Novinky v oblasti zpracování osobních údajů

Webinář 12. července 2022

Tereza Hošková, Jiří Kvaček

Weinhold Legal

Organizační informace

- Prezentace bude rozesílána po skončení webináře
- Dotazy pište, prosím, do chatu
- Dotazy budou zodpovídány po skončení přednáškového bloku

Zkratky

- Použité zkratky:
  - Subjekt údajů (SÚ)
  - Osobní údaje (OÚ)
  - Technická a organizační opatření (TOMs)
  - Obecné nařízení (EU) 2016/679 (GDPR)
  - Úřad pro ochranu osobních údajů (ÚOOÚ)
  - Soudní dvůr Evropské unie (SDEU)
  - Evropský sbor pro ochranu osobních údajů (EDPB)
  - Nejvyšší správní soud (NSS)

Agenda webináře

- Novinky v legislativě
  - Cookies
  - Aktuální situace v oblasti předávání OÚ do USA
- Nové pokyny EDPB
  - Pokyny k právu na přístup k OÚ
  - Příklady porušení zabezpečení
- Z rozhodovací praxe českého dozorového úřadu – ÚOOÚ
- Rozhodovací praxe českých soudů
- Zajímavosti ze zahraniční rozhodovací praxe
- Dotazy

Novinky v legislativě I.

Cookies

Novela zákona o elektronických komunikacích

- Zákon č. 374/2021 Sb., kterým se mění zák. č. 127/2005 Sb., o elektronických komunikacích a o změně některých zákonů
- Účinnost od 1. 1. 2022
- Účelem především ochrana spotřebitele
- Hlavní body: **1) Cookies, 2) Telemarketing**

Cookies – o co jde?

- *„…malé množství dat, která www server pošle prohlížeči, který je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládají se do nich uživatelské předvolby apod.“*
- Druhy cookies
  - Technické
  - Statistické
  - Analytické
  - Marketingové
- Souhlas s uložením a čtením cookies v prohlížeči uživatele (kromě výjimky u technických) x účel podle GDPR

Cookies – kdy je třeba souhlas s jejich používáním?

- Do 31. prosince 2021
  - V ČR princip **opt-out** (cookies se používají do doby, než je uživatel odmítne/vypne)
  - Povinnost *„předem prokazatelně informovat o rozsahu a účelu jejich zpracování“* a dát možnost takové zpracování odmítnout
  - Rozpor s právem EU (GDPR, směrnice ePrivacy)
- Od 1. ledna 2022
  - Princip **opt-in** (vyžaduje se aktivita uživatele)
  - Povinnost „[správce] *získá od [...] účastníků nebo uživatelů předem prokazatelný souhlas s rozsahem a účelem [...] zpracování*“
  - Týká se „*každého*“, kdo používá nebo hodlá používat sítě el. komunikací k ukládání údajů nebo k získávání přístupu k údajům uloženým v koncových zařízeních uživatelů

Cookies – kdy je třeba souhlas s jejich používáním?

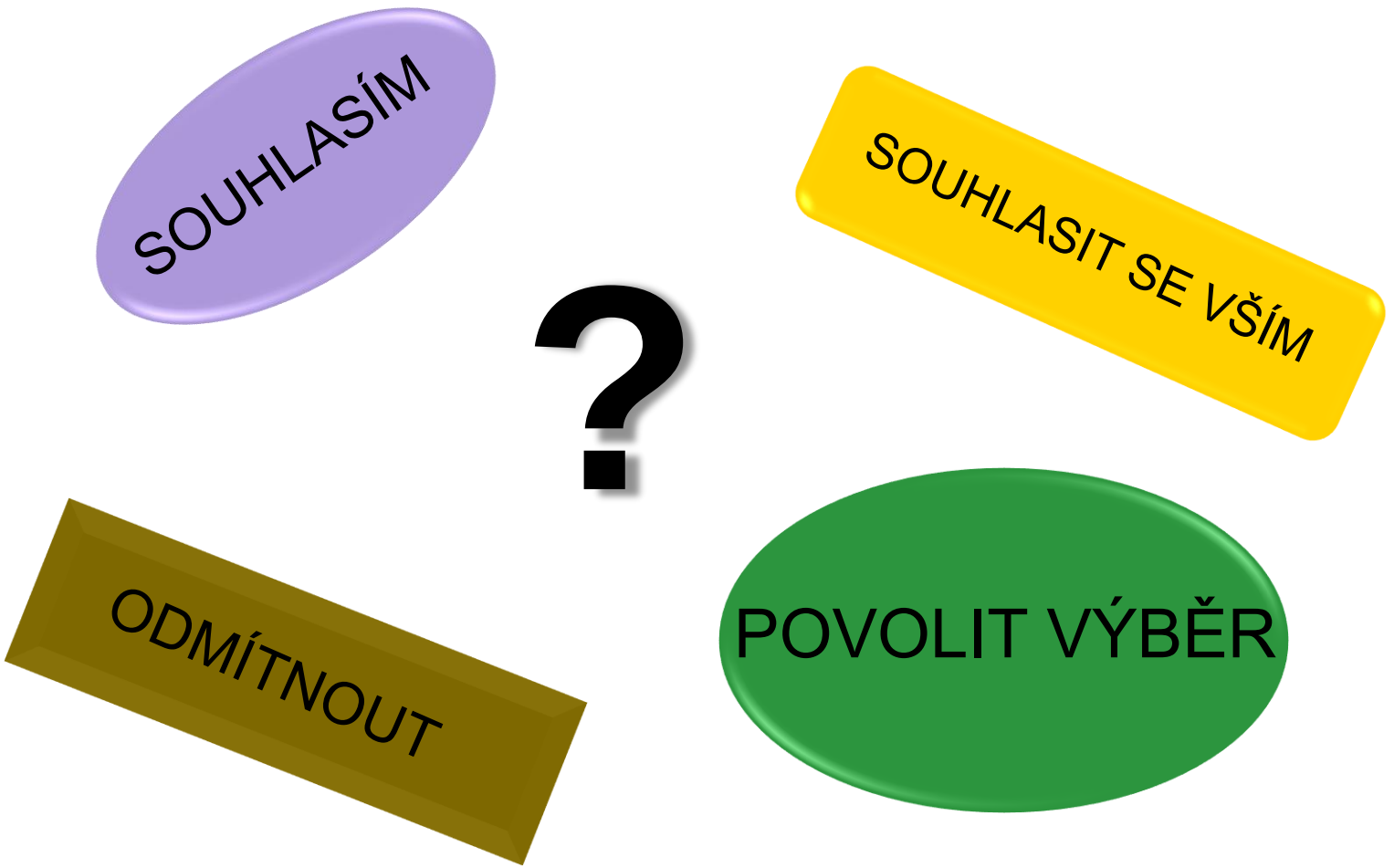
- Cookies nezbytné pro zajištění provozu
  - „technické ukládání“, zajištění přenosu zpráv, pro poskytnutí služby
  - není nutný souhlas (výjimka)

- Cookies pro marketingové účely / statistické / analytické
  - je nutný svobodný souhlas

Cookies – podoba souhlasu

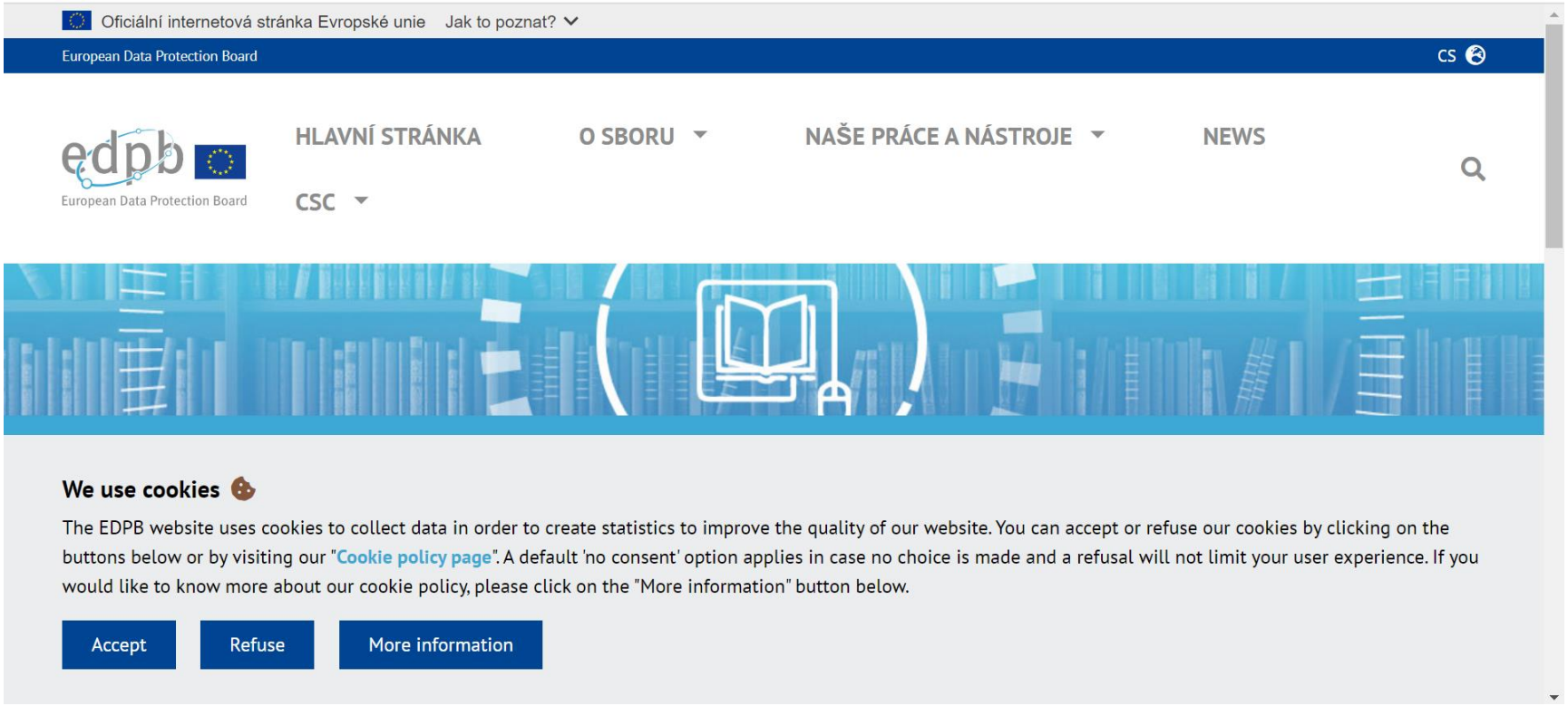
- Podoba souhlasu
  - Pop-up lišta doplněná o cookies policy
  - JISK: Jednoznačný – Informovaný – Svobodný – Konkrétní
  - Snadno odvolatelný
- Nepřípustné praktiky
  - Režim opt-out
  - Neudělení souhlasu ztěžuje užívání stránky
  - Scrolling na stránce jako způsob udělení souhlasu
  - Cookie wall
  - Nastavení prohlížeče
  - Zavření lišty jako způsob udělení souhlasu

Cookies – podoba souhlasu



Weinhold Legal

Příklady – jak by to mělo správně vypadat



Weinhold Legal

Novinky v legislativě II.

Předávání OÚ do USA

Možné nástroje pro předávání

- Mezi EU a USA probíhá předávání velkého množství dat
  - dle EDPB mezinárodní obchod v hodnotě 900 miliard EUR

1. Rozhodnutí EK o odpovídající úrovni ochrany
2. Standardní smluvní doložky (SSD) dle čl. 46 GDPR
3. Závazná podniková pravidla (BCR) dle čl. 47 GDPR
4. Výjimky dle čl. 49 GDPR pro specifické situace (souhlas subjektu údajů, nezbytnost předání pro splnění smlouvy apod.)

Základní právní rámec – vývoj

- EU-USA Privacy Shield (štít ochrany soukromí)
  - Rozhodnutí Evropské komise o odpovídající úrovni ochrany
  - Sloužil k předávání OÚ do USA certifikovaným subjektům
  - Zrušen rozsudkem SDEU Schrems II ze dne 16. července 2020 (zejména s odkazem na široké pravomoci amerických zpravodajských služeb)
- Standardní smluvní doložky
  - Původní standardní smluvní doložky (2010)
  - Nové standardní smluvní doložky
    - Účinné od 27. června 2021
    - Povinné od 27. září 2021 v nových smlouvách
    - Adaptace existujících smluv do 27. prosince 2022

Standardní smluvní doložky

- Nové standardní smluvní doložky dle čl. 46 GDPR
  - Nejsou závazné pro orgány veřejné moci třetích zemí (smluvní charakter)
  - Prováděcí rozhodnutí Komise (EU) 2021/914 ze dne 4. června 2021 o nadstandardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízení evropského parlamentu a Rady (EU) 2019/679 (GDPR)
  - Nezbytnost provádět TIA (Transfer Impact Assessment)
  - ÚOOÚ: každý správce předávající osobní údaje zpracovateli do USA na základě SSD nebo správce, který zatím o předání uvažuje, má řešit s dovozcem údajů konkrétní dopady rozsudku Schrems II, hledat a navrhovat řešení v podobě dalších bezpečnostních záruk

Principy nového transatlantického rámce ochrany OÚ

- Nový základ rozhodnutí EK – pružnější globální nástroj
- Cíl: podpora ekonomiky po pandemii, utužení západní spolupráce
- Dohodnuté zásady
  - Volný a bezpečný přenos dat
  - Pravidla a závazné záruky pro omezení přístupu amerických zpravodajských služeb k údajům + dohled
  - Systém nápravy a řešení stížností občanů EU, dohled a přezkum
  - Povinnost certifikace pro společnosti z USA
- Aktuálně
  - Zpracování nových zásad do právních dokumentů
  - Proklamace o přijetí ze strany USA do konce roku 2022

Nové pokyny EDPB

Nové pokyny EDPB

- Pokyny č. 05/2022 na užití technologie rozpoznávání tváře (face recognition) v oblasti vymáhání práva ze dne 12. května 2022
- Pokyny č. 4/2022 k výpočtu správních pokut dle GDPR
- Pokyny č.10/2020 k omezení dle článku 23 GDPR
- **Pokyny č.1/2021 k příkladům ohlašování porušení zabezpečení osobních údajů**
- Pokyny č. 5/2021 k užití článku 3 GDPR o místní působnosti a ustanovení dle kapitoly V. GDPR o předávání osobních údajů do třetích zemí
- **Pokyny č. 1/2022 k právům subjektu údajů – právo na přístup**
- Pokyny č. 2/2022 k užití článku 60 GDPR týkajícího se spolupráce mezi vedoucím dozorovým úřadem a dalšími dotčenými dozorovými úřady
- Pokyny č. 3/2022 k „dark patterns“ (temné vzorce) v rozhraních platforem sociálních médií
- Pokyny č. 4/2021 ke kodexům chování jako nástroji k předávání osobních údajů do třetích zemí nebo mezinárodním organizacím

- Veřejná konzultace: Pokyny č. 07/2022 k certifikaci jako nástroji předávání

Pokyny k právu SÚ na přístup k OÚ – I.

- Základní právo SÚ (SÚ může žádat pouze svoje údaje)
- Nezaměňovat s právem na svobodný přístup k informacím
- Obsah práva
  - Informace o tom, zda jsou OÚ zpracovávány
  - Přístup k nim
  - Další informace o zpracování
- Forma žádosti a její posouzení
  - Forma není stanovena
  - Doporučení: vytvoření vhodného veřejně dostupného formuláře; sběrná e-mailová adresa
  - Kontrola identity žadatele

Pokyny k právu SÚ na přístup k OÚ – II.

- Rozsah poskytnutí OÚ
- Způsob poskytnutí OÚ
  - Kopie, opisy
  - Listinná nebo elektronická forma
  - Možnost nahlédnutí do systému (udělení oprávnění) a umožnění stažení (permanentní výstup)
  - Zpoplatnění
- Omezení a výjimky
  - Zjevně nedůvodná nebo nepřiměřená žádost
  - Omezení lokální právní úpravou (čl. 23 GDPR)
  - Práva třetích osob

Pokyny k příkladům ohledně ohlašování případů porušení zabezpečení OÚ

- 2017 Pokyny k ohlašování případů porušení zabezpečení OÚ
- 2022 Pokyny s praktickými příklady zohledňující nabyté zkušenosti
- Připomenutí
  - Druhy případů porušení
  - Povinnost evidovat a oznamovat
  - Dostatečná TOMs
  - Nastavení procesů pro vyšetřování a oznamování
  - Pravidelná školení
- Úniky: ransomware, lidská chyba, exfiltrace dat aj.

Z rozhodovací praxe českého dozorového orgánu - ÚOOÚ

Proces postihování nedodržování pravidel GDPR

- Zdroj informací/podnětů:
  - Provedená kontrola (podle kontrolního plánu)
  - Stížnost SÚ
  - Ohlášení případu porušení zabezpečení OÚ
- Protokol o kontrole, námitky
- Správní řízení (dvouinstanční)
- Soudní přezkum

Kontroly provedené ÚOOÚ v letech 2021 a 2022

Kontroly provedené ÚOOÚ – I.

1. Správa OÚ samotným SÚ
   - Přenášení odpovědnosti za plnění povinností správce na SÚ při realizaci práv subjektů údajů
   - Předmětem kontroly i zpracovatelské vztahy a TOMs
2. Neoprávněné přeregistrace pojištěnců
   - Nedostatečná TOMs pro přijímání žádostí a v oblasti interních předpisů
   - Porušení zásady přesnosti OÚ
   - Od ÚOOÚ uložena konkrétní opatření k nápravě

Kontroly provedené ÚOOÚ – II.

3. Informační systém využívaný veřejnými vysokými školami
   - Moduly „Uchazeč“ a „Studium“
   - Rozsah nepřiměřený účelu a zákonnému důvodu

4. Průzkum veřejného mínění v obci
   - GDPR naprosto neřešeno
   - Zpracování bez zákonného důvodu, netransparentnost, chybějící zpracovatelská smlouva aj.

Kontroly provedené ÚOOÚ – III.

5. Kamerové systémy
   - Atrapa = nejedná se o zpracování OÚ, tj. nespadá pod GDPR
   - Obecně: dobré TOMs, přiměřená doba uchovávání, přiměřený rozsah zpracování (pokrytí kamerami), dostupné informace, korektní zpracovatelské vztahy a jasné pokyny, řádné označení monitorovaných prostor, kvalitní vnitřní předpisy, zanesení informací v záznamech o činnostech zpracování

Rozhodovací praxe českých soudů

Soudní rozhodnutí - NSS

- NSS ve věci MALL.CZ dovodil, že odpovědnost za porušení zabezpečení není vždy absolutní
  - Pokud jsou zavedena vhodná opatření, a i přesto dojde k úniku dat, nemusí za to správce nést odpovědnost
  - Zásadní je „vhodnost“ opatření
  - Sp. zn. 1 As 238/2021 – 33 ze dne 11. listopadu 2021

- NSS potvrdil pokutu uloženou ÚOOÚ kontrolované nemocnici za nedostatečné zajištění bezpečnosti při zpracování osobních údajů
  - Uložena pokuta 40.000 Kč
  - Sp. zn. 10 As 190/2020 – 39 ze dne 25. února 2022

Zajímavosti ze zahraniční rozhodovací praxe

Zahraniční rozhodovací praxe

- Francie: Cloudové služby
  - Cloudové služby poskytované společností z USA na území EU – vyjádření k přijatým zárukám
  - Umístění výlučně na území EU
  - Dešifrovací kódy svěřené osobě se sídlem mimo USA (mimo sféru vlivu zpravodajských služeb)
- Irsko: 17 mil. EUR pokuta pro META (dříve Facebook)
  - 12 porušení (oznámení od SÚ)
  - 30 mil. postižených SÚ za dobu 6 měsíců
  - Meta nebyla schopna prokázat zavedení vhodných TOMs
  - Přeshraniční zpracování – zapojení dalších lokálních úřadů (kolektivní rozhodnutí)

Otázky?

Další setkání
s Weinhold Legal

Kde se můžeme setkat příště?

Srpen 2022

- Dopad růstu inflace na veřejné zakázky

Září 2022

- Obchodněprávní judikatura

Říjen 2022

- Porušení zabezpečení osobních údajů

DĚKUJEME ZA POZORNOST

A TĚŠÍME SE NA DALŠÍ SETKÁNÍ A SPOLUPRÁCI

Hodnocení spokojenosti

Kontakty

Tereza Hošková

Vedoucí advokátka

E: Tereza.Hoskova@weinholdlegal.com

M: +420 720 965 304

Jiří Kvaček

Advokát

E: Jiri.kvacek@weinholdlegal.com

M: +420 601 697 834

www.weinholdlegal.com