www.pwc.cz/ras

Nezávislá zpráva o ověření prohlášení společnosti Heureka Shopping s.r.o týkající se zpracování zákaznických e-mailových adres

19.1. 2018

Představenstvu společnosti Heureka Shopping s.r.o.

pwc

Obsah

Předmět zprávy a prohlášení

Představenstvo společnosti Heureka Shoppping s.r.o. (dále „Společnost“) nás pověřilo, abychom provedli ověření způsobu zpracování zákaznických emailových adres v návaznosti na definovaná prohlášení, a to:

a. Zavedené interní procesy zajišťují kontrolovaný přístup k emailovým adresám zákazníka. Tento řízený přístup zabraňuje zneužití emailových adres.

b. Adresa zákazníka je transformována Společností do speciálního formátu zabraňujícímu jejímu dalšímu zneužití nebo využití pro jiné podnikatelské činnosti.

Naše ověření bylo provedeno pro potřeby Společnosti za účelem jejího informování svých zákazníků, o způsobu zpracování zákaznických emailových adres v návaznosti na její interní procesy v souladu s výše uvedenými prohlášeními. Ověřovali jsme metodický postup, který je Společností uplatňován.

Naše ověření výroků je platné k 19.1.2018, neposkytujeme žádnou záruku týkající se změn po tomto datu.

Odpovědnosti

Odpovědnost statutárního orgánu Společnosti

Vedení Společnosti je odpovědné za realizaci vnitřních procesů zajišťujících dodržování prohlášení týkající se zpracování emailových adres zákazníků.

Úloha auditora

Naší úlohou je vydat na základě provedených procedur zprávu o tom, zda je způsob zpracování emailových adres zákazníků na základě interních procesů Společnosti v souladu s prohlášeními uvedenými výše v bodech a. a b.

Ověření jsme provedli v souladu se standardem ISAE 3000 „Ověřovací zakázky, které nejsou audity ani prověrkami historických finančních informací“. V souladu s těmito předpisy jsme povinni dodržovat etické požadavky a naplánovat a provést ověření tak, abychom získali přiměřenou jistotu o tom, zda interní procesy Společnosti upravující způsob zpracování emailových adres zákazníků jsou v souladu s prohlášeními uvedenými výše v bodech a. a b.

Shrnutí procedur provedených auditorem

Naše postupy zahrnovaly, mimo jiné, následující procedury:

- Obdržení prohlášení Společnosti a detailní seznámení s jejich obsahem
- Vytvoření seznamu kontrol nutných pro ověření prohlášení Společnosti (Příloha 1)
- Testování kontrol a hodnocení výsledků

Souhrn výsledků našeho testování ve vztahu k dodržování prohlášení společnosti je popsán v příloze 2.

Jsme přesvědčeni, že získané důkazní informace poskytují dostatečný a vhodný základ pro vyjádření našeho výroku.

Výrok

Podle našeho názoru interní procesy Společnosti upravující způsob zpracování emailových adres zákazníků jsou v souladu s prohlášeními:

a. Zavedené interní procesy zajišťují kontrolovaný přístup k emailovým adresám zákazníka. Tento řízený přístup zabraňuje zneužití emailových adres.

b. Adresa zákazníka je transformována Společností do speciálního formátu zabraňujícímu jejímu dalšímu zneužití nebo využití pro jiné podnikatelské činnosti.

Omezení pro užívání a distribuci

Naše Zpráva je určena pro účely Společnosti a pro účel uvedený v úvodu naší Zprávy. Kopie mohou být poskytnuty k distribuci existujícím i budoucím zákazníkům a partnerům Společnosti s tím, že nám nevzniká vůči nim žádný závazek a že bude Zpráva použita výhradně k uvedenému účelu.

PwC nenese žádnou odpovědnost ve vztahu k této zprávě (smluvní, deliktní (včetně nedbalosti) nebo jakékoli jiné) ve vztahu k jiným subjektům než ke Společnosti. Respektive, bez ohledu na formu akcí, ať již smluvních, úmyslného porušení práva nebo jiných akcí, v rámci možností povolených zákonem, PwC nepřebírá žádnou odpovědnost a případné důsledky vycházející z užití této zprávy pro všechny strany (s výjimkou Společnosti), nebo z jakéhokoli jiného rozhodnutí přijatého na základě této zprávy.

Tato zpráva by vždy měla být čtena včetně obou příloh.

Tomáš Kuča

Partner

19. ledna 2018

PricewaterhouseCoopers Česká republika s.r.o.

Příloha 1 – seznam testovaných kontrol

Testovaná oblast	Popis kontroly	Výsledek
Neprodukční databáze	Anonymizace emailových adres se provádí přímo při přenosu dat z produkční databáze do neprodukční databáze. Pro anonymizaci je využita dostatečná hashovací funkce SHA1 + salt. Salt je ovšem pouze statická a v případě jejího úniku může být odvozen zdroj hashe.	Bez výhrad s doporučením: Zavést používání dynamické *salt* místo její statické hodnoty.
	Zákaznická emailová adresa nemůže být přenesena do neprodukční databáze.	Bez výhrad
	V případě selhání procesu anonymizace či datového přenosu nejsou data dostupná z neprodukční databáze.	Bez výhrad
	Při kontrole se v neprodukční databázi nacházela pouze anonymizovaná data.	Bez výhrad
Produkční databáze	Přístup k produkční databázi je umožněn pouze uživatelům skupiny hadmin. Tato skupina obsahuje pouze jasně definované množství osob, které jsou výhradně systémovými administrátory.	Bez výhrad
	Přístup k fyzickým kopiím dat z produkční databáze je umožněn pouze uživateli MySQL.	Bez výhrad
	SUDO příkazy jsou logovány.	Bez výhrad
	Přístup do produkční databáze je umožněn výhradně IT systémovým administrátorům.	Bez výhrad
Zálohování produkční databáze	Proces zálohování dat je dostatečný vzhledem k povaze zálohovaných dat.	Bez výhrad
	Přístup k tvorbě záloh je umožněn pouze odpovědným systémovým administrátorům.	Bez výhrad
	Zálohy jsou dostupné pouze aplikačním uživatelům mysql a superuser root.	Bez výhrad
API pro zákazníky	Emailová adresa je hashována okamžitě po obdržení dat přes API.	Bez výhrad
	API pro zákazníky je užito jen v definovaných oblastech. Všechny tyto oblasti byly testovány.	Bez výhrad

Příloha 1 – seznam testovaných kontrol

Testovaná oblast	Popis kontroly	Výsledek
Hashovací funkce	Hashování emailových adres je uspokojivé a zamezuje zpětnému odhalení emailové adresy.	Bez výhrad
	Zákaznické emailové adresy v rámci celého projektu Heureka.cz jsou užity pouze v definovaných případech. Všechny tyto případy užití byly testovány.	Bez výhrad
	Emailová adresa v čitelné podobě je vymazána ihned po odeslání dotazníku zákazníkovi.	Bez výhrad
	Emailová adresa zákazníka je také vymazána v případě selhání odeslání dotazníku.	Bez výhrad
MySQL konfigurace	Konfigurační data MySQL jsou dostupná výhradně pro specifikovanou skupinu systémových administrátorů.	Bez výhrad

Příloha 2 – odůvodnění výroku

Proces anonymizace dat funguje správně a žádná zákaznická emailová adresa nemůže být přenesena do neprodukční databáze pokud není anonymizována. Přístup do produkční databáze a ke konfiguračním datům je vyhrazen pouze pro příslušné administrátory, jejichž aktivita je logována. Proces zálohování produkční databáze je uspokojivý vzhledem k povaze dat. Přístup k zálohovaným datům je vyhrazen pouze příslušným autorizovaným účtům.

Emailové adresy jsou hashovány do podoby, ve které není možné je přečíst. Hashovací funkce a proces hashování fungují dostatečně vzhledem k povaze dat. S emailovými adresami je v rámci projektu Heureka.cz nakládáno pouze v definovaných testovaných oblastech. K odstranění emailových adres v čitelné podobě dochází v definované časové periodě.