajů (viz § 21 zákona o ochraně osobních údajů);
- případné poučení o dobrovolnosti/povinnosti poskytnout osobní údaje ve smyslu § 11 odst. 2 zákona o ochraně osobních údajů.

[10] Použití tzv. session cookies nevyžaduje explicitní souhlas subjektu údajů, naproti tomu při použití tzv. persistentních nebo tracking cookies se vyžaduje souhlas subjektu údajů – viz např. čl. 66 směrnice 2009/136/ES, Opinion 04/2012 on Cookie Consent Exemption zpracovaný WP29, souhlas uživatele při použití cookies (vyžadujících souhlas) musí být zajištěn před jejich zápisem do počítače uživatele.

Provozování internetových obchodů (e-shopů)
Metodika pro splnění základních povinností ukládaných zákonem
o ochraně osobních údajů

Editor:
Grafická úprava a redakce: Tiskový odbor ÚOOÚ, leden 2014

Úřad pro ochranu osobních údajů
Plk. Sochora 27, 170 00 Praha 7
E-mail: posta@uoou.cz
Internetová adresa: www.uoou.cz