VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

ZOBRAZENÍ A ÚPRAVA INFORMACÍ V TRANSPARENCY AND CONSENT FRAMEWORK

TRANSPARENCY AND CONSENT FRAMEWORK DATA LISTING AND EDITING

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE **Bc. ALEŠ POSTULKA**
AUTHOR

VEDOUCÍ PRÁCE **Ing. LIBOR POLČÁK, Ph.D.**
SUPERVISOR

BRNO 2021

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav informačních systémů (UIFS) Akademický rok 2020/2021

Zadání diplomové práce

Student: **Postulka Aleš, Bc.**
Program: Informační technologie a umělá inteligence Specializace: Informační systémy a databáze
Název: **Zobrazení a úprava informací v Transparency and Consent Framework**
Transparency and Consent Framework Data Listing and Editing
Kategorie: Web

Zadání:

1. Seznamte se s IAB Europe Transparency and Consent Framework (TCF).
2. Nastudujte možnosti tvorby rozšíření do webových prohlížečů.
3. Navrhněte rozšíření pro webové prohlížeče, které bude zobrazovat informace z TCF uložené navštívenou stránkou. Umožněte uživateli předem nastavit poskytnutí specifických souhlasů, nesouhlasů, respektive vznesení námitek proti zpracování.
4. Návrh implementujte. Rozšíření bude vícejazyčné.
5. Implementaci otestujte. V rámci testů se pokuste ověřit, do jaké míry webové stránky respektují přání uživatele rozšíření.
6. Práci vyhodnoťte a navrhněte možná budoucí rozšíření.

Literatura:

- IAB Europe. IAB Europe Transparency & Consent Framework Implementation Guidelines. https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/TCF-Implementation-Guidelines.md, Version 2.
- Célestin Matte, Nataliia Bielova, and Cristiana Santos. 2019. Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. ArXiv eprint 1911.09964, dostupné onlinehttps://arxiv.org/abs/1911.09964.
- WP29 - Article 29 Data Protection Working Party. 2010. Opinion 2/2010 on online behavioural advertising. WP171, dostupné online https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf.
- WP29 - Article 29 Data Protection Working Party. 2011. Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising. WP188, dostupné online https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf.

Při obhajobě semestrální části projektu je požadováno:

- Body 1.-3. zadání.

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Polčák Libor, Ing., Ph.D.**
Vedoucí ústavu: Kolář Dušan, doc. Dr. Ing.
Datum zadání: 1. listopadu 2020
Datum odevzdání: 19. května 2021
Datum schválení: 26. října 2020

Abstrakt

Tato práce se zabývá tvorbou vícejazyčného rozšíření pro webové prohlížeče Mozilla Firefox a Google Chrome. Účelem rozšíření je umožnění automatizované správy poskytnutých souhlasů se zpracováním osobních údajů na webových stránkách využívajících rámec Transparency and Consent Framework. Rozšíření bylo vytvořeno na základě poznatků o tomto rámci a o právních normách GDPR a směrnici ePrivacy, které se zabývají ochranou osobních údajů. Při implementaci byly využity také znalosti o způsobu tvorby rozšíření pro webové prohlížeče pomocí WebExtensions. Při testování byl v prohlížeči Mozilla Firefox souhlas úspěšně vynucen na 96,2 % testovaných webových stránkách. V prohlížeči Google Chrome bylo úspěchu dosaženo u 82,1 % testovaných stránek. Banner vyžadující souhlas nebyl zobrazen na 33 % stránek u prohlížeče Mozilla Firefox a na 31,1 % stránek u prohlížeče Google Chrome.

Abstract

This thesis deals with the development of multilingual for web browsers Mozilla Firefox and Google Chrome. The purpose of the extension is to enable the automated management of provided consents to the processing of personal data on websites using the Transparency and Consent Framework. Extension was developed on the basis of knowledge about this framework and about legal norms GDPR and ePrivacy Directive, which deal with the protection of personal data. Knowledge of the method of developing extensions for web browsers using WebExtensions was also used during the implementation. During testing, consent was successfully enforced in 96,2 % of tested websites in Mozilla Firefox. In Google Chrome, success has been achieved in 82,1 % of tested websites. The banner requiring consent was not displayed in 33 % of websites in Mozilla Firefox and in 31,1 % of websites in Google Chrome.

Klíčová slova

ochrana osobních údajů, Transparency and Consent Framework, Consent Management Platform, CMP API, rozšíření pro webové prohlížeče, WebExtensions, JavaScript

Keywords

personal data protection, Transparency and Consent Framework, Consent Management Platform, CMP API, web extension, WebExtensions, JavaScript

Citace

POSTULKA, Aleš. *Zobrazení a úprava informací v Transparency and Consent Framework.* Brno, 2021. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Libor Polčák, Ph.D.

Zobrazení a úprava informací v Transparency and Consent Framework

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Libora Polčáka Ph.D. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....
Aleš Postulka
13. května 2021

Poděkování

Chtěl bych poděkovat Ing. Liboru Polčákovi Ph.D. za ochotu a cenné rady v průběhu tvorby této práce.

Obsah

Kapitola 1

Úvod

Od doby, kdy vstoupilo v platnost nařízení Evropské unie GDPR, se začaly na webových stránkách objevovat bannery vyžadující poskytnutí souhlasu se zpracováním osobních údajů. V tak velkém množství mohou být tyto bannery spíše obtěžující, a uživatelé jim tak nemusí věnovat příliš velkou pozornost. To může vést k situaci, kdy uživatel klikne na tlačítko potvrzující souhlas bez vědomí, k čemu konkrétně souhlas poskytl.

Cílem této práce je navrhnout a implementovat vícejazyčné rozšíření pro webové prohlížeče Mozilla Firefox a Google Chrome. Rozšíření bude umožňovat správu souhlasů se zpracováním osobních údajů na webových stránkách využívajících rámec Transparency and Consent Framework. Uživatel bude mít možnost nastavení udělování souhlasu případně nesouhlasu s jednotlivými účely zpracování a s jednotlivými prodejci. Při navštívení webové stránky využívající rámec Transparency and Consent Framework pak bude dle uživatelských preferencí automaticky vytvořen souhlas se zpracováním osobních údajů a následně bude uložen do navštíveného webu. Informace o poskytnutém souhlasu bude možné zobrazit pomocí vyskakovacího okna rozšíření.

Kapitola 2 se věnuje ochraně osobních údajů. Jsou zde popsány právní normy GDPR a směrnice ePrivacy, které definují pravidla ochrany osobních údajů a jejich zpracování. Popsáno je také vzájemné působení těchto norem. Dále jsou v kapitole popsány způsoby cílení internetové reklamy včetně principu Real Time Bidding.

V kapitole 3 je popsán rámec Transparency and Consent Framework (TCF), jehož cílem je usnadnit zajištění dodržení výše zmíněných právních norem při shromažďování a zpracovávání osobních údajů na internetu. Je zde popsán řetězec používaný pro uložení souhlasu se zpracováním osobních údajů. Následně jsou uvedeny definice účelů a funkcí zpracování osobních údajů. Na konci kapitoly je popsáno rozhraní CMP API, které umožňuje přístup k informacím uloženým v TCF.

Tvorba rozšíření pro internetové prohlížeče je popsána v kapitole 4. V této kapitole je popsáno API WebExtensions, které je v současnosti asi nejblíže standardu pro tvorbu rozšíření nezávislých na konkrétních prohlížečích. Dále je popsána struktura rozšíření a způsob vytvoření vícejazyčného rozšíření.

Existující rozšíření, která se zabývají souhlasy se zpracováním osobních údajů jsou popsána v kapitole 5. Některá z nich jsou založena na využití starší, již nepodporované verze rámce Transparency and Consent Framework. U jiných je pak například snaha pouze skrýt bannery, vyžadující souhlas se zpracováním osobních údajů, bez ohledu na to, zda, a k jakým účelům bude souhlas udělen.

Kapitola 6 je zaměřena na návrh samotného rozšíření pro webové prohlížeče. Je zde navržen způsob získávání informací uložených v TCF a jejich následné zobrazení. V kapitole

je dále popsán způsob nastavování uživatelských preferencí pro jednotlivé účely zpracování osobních údajů a možné způsoby ukládání vytvořeného souhlasu, tak aby byl tento souhlas navštívenou webovou stránkou akceptován.

Implementace navrženého rozšíření je popsána v kapitole 7. V kapitole je popsaná struktura rozšíření, manifest rozšíření a implementace zobrazení informací o poskytnutém souhlasu, nastavení a poskytování souhlasu navštívené webové stránky. Popsán je také generátor překladů, který byl vytvořen za účelem usnadnění správy lokalizovaných textů, které rozšíření využívá.

Informace o provedeném testování jsou uvedeny v kapitole 8. Kapitola obsahuje popis způsobu testování, výsledky testování, a také zajímavé chování webových stránek a CMP, které bylo pozorováno v průběhu testování rozšíření.

V závěru práce jsou shrnuty dosažené výsledky, popsány nedostatky vytvořeného rozšíření a uvedeny návrhy na jejich odstranění.

Kapitola 2

Ochrana osobních údajů

Tato kapitola se zabývá osobními údaji. Zaměřena je zejména na ochranu těchto informací, jejich shromažďování a zpracování za účelem zobrazení personalizované reklamy. První část kapitoly je věnována právním normám zabývajícím se ochranou osobních údajů. Těmito normami jsou *Obecné nařízení o ochraně osobních údajů (GDPR)* a *Směrnice o soukromí a elektronických komunikacích (ePrivacy Directive)*. V další části jsou popsány principy internetové reklamy a princip Real Time Bidding, který slouží pro obchodování s digitální reklamou v reálném čase. Poslední část pak popisuje pravidla pro získávání souhlasů se zpracováním osobních údajů a s odkazy na provedené průzkumy ukazuje, že velké množství webových stránek v této oblasti porušuje nařízení GDPR a směrnici ePrivacy.

V kapitole je několikrát odkazováno na dokumenty vytvořené pracovní skupinou WP29 (Working Party 29). Jednalo se o evropský poradní orgán, který byl nezávislý a zaměřoval se na ochranu dat a soukromí. Vznikem GDPR byla WP29 nahrazena *Evropským sborem pro ochranu osobních údajů (EDPB)* [37].

2.1 Obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů, známé taky pod zkratkou *GDPR* (General Data Protection Regulation), je nařízení vydané Evropskou unií (EU). Zákon vstoupil v platnost 25. května 2018 a jeho cílem je zvýšit ochranu osobních údajů občanů [36]. Tímto zákonem se musejí řídit všechny (ne pouze ty v EU) fyzické osoby, firmy a organizace, které shromažďují nebo zpracovávají osobní údaje občanů evropské unie [18].

Hlavním důvodem vzniku nařízení GDPR bylo to, že předchozí směrnice na ochranu osobních údajů z roku 1995 již byla zastaralá a nedostačující vzhledem k současným a rychle se rozvíjejícím technologiím, zejména pak zaostávala za stále se rozšiřujícími možnostmi využití internetu, popisuje Škorničková [37]. Jedním z dalších důvodů pro vytvoření nového nařízení na ochranu osobních údajů bylo shromažďování osobních údajů občanů EU tajnými službami některých států mimo Evropskou unii.

GDPR bylo navrženo tak, aby chránilo osobní údaje bez ohledu na použitou technologii ke zpracování těchto údajů, a aby mohlo být použito při manuálním i automatizovaném zpracování osobních údajů. Stejně tak není nařízení o ochraně osobních údajů závislé na způsobu uložení osobních údajů [6].

Souběžně s nařízením GDPR mělo být vydáno také *Nařízení o soukromí a elektronických komunikacích (ePrivacy Regulation)*. Webová stránka gdpr.eu [32] uvádí, že toto nařízení mělo nahradit a rozšířit směrnici o ochraně osobních údajů a elektronických komunikacích

(ePrivacy Directive). I přes existující návrhy nebylo toto nařízení doposud vydáno, a tak je stále v platnosti již zmíněná směrnice, která je popsaná níže v sekci 2.2. Rozdíl mezi směrnicí (directive) a nařízením (regulation) je takový, že směrnice musí být zeměmi Evropské unie začleněna do státního práva, kdežto nařízení se od data vstupu v platnost stává právně závazným v celé Evropské unii.

Osobní údaje

Jako osobní údaje jsou dle GDPR článku 4 odst. 1 [26] označovány informace, které se vztahují k identifikované nebo identifikovatelné žijící osobě. Mezi osobní údaje jsou řazeny také jednotlivé informace, které mohou jako celek přispět k identifikaci určité osoby. Dále pak osobní údaje, u nichž lze i přes pseudonymizaci[1], zašifrování, nebo odstranění informací umožňujících identifikaci, zpětně identifikovat osobu, jsou stále považovány za osobní údaje. Anonymizované[2] údaje již naopak za osobní údaje považovány nejsou. Za osobní údaje jsou například považovány [6]:

- jméno a příjmení,
- pohlaví,
- datum narození a věk,
- osobní stav,
- adresa,
- e-mail,
- číslo identifikační karty (občanského průkazu, cestovního pasu apod.),
- lokační údaje,
- IP adresa,
- identifikátor telefonu pro inzerenty,
- údaje vlastněné lékařem nebo nemocnicí, které mohou jednoznačně identifikovat určitou osobu.

V článku 9 nařízení GDPR [26] je také definováno několik kategorií osobních údajů, které jsou označovány jako *citlivé*, a na které se vztahují přísnější podmínky pro zpracování [13]:

- rasový či etnický původ,
- politické názory,
- náboženské nebo filozofické vyznání,
- členství v odborech,

[1] *Pseudonymizace osobních údajů* – „zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě“ GDPR článek 4 odst. 5 [26].

[2] „*Anonymizované údaje* jsou takové údaje, které ani nepřímo nepomáhají v identifikaci určitého člověka a nejsou s ním tedy nijak spojitelná.“ – Škorničková [37].

- údaje o zdravotním stavu,
- genetické a biometrické údaje zpracovávané za účelem identifikace člověka,
- sexuální orientace,
- pravomocné odsouzení a trestní delikty.

Zpracování údajů

Zpracování osobních údajů je v GDPR článku 4 odst. 2 [26] definováno jako jakákoliv operace nebo soubor operací, které využívají osobní údaje. Mezi tyto operace patří shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření, seřazení či zkombinování, omezení a odstranění osobních údajů. Jako zpracování osobních údajů je označováno například [5]:

- uložení IP adresy nebo MAC adresy,
- uložení identifikátoru zařízení,
- zobrazování personalizované reklamy,
- zasílání propagačních e-mailů,
- zveřejnění fotografie osoby na web,
- správa výplatní listiny.

Tvůrci GDPR se zaměřili také na shromažďování osobních údajů dětí. Evropská komise [16] uvádí, že informace určené dítěti by měly být prezentovány pomocí jasného a jednoduchého jazyka. U většiny online služeb, zejména u sociálních služeb, platforem pro stahování hudby a nakupování online her, je vyžadován souhlas zákonného zástupce. Článek 8 nařízení GDPR [26] definuje rozsah pro věkovou hranici, kdy je vyžadován souhlas zákonného zástupce, na 13-16 let. Konkrétní věkovou hranici si pak určují samotné členské státy na základě tohoto rozsahu.

2.2 Vzájemné působení mezi GDPR a směrnicí ePrivacy

S nástupem digitálního věku bylo potřeba vytvořit právní nástroj pro zajištění ochrany soukromí ve světě internetu. Tím se stala v roce 2002 *Směrnice o soukromí a elektronických komunikacích (ePrivacy Directive)* [24], která je zaměřena zejména na důvěrnost komunikace, na pravidla sledování a trasování uživatelů digitálních technologií a na zpracování osobních údajů. V roce 2009 byla tato směrnice aktualizována. Jednou z důležitých změn bylo přidání podmínky do odstavce 3 v článku 5 [24] takové, že shromažďování a zpracovávání osobních údajů je možné pouze na základě souhlasu uživatele. Mezi další hlavní změny patřila například nutnost oznámení v případě úniku osobních údajů (ztráta nebo neoprávněný přístup), zahrnutí různých elektronických štítků a posílení donucovacích pravidel [8]. Jak již bylo zmíněno výše v sekci 2.1, tato směrnice měla být souběžně s vydáním GDPR nahrazena Nařízením o ochraně soukromí a elektronických komunikacích. Přestože existuje návrh tohoto dokumentu, nebylo nařízení doposud vydáno. Stále tedy zůstává v platnosti směrnice dále označována jako *směrnice ePrivacy*.

Nařízení GDPR a směrnice ePrivacy se v mnoha ohledech překrývají, a tak nemusí být zřejmé, který dokument je v takovou chvíli směrodatný. Tímto se na základě podnětu belgického úřadu pro ochranu osobních údajů zabýval Evropský sbor pro ochranu osobních údajů. 12. 3. 2019 bylo sborem vydáno *Stanovisko č. 5/2019* [29], ve kterém jsou zkoumány oblasti působnosti těchto dokumentů, a ve kterém je definováno jakým způsobem mají být dokumenty používány v případech, které řeší oba tyto dokumenty.

Směrnice ePrivacy je ve Stanovisku č. 5/2019 označována jako *lex specialis*. Toto označení se používá pro zákony, které ve specifických aspektech doplňují nebo rozšiřují zákony obecné. GDPR je naopak označováno jako *lex generalis*, tedy obecný zákon. Že je GDPR obecným zákonem vyplývá již ze samotného názvu *Obecné nařízení o ochraně osobních údajů*.

Ve Stanovisku č. 5/2019 byly definovány dva koncepty, koncept *upřesnění* a koncept *doplnění*. Koncept *upřesnění* říká, že zpracování osobních údajů v oblasti elektronických komunikací je nařízení GDPR upřesňováno ustanoveními směrnice ePrivacy. Uplatňuje se tedy právní zásada, podle které má směrnice ePrivacy přednost před obecným nařízením GDPR v případech, kdy směrnice ePrivacy *upřesňuje* ustanovení nařízení GDPR. Na ostatní oblasti týkající se zpracování osobních údajů, které jsou mimo rozsah působnosti směrnice ePrivacy, pak stále platí obecné nařízení GDPR. Koncept upřesnění je využíván například v situaci, kdy jsou osobní údaje uchovávány v zařízení uživatele. V tomto případě má přednost směrnice ePrivacy, která definuje, že pro možnost uchovávání nebo přistupování k osobním údajům v zařízení uživatele je potřeba od daného uživatele nejprve obdržet souhlas se zpracováním osobních údajů. Koncept *doplnění* zase znamená, že některá ustanovení směrnice ePrivacy doplňují ustanovení definovaná v nařízení GDPR. Ustanovení směrnice GDPR jsou směrnicí ePrivacy doplňovány v případě, že se jedná o zpracování osobních údajů v oblasti elektronických komunikací.

2.3 Reklama na internetu

Zobrazování reklamy je využíváno pro financování služeb, které jsou na internetu dostupné zdarma (mzdy zaměstnanců, výdaje za techniku, energie, atd.) [25, 35]. Tyto služby pronajímají plochu na svých webových stránkách inzerentům třetích stran. Mezi nejpoužívanější způsoby cílení internetové reklamy patří tyto [35]:

- *Kontextová reklama* – Reklama je typem obsahu podobná obsahu webové stránky, na které je zobrazena. Inzerent pro danou reklamu specifikuje, na kterých webech (domény, části URL, kategorie webu apod.) má být reklama zobrazována. Reklama tak je zobrazována na webových stránkách odpovídajících definovaným parametrům, ale není cílena na konkrétní uživatele. Vzhledem k existenci pokročilejších technik zobrazování reklamy již není tento způsob příliš využíván.

- *Behaviorální*[3] *reklama* – Tento typ cílení reklamy využívá sběru informací o chování uživatelů. Na jejich základě jsou vytvářeny profily těchto uživatelů. V profilech je množství atributů, které dané uživatele specifikují. Konkrétní reklama je pak zobrazena těm uživatelům, jejichž profil obsahuje takovou kombinaci atributů, která odpovídá definici vytvořené inzerentem dané reklamy. Například společnost Facebook využívá celkem 240 000 atributů, kdy každý uživatel má přiřazených průměrně 523,7

[3] Behaviorální = týkající se chování

z nich. Společnost Google pak uchovává průměrně 42,3 atributů u jednotlivých uživatelů.

Mechanismy pro cílení reklamy jsou řízeny tzv. poskytovateli reklamních sítí, kteří spojují poskytovatele webových stránek a inzerenty s cílem zajistit co nejefektivnější zobrazování reklamy, popisuje WP29 [25]. Poskytovatelé reklamních sítí spolu často spolupracují pomocí systému aukcí jejichž princip je popsán níže v podsekci *Real Time Bidding*.

- *Retargeting* – Způsob cílení reklamy využívaný zejména provozovateli e-shopů za účelem přilákat zpět uživatele, kteří sice daný e-shop již navštívili, ale neuskutečnili v něm žádný nákup.
- *Vlastní výběr osob (custom audience* nebo *customer match)* – Je používán nejčastěji k oslovení dřívějších zákazníků za účelem informování například o slevových akcích, nových produktech a podobně. K šíření takové reklamy jsou využívány e-maily, SMS zprávy nebo telefonní hovory. E-mailové adresy a telefonní čísla jsou inzerentovi známé právě díky předchozím nákupům uživatelů, při kterých tyto údaje uvedli.
- *Inzerce osobám podobným mému výběru (look-alike audience* nebo *similar audience)* – Tato metoda cílení reklamy je využívána pro získání nových návštěvníků (zákazníků) webové stránky. Z informací o návštěvnících webové stránky je odvozena charakteristika těchto uživatelů. Reklama je poté cílena na uživatele, kteří mají podobnou charakteristiku jako již existující uživatelé.

Real Time Bidding

Real Time Bidding (RTB) je princip, který je využíván pro nákup a prodej digitálních reklamních ploch v reálném čase. Tento proces je prováděn pomocí veřejných aukcí. Aukce jsou prováděny ve chvíli, kdy je uživateli načítána požadovaná webová stránka a zpravidla trvají pouze několik milisekund.

Do procesu RTB je standardně zahrnováno šest rolí, kdy každý z aktérů (společností) může v RTB zastávat více těchto rolí [30]:

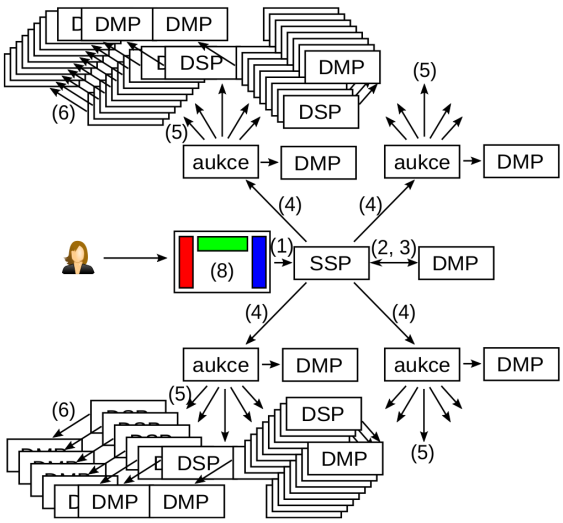
- *Reklamní burzy* nebo *aukční servery (Advertising exchanges)* – Porovnávají cenové nabídky a relevantnost jednotlivých reklam. Jedná se o jakési prostředníky mezi inzerenty a provozovateli webových stránek, kteří pracují s nabídkami ale i poptávkami.
- *DMP (Data Management Platforms)* – Tyto společnosti shromažďují data z různých zdrojů. Tato data analyzují a kategorizují. Součástí dat jsou také poptávky, které jsou využívány pro podporu zobrazování personalizované reklamy.
- *DSP (Demand Side Platforms)* – DSP jsou společnosti, které zaštiťují množství inzerentů. Pokud atributy profilu uživatele, kterému má být reklama zobrazena, odpovídají požadavkům na cílovou skupinu uživatelů definovanou inzerentem, je s využitím DSP podána cenová nabídka na zobrazení reklamy.
- *SSP (Suply Side Platforms)* – Jsou využívány ke správě a prodeji reklamních ploch na webových stránkách provozovatelů.
- *Provozovatelé webových stránek (Publishers)* – Jsou společnosti, které prostřednictvím SSP nabízejí reklamní plochu na svých webových stránkách. Zobrazování reklam je často jejich jediným zdrojem příjmů.

- *Inzerenti (Advertisers)* – Organizace, které chtějí zobrazovat reklamy na webových stránkách provozovatelů.

RTB se standardně řídí konkrétními specifikacemi (protokoly), které stanovují způsob shromažďování a sdílení údajů uživatelů a způsob poskytování reklam. Nejvýznamnějším je protokol *OpenRTB* [19] vyvinutý společností IAB Europe a protokol od společnosti Google zvaný *Authorized Buyers* [2].

Informace, které jsou za účelem získání personalizované reklamy sdíleny, se mohou lišit. Existuje však řada standardních informací, které jsou sdíleny ve většině žádostí o zobrazení internetové reklamy [30].

- IP adresa uživatele,
- identifikátor uživatele,
- řetězec *user-agent* za účelem identifikace prohlížeče a zařízení,
- informace o aktuální nebo domácí poloze uživatele,
- informace o časovém pásmu uživatele,
- jazyk systému uživatele,
- a další.



Obrázek 2.1: Ilustrativní schéma šíření informací v rámci RTB. Převzato z [35].

Šíření informací v RTB, které je znázorněno na obrázku 2.1, probíhá následovně [35]:

1. Provozovatel webové stránky předá svým SSP, se kterými má uzavřenou smlouvu, požadavek na zobrazení reklamy.
2. SSP následně kontaktují DMP, se kterými spolupracují.
3. DMP identifikují uživatele na základě skriptů vykonaných v prohlížeči a informaci zašlou zpět SSP.

4. Získané informace o uživateli jsou spolu s požadavkem na zobrazení reklamy rozeslány různým aukčním serverům.

5. Aukční servery mohou doplnit získané data o uživateli dalšími daty získanými od svých DMP. Následně jsou rozeslány požadavky na nabídky v aukci organizacím DSP.

6. DSP, které obdržely požadavek na nabídku v aukci mohou doručené informace o uživateli opět rozšířit o informace ze společností DMP, se kterými spolupracují.

7. DSP odešlou aukčním serverům své nabídky.

8. Jednotlivé aukční servery poté pošlou SSP nejlepší nabídky.

9. Kromě zobrazení reklamy může DSP s nejlepší nabídkou distribuovat do prohlížeče uživatele vlastní skripty v jazyce JavaScript a namapovat vlastní identifikátor na pseudonym používaný aukčními servery pro dané zařízení (tzv. Cookie Matching).

2.4 Souhlas se zpracováním osobních údajů na internetu

Jak již bylo zmíněno výše v sekci 2.2, je potřeba aby ke shromažďování a zpracovávání osobních údajů poskytl uživatel souhlas. WP29 popisuje v pokynech pro souhlas [27] prvky souhlasu a způsoby získání souhlasu, které musejí být splněny, aby byl souhlas platný a v souladu s článkem 7 nařízení GDPR [26] a směrnicí ePrivacy [24]. Souhlas je považován za platný pokud je *svobodný, konkrétní, informovaný a jednoznačný.*

Za *svobodný* je souhlas považován, pokud byla uživateli umožněna skutečná volba zda souhlas poskytne či nikoliv. Pokud uživatel tuto volbu nemá nebo je souhlas nezbytnou součástí k používání dané služby, není takový souhlas považován za svobodný a tedy ani za platný. Souhlas není svobodný ani v situaci kdy jej bez újmy nelze odmítnout či odvolat.

Konkrétní souhlas je takový souhlas, který uživatel poskytne pro *konkrétní* účely shromažďování a zpracovávání osobních údajů, a u kterého má uživatel možnost volby udělení souhlasu pro každý z těchto účelů. Pokud tedy uživatel není informován o konkrétních účelech shromažďování a zpracování údajů nebo nemá možnost volby udělení souhlasu pro jednotlivé účely, nejedná se o konkrétní souhlas a není považován za platný.

Před získáním souhlasu uživatele je potřeba mu poskytnout informace, které mu umožní přijmout informovaná rozhodnutí, chápat předměty jeho souhlasu, a které jej seznámí s právem svůj souhlas odvolat. WP29 definovala informace, jejichž poskytnutí je nutné pro získání platného *informovaného* souhlasu:

- totožnost správce,
- účel každé operace zpracování, pro kterou je souhlas požadován,
- jaké údaje budou shromažďovány a zpracovávány,
- existence práva souhlas odvolat,
- informace o využití údajů,
- a možná rizika předávání údajů.

S požadavkem na informovaný souhlas úzce souvisí požadavek, aby byly informace týkající se zpracování osobních údajů, na jejichž základě se uživatel rozhoduje o poskytnutí souhlasu, *transparentní*. To znamená, že tyto informace musejí být pro uživatele snadno dostupné, srozumitelné a musejí být předkládány pomocí jasných a jednoduchých jazykových prostředků. WP29 vypracovala dokument s pokyny pro transparentnost [28], ve kterém jsou mimo jiné popsány prvky a pravidla transparentnosti podle GDPR. Informace poskytované uživateli, které se týkají zpracování osobních údajů musejí:

- být stručné, transparentní, srozumitelné a snadno přístupné,
- používat jasné a jednoduché jazykové prostředky, obzvláště při poskytování informací dětem,
- být poskytnuty písemně, elektronicky nebo jinými prostředky,
- být na vyžádání poskytnuty ústně,
- být poskytnuty bezplatně.

Souhlas se zpracováním osobních údajů musí být udělen aktivním jednáním nebo prohlášením uživatele, aby bylo *jednoznačné*, že uživatel s konkrétním zpracováním souhlasil. Pokud tedy budou pro získání souhlasu využívána předem zaškrtnutá políčka pro udělení konkrétního souhlasu, je takový souhlas neplatný. Za aktivní jednání s cílem udělit souhlas se zpracováním osobních údajů není považováno udělení souhlasu pouhým pokračováním používání služby.

WP29 v pokynech pro souhlas také zdůrazňuje, že souhlas se zpracováním osobních údajů musí být uživatelem udělen vždy před zahájením zpracování osobních údajů, které takový souhlas vyžadují. Nový souhlas je pak vyžadován pokaždé, kdy dojde ke změně či přidání účelů zpracování osobních údajů.

Průzkum, provedený Célestinem Matte a kol. [34] ukazuje, že velké množství webů nějakým způsobem porušuje podmínky pro získání souhlasu definované nařízením GDPR a směrnicí ePrivacy. V článku byly identifikovány čtyři potenciální porušení pokynů pro získávání souhlasů:

- Uložení souhlasu před potvrzením volby uživatele – webová stránka uloží souhlas se zpracováním údajů dříve, než uživatel potvrdí své volby k jednotlivým účelům zpracování.
- Neposkytnutí možnosti nesouhlasit se zpracováním osobních údajů - webová stránka neumožní uživateli vznést námitku proti zpracování údajů. Webová stránka uživatele například pouze informuje o použití cookies a zpracování osobních údajů.
- Přednastavený souhlas – webová stránka dává uživateli možnost volby, ale některé z těchto voleb jsou přednastaveny na hodnotu „souhlasím“.
- Nerespektování volby uživatele – webová stránka uloží pozitivní souhlas se všemi účely zpracování bez ohledu na volby provedené uživatelem.

Z celkem 560 zkoumaných webových stránek se jich 304 (54.26 %) dopouštělo alespoň jednoho porušení zákona. Nejčastěji webové stránky využívaly přednastavení souhlasu se zpracováním. Tohoto prohřešku se dopustilo hned 236 z 508 (46.5 %) testovaných webových

stránek. Polčák [35] pak ve své analýze ukazuje, že situace na českém webu není příznivější. Touto analýzou byly dokonce objeveny webové stránky, které o zpracování osobních údajů vůbec neinformují i přesto, že využívají aukční servery z ekosystému RTB, a je tedy pravděpodobné, že ke zpracování osobních údajů dochází.

Kapitola 3

Transparency and Consent Framework

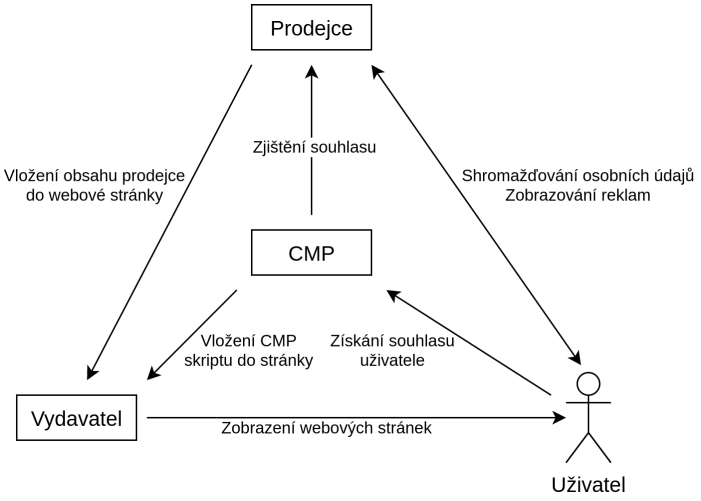
Transparency and Consent Framework (TCF) byl vytvořen asociací IAB Europe jako reakce na vydání GDPR. TCF je aktuálně dostupný ve verzi 2.0. Některé webové stránky však stále využívají předchozí verzi 1.1, které však byla 15. 8. 2020 ukončena podpora [21].

Úkolem TCF je pomoci všem stranám zainteresovaným do digitální reklamy zajistit dodržení GDPR a směrnice ePrivacy při zpracování osobních údajů, přístupu nebo ukládání informací do zařízení uživatele, mezi které patří například cookies, reklamní identifikátory, identifikátory zařízení apod. [21].

TCF poskytuje prostředí, ve kterém mohou vydavatelé webových stránek sdělit uživateli, jaká data budou shromažďována a jakým způsobem je bude daná webová stránka a společnosti, se kterými spolupracuje, využívat [21]. Transparency and Consent Framework rozlišuje tři účastnící se strany [11] jejichž vzájemné vazby jsou ilustrovány na obrázku 3.1.

- *Vydavatel (Publisher)* – provozovatel digitálního obsahu (webové stránky, aplikace, apod.), v němž dochází ke shromažďování a zpracování osobních údajů. Je zodpovědný za zobrazení uživatelského rozhraní rámce uživateli a za vytvoření právního základu pro prodejce, kteří mohou zpracovávat osobní údaje návštěvníků digitálního obsahu vydavatele.
- *Prodejce (Vendor)* – společnost, která se podílí na zobrazování reklamy v digitálním obsahu vydavatele.
- *Platforma pro správu souhlasů (CMP – Consent Management Platform)* – prostředník mezi vydavatelem, prodejci a koncovým uživatelem, který usnadňuje ustavení právního základu a získání souhlasu se zpracováním osobních údajů. CMP je společnost, která centralizuje a spravuje transparentnost, souhlas a námitky koncových uživatelů. Typicky také pod jménem vydavatele zobrazuje uživateli uživatelské rozhraní pro získání souhlasu se zpracováním osobních údajů.

Součástí TCF je *Globální seznam prodejců (GVL – Global Vendor List)*. Jedná se o dokument ve formátu JSON, který obsahuje pravidelně aktualizovaný seznam prodejců registrovaných do TCF. Tento dokument je veřejně dostupný online [10] a jeho obsah je zdokumentován v GitHub repozitáři rámce Transparency and Consent Framework [22]. Kromě seznamu prodejců je dostupný také seznam CMP, který je rovněž dostupný online [9] a dokumentace jeho obsahu je v již zmíněném GitHub repozitáři.



Obrázek 3.1: Vztahy mezi jednotlivými stranami zainteresovanými do TCF.

3.1 Transparency and Consent String

Pro uložení souhlasu uživatele je v TCF definován řetězec *Transparency and Consent String (TC String)* [22]. Řetězec je vytvářen za účelem zapouzdření všech důležitých informací týkajících se uděleného souhlasu:

- Obecná metadata – standardní značky určující detaily daného řetězce jako např. verze kódování, datum poslední úpravy, datum vzniku atd. Dále jsou v této části obsaženy podmínky transparentnosti a souhlasu jako např. verze GVL, informace o CMP atd.
- Souhlas uživatele – souhlas poskytnutý uživatelem pro zpracování osobních údajů. Obsahuje dvě části: souhlasy podle účelů a souhlasy podle prodejců.
- Oprávněný zájem – záznamy o oprávněných zájmech prodejců a informace o tom, zda uživatel proti jednotlivým oprávněným zájmům vznesl námitku.
- Omezení vydavatele – omezení ze strany vydavatele na zpracování osobních údajů prodejcem v kontextu uživatelů obchodujících s jejich digitálním majetkem.
- Transparentnost a souhlas vydavatele – tato část může obsahovat vlastní právní základ a uživatelův souhlas pro zpracování osobních údajů.
- Právní základy mimo TCF – informace o prodejcích, kteří využívají právní normy mimo ty definované TCF.
- Zveřejnění konkrétní jurisdikce[1] – údaje o státu, ve kterém má vydavatel sídlo, případně o státu, jehož legislativou se vydavatel řídí. Obsahuje také informaci zda byl uživatel seznámen s účelem 1 (viz sekce 3.2), protože je tento účel některými jurisdikcemi řešen jinak.

[1] „Jurisdikce je slovo latinského původu a vyjadřuje právo posuzovat případ. V užším smyslu znamená jurisdikce soudní pravomoc a soudní příslušnost. V širším smyslu se týká nejen soudů, nýbrž i úřadů správních (politických, samosprávných, disciplinárních senátů aj.), včetně vymezení rozsahu územní a věcné oblasti, ve které svou pravomoc mohou uplatnit.“ [20]

Řetězec může být vytvořen až po potvrzující akci, která jednoznačně vyjadřuje souhlas uživatele. Vytvářet by jej měly pouze registrovaná CMP s využitím přiděleného identifikátoru. Prodejci ani žádná jiná třetí strana naopak nesmí TC String vytvářet ani upravovat.

V TCF jsou definovány dva typy řetězce souhlasu, *globální (global)* a *specifický pro službu (service-specific)*. *Globální* řetězec je uložen globálně a je sdílen mezi CMP. Globální řetězec nesmí obsahovat část *omezení vydavatelů* ani část *transparentnost a souhlas vydavatele*. Řetězec *specifický pro službu* je využíván pouze službou, kterou byl tento řetězec vytvořen a není sdílen napříč CMP ani jinými službami.

Při vytváření řetězce je nejprve potřeba převést požadované informace na bitový vektor. Vytvořený bitový vektor je následně zakódován pomocí algoritmu *Base64*, ve kterém jsou místo znaků *plus* (+) a *lomítko* (/) použity znaky *podtržítko* (_) a *pomlčka* (–).

3.2 Definice účelů a funkcí

V TCF jsou definovány účely a funkce [11], ke kterým je možné udělit souhlas. Pro tyto účely a funkce jsou vytvořené oficiální překlady do různých světových jazyků. Překlady jsou volně dostupné online ve formátu JSON [15]. Níže uvedené definice jsou převzaty z [11] a názvy účelů jsou převzaty z oficiálního českého překladu [15]. Detailnější informace o účelech a funkcích jsou uvedeny v příloze A.

Účely (Purposes)

Definované účely pro zpracování dat, včetně osobních dat uživatele, účastníky TCF u kterých má uživatel možnost volby.

1. Ukládání a/nebo přístup k informacím v zařízení.
2. Základní nastavení reklamy.
3. Vytvoření profilu pro personalizovanou reklamu.
4. Výběr personalizované reklamy.
5. Vytvoření profilu pro personalizovaný obsah.
6. Výběr personalizovaného obsahu.
7. Měření výkonu reklamy.
8. Měření výkonu obsahu.
9. Používání výzkumu trhu pro získání poznatků o uživatelích.
10. Vývoj a zlepšování produktů.

Zvláštní účely (Special Purposes)

Definované zvláštní účely pro zpracování dat včetně osobních, u kterých uživatel nemá možnost volby.

1. Zajištění bezpečnosti, předcházení podvodům a odstraňování chyb.
2. Technické doručení (zobrazení) reklamy nebo obsahu.

Funkce (Features)

Definované funkce zpracování osobních údajů účastníky TCF, pro které není uživateli umožněna volba.

1. Párování a kombinování zdrojů offline dat.
2. Propojení různých zařízení.
3. Přijetí a použití automaticky zasílaných specifických vlastností zařízení pro identifikaci.

Zvláštní funkce (Special Features)

Definované zvláštní funkce zpracování osobních údajů, pro které má uživatel možnost volby.

1. Používání přesných údajů o geografické poloze.
2. Aktivní vyhledávání identifikačních údajů v rámci vlastností zařízení.

Skupiny účelů a/nebo funkcí (Stacks)

Jedná se o definované kombinace účelů a/nebo speciálních funkcí, které mohou při udělování souhlasu nahrazovat jednotlivé účely nebo speciálních funkcí. V podstatě se tedy jedná o pojmenování určitých kombinací účelů nebo speciálních funkcí. Například skupina číslo 2 s názvem „Základní nastavení reklamy a měření výkonu reklamy“ je kombinací účelů 2 a 7.

3.3 Consent Management Platform API

Specifikace TCF definují *Consent Management Platform API (CMP API)* [7]. Jedná se o rozhraní, kterým CMP umožňuje přístup k informacím o transparentnosti a o souhlasu získaném od uživatele. Každé CMP musí poskytovat funkci `__tcfapi(command, version, callback, parameter)`, pomocí které je možné k informacím přistupovat. Dle specifikace jsou definovány čtyři příkazy (commands), které musejí být podporovány:

1. `getTCData` pro získání všech informací uložených v řetězci TC String včetně řetězce samotného a několika dalších informací.
   - command: `'getTCData'`,
   - version: `2`,
   - callback: `function(tcData: TCData, success: boolean)`,
   - parameter (volitelné): seznam id prodejců, ke kterým mají být informace získány.
2. `ping` pro získání informace, zda již byl načten hlavní skript CMP, údajů o CMP a informace o tom, jestli je aplikováno GDPR.
   - command: `'ping'`,
   - version: `2`,
   - callback: `function(pingReturn: PingReturn)`,

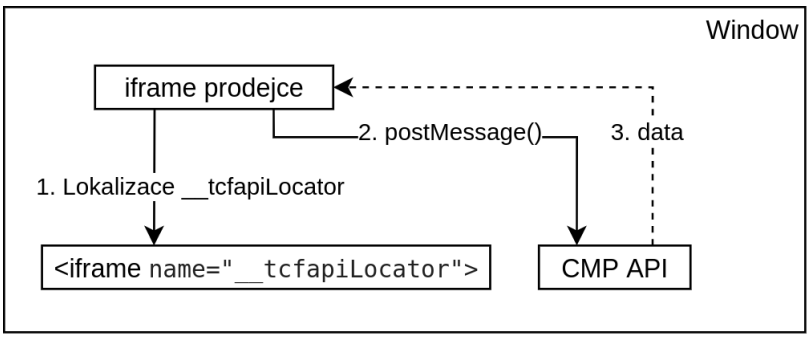
3. `addEventListener`, který slouží pro zaregistrování funkce uvedené v parametru callback jako posluchače (listener), tato funkce bude provedena vždy ve chvíli, kdy dojde ke změně řetězce TC String. Funkce bude spuštěna s objektem `TCData`, který obsahuje informace z aktuálního řetězce TC String a unikátní identifikátor (`listenerId`) přidělený zaregistrované funkci.

   - command: `'addEventListener'`
   - version: 2,
   - callback: `function(tcData: TCData, success: boolean)`

4. `removeEventListener` slouží k odstranění funkce zaregistrované pomocí předchozího příkazu.

   - command: `'removeEventListener'`
   - version: 2,
   - callback: `function(success: boolean)`
   - parameter: `listenerId`, unikátní identifikátor, který CMP přiřadilo pro callback registrovaný pomocí `addEventListener`.

Obsah prodejců je do stránky vkládán pomocí elementů `iframe`, a prodejci tak nemohou přímo přistupovat k CMP API v nadřazeném rámci. Jedinou možností je využití funkce `postMessage()`. Pro nalezení rámce obsahujícího CMP API je na stránku vždy umístěn element `iframe` s atributem `name="__tcfapiLocator"`. Rozhraní se pak nachází v rodičovském uzlu tohoto elementu [7]. Na obrázku 3.2 je ilustrováno nalezení rámce obsahujícího implementaci rozhraní CMP a následné zaslání požadavku s využitím funkce `postMessage()`.



Obrázek 3.2: Schéma lokalizace CMP API a zaslání požadavku pomocí `postMessage()`.

Kapitola 4

Rozšíření webového prohlížeče

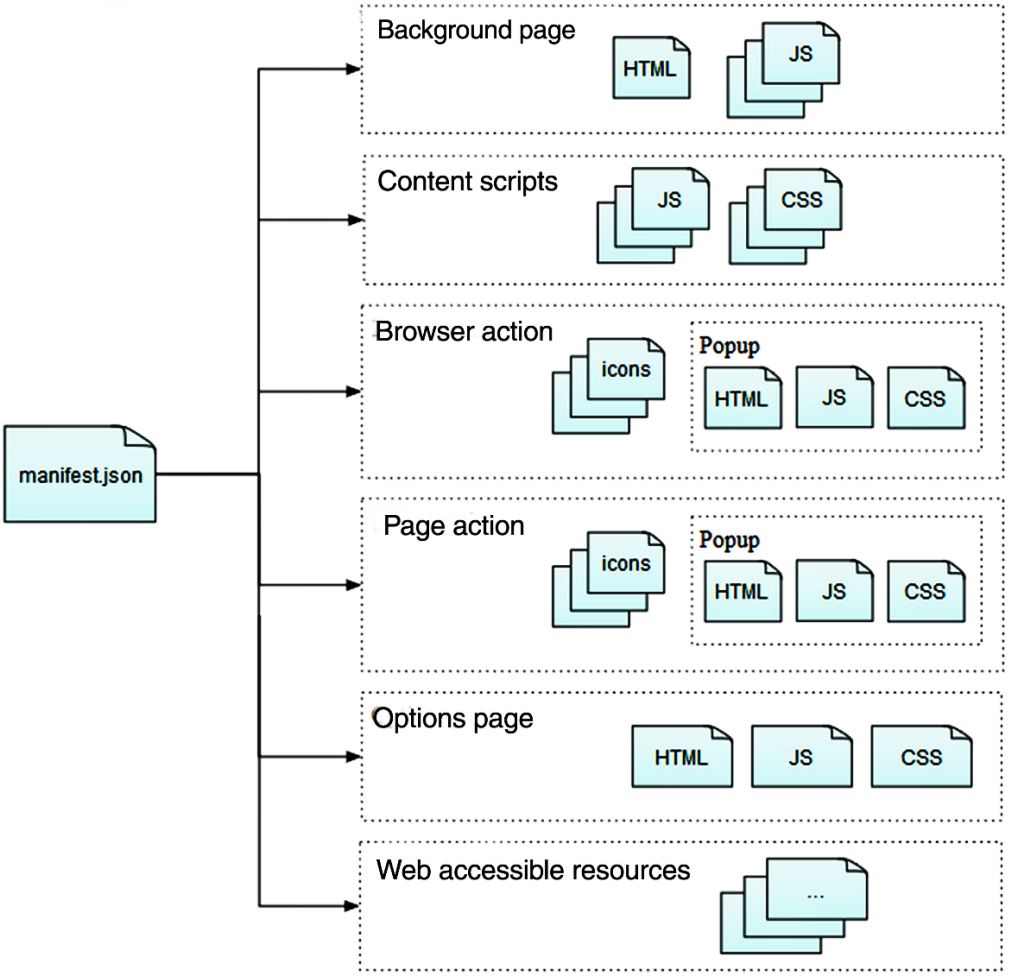
Rozšíření webových prohlížečů jsou využívány k úpravě nebo vylepšení možností webového prohlížeče. Pro tvorbu webových rozšíření jsou využívány standardní webové technologie *HTML*, *JavaScript*, *CSS* a některá *API jazyka JavaScript*. V současné době poskytují všechny rozšířené webové prohlížeče API pro usnadnění vývoje rozšíření pro tyto prohlížeče. Vhledem k tomu, že každý prohlížeč má vlastní API, bylo zpočátku komplikované vytvářet rozšíření kompatibilní napříč webovými prohlížeči. Postupem času však vzniklo API nazývané *WebExtensions* [3]. Účelem tohoto API bylo vytvoření jakéhosi standardu pro tvorbu webových rozšíření, aby tato rozšíření byla použitelná ve všech nejpoužívanějších webových prohlížečích. Mezi nejpopulárnější prohlížeče v současné době patří Microsoft Edge, Google Chrome, Opera a již zmíněná Mozilla Firefox. První tři zmíněné (Edge, Chrome a Opera) využívají jsou v současné době založeny na jádru Chromium. Firefox je pak postaven na vlastním jádru Gecko. I přes snahu vytvořit univerzální způsob tvorby rozšíření je zde stále několik problémů s kompatibilitou napříč webovými prohlížeči [3]:

- Jmenný prostor API – existují dva jmenné prostory pro přístup k funkcím API. Prohlížeče založené na jádru Chromium využívají jmenný prostor `chrome.*`, Firefox zase využívá jmenný prostor `browser.*`. Přestože Firefox podporuje i jmenný prostor `chrome.*`, je doporučeno využívat `browser.*`.
- Zpracování asynchronních událostí – prohlížeče s jádrem Chromium využívají *callback*. Firefox pro zpracování asynchronních událostí využívá objekt `Promise`, který je modernějším způsobem zpracovávání asynchronních událostí. Firefox rovněž umožňuje využít *callback* při použití jmenného prostoru `chrome.*`.
- Dostupnost funkcí API – dostupnost některých funkcí API se může lišit v závislosti na konkrétním prohlížeči. Dostupnost funkcí API v konkrétních prohlížečích je zdokumentována na webu MDN Web Docs [4].
- Atributy v souboru manifest.json – jednotlivé prohlížeče se liší v podpoře některých atributů v souboru manifest.json. Podpora jednotlivých atributů v prohlížečích je opět zdokumentována na webu MDN Web Docs [17].
- Vytvoření balíku – Firefox, Chrome a Opera využívají standardní archiv ve formátu zip, v jehož kořenovém adresáři musí být umístěn soubor manifest.json. U Microsoft Edge je však potřeba vytvořit ještě další balík pro umístění na Microsoft Store.
- Publikování rozšíření – každý prohlížeč má vlastní obchod s rozšířeními. Je tedy potřeba zveřejnit rozšíření pro každý prohlížeč zvlášť. Jednotlivé prohlížeče se také liší

způsobem schvalování a dobou potřebnou pro schválení rozšíření. Prohlížeče Firefox a Chrome poskytují nástroje pro usnadnění publikování rozšíření. U prohlížečů Chrome a Edge je dokonce vyžadován registrační poplatek pro možnost publikování rozšíření.

Rozdíly popsané v prvních dvou bodech je možné vyřešit použitím knihovny *WebExtension browser API Polyfill* [23]. Knihovna umožňuje použití jmenného prostoru `browser.*` a objektů `Promise` pro zpracování asynchronních událostí bez ohledu na cílový prohlížeč. V případě, kdy je rozšíření s touto knihovnou nainstalováno v prohlížeči Mozilla Firefox, není kód rozšíření nikterak upravován. Pokud je však rozšíření nainstalováno v prohlížeči Google Chrome (nebo jiném prohlížeči s jádrem Chromium), vytvoří knihovna obaly potřebné pro zajištění kompatibility s tímto prohlížečem.

4.1 Struktura rozšíření



Obrázek 4.1: Schéma struktury webového rozšíření. Převzato z [1].

Na obrázku 4.1 je ilustrováno schéma rozšíření webového prohlížeče. V dokumentaci společnosti Mozilla [1] jsou rozšíření pro webové prohlížeče popsány jako kolekce souborů zabalených pro distribuci a instalaci. V kořenovém adresáři musí být obsažen soubor *manifest.json*. Tento soubor ve formátu JSON je jakýmsi konfiguračním souborem rozšíření. Obsahuje údaje jako název, verze, požadovaná oprávnění nebo cesty k jednotlivým souborům rozšíření.

Další součástí webových rozšíření jsou *skripty pracující na pozadí* (*background scripts*). Tyto skripty jsou načteny při instalaci a běží nezávisle na webové stránce nebo okně prohlížeče. Tyto skripty mohou využívat libovolné součásti WebExtension API pro které mají udělené oprávnění, ale nemohou přistupovat k obsahu webových stránek. Typicky jsou využívány pro vykonávání dlouhodobých operací.

Webová rozšíření mohou také obsahovat takzvané *obsahové skripty* (*content scripts*). Tyto skripty jsou vloženy do webové stránky a využívají se k manipulaci s touto stránkou. Obsahové skripty mohou přistupovat a manipulovat s DOM webové stránky, ale nemohou přistupovat ke skriptům webových stránek. S těmito skripty však mohou komunikovat pomocí zpráv s využitím API `window.postMessage()`. Obsahové skripty mohou také komunikovat se skripty běžícími na pozadí (background scripts) pomocí *message-passing API*.

Součástí webových rozšíření mohou být také postranní panely, zobrazované na levé straně webové stránky, dále pak vyskakovací okna, která jsou zobrazována po kliknutí na tlačítko rozšíření v panelu nástrojů, a také stránky s nastavením pro přizpůsobení rozšíření.

4.2 Vícejazyčné rozšíření

V dokumentaci WebExtensions [12] je uvedeno, že pro vytvoření vícejazyčného rozšíření je potřeba do kořenového adresáře rozšíření umístit adresář s názvem *_locales*. V tomto adresáři pak budou umístěny podadresáře pro jednotlivé jazyky, které má rozšíření podporovat. Tyto podadresáře budou nazvány ISO kódy[1] zvolených jazyků a budou obsahovat soubor ve formátu JSON nazvaný *messages.json*. V těchto souborech budou umístěny překlady textů pro daný jazyk. Struktura vícejazyčného rozšíření pak bude vypadat následovně:

```
extension-root
├── _locales
│   ├── cs
│   │   └── messages.json
│   ├── en
│   │   └── messages.json
│   ├── de
│   │   └── messages.json
│   └── ...
├── manifest.json
├── background.js
└── ...
```

K překladům jednotlivých textů lze poté přistupovat v JS skriptech pomocí API funkce `i18n.getMessage(messageName, substitutions)`. Překlady lze využívat také v souboru manifest.json, kde se získávají pomocí řetězce `__MSG_<messageName>__`, tedy například `"name": "__MSG_extensionName__"`. V souboru manifest.json je možné také nastavit výchozí jazyk rozšíření pomocí atributu `default_locale`.

[1] https://cs.wikipedia.org/wiki/Seznam_k%C3%B3d%C5%AF_ISO_639-1

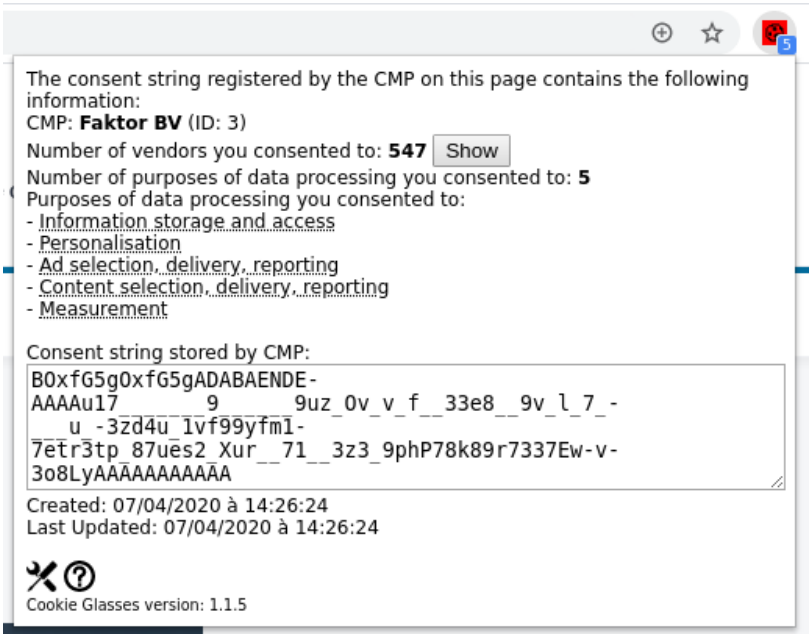
Kapitola 5

Existující řešení

Tato kapitola je věnována existujícím rozšířením, které se zabývají problematikou souhlasu se zpracováním osobních údajů. Popisované rozšíření jsou dostupné v oficiálních obchodech prohlížečů Mozilla Firefox[1] a Google Chrome[2].

5.1 Cookie Glasses

Rozšíření vzniklo jako součást již zmíněného průzkumu, který provedl Matte a kol. [34]. Rozšíření umožňuje zobrazování informací o poskytnutém souhlasu se zpracováním osobních údajů. Vyskakovací okno rozšíření je zobrazeno na obrázku 5.1. Rozšíření má podporu webových stránek využívajících TCF v1.1. Vzhledem k podpoře zastaralé verze TCF je dnes rozšíření již v podstatě nepoužitelné.



Obrázek 5.1: Vyskakovací okno rozšíření Cookie Glasses. Převzato z [33].

[1] https://addons.mozilla.org
[2] https://chrome.google.com/webstore/category/extensions

5.2 Global Consent Manager[3]

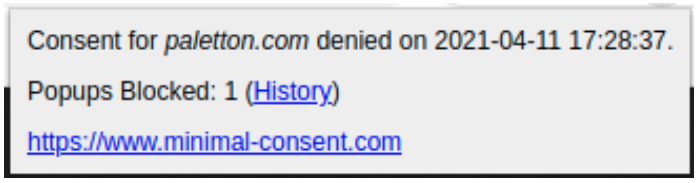
Toto rozšíření slouží k automatickému poskytování souhlasu se zpracováním osobních údajů. Rozšíření podporuje webové stránky využívající Transparency and Consent Framework. Dle data poslední aktualizace (20. 8. 2019) se však jedná opět o zastaralou verzi TCF, tedy verzi 1.1, a rozšíření je tak již nefunkční.

5.3 Minimal Consent[4]

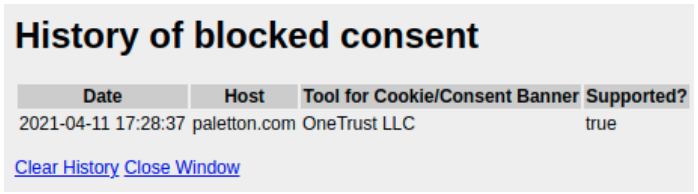
Cílem tohoto rozšíření je skrytí banneru požadujícího souhlas a poskytnutí minimálního souhlasu se zpracováním osobních údajů. Rozšíření na webových stránkách vyhledává bannery vyžadující souhlas se zpracováním osobních údajů a pomocí manipulace s DOM se snaží automaticky udělit souhlas.

Rozšíření neposkytuje žádné nastavení ani možnost zobrazení informací o poskytnutém souhlasu. Zobrazována je pouze informace o tom, zda byl na stránce banner zablokován (viz obrázek 5.2). Případně je možné ještě zobrazit historii všech stránek na nichž byly bannery zablokovány (viz obrázek 5.3).

Dle informací uvedených na webových stránkách rozšíření[5], již není toto rozšíření udržováno.



Obrázek 5.2: Vyskakovací okno rozšíření Minimal Consent.



Obrázek 5.3: Historie stránek, na kterých byl banner zablokován.

5.4 re:consent[6]

Dle popisu by rozšíření mělo zobrazovat účely zpracování, ke kterým uživatel udělil souhlas. Rozšíření by mělo také umožňovat uživateli změnit své rozhodnutí a automaticky uložit nový souhlas. Rozšíření je cíleno na webové stránky využívající TCF. Dále také na Facebook a Google. Na žádné z testovaných stránek však toto rozšíření nebylo funkční. Pravděpodobně je tedy opět podporována pouze zastaralá verze TCF v1.1.

[3] http://www.globalconsentmanager.com
[4] https://www.minimal-consent.com
[5] https://www.minimal-consent.com/
[6] https://cliqz.com/en/magazine/re-consent

5.5 I don't care about cookies[7]

Cílem tohoto rozšíření je blokovat nebo skrývat bannery vyžadující souhlas se zpracováním osobních údajů. Pokud je to nezbytné k odstranění banneru, rozšíření poskytne souhlas případně nesouhlas automaticky. Rozšíření však nepracuje s konkrétními účely zpracování. Cílem je tedy pouze odstranění banneru, a to jakýmkoliv způsobem.

5.6 Shrnutí

Průzkum existujících rozšíření, která se zabývají problematikou souhlasu se zpracováním osobních údajů, ukázal, že současně neexistuje žádné rozšíření s podporou aktuální verze TCF, a že žádné z existujících rozšíření neumožňuje uživateli nastavení udělení souhlasu, nebo nesouhlasu pro jednotlivé účely zpracování. Rozšíření využívající starší verzi TCF jsou již v současné době, vzhledem k ukončení podpory této verze, nefunkční. U ostatních rozšíření pak není možné zjistit, k čemu konkrétně byl souhlas se zpracováním osobních údajů udělen.

[7] https://www.i-dont-care-about-cookies.eu

Kapitola 6

Návrh rozšíření

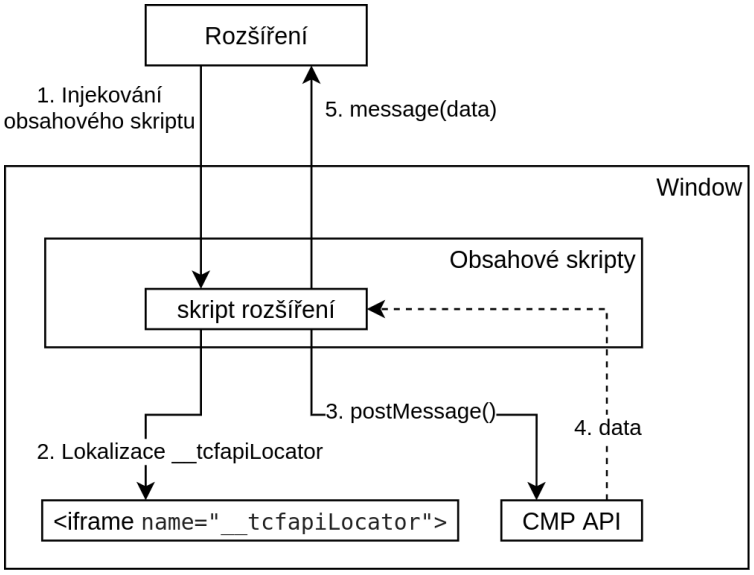
V současné době většina webových stránek shromažďuje a zpracovává osobní údaje uživatelů. Jak již bylo popsáno v kapitole 2, je k tomuto potřeba předchozí souhlas uživatele. Nastala tak situace, že při návštěvě téměř každé webové stránky je uživateli zobrazeno vyskakovací okno, banner apod. vyžadující poskytnutí souhlasu se zpracováním osobních údajů. Poskytování tak velkého množství souhlasů může být pro uživatele obtěžující. O to víc v situaci kdy si uživatel chce rozhodnout, ke kterým účelům a/nebo funkcím souhlas poskytne místo pouhého „odkliknutí“ souhlasu. Na některých webových stránkách může být navíc značně složité nalézt informace o již poskytnutém souhlasu, případně tento souhlas upravit.

Cílem této práce je vytvoření rozšíření pro webové prohlížeče, které bude umožňovat zobrazovaní informací z řetězce TC String uloženého aktuální webovou stránkou. Rozšíření má dále umožnit uživateli předem nastavit souhlas, nesouhlas a případně námitku proti zpracování osobních údajů pro jednotlivé účely zpracování. Rozšíření by pak na základě těchto preferencí mělo webovým stránkám automaticky poskytovat souhlas se zpracováním osobních údajů. Rozšíření by mělo být vícejazyčné.

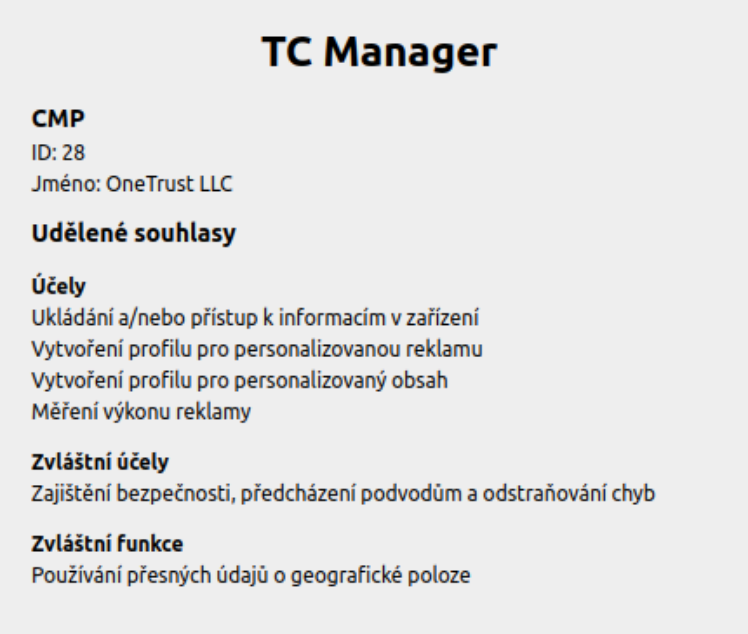
Základ rozšíření bude podporovat dva jazyky – češtinu a angličtinu. Pro popisy jednotlivých účelů zpracování budou využity již zmíněné oficiální překlady [15]. Tyto popisy budou poskytovány ve všech jazycích, pro které jsou překlady vytvořeny. Jazyk rozšíření bude volen při instalaci na základě jazyka systému, na který bude rozšíření instalováno. Pokud jazyk prohlížeče nebude odpovídat jednomu z podporovaných jazyků rozšíření, bude jazyk nastaven na angličtinu.

Na obrázku 6.1 je znázorněn postup získávání informací z TCF. Rozšíření vloží do webové stránky obsahový skript, který se, při požadavku na získání informací z CMP API, nejprve pokusí lokalizovat element `iframe` s atributem `name="__tcfapiLocator"`. Poté bude s využitím tohoto elementu lokalizován rámec obsahující CMP API, které by se mělo nacházet v rodičovském uzlu nalezeného elementu. Obsahový skript bude následně na CMP API zasílat své požadavky s využitím funkce `postMessage()` a získaná data bude posílat samotnému rozšíření, které je podle potřeby zpracuje.

Aktuální informace o uděleném souhlasu pro danou webovou stránku budou získávány pomocí požadavku `getTCData` a zobrazovány ve vyskakovacím okně rozšíření, jehož návrh je na obrázku 6.2.



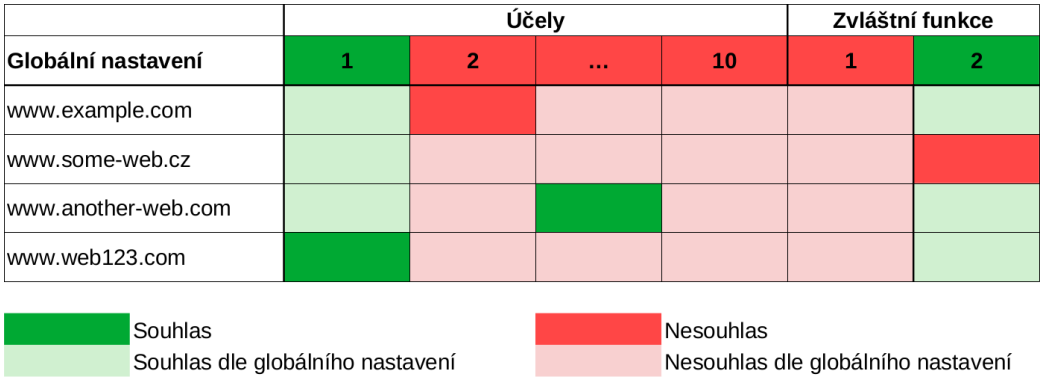
Obrázek 6.1: Ilustrace komunikace mezi rozšířením a CMP API.



Obrázek 6.2: Návrh vyskakovacího okna pro zobrazení informací uložených v TCF.

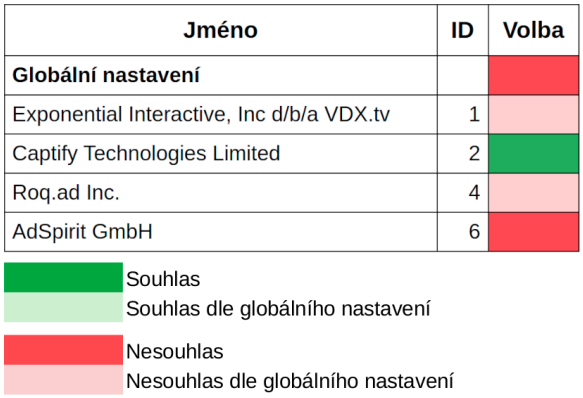
6.1 Nastavení preferencí

Nastavování preferencí pro udělování souhlasu, či nesouhlasu k jednotlivým účelům zpracování bude uživatel provádět na stránce nastavení rozšíření pomocí tabulky znázorněné na obrázku 6.3. Tabulka je inspirována nastavením v rozšíření uMatrix [31] a umožňuje uživateli vytvořit výchozí nastavení udělování souhlasů pro jednotlivé účely zpracování, ale také specifikovat své preference pro již navštívené webové stránky, u nichž byla detekována přítomnost TCF.



Obrázek 6.3: Návrh nastavení souhlasu s účely a zvláštními funkcemi zpracování osobních údajů.

Při poskytování souhlasu je potřeba také určit, kterým prodejcům má být souhlas udělen. Obrázek 6.4 ukazuje návrh nastavení souhlasu prodejcům. Jedná se o tabulku, která bude, stejně jako nastavení souhlasu s účely zpracování, obsahovat *globální (výchozí)* nastavení. Tabulka bude dále obsahovat seznam prodejců zaregistrovaných v TCF. Tento seznam bude získáván z *Globálního seznamu prodejců* zmíněného v kapitole 3.



Obrázek 6.4: Návrh nastavení souhlasu prodejcům.

Obě tyto tabulky budou fungovat na stejném principu. Položky *globálního nastavení* mohou nabývat hodnot *souhlas* a *nesouhlas*. Položky nastavení pro jednotlivé domény nebo prodejce pak mohou navíc nabývat hodnot *souhlas dle globálního nastavení*, nebo *nesouhlas dle globálního nastavení*, které říkají, že pro danou položku je hodnota děděna z příslušné položky globálního nastavení.

Veškerá nastavení budou ukládána v synchronizovaném úložišti prohlížeče. Toto úložiště má omezenou kapacitu, kdy je do obsazené kapacity počítán každý uložený znak. Nastavení tak bude potřeba ukládat co nejúsporněji. Nastavení účelů zpracování bude ukládáno například pod klíčem `p`, namísto celého názvu `purposes`. Jednotlivé hodnoty nastavení budou, místo například booleovských hodnot, reprezentovány pouze čísly. Na první pohled se může zdát, že se jedná o rozdíl pouhých několika znaků. Při rostoucím počtu záznamů s nastavením jednotlivých domén už ale bude docházet k výrazné úspoře využité kapacity úložiště.

6.2 Ukládání souhlasu

TCF ve verzi 2.0 nedefinuje způsob ukládání řetězce obsahujícího souhlas uživatele. A vzhledem k politikám TCF [11], které říkají, že tento řetězec by měl být vytvářen pouze CMP a nesmí být vytvářen žádnou třetí stranou, není definována ani žádná standardní funkce umožňující uložení vlastního řetězce nesoucího informace o souhlasu se zpracováním osobních údajů. Na straně uživatele (webového prohlížeče) však existují pouze tři možnosti uložení tohoto souhlasu, a to *cookies*, *lokální úložiště prohlížeče (Local Storage)* a *lokální databáze prohlížeče (Web SQL)*.

Na základě předběžného průzkumu webových stránek používajících TCF v2.0 bylo zjištěno, že webové stránky ukládají souhlas nejčastěji v podobě *cookie* s názvem *euconsent-v2*, *eupubconsent-v2*, nebo *cconsent-v2*. Objeveno bylo také ukládání do cookies s jiným názvem, ale i do lokálního úložiště webové stránky. Řetězec se souhlasem navíc může být pouze jednou částí strukturované hodnoty. Například CMP *Google LLC* ukládá řetězec se souhlasem do cookie s názvem *FCCDCF*, jehož hodnota je dvourozměrné pole, do kterého je souhlas ukládán na přesně danou pozici. Pokud je tedy souhlas ukládán jiným způsobem než do výše zmíněných cookies, není možné kontrolovat a případně nahrazovat celé hodnoty cookies a položek lokálního úložiště. Pro nalezení souhlasu i ve složené hodnotě, budou v hodnotách pomocí regulárního výrazu vyhledáváni kandidáti, kteří by potenciálně mohli být nositeli souhlasu. U těchto kandidátů pak bude pomocí dekódování řetězce zjišťováno, zda se skutečně jedná o řetězec uchovávající informace o souhlasu.

K lokálnímu úložišti webové stránky nemůže rozšíření standardně přistupovat. Toto omezení je však možné obejít vložením JavaScriptového kódu, přímo do stránky. Tento kód již k lokálnímu úložišti stránky přistoupit může, a umožní tak rozšíření v lokálním úložišti vyhledávat a nahrazovat souhlas se zpracováním osobních údajů.

Kapitola 7

Implementace a publikování

Jedním z cílů implementace bylo vytvoření rozšíření nezávislého na konkrétním webovém prohlížeči. Rozšíření využívá knihovnu *WebExtension browser API Polyfill*[1], která již byla popsána v kapitole 4. Rozšíření bylo implementováno primárně pro webové prohlížeče Mozilla Firefox a Google Chrome. Mělo by však být kompatibilní i s prohlížeči Microsoft Edge a Opera. Na těchto prohlížečích ale rozšíření nebylo testováno.

Pro dosažení nezávislosti na konkrétním webovém prohlížeči je důležité hlídat podporu použitých funkcí z WebExtensions API v jednotlivých prohlížečích. V implementovaném rozšíření jsou z WebExtensions API využity následující funkce [14]:

- `browser.runtime` – Poskytuje informace o rozšíření a prostředí, ve kterém běží.
  - `onInstalled.addListener()` – Zaregistruje funkci, která je poté volána vždy při instalaci rozšíření, aktualizaci rozšíření a aktualizaci prohlížeče.
  - `onMessage.addListener()` – Zaregistruje funkci, která je volána při přijetí zprávy z jiné části rozšíření.
  - `openOptionsPage()` – Otevře stránku s nastavením rozšíření.
  - `getURL()` – Převede relativní cestu od souboru `manifest.json` na cestu absolutní.
  - `getManifest()` – Získá údaje obsažené v manifestu rozšíření.
- `browser.tabs` – Slouží pro práci se záložkami prohlížeče.
  - `query()` – Získá všechny záložky, které odpovídají zadaným vlastnostem.
  - `sendMessage()` – Zašle zprávu obsahovému skriptu ve specifikované záložce.
- `browser.storage.sync` – Úložiště, jehož obsah je synchronizován se všemi instancemi prohlížeče, ve kterých je uživatel přihlášen.
  - `get()` – Získá jednu nebo více položek z úložiště.
  - `set()` – Uloží do úložiště jednu nebo více položek. Hodnoty existujících položek jsou aktualizovány.
- `browser.cookies` – Umožňuje správu cookies.
  - `getAll()` – Získá všechny cookies, které odpovídají zadaným parametrům.

[1] https://github.com/mozilla/webextension-polyfill

  - `set()` – Uloží cookie se zadanými daty. Pokud již cookie existuje, je přepsáno.

- `browser.webRequest` – Umožňuje práci s HTTP požadavky.
  - `onBeforeRequest.addListener()` – Zaregistruje funkci, která je spuštěna ve chvíli, kdy má být odeslán HTTP požadavek, ale hlavičky požadavku ještě nejsou dostupné.
  - `filterResponseData()` – Vytvoří objekt `StreamFilter`, pomocí kterého je poté možné monitorovat a upravovat odpovědi na HTTP požadavky.

- `browser.i18n` – Funkce umožňující pro internacionalizaci rozšíření.
  - `getMessage()` – Získá lokalizovaný řetězec pro zadanou zprávu.
  - `getUILanguage()` – Získá aktuální jazyk webového prohlížeče.

S výjimkou funkce `browser.webRequest.filterResponseData()`, jsou všechny tyto funkce podporovány všemi nejpopulárnějšími prohlížeči – Mozilla Firefox, Google Chrome, Microsoft Edge a Opera. Funkce `filterResponseData()` je podporována pouze v prohlížeči Mozilla Firefox. Je tedy potřeba kontrolovat její dostupnost tak, jako je znázorněno v kódu 7.1. Dle dostupné dokumentace je zde také problém s kompatibilitou synchronizovaného úložiště v prohlížeči Opera. Při ověřování na tomto prohlížeči však práce se synchronizovaným úložištěm nevykazovala žádné chyby. Prohlížeč Opera tak pravděpodobně interně převádí požadavky na přístup k synchronizovanému úložišti (`sync`) na požadavky na přístup k lokálnímu úložišti (`local`).

```
if (typeof browser.webRequest.filterResponseData === 'function') {
  // funkce je dostupna
}
```

Kód 7.1: Kontrola dostupnosti funkce `browser.webRequest.filterResponseData()`.

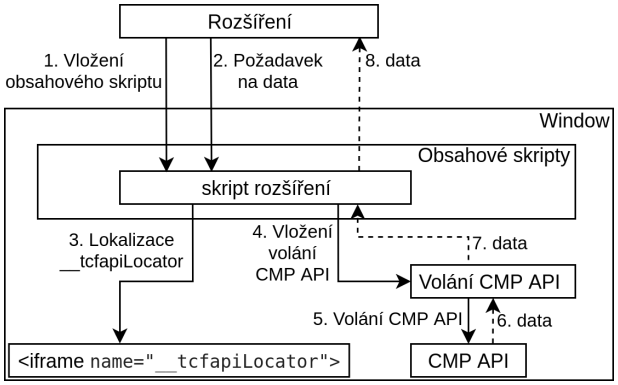
Funkce `browser.i18n.getMessage()` je v rozšíření používaná poměrně často. Za účelem zkrácení zápisu byl ve skriptu `common/common.js` pro tuto funkci vytvořen alias `const getMessage = browser.i18n.getMessage`. Lokalizované texty je tak možné získávat pouze zkráceným voláním `getMessage()`.

Všechny texty rozšíření jsou definovány ve více jazycích a je potřeba je zobrazovat dynamicky. HTML soubory tak definují pouze strukturu vyskakovacího okna a stránek s nastavením. Zobrazování lokalizovaných textů je implementováno především ve skriptech `popup/content_display.js` a `options/content_display.js`.

V průběhu implementace se ukázalo, že způsob komunikace s rozhraním CMP API popsaný v kapitole 6 není na některých stránkách zcela funkční. Způsob komunikace tak bylo potřeba upravit. Na obrázku 7.1 je znázorněn upravený způsob komunikace s rozhraním CMP API. Místo volání funkce `postMessage()` je volání CMP API vloženo přímo do stránky.

7.1 Struktura rozšíření

V kořenovém adresáři rozšíření se nachází adresář `src` a soubor `Makefile`. `Makefile` slouží k přípravě rozšíření pro instalaci do prohlížeče a k vytváření balíčků určených k publikování v obchodech s doplňky webových prohlížečů. V adresáři `src` jsou umístěny zdrojové kódy rozšíření, které jsou uspořádány do následující struktury:



Obrázek 7.1: Upravený způsob komunikace s CMP API.

- **`_locales`** – Adresář obsahující překlady textů ve struktuře definované v sekci 4.2.
- **`background_scripts`** – Adresář obsahující skripty běžící na pozadí.
- **`common`** – Adresář se skripty, v nichž jsou definovány konstanty a funkce používané v různých částech rozšíření. Nachází se zde také soubor **`fonts.css`** definující základní nastavení fontů.
- **`content_scripts`** – Adresář s obsahovými skripty.
- **`options`** – Adresář se soubory, které implementují nastavení rozšíření.
- **`popup`** – Adresář se soubory implementujícími vyskakovací okno rozšíření.
- **`resources`** – Adresář se seznamem CMP a prodejců TCF a s obrázky použitými v rozšíření.
- adresáře **`firefox`** a **`chrome`** – Obsahují manifesty kompatibilní s prohlížeči Mozilla Firefox a Google Chrome.
- **`package.json`** – Soubor definující závislosti rozšíření.
- ***`node_modules`*** – Adresář s nainstalovanými závislostmi. Je vytvořen až při instalaci těchto závislostí.

7.2 Makefile

Makefile slouží k nastavení rozšíření pro konkrétní prohlížeč, instalaci závislostí a případné vytvoření balíčku určeného k publikování v obchodech s doplňky webových prohlížečů. V souboru je definováno celkem sedm cílů:

- **`dependencies`** – Nainstaluje potřebné závislosti. Pro instalaci závislostí je potřeba, aby byl nainstalován správce balíčků **`npm`**[2].
- **`firefox`** – Provede cíl **`dependencies`** a zkopíruje soubor **`firefox/manifest.json`** do adresáře **`src`**.

[2] https://www.npmjs.com/

- `chrome` – Provede cíl `dependencies` a zkopíruje soubor `chrome/manifest.json` do adresáře `src`.
- `firefox-pack` – Provede cíl `firefox` a zabalí obsah adresáře `src` do archivu s názvem `tcmanager-firefox.zip`. V archivu nejsou obsaženy soubory `package.json` a `package-lock.json` a adresáře `firefox` a `chrome`.
- `chrome-pack` – Tento cíl je stejný jako cíl `firefox-pack`. Liší se pouze v názvu cílového archivu, který je v tomto cíli `tcmanager-chrome.zip`.
- `clean` – Odstraní z adresáře `src` soubor `manifest.json` a adresář `node_modules`, který obsahuje nainstalované závislosti.
- `all` – Provede v pořadí cíle `firefox-pack`, `chrome-pack` a `clean`.

7.3 Manifest

Soubor `manifest.json` je základním souborem rozšíření. Obsahuje základní informace o rozšíření jako je název, popis, verze rozšíření, jméno autora a ikony. Jsou zde definována také oprávnění potřebná pro správný běh rozšíření. Jedná se o oprávnění přístupu k úložišti, aktivní záložce, cookies a pro přístup k HTTP požadavkům.

V manifestu jsou dále definovány skripty běžící na pozadí, obsahové skripty, stránka s nastavením `options.html` a výchozí akce prohlížeče po kliknutí na ikonu rozšíření v panelu nástrojů prohlížeče. Touto akcí je zobrazení vyskakovacího okna `popup.html`.

Rozšíření je vícejazyčné, a proto byl v souboru `manifest.json` definován také výchozí jazyk. Ten byl pomocí klíče `default_locale` s hodnotou `en` nastaven na angličtinu. Výchozí jazyk je využíván v situaci, kdy pro aktuální jazyk není nalezen požadovaný překlad.

Manifest pro prohlížeč Mozilla Firefox (`firefox/manifest.json`) obsahuje navíc také identifikátor rozšíření, který je definován klíčem `browser_specific_settings`. Tento identifikátor je potřeba definovat pro možnost použití synchronizovaného úložiště `sync`.

7.4 Zobrazení informací o poskytnutém souhlasu

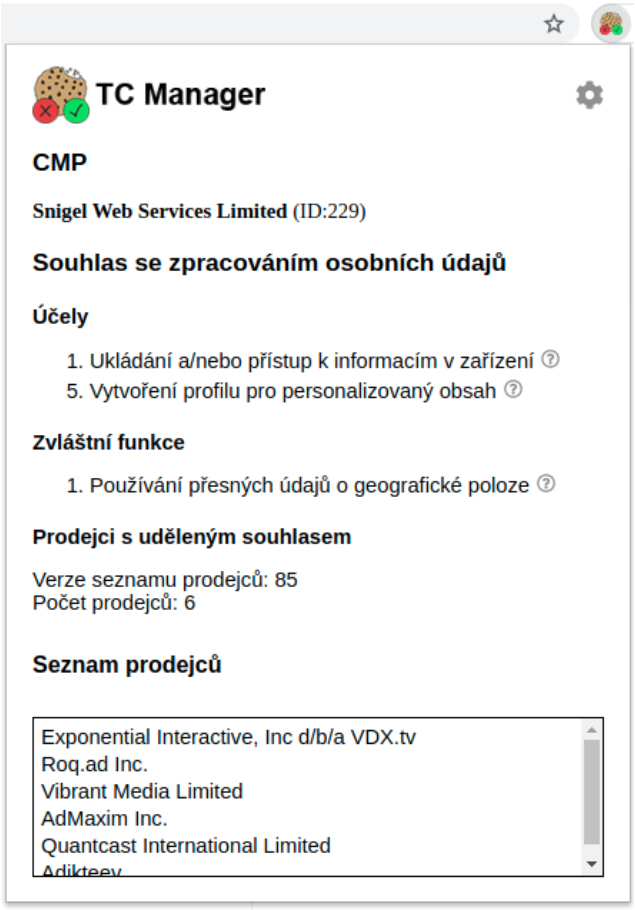
Informace o poskytnutém souhlasu aktuální webové stránce jsou zobrazovány ve vyskakovacím okně rozšíření, jehož výsledná podoba je na obrázku 7.2. Získání uložených informací zajišťuje skript `popup/popup.js`. Zobrazení těchto informací je poté provedeno skriptem `popup/content_display.js`.

Po otevření vyskakovacího okna je aktivní záložce zaslána zpráva s příkazem `'ping'` za účelem zjištění přítomnosti TCF a případně stavu načtení rozhraní CMP API.

```
function sendMessage (message, listener) {
  const query = browser.tabs.query({currentWindow: true, active: true});

  query.then(tabs => {
    browser.tabs.sendMessage(tabs[0].id, message)
    .then(listener, displayNoTCFMessage);
  });
}
```

Kód 7.2: Funkce pro zaslání zprávy aktivní záložce.



Obrázek 7.2: Vyskakovací okno rozšíření.

Zpráva je zachycena obsahovým skriptem `content_scripts/message_listener.js`. Tento skript získá požadované informace pomocí funkce `__tcfapi()`, která je implementována ve skriptu `content_scripts/__tcfapi.js`. Funkce se nejprve pokusí lokalizovat rámec s atributem `name="__tcfapiLocator"`. Pokud je tento rámec nalezen, je získán nadřazený element tohoto rámce. V opačném případě je pomocí `document.documentElement` získán element celého dokumentu. Do získaného elementu je následně pomocí funkce `inject()` vložen kód přistupující k rozhraní CMP API. Vložený kód předá získaná data obsahovému skriptu vyvoláním vlastní události (`CustomEvent`).

```
__tcfapi('getTCData', 2, (returnData, success) => {
  document.dispatchEvent(new CustomEvent('tcfapiEvent', {
    detail: {data: returnData, success: success}
  }));
});
```

Kód 7.3: Ukázka vloženého volání CMP API s vyvoláním události `CustomEvent`.

Obsahový skript informace následně zašle vyskakovacímu oknu. Pokud stránka TCF využívá, bude v odpovědi na zprávu obsažen, mimo jiné, atribut `cmpLoaded`. Je-li hodnota tohoto atributu `true`, znamená to, že rozhraní CMP API bylo plně načteno, a je tedy možné získat informace o uloženém souhlasu.

V případě, že stránka TCF využívá a skripty CMP API jsou načteny, zašle vyskakovací okno aktivní záložce další zprávu. Tentokrát s příkazem `'getTCData'` pro získání informací o uloženém souhlasu. Zpracování této zprávy probíhá stejným způsobem jako zpracování zprávy s příkazem `'ping'`. Získané informace jsou poté do vyskakovacího okna vykresleny skriptem `popup/content_display.js`. Zobrazeny jsou účely a zvláštní funkce zpravování, ke kterým byl souhlas udělen. Dále je zobrazen také seznam prodejců, jimž byl dle získaných informací souhlas se zpracováním osobních údajů poskytnut. Názvy účelů a funkcí jsou získávány pomocí funkce `getMessage()`. Jméno CMP je dle získaného ID vyhledáno v souboru `resources/cmp-list.json`.

7.5 Nastavení

Nastavení rozšíření obsahuje čtyři sekce. *Nastavení souhlasu s účely zpracování* je sekce určená k nastavování souhlasu či nesouhlasu s jednotlivými účely a zvláštními funkcemi zpracování. Sekce *popisy účelů* pak obsahuje názvy a popisy účelů a zvláštních funkcí zpracování osobních údajů. Třetí sekce *nastavení souhlasu prodejcům* slouží jako možnost nastavení udělování souhlasu jednotlivým prodejcům. Poslední sekce nazvaná *o rozšíření* obsahuje základní informace o rozšíření – aktuální verzi, informace o autorovi a informace o zdroji použitých ikon.

Sekce *popis účelů* a *o rozšíření* pouze zobrazují data, a tak nebudou více popisovány. Sekce *nastavení souhlasu s účely zpracování* a *nastavení souhlasu prodejcům* jsou detailněji popsány níže.

Nastavení souhlasu s účely zpracování

Logika stránky s nastavením souhlasu s účely zpracování je implementována ve skriptu `options/options.js`. Všechna nastavení jsou uložena v synchronizovaném úložišti ve formátu JSON. Pro vykreslení tabulky je potřeba nastavení nejprve načíst. Načtení z úložiště je provedeno pomocí funkce `browser.storage.sync.get()`. Po načtení je nejprve zobrazen řádek s globálním nastavením. Nastavení jednotlivých domén jsou poté postupně procházena v cyklu a vkládána do tabulky. Ukázka výsledné tabulky je na obrázku 7.3.

Použít globální nastavení | Odstranit nastavení domén | Obnovit výchozí nastavení

	Účely										Zvláštní funkce		Akce
Globální nastavení	1	2	3	4	5	6	7	8	9	10	1	2	
paletton.com	námitka	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	
www.seznam.cz	zděděno	zděděno	souhlas	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	
www.sitepoint.com	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	
www.tecmint.com	námitka	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	zděděno	
www.w3schools.com	zděděno	zděděno	zděděno	zděděno	námitka	zděděno	zděděno	zděděno	zděděno	zděděno	souhlas	zděděno	

Obrázek 7.3: Nastavení pro poskytování souhlasu k jednotlivým účelům zpracování osobních údajů.

Nastavení jednotlivých účelů a zvláštních funkcí je možné změnit kliknutím na příslušnou buňku v řádku *globální nastavení* nebo v řádku s nastavením pro konkrétní doménu. Po najetí myší na buňku s nastavením je zobrazen popisek s názvem účelu, nebo zvláštní funkce, ke kterému se nastavení buňky vztahuje. Ve sloupci *Akce* jsou umístěna dvě tlačítka.

Tlačítko s ikonou šipky obnoví nastavení domény v daném řádku. To znamená, že nastavení všech účelů a zvláštních funkcí budou dědit hodnoty z globálního nastavení. U globálního nastavení toto tlačítko nastaví pro všechny účely a funkce nesouhlas. Tlačítko s ikonou koše pak umožňuje odstranit z nastavení celý záznam o dané doméně. Nad tabulkou jsou navíc k dispozici ještě tři tlačítka:

- *Použít globální nastavení* – Obnoví nastavení pro všechny uložené domény.
- *Odstranit nastavení domén* – Odstraní záznamy o všech uložených doménách.
- *Obnovit výchozí nastavení* – Nastaví všechny položky globálního nastavení na nesouhlas a položky domén nastaví na dědění hodnoty globálního nastavení.

Ukládání nastavení je prováděno automaticky ihned po provedení libovolné změny. Kód 7.4 znázorňuje strukturu uloženého nastavení.

```
www.w3schools.com: {
  p: [2,2,2,2,0,2,2,2,2,2],
  sf: [1,2]
}
```

Kód 7.4: Ukázka nastavení souhlasu se zpracováním osobních údajů pro doménu www.w3schools.com. Klíč `p` obsahuje nastavení pro účely zpracování (purposes) a klíč `sf` obsahuje nastavení pro zvláštní funkce (special features). Hodnoty v poli určují nastavení pro jednotlivé účely a zvláštní funkce. Pozice hodnoty v poli určuje číslo účelu nebo zvláštní funkce. Hodnota `0` znamená nesouhlas, hodnota `1` souhlas a hodnota `2` říká, že pro daný účel nebo zvláštní funkci má být použita volba globálního nastavení. Nastavení se shoduje s obrázkem 7.3.

Nastavení souhlasu prodejcům

Princip fungování této části nastavení je velmi podobný nastavení souhlasu s účely zpracování. Logika je implementována v souboru `options/options_vendors.js`. Obrázek 7.4 ukazuje část vykreslené tabulky s nastavením. Hodnoty nastavení jsou opět ukládány v synchronizovaném úložišti. V TCF je aktuálně zaregistrováno přes 700 prodejců. Pro úsporu kapacity úložiště tak jsou volby ukládány pouze ve formátu `ID: Volba`. Jméno prodejce a odkaz na politiku jsou při načítání nastavení získávány ze seznamu prodejců umístěného v souboru `resources/vendor-list.json`.

Použít globální nastavení

Jméno	ID	Odkaz na politiku	Volba
Globální nastavení			**námitka**
Exponential Interactive, Inc d/b/a VDX.tv	1	Odkaz	zděděno
Captify Technologies Limited	2	Odkaz	souhlas
Roq.ad Inc.	4	Odkaz	zděděno
AdSpirit GmbH	6	Odkaz	námitka

Obrázek 7.4: Nastavení pro udělování souhlasu jednotlivým prodejcům.

7.6 Poskytování souhlasu

Poskytnutí souhlasu je akce, při které je aktuální webové stránce vnucen rozšířením souhlas vytvořený na základě nastavení uživatele. Proces poskytnutí souhlasu začíná v obsahovém skriptu `create_consent_request.js`, protože k vytvoření souhlasu je potřeba získat základní údaje o CMP použitém na navštívené webové stránce. Obsahový skript po načtení webové stránky zjišťuje, zda stránka využívá TCF. Zjišťování přítomnosti TCF probíhá v intervalu 500 ms po dobu až 15 s. Opakovaná kontrola přítomnosti TCF je nutná z toho důvodu, že po načtení webové stránky může ještě nějakou dobu trvat, než jsou skripty CMP API plně načteny a než začnou poskytovat požadované informace. Po zjištění základních údajů jsou načteny všechny položky lokálního úložiště stránky a jsou společně se získanými údaji a URL stránky zaslány skriptu `background/consent_string_creation.js`, běžícímu na pozadí. Pro tento skript jsou přijaté údaje zároveň signálem k vytvoření a uložení souhlasu.

Při vytváření souhlasu je nejprve pro danou doménu načteno nastavení. Na základě tohoto nastavení je následně funkcí `createTCModel()` vytvořen objekt obsahující všechny potřebné informace k vytvoření řetězce souhlasu. Informace z vytvořeného objektu jsou poté, dle specifikací TCF, převedeny na bitový vektor. Řetězec souhlasu je pak vytvořen zakódováním bitového vektoru funkcí `encode()`.

Vytvořený souhlas je ukládán do cookies, případně do některé z položek lokálního úložiště webové stránky. Nejprve jsou načteny již existující cookies a v jejich hodnotách jsou pomocí regulárního výrazu hledány potenciální řetězce souhlasu. S využitím knihovny *tc-string-parse*[3] je poté u každého nalezeného řetězce ověřováno, zda se skutečně jedná o řetězec nesoucí informace o souhlasu se zpracováním osobních údajů. Pokud je takový řetězec nalezen, je v cookie nahrazen vytvořeným řetězcem a upravené cookie je opět uloženo. V případě, že řetězec souhlasu v existujících cookies nalezen není, je souhlas uložen do nejčastějších cookies s názvy *euconsent-v2*, *eupubconsent-v2* a *cconsent-v2*, které byly v průběhu implementace identifikovány jako nejčastěji používané cookies pro uložení souhlasu se zpracováním osobních údajů. Po cookies jsou stejným způsobem prohledávány a případně upravovány položky lokálního úložiště stránky, které byly součástí požadavku na vytvoření souhlasu. Všechny položky, v nichž byl řetězec souhlasu nalezen a upraven, jsou poté zaslány zpět obsahovému skriptu `create_consent_request.js`, který tyto upravené položky uloží zpět do lokálního úložiště stránky.

Poskytování souhlasu je implementováno také pomocí zachytávání HTTP komunikace a úpravy HTTP odpovědí. Zachycovány jsou požadavky, jejichž URL odpovídá jednomu z definovaných vzorů. Zachycování veškeré HTTP komunikace by totiž bylo velmi neefektivní. Aktuálně jsou skriptem `background/web_request_listeners.js` zachytávány požadavky na subdomény domény *consensu.org*, požadavky na skript *zdconsent.js* a požadavky na URL v jejíž cestě se nachází řetězec *tcfv2*. Doména *consensu.org* je jako možnost ukládání souhlasu definovaná přímo v TCF. Skript *zdconsent.js* je používán webovými stránkami využívajícími CMP *Evidon, Inc.* Ve skriptu byly objeveny předdefinované hodnoty řetězců nesoucích informace o souhlasu. URL s řetězcem *tcfv2* je využíváno stránkami s CMP *Sourcepoint Technologies, Inc.*

Samotná úprava odpovědi pak probíhá podobným způsobem jako při vyhledávání a nahrazování souhlasu v existujících cookies a položkách lokálního úložiště. Po načtení celé HTTP odpovědi jsou v této pomocí regulárního výrazu nalezeny všechny řetězce, které jsou potenciálními nositeli souhlasu. Tyto řetězce jsou poté otestovány, zda se skutečně

[3] https://www.npmjs.com/package/tc-string-parse

jedná o zakódovaný souhlas. V případě, že se o souhlas jedná, je tento řetězec nahrazen řetězcem vytvořeným na základě uživatelského nastavení. Po zkontrolování a případném nahrazení všech nalezených řetězců je upravená odpověď zaslána webové stránce, která odeslala požadavek. Základní údaje o CMP, potřebné k vytvoření souhlasu, jsou v tomto případě získávány z řetězců souhlasu nalezených v zachycené HTTP odpovědi.

Úprava HTTP odpovědí je, vzhledem ke kompatibilitě použitých funkcí z WebExtensions API, aktivní pouze v prohlížeči Mozilla Firefox.

Některé stránky využívají pomocné cookie, jehož existence, nebo hodnota určuje, zda byl banner vyžadující souhlas uzavřen či nikoliv. Banner se tak zobrazuje i po obnovení stránky i přesto, že CMP API vrací správné informace. V takovém případě je nutné udělit souhlas manuálně pomocí banneru. Rozšíření vytváří, společně se souhlasem, také cookie *OptanonAlertBoxClosed*. Toto cookie zabraňuje na stránkách s CMP *OneTrust LLC* zobrazování banneru i po úspěšném vynucení vlastního souhlasu.

U stránek s CMP *Quantcast International Limited* docházelo k zobrazování banneru při každé změně souhlasu. Rozhraní CMP API však vracelo správné informace. Zobrazování banneru je tak na stránkách s tímto CMP zcela blokováno.

7.7 Generátor překladů

Rozšíření je vícejazyčné s podporou všech textů v češtině a angličtině a s podporou popisů účelů zpracování ve všech jazycích, pro které jsou dostupné překlady těchto účelů. Aktuálně je dostupných 32 překladů účelů zpracování[4]. Manuální udržování takového množství překladů by bylo náročné.

Pro snadné udržování překladů byl vytvořen jednoduchý skript v jazyce Python. Tento skript zpracovává překlady postupně pro jednotlivé definované jazyky. Nejprve stáhne překlady pro daný jazyk[5]. Po stažení jsou překlady transformovány do souboru JSON v požadovaném formátu pro rozšíření. Pro češtinu a angličtinu jsou navíc přidány další potřebné překlady, které jsou definovány ve zvláštním souboru `messages.json`. Ukázka struktury tohoto souboru je v kódu 7.5. Výstupem skriptu je adresář `_locales`, který obsahuje všechny vytvořené překlady ve struktuře popsané v sekci 4.2. Vytvořený adresář pak již stačí pouze zkopírovat do adresáře se zdrojovými kódy rozšíření.

```
{
  "extension_name": {
    "cs": "TC Manager",
    "en": "TC Manager"
  },
  ...
}
```

Kód 7.5: Ukázka souboru `messages.json` pro generátor překladů.

[4] https://register.consensu.org/Translation

[5] https://vendor-list.consensu.org/v2/purposes-{jazyk}.json, kde `{jazyk}` je ISO kód jazyka

Kapitola 8

Testování

Rozšíření bylo otestováno na 106 webových stránkách, které využívají TCF. Z těchto webových stránek jich bylo 71 získáno z části seznamu nejnavštěvovanějších stránek TRANCO[1]. Zbylých 35 stránek bylo získáno procházením webu v průběhu implementace a testování rozšíření.

Testováno bylo především vkládání souhlasu dle nastavení uživatele. Za úspěšné vložení souhlasu byl považován stav, kdy rozhraní CMP API vrátilo informace shodující se s vkládaným souhlasem (s nastavením uživatele). Při neúspěšném vložení souhlasu byl analyzován způsob uložení souhlasu dané webové stránky.

U většiny z testovaných stránek se nepodařilo vložit vlastní souhlas ihned při prvním načtení stránky a stránku bylo potřeba po jejím načtení ještě alespoň jednou obnovit. K tomu dochází z důvodu, že CMP API načítá informace o souhlasu pouze po načtení stránky. Upravený souhlas si tak rozhraní načte až po obnovení stránky. U stránek, které pro uložení souhlasu nevyužívají běžné cookies (euconsent-v2, eupubconsent-v2, cconsent-v2) je potřeba udělit souhlas manuálně pomocí banneru, aby bylo cookie se souhlasem vytvořeno a mohlo být poté přepsáno vlastním souhlasem. U těchto stránek je, ve většině případů, potřeba po manuálním udělení souhlasu ještě jednou až dvakrát stránku obnovit, aby CMP API reflektovalo vložený souhlas. Pro úspěšné vložení souhlasu bylo tedy potřeba provést jeden z následujících postupů:

(a) *Žádná akce* – Po načtení stránky není zobrazen banner a CMP API vrací informace shodující se s nastavením uživatele. Od uživatele není vyžadována žádná akce.

(b) *Obnovení stránky* – Při načtení stránky je zobrazen banner. Stránka používá pro uložení souhlasu jedno z nejčastějších cookies. Uživatel musí pouze obnovit stránku, aby došlo k načtení vnuceného souhlasu a tím i ke skrytí banneru.

U stránek s CMP Quantcast International Limited a některých stránek s CMP OneTrust LLC není banner zobrazen, protože se jej podařilo zablokovat. CMP API však při prvním načtení stránky vždy vrací informace o tom, že nebyl udělen souhlas s žádným účelem zpracování ani prodejcem, přestože v nastavení je k některým souhlas udělen. I v tomto případě je potřeba stránku obnovit, aby byl načten vnucený souhlas.

(c) *Ruční udělení souhlasu* – Po načtení stránky je zobrazen banner, ale CMP API vrací informace odpovídající nastavení uživatele. Uživateli stačí pouze jakýmkoliv způso-

[1] https://tranco-list.eu/

bem uzavřít banner. Vnucený souhlas zůstane načtený, a stránku tak již není třeba obnovovat.

(d) *Ruční udělení souhlasu a jedno až dvě obnovení stránky* – Při načtení stránky je zobrazen banner a k jeho skrytí nedojde ani po opakovaném obnovení stránky. V takovém případě stránka ukládá souhlas do cookie s neznámým názvem, do lokálního úložiště. U takové stránky je potřeba, aby uživatel udělil souhlas manuálně a jednou až dvakrát stránku obnovit, aby došlo k detekování místa s uloženým souhlasem, nahrazení tohoto souhlasu předdefinovaným souhlasem a následně k načtení vnuceného souhlasu.

Testování bylo prováděno manuálně. U každé testované stránky byly postupně aplikovány uvedené postupy, a průběžně byly kontrolovány informace poskytované rozhraním CMP API. Každá stránka byla otestována v prohlížeči Mozilla Firefox i Google Chrome.

Jak již bylo uvedeno v úvodu této kapitoly, rozšíření bylo testováno na 106 webových stránkách. V prohlížeči Mozilla Firefox se podařilo vložit souhlas na 102 (96,2 %) testovaných stránek. U prohlížeče Google Chrome to pak bylo 87 (82,1 %) stránek. Seznam testovaných stránek je uveden v příloze B.

Tabulka 8.1 zobrazuje zastoupení jednotlivých CMP v testovaných stránkách. Poslední sloupec tabulky ukazuje úspěšnost vložení vlastního souhlasu pro stránky které využívají dané CMP. Označení `f` a `ch` značí, že pro dané CMP se podařilo uložit vlastní souhlas pouze v prohlížeči Mozilla Firefox, respektive Google Chrome. Z tabulky lze vypozorovat, že nejčastěji používanými CMP jsou *OneTrust LLC*, *Quantcast International Limited* a *Sourcepoint Technologies, Inc.*

CMP	**Počet stránek**	**Úspěšně vložený souhlas**
OneTrust LLC	28	28
Quantcast International Limited	16	16
Sourcepoint Technologies, Inc.	13	f 13
LiveRamp	6	6
Google LLC	5	5
consentmanager.net	4	4
Didomi	4	3
1&1 Mail & Media GmbH	2	2
Conversant Europe Ltd.	2	2
Evidon, Inc.	2	f 2
Healthline Media, Inc.	2	2
iubenda	2	2
Seznam, a.s.	2	2
TrustArc Inc	2	2
Ostatní (po 1 stránce)	16	13
Celkem	106	f – 102, ch – 87

Tabulka 8.1: Zastoupení jednotlivých CMP v testovaných stránkách a úspěšnost vložení vlastního souhlasu. f – Pouze Mozilla Firefox. ch – pouze Google Chrome.

Stránky s CMP OneTrust LLC a Quantcast International Limited ukládaly souhlas do cookie *eupubconsent-v2*, nebo *euconsent-v2*. U těchto stránek tak stačilo na obou prohlížečích pouhé obnovení stránky k úspěšnému vložení souhlasu.

U stránek s CMP Sourcepoint Technologies, Inc. (a Evidon, Inc.) byl souhlas úspěšně vkládán pouze v případě prohlížeče Mozilla Firefox. Toto chování bylo očekávané, protože tyto CMP získávají řetězec souhlasu pomocí HTTP komunikace a HTTP odpovědi je možné upravovat pouze v prohlížeči Firefox. Souhlas byl u těchto stránek úspěšně vložen již po načtení stránky. U CMP Sourcepoint Technologies bylo potřeba pouze ručně udělit souhlas, což však nemělo vliv na informace, které vracelo rozhraní CMP API. Na stránkách s CMP Evidon, Inc. je rozšířením blokován i banner vyžadující souhlas, a tak po načtení stránky nebyla potřeba žádná další akce.

U webových stránek *howstuffworks.com* a *thefreedictionary.com* byl zobrazován banner pokaždé, kdy došlo ke změně souhlasu ze strany rozšíření a CMP API vracelo informace o tom, že souhlas nebyl udělen. Tyto stránky pravděpodobně ukládají souhlas na více míst a provádějí porovnání. Při nekonzistenci je pak zobrazen banner žádající o udělení souhlasu.

Na stránkách *giphy.com* a *aljazeera.com* je pravděpodobně TCF špatně nasazeno. V obou případech totiž CMP API nevracelo žádné informace o poskytnutém souhlasu ani po jeho manuálním udělení.

Zajímavé bylo také chování stránek *edition.cnn.com* a *thetradedesk.com*. Tyto stránky vraceli informace o souhlasu pouze s některými účely a prodejci i přesto, že byl nastaven souhlas se všemi účely zpracování a se všemi prodejci.

U CMP *Seznam, a.s.* bylo zjištěno, že CMP API načítá informace o souhlasu z cookie *euconsent-v2*. Ovšem pouze v případě, že v daném prohlížeči není uživatel přihlášen k Seznam účtu. Pokud je uživatel přihlášený, jsou informace o souhlasu získávány z tohoto účtu. Tyto informace jsou obsaženy v různých HTTP odpovědích. I přes úpravu obsahu těchto odpovědí v prohlížeči Firefox se v případě přihlášeného uživatele nepodařilo souhlas vynutit. Je možné, že je zde prováděna kontrola konzistence porovnáním řetězců souhlasu z různých zdrojů, a že všechny tyto zdroje nebyly objeveny.

Při testování byla dokonce objevena webová stránka, u které zjevně docházelo k porušení nařízení GDPR. Na stránce *ok.ru* byly již při jejím prvním načtení uloženy informace o souhlasu se všemi účely, zvláštními účely a s CMP API na stránce *ok.ru* vracelo informace o tom, že byl poskytnut souhlas se všemi účely a zvláštními funkcemi zpracování a s 554 prodejci.

U testovaných stránek nedošlo k zobrazení banneru ve 35 (33 %) případech v prohlížeči Mozilla Firefox. V prohlížeči Google Chrome nebyl banner zobrazen na 33 (31,1 %) webových stránkách. Započítány jsou zde i stránky, u kterých je banner blokován ihned po jejich načtení, a není tedy zobrazen i přesto, že CMP API ještě nemá načtený žádný souhlas se zpracováním osobních údajů.

8.1 Respektování volby uživatele

V případě úspěšného vložení souhlasu bylo potřeba také ověřit, zda webové stránky volbu uživatele respektují. Respektování volby uživatele bylo ověřováno na 15 webových stránkách, kterým se podařilo vnutit předdefinovaný souhlas. K testování bylo vybráno deset zahraničních a pět českých webových stránek. Kontrolovány byly řetězce souhlasu obsažené v HTTP požadavcích třetích stran a přítomnost obsahu prodejců na webové stránce. Řetězce souhlasu v HTTP požadavcích byly dekódovány pomocí online nástroje *@iabtcf*[2]. Dekódované údaje byly následně porovnávány s nastavením rozšíření, ve kterém byla všem účelům, zvláštním funkcím i prodejcům nastavena námitka proti zpracování.

[2] https://iabtcf.com/#/decode

Web	Souhlas v HTTP požadavcích	Obsah prodejců
9gag.com	shodný s nastavením	ano
arstechnica.com	shodný s nastavením	ano
de.softonic.com	shodný s nastavením	ano
edition.cnn.com	shodný s nastavením	ano
elpais.com	žádný požadavek obsahující souhlas	ne
eu.usatoday.com	shodný s nastavením	ano
genius.com	shodný s nastavením	ano
gizmodo.com	shodný s nastavením	ano
imgur.com	žádný požadavek obsahující souhlas	ne
ok.ru	žádný požadavek obsahující souhlas	ne
aktualne.cz	shodný s nastavením	ano
idnes.cz	shodný s nastavením	ano
blesk.cz	shodný s nastavením	ano
extra.cz	shodný s nastavením	ano
livesport.cz	shodný s nastavením	ano

Tabulka 8.2: Výsledky testování respektování souhlasu.

Tabulka 8.2 zobrazuje výsledky testování respektování volby uživatele. U třech testovaných webových stránek nebyly objeveny žádné požadavky třetích stran, které by obsahovaly řetězec souhlasu. Na těchto stránkách se nevyskytoval ani žádný obsah prodejců. U ostatních testovaných stránek byly v řetězci souhlasu, který byl předáván v HTTP požadavcích, obsaženy informace shodné s nastavením rozšíření. Stránky však obsahovaly obsah prodejců, přestože byla proti všem prodejcům vznesena námitka. U prodejců ale nebylo zjištěno vytváření cookies. Pravděpodobně tak žádné shromažďování osobních údajů neprováděli.

Z testování lze usoudit, že webové stránky volbu uživatele respektují. Pro více směrodatné výsledky by však bylo potřeba provést rozsáhlejší a hlavně automatizovaný průzkum. Relevantní by mohla být také analýza, zda volby uživatele respektují i samotní prodejci.

8.2 Shrnutí

Rozšíření bylo testováno celkem na 106 webových stránkách. Při testování v prohlížeči Mozilla Firefox se podařilo vnutit souhlas na 102 (96,2 %) testovaných webových stránek. V prohlížeči Google Chrome se pak jednalo o 87 (82,1 %) testovaných stránek. U některých webových stránek dokonce nedošlo ani ke zobrazení banneru. Konkrétně se jednalo o 35 (33 %) stránek při použití prohlížeče Mozilla Firefox a 33 (31,1 %) stránek při testování v prohlížeči Google Chrome. V ostatních případech byla k úspěšnému vnucení souhlasu potřeba interakce uživatele.

Na vybraném vzorku 15 webových stránek bylo testováno, zda tyto stránky vnucený souhlas respektují. U stránek byl kontrolován řetězec souhlasu, který byl zasílán prodejcům jako součást HTTP požadavků. Informace o souhlasu, uložené v tomto řetězci, se u všech stránek shodovaly s nastavením rozšíření. Webové stránky sice následně obsahovaly obsah prodejců, přestože proti nim byla vznesena námitka, tito prodejci však nevytvářeli cookies. Je tedy možné říci, že souhlas byl webovými stránkami i prodejci respektován.

Kapitola 9

Závěr

Cílem této práce bylo navrhnout a implementovat rozšíření pro webové prohlížeče, které bude umožňovat zobrazování a ukládání informací o souhlasu se zpracováním osobních údajů na webových stránkách využívajících rámec Transparency and Consent Framework (TCF).

Nejprve bylo potřeba se seznámit s nařízením GDPR, směrnicí ePrivacy a dalšími dokumenty zabývajícími se problematikou shromažďování a zpracování osobních údajů na internetu. Dále bylo potřeba se seznámit s principy cílení internetové reklamy a s podmínkami, jejichž splnění je nutné, aby mohl být souhlas se zpracováním osobních údajů považován za platný.

Před vytvořením návrhu a implementace bylo klíčové seznámení s TCF, rozhraním CMP API a řetězcem pro ukládání souhlasu, které tento rámec definuje. Dále bylo potřeba nastudovat možnosti tvorby rozšíření pro webové prohlížeče, a to s využitím WebExtensions API.

Na základě těchto informací bylo navrženo vícejazyčné rozšíření, které využívá oficiální překlady účelů zpracování osobních údajů. Byl navržen způsob získávání informací z TCF a jejich zobrazení uživateli. Navrženo bylo také grafické rozhraní pro nastavování uživatelských preferencí a možnosti ukládání vytvořených souhlasů. Na konci kapitoly zabývající se návrhem rozšíření byly navrženy způsoby ukládání souhlasu v podobě cookies a záznamů lokálního úložiště webové stránky.

Navržené rozšíření bylo následně implementováno. Oproti návrhu byl, za účelem větší spolehlivosti, upraven způsob komunikace s CMP API na vkládání kódu přímo do navštívené webové stránky. Poskytování souhlasu bylo, pro prohlížeč Mozilla Firefox, implementováno navíc ještě ve formě zachycování HTTP komunikace a přepisování řetězců souhlasu v HTTP odpovědích.

Pro usnadnění správy překladů byl vytvořen skript v jazyce Python, jehož výstupem je adresář `_locales`, který obsahuje všechny potřebně překlady, a tak jej stačí pouze zkopírovat do adresáře se zdrojovými kódy rozšíření.

Vytvořené rozšíření bylo pojmenováno *TC Manager* a bylo publikováno v obchodě s doplňky pro prohlížeč Mozilla Firefox[1]. Zdrojové kódy rozšíření[2] i generátoru překladů[3] jsou dostupné v repozitářích na serveru GitHub.

Rozšíření bylo otestováno na 106 webových stránkách využívajících TCF. Cílem testování bylo zjištění úspěšnosti poskytování souhlasu dle uživatelského nastavení. V prohlížeči

[1] https://addons.mozilla.org/cs/firefox/addon/tc-manager
[2] https://github.com/Alespost/TCManager
[3] https://github.com/Alespost/tc-manager-locales-generator

Mozilla Firefox se souhlas podařilo vložit na 102 (96,2 %) testovaných stránek. V prohlížeči Google Chrome byl souhlas úspěšně vložen na 87 (82,1 %) stránek. Nejčastěji používaným CMP bylo OneTrust LLC. U většiny testovaných stránek byla pro uložení souhlasu potřeba alespoň jedna akce uživatele, například obnovení stránky. Na některých testovaných stránkách bylo pozorováno zajímavé chování, jako třeba synchronizace souhlasu s účtem přihlášeného uživatele, zobrazování pouze některých účelů zpracování, či chybná implementace nebo nasazení CMP API.

Další vývoj této práce by mohl být zaměřen na zvýšení úspěšnosti poskytování souhlasu dle nastavení uživatele. Za účelem snížení počtu zobrazovaných bannerů a snížení potřeby interakce uživatele, by mohla být implementována detekce banneru a jeho automatické odsouhlasení s následným obnovením stránky. Zde by však bylo potřeba hlídat vliv na dobu načítání webové stránky. V rámci dalšího vývoje by mohla být také zlepšena uživatelská přívětivost nastavení s účely zpracování, protože zobrazování pouze čísel účelů a zvláštních funkcí pro uživatele příliš přívětivé není.

Literatura

[1] *Anatomy of an extension* [online]. MDN contributors [cit. 2020-12-19]. Dostupné z: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Anatomy_of_a_WebExtension.

[2] *Authorized Buyers: Real-time Bidding* [online]. Google [cit. 2020-11-24]. Dostupné z: https://developers.google.com/authorized-buyers/rtb/.

[3] *Browser Extensions* [online]. MDN contributors [cit. 2020-12-19]. Dostupné z: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions.

[4] *Browser support for JavaScript APIs* [online]. MDN contributors [cit. 2020-12-19]. Dostupné z: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Browser_support_for_JavaScript_APIs.

[5] *Co je to zpracování údajů?* [online]. Evropská komise [cit. 2020-10-22]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_cs.

[6] *Co jsou to osobní údaje?* [online]. Evropská komise [cit. 2020-10-22]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_cs.

[7] *Consent Management Platform API* [online]. IAB Europe [cit. 2020-11-30]. Dostupné z: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20CMP%20API%20v2.md.

[8] *Data Protection Glossary: E-privacy Directive 2009/136/EC* [online]. EUROPEAN DATA PROTECTION SUPERVISOR [cit. 2020-11-14]. Dostupné z: https://edps.europa.eu/node/3100#e-privacy_directive2009-136-ec.

[9] *Global CMP List* [online]. IAB Europe [cit. 2020-11-30]. Dostupné z: https://cmplist.consensu.org/v2/cmp-list.json.

[10] *Global Vendor List* [online]. IAB Europe [cit. 2020-11-30]. Dostupné z: https://vendorlist.consensu.org/v2/vendor-list.json.

[11] *IAB Europe Transparency & Consent Framework Policies* [online]. IAB Europe [cit. 2020-10-12]. Dostupné z: https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/.

[12] *Internationalization* [online]. MDN contributors [cit. 2020-12-19]. Dostupné z: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Internationalization.

[13] *Jaké osobní údaje jsou považovány za citlivé?* [online]. Evropská komise [cit. 2020-11-04]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_cs.

[14] *JavaScript APIs* [online]. MDN contributors [cit. 2020-12-19]. Dostupné z: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Browser_support_for_JavaScript_APIs.

[15] *List of translations for purpose descriptions v2.0* [online]. IAB Europe [cit. 2020-11-30]. Dostupné z: https://register.consensu.org/Translation.

[16] *Lze shromažďovat osobní údaje dětí?* [online]. Evropská komise [cit. 2020-11-06]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_cs.

[17] *Manifest.json* [online]. MDN contributors [cit. 2021-04-19]. Dostupné z: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/API.

[18] *Na co se obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation neboli GDPR) vztahuje?* [online]. Evropská komise [cit. 2020-10-22]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_cs.

[19] *OPENRTB (REAL-TIME BIDDING)* [online]. IAB Technology Laboratory [cit. 2020-11-24]. Dostupné z: https://iabtechlab.com/standards/openrtb/.

[20] *Slovník právních pojmů: Jurisdikce* [online]. Advokátní kancelář JUDr. Prokop Beneš [cit. 2020-11-30]. Dostupné z: https://www.bcak.cz/slovnik-pravnich-pojmu/jurisdikce/.

[21] *TCF – Transparency & Consent Framework* [online]. IAB Europe [cit. 2020-10-10]. Dostupné z: https://iabeurope.eu/transparency-consent-framework/.

[22] *Transparency and Consent String with Global Vendor & CMP List Formats* [online]. IAB Europe [cit. 2020-11-30]. Dostupné z: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md.

[23] *WebExtension browser API Polyfill* [online]. Mozilla [cit. 2021-04-21]. Dostupné z: https://github.com/mozilla/webextension-polyfill/.

[24] *Směrnice Evropského parlamentu a Rady 2002/58/ES* [online]. Evropský parlament a rada, 25. listopadu 2009 [cit. 2020-12-19]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:02002L0058-20091219&from=CS.

[25] *Opinion 2/2010 on online behavioural advertising* [online]. WP29 – Article 29 Data Protection Working Party, 22. června 2010 [cit. 2020-11-18]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf.

[26] *Nařízení Evropského parlamentu a Rady (EU) 2016/679* [online]. Evropský parlament, 27. dubna 2016 [cit. 2020-12-15]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=CS.

[27] *Guidelines on consent under Regulation 2016/679* [online]. WP29 – Article 29 Working Party, 28. listopadu 2017. 2018-04-10 [cit. 2020-11-25]. Dostupné z: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030.

[28] *Guidelines on Transparency under Regulation 2016/679* [online]. WP29 – Article 29 Working Party, 29. listopadu 2017. 2018-04-11 [cit. 2020-11-25]. Dostupné z: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025.

[29] *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities* [online]. European Data Protection Board, 12. března 2019 [cit. 2020-11-12]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.

[30] *Update report into adtech and real time bidding* [online]. Information Commissioner's Office, 20. června 2019 [cit. 2020-11-18]. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf.

[31] Hill, R. *UMatrix* [online]. [cit. 2020-12-02]. Dostupné z: https://github.com/gorhill/uMatrix.

[32] Koch, R. *Cookies, the GDPR, and the ePrivacy Directive* [online]. GDPR EU [cit. 2020-11-12]. Dostupné z: https://gdpr.eu/cookies/.

[33] Matte, C. *Cookie Glasses* [online]. GitHub [cit. 2021-04-11]. Dostupné z: https://github.com/Perdu/Cookie-Glasses.

[34] Matte, C., Bielova, N. a Santos, C. *Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework* [online]. arXiv.org, 2020 [cit. 2020-10-10]. Dostupné z: https://arxiv.org/abs/1911.09964.

[35] Polčák, L. Soukromí uživatelů v prostředí internetové reklamy na českém webu. *DSM Data Security Management* [online]. 2020, č. 1, s. 11–16, [cit. 2020-11-18]. ISSN 1211-8737. Dostupné z: https://tate.cz/dsm-zdarma.

[36] Wolford, B. *What is GDPR, the EU's new data protection law?* [online]. GDPR EU [cit. 2020-10-22]. Dostupné z: https://gdpr.eu/what-is-gdpr/.

[37] Škorničková, E. *GDPR | Obecné nařízení o ochraně osobních údajů – prakticky* [online]. [cit. 2020-10-22]. Dostupné z: https://www.gdpr.cz.

Příloha A

Účely a funkce zpracování osobních údajů

Tato příloha obsahuje seznamy účelů, speciálních účelů, funkcí a speciálních funkcí zpracování osobních údajů včetně uživatelsky přívětivých popisů. Informace uvedené v této příloze byly převzaty z [15].

Účely (Purposes)

1. Ukládání a/nebo přístup k informacím v zařízení.
   - *Popis:* Ve vašem zařízení se mohou ukládat soubory cookie, identifikátory zařízení nebo další informace nebo k nim ve vašem zařízení může být umožněn přístup pro účely, které vám byly sděleny.
2. Základní nastavení reklamy.
   - *Popis:* Reklamy se mohou zobrazovat na základě obsahu, který prohlížíte, aplikace, kterou používáte, vaší přibližné polohy nebo typu vašeho zařízení.
3. Vytvoření profilu pro personalizovanou reklamu.
   - *Popis:* Na základě vašeho chování na internetu může být vytvořen váš profil, aby vám mohla být zobrazena relevantní reklama.
4. Výběr personalizované reklamy.
   - *Popis:* Na základě vašeho profilu se vám může zobrazovat personalizovaná reklama.
5. Vytvoření profilu pro personalizovaný obsah.
   - *Popis:* Na základě vašeho chování na internetu může být vytvořen váš profil, a to proto, aby vám mohl být zobrazován obsah, který je pro vás relevantní.
6. Výběr personalizovaného obsahu.
   - *Popis:* Na základě vašeho profilu se vám může zobrazovat personalizovaný obsah.
7. Měření výkonu reklamy.

   - *Popis:* Výkon a účinnost reklamy, kterou vidíte nebo na kterou reagujete, mohou být měřeny.

8. Měření výkonu obsahu.
   - *Popis:* Účinnost a výkon obsahu, který vidíte nebo na který reagujete, mohou být měřeny.

9. Používání výzkumu trhu pro získání poznatků o uživatelích.
   - *Popis:* Výzkum trhu lze využít k získání více informací o uživatelích, kteří navštěvují stránky/aplikace a jimž jsou zobrazeny reklamy.

10. Vývoj a zlepšování produktů.
    - *Popis:* Vaše údaje lze využít ke zlepšení stávajících systémů a softwaru a k vývoji nových produktů.

Zvláštní účely (Special Purposes)

1. Zajištění bezpečnosti, předcházení podvodům a odstraňování chyb.
   - *Popis:* Vaše údaje lze použít k monitorování podvodných aktivit a k jejich prevenci a k zajištění řádného a bezpečného fungování systémů a postupů.

2. Technické doručení (zobrazení) reklamy nebo obsahu.
   - *Popis:* Vaše zařízení může přijímat a odesílat informace, které vám umožní zhlédnout reklamu a obsah a reagovat na ně.

Funkce (Features)

1. Párování a kombinování zdrojů offline dat.
   - *Popis:* Data z offline zdrojů lze kombinovat s vaší online aktivitou za účelem podpory jednoho nebo více účelů.

2. Propojení různých zařízení.
   - *Popis:* Abychom mohli lépe naplnit jeden či více účelů, můžeme určit, že vám nebo vaší domácnosti patří různá zařízení.

3. Přijetí a použití automaticky zasílaných specifických vlastností zařízení pro identifikaci.
   - *Popis:* Vaše zařízení může být odlišeno od jiných zařízení na základě informací, které vaše zařízení automaticky zasílá, jako např. IP adresa nebo typ prohlížeče.

Zvláštní funkce (Special Features)

1. Používání přesných údajů o geografické poloze.
   - *Popis:* Přesné údaje o vaší geografické poloze lze použít za účelem podpory jednoho nebo více účelů. Znamená to, že vaši polohu lze určit s přesností na několik metrů.
2. Aktivní vyhledávání identifikačních údajů v rámci vlastností zařízení.
   - *Popis:* Vaše zařízení lze identifikovat na základě prohledání jedinečné kombinace vlastností vašeho zařízení.

Příloha B

Seznam testovaných webových stránek

Tabulka B.1 obsahuje seznam webových stránek, na kterých bylo rozšíření testováno. Sloupec *úspěch* obsahuje informace o tom, zda se dané webové stránce podařilo vnutit vlastní souhlas. Písmeno *f* označuje úspěšné vynucení souhlasu v prohlížeči Mozilla Firefox. Písmeno *ch* označuje úspěšné vynucení souhlasu v prohlížeči Google Chrome. Znak – (pomlčka) znamená, že dané webové stránce se nepodařilo vnutit souhlas ani v jednom z těchto dvou prohlížečů. Ve sloupci *postup* je vždy uveden jeden z postupů, jehož provedení je nezbytné k úspěšnému vnucení souhlasu na dané webové stránce. Označení postupů je shodné se značením postupů popsaných v kapitole 8:

(a) *Žádná akce*

(b) *Obnovení stránky*

(c) *Ruční udělení souhlasu*

(d) *Ruční udělení souhlasu a jedno až dvě obnovení stránky*

Webová stránka	**CMP**	**Postup**	**Úspěch**
9gag.com	Quantcast International Limited	b	f, ch
arstechnica.com	OneTrust LLC	b	f, ch
de.softonic.com	Didomi	d	f, ch
edition.cnn.com	OneTrust LLC	b	f, ch
elpais.com	Didomi	b	f, ch
eu.usatoday.com	OneTrust LLC	b	f, ch
genius.com	OneTrust LLC	b	f, ch
giphy.com	Didomi	–	–
gizmodo.com	Sourcepoint Technologies, Inc.	c	f
global.techradar.com	Quantcast International Limited	b	f, ch
imgur.com	Quantcast International Limited	b	f, ch
it.altervista.org	iubenda	d	f, ch
lifehacker.com	Sourcepoint Technologies, Inc.	c	f
mashable.com	Evidon, Inc.	a	f
ok.ru	consentmanager.net	d	f, ch

slashdot.org	consentmanager.net	d	f, ch
slate.com	OneTrust LLC	b	f, ch
time.com	OneTrust LLC	b	f, ch
variety.com	OneTrust LLC	b	f, ch
venturebeat.com	LiveRamp	b	f, ch
web.de	1&1 Mail & Media GmbH	b	f, ch
accuweather.com	Google LLC	d	f, ch
aljazeera.com	Ensighten, Inc	–	–
bloomberg.com	Sourcepoint Technologies, Inc.	c	f
businessinsider.de	Sourcepoint Technologies, Inc.	c	f
buzzfeed.com	Quantcast International Limited	b	f, ch
dailymail.co.uk	Associated Newspapers Ltd	d	f, ch
dailymotion.com	DAILYMOTION SA	d	f, ch
digitaltrends.com	Cookiebot	d	f, ch
entrepreneur.com	Google LLC	d	f, ch
express.co.uk	Quantcast International Limited	b	f, ch
fandom.com	Wikia, Inc.	c	f, ch
fastcompany.com	Conversant Europe Ltd.	d	f, ch
forbes.com	TrustArc Inc	c	f, ch
gmx.net	1&1 Mail & Media GmbH	b	f, ch
healthline.com	Healthline Media, Inc.	d	f, ch
hollywoodreporter.com	OneTrust LLC	b	f, ch
howstuffworks.com	System1 LLC	–	–
in.gr	Quantcast International Limited	b	f, ch
inc.com	Conversant Europe Ltd.	d	f, ch
investing.com	OneTrust LLC	b	f, ch
investopedia.com	OneTrust LLC	b	f, ch
ladbible.com	Sourcepoint Technologies, Inc.	c	f
lemonde.fr	iubenda	d	f, ch
livescience.com	Quantcast International Limited	b	f, ch
marca.com	Didomi	d	f, ch
marketwatch.com	Sourcepoint Technologies, Inc.	c	f, ch
mediamath.com	LiveRamp	b	f, ch
medicalnewstoday.com	Healthline Media, Inc.	d	f, ch
merriam-webster.com	OneTrust LLC	b	f, ch
mirror.co.uk	Quantcast International Limited	b	f, ch
msn.com	OneTrust LLC	b	f, ch
newscientist.com	CIVIC COMPUTING LTD	d	f, ch
newsweek.com	LiveRamp	b	f, ch
newyorker.com	OneTrust LLC	b	f, ch
proiezionidiborsa.it	Google LLC	d	f, ch
researchgate.net	Quantcast International Limited	b	f, ch
sciencedaily.com	Quantcast International Limited	b	f, ch
sky.com	Sourcepoint Technologies, Inc.	c	f
speedtest.net	Evidon, Inc.	a	f

spiegel.de	Sourcepoint Technologies, Inc.	c	f
techtarget.com	Sourcepoint Technologies, Inc.	c	f
telegraph.co.uk	Sourcepoint Technologies, Inc.	c	f
theatlantic.com	Quantcast International Limited	b	f, ch
thefreedictionary.com	Farlex Inc	–	–
thesaurus.com	OneTrust LLC	b	f, ch
thesun.co.uk	Sourcepoint Technologies, Inc.	c	f
thetimes.co.uk	Sourcepoint Technologies, Inc.	c	f
vice.com	Sourcepoint Technologies, Inc.	c	f
w3schools.com	Snigel Web Services Limited	b	f, ch
webmd.com	TrustArc Inc	b	f, ch
seznam.cz	Seznam.cz, a.s.	a	f, ch
paletton.com	OneTrust LLC	b	f, ch
sourceforge.net	consentmanager.net	d	f, ch
pcgamesn.com	consentmanager.net	d	f, ch
aktualne.cz	OneTrust LLC	b	f, ch
cpex.cz	OneTrust LLC	b	f, ch
idnes.cz	OneTrust LLC	b	f, ch
blesk.cz	OneTrust LLC	b	f, ch
extra.cz	OneTrust LLC	b	f, ch
livesport.cz	OneTrust LLC	b	f, ch
novinky.cz	Seznam.cz, a.s.	d	f, ch
sitepoint.com	Quantcast International Limited	b	f, ch
tecmint.com	Quantcast International Limited	b	f, ch
bab.la	OneTrust LLC	b	f, ch
vdx.tv	OneTrust LLC	b	f, ch
quantcast.com	Quantcast International Limited	b	f, ch
thetradedesk.com	OneTrust LLC	b	f, ch
venatus.com	Quantcast International Limited	b	f, ch
site.adform.com	OneTrust LLC	b	f, ch
adara.com	LiveRamp	b	f, ch
rakutenadvertising.com	LiveRamp	b	f, ch
justpremium.com	Quantcast International Limited	b	f, ch
liveramp.fr	LiveRamp	b	f, ch
richaudience.com	Rich Audience International SL	b	f, ch
uniconsent.com	Transfon Ltd	b	f, ch
karaoketexty.cz	Google LLC	b	f, ch
womanonly.cz	Complianz BV	d	f, ch
refresher.cz	OneTrust LLC	b	f, ch
tutorialspoint.com	Google LLC	d	f, ch
sfbx.io	AppConsent by SFBX®	d	f, ch
mapy.in-pocasi.cz	OneTrust LLC	b	f, ch
sibboventures.com	SIBBO VENTURES SLU	d	f, ch
onetag.com	OneTag Ltd	d	f, ch
ogury.com	Ogury Ltd	d	f, ch

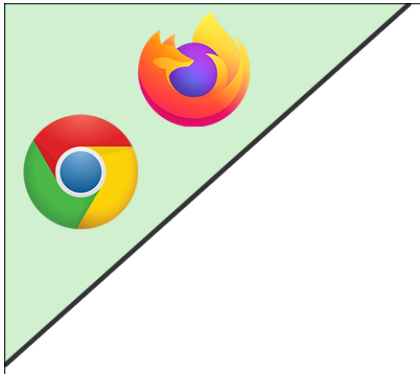
wellandgood.com	OneTrust LLC	b	f, ch

Tabulka B.1: Seznam testovaných stránek s informacemi o úspěchu vložení vlastního souhlasu.

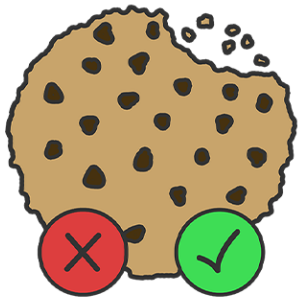
Příloha C

Shrnující slajd na konferenci Excel@FIT

Shrnující slajd je umístěn na další straně.



Autor: Aleš Postulka, vedoucí práce: Ing. Libor Polčák, Ph.D.



Zobrazení a úprava informací v Transparency and Consent Framework

- Rozšíření pro webové prohlížeče
- Správa souhlasů se zpracovaním osobních údajů

Příloha D

Obsah přiloženého paměťového média

- `/text/pdf` – Technická zpráva ve formátu PDF.
- `/text/latex` – Zdrojové kódy technické zprávy.
- `/TCManager` – Zdrojové kódy rozšíření.
- `/locales-generator` – Zdrojové kódy generátoru překladů.