Rychlý průvodce pro aplikační roli GDPR

1. Úvodní terminologie a informace

Tento manuál poskytuje informace ohledně nařízení GDPR a jeho řešení v aplikaci O2 Car Control (dále jen aplikace). Podrobně se zabývá vysvětlením základních údajů nařízení a způsobem, jakým jsou jednotlivá práva v aplikaci řešena.

Základní terminologie:

GDPR – General Data Protection Regulation. Obecné nařízení Evropského parlamentu a Rady Evropy (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Nařízení je platné od 25. 5. 2018.

Osobní údaje – osobní údaje (dále OÚ) Subjektu údajů

Subjekt údajů – fyzická osoba, občan EU

Uživatel – uživatel aplikace ve firmě zákazníka bez přístupu do Administrace (= Subjekt údajů)

Pověřenec GDPR – uživatel aplikace zákazníka s nastaveným právem GDPR pro přístup na GDPR reporty a k nástroji Anonymizace

Admin firmy – uživatel aplikace s nastavenou Uživatelskou rolí Admin pro celou firmu zákazníka

Admin oddělení – uživatel aplikace s nastavenou Uživatelskou rolí Admin pro oddělení ve firmě zákazníka

Prohlášení firmy zákazníka
Firma zákazníka je správcem osobních údajů (dále jen „Správce“) dle příslušných ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění (dále jen „ZOOÚ“) a nařízení Evropského parlamentu a Rady Evropy (EU) č. 2016/679 ze dne 27. dubna 2016 (dále jen „GDPR“). Firma zákazníka je tak povinna zajistit, aby osobní údaje Uživatelů/subjektů údajů, které jsou jím získávány, byly získávány v souladu se ZOOÚ a GDPR, že jsou přesné, odpovídají stanovenému účelu a jsou pouze v takovém rozsahu, který je nezbytný pro užívání aplikace. Toto není obsahem řešení GDPR v aplikaci.

GDPR poskytuje Subjektům údajů zejména tato práva:

Právo na přístup (Kapitola III, čl. 15) – je právem na ověření zákonnosti zpracování osobních údajů fyzických osob (Subjektů údajů). Každý subjekt údajů tedy bude mít právo vědět a být informován o:

- Účelech zpracování;
- Kategorii dotčených osobních údajů;
- Příjemcích nebo kategorii příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
- Plánované době, po kterou budou osobní údaje uloženy;
- Existenci práva požadovat od správce opravu nebo výmaz osobních údajů, právo vznést námitku;

- Právu podat stížnost u dozorového úřadu;
- Veškerých dostupných informacích o zdroji osobních údajů, pokud nejsou získány od Subjektu údajů;
- Skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování.

Přenositelnost údajů (Kapitola III, čl. 20) – je rozšířeným právem přístupu a může být uplatněno za splnění dvou podmínek, které musí nastat současně:

- Zpracování je založeno na souhlasu Subjektu údajů nebo na smlouvě a
- je prováděno automatizovaně.

V případě automatizovaného zpracování osobních údajů, které je založeno na uděleném souhlasu nebo na uzavřené smlouvě, má osoba právo na tzv. přenositelnost těchto údajů. To spočívá v povinnosti správce předat nositeli údajů všechny o něm zpracovávané informace ve strukturovaném, běžně používaném, strojově čitelném formátu. Uplatněním tohoto práva získává osoba větší kontrolu nad svými osobními údaji a má rovněž možnost je v takto získané podobě předat jinému správci.

Právo na opravu (Kapitola III, čl. 16) – znamená, že v případě, kdy Subjekt údajů má podezření na nesprávnost jeho údajů a to subjektivní nebo objektivní povahy, může požádat daného správce o nápravu. S přihlédnutím k účelům zpracování má Subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení. Správce by měl zajistit podmínky pro to, aby žádosti na opravu mohly být podávány online, zejména v případě zpracování osobních údajů elektronickými prostředky.

Právo na výmaz (Kapitola III, čl. 17) – je právem, které ukládá správci osobních údajů povinnost bez zbytečného odkladu vymazat osobní údaje Subjektu údajů, pokud je dán jeden z těchto důvodů:

- Osobní údaje již nejsou potřebné pro účel, pro který byly shromažďovány nebo zpracovávány.
- Subjekt údajů odvolá souhlas, pokud je zpracování založeno na souhlasu, a neexistuje žádný další právní důvod pro zpracování.
- Subjekt údajů vznese námitku proti zpracování z důvodu oprávněných zájmů správce osobních údajů, jako je např. vedení záznamů o zaměstnancích.
- Osobní údaje byly zpracovány protiprávně.
- Pokud není dán rodičovský souhlas se zpracováním osobních údajů dětí.
- Právní povinnost stanovená právem Unie nebo členským státem.

Právo být zapomenut (Kapitola III, čl. 17) – je rozšířeným právem na výmaz. Spočívá v provedení přiměřených kroků, včetně technických opatření, k vymazání veškerých odkazů na osobní údaje žadatele/subjektu údajů a jejich kopie. GDPR uvádí řadu výjimek, zejména v případech, kdy jsou osobní údaje zpracovávány státními institucemi. Aby měl správce povinnost zlikvidovat osobní údaje, musí být splněna alespoň jedna z těchto podmínek:

- Osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
- Subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování;
- Subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování;
- Osobní údaje byly zpracovány protiprávně;
- Osobní údaje musí být vymazány ke splnění právní povinnosti;

- Osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 Obecného nařízení.

Právo vznést námitku proti zpracování – znamená, že pokud konkrétní Subjekt údajů nebude mít možnost uplatnit právo na výmaz, tak potom mu GDPR umožňuje uplatnit alespoň právo vznést námitku a tím donutit správce k omezenému zpracování těch údajů, které jsou předmětem uplatněné námitky. Na možnost vznést námitku musí být ze strany správce fyzická osoba/Subjekt údajů výslovně upozorněna. Námitku lze vznést i proti zpracování osobních údajů pro účely přímého marketingu nebo profilování. Pokud Subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány**.**
Ve vztahu k těmto požadovaným právům byly v aplikaci identifikovány všechny zpracovávané osobní údaje. Zavedl se detailní monitoring náhledu na osobní údaje, byla vytvořena nová Aplikační role pro Pověřence GDPR. Uživatel s touto rolí (GDPR) má dostupné reporty, které informují o osobních údajích a přístupu k nim. Pro realizaci práva být zapomenut je vytvořen nástroj Anonymizace osobních údajů.

Veškerá činnost uživatelů aplikace, zejména ve vztahu k náhledu a editaci osobních údajů Subjektů údajů je monitorována a zaznamenávána v Historii aplikace. Záznamy v Historii obsahují informace o přístupu všech uživatelů aplikace včetně administrátora firmy a technické podpory k osobním údajům.

Admin → Historie → Historie operací se záznamy

Historie operací se záznamy

Stránka: 1 / 2 Záznamů: 73

Datum	Typ dokumentu	ID	Dokument	Akce	Provedl
16.5.2018 10:42	Uživatel	7066	Karel Srba	Otevření	Petr Macháček
16.5.2018 10:42	Uživatel	7063	Jan Novák	Otevření	Petr Macháček
16.5.2018 10:41	Report	298	Report GDPR Výpis údajů evidovaných k subjektu údajů	Otevření	Petr Macháček
16.5.2018 10:41	Report	298	Report GDPR Výpis údajů evidovaných k subjektu údajů	Otevření	Petr Macháček
16.5.2018 10:41	Report	299	Report GDPR Výpis historie náhledů na osobu	Otevření	Petr Macháček
16.5.2018 10:41	Report	298	Report GDPR Výpis údajů evidovaných k subjektu údajů	Otevření	Petr Macháček

Součástí aplikace jsou bezpečnostní opatření, vztahující se k uživatelským heslům (parametry na silné heslo, každoroční expirace hesla…).

2. Definice aplikační role GDPR

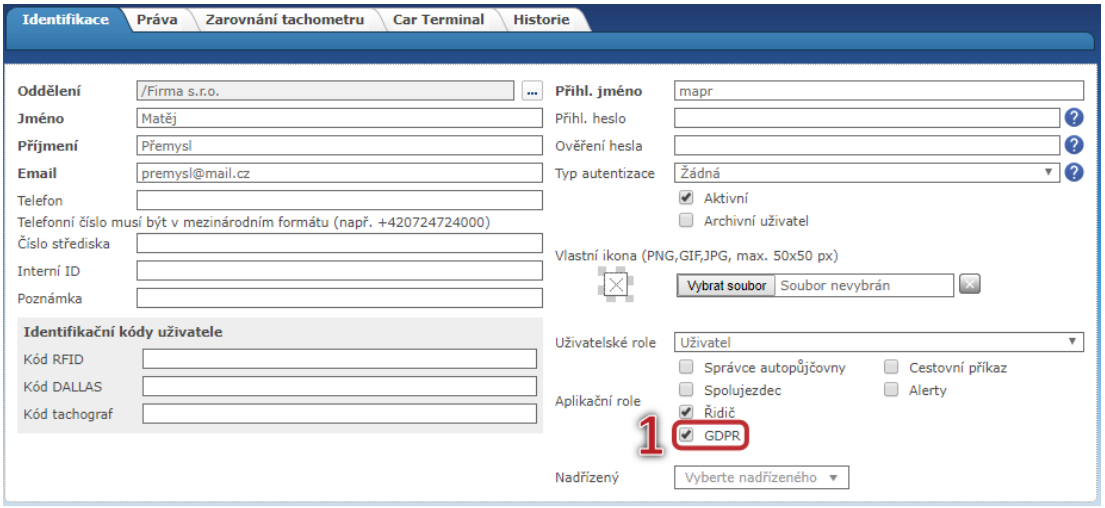
Řešitelem požadavků na uplatnění práv Subjektu údajů plynoucích z normy GDPR je uživatel, konkrétně Pověřenec GDPR firmy zákazníka s nastavenou Aplikační rolí GDPR. Pověřenec GDPR ve firmě zákazníka nemusí být totožný s administrátorem firmy. Administrátor může Aplikační roli GDPR přidělit jakémukoliv uživateli dané firmy.

Aplikační role GDPR zpřístupní uživateli:

- Report GDPR Výpis údajů evidovaných k Subjektu údajů
- Report GDPR Výpis historie náhledů na osobu
- nástroj Anonymizace

Povolení aplikační role **GDPR (1)** naleznete v detailu uživatele, mezi aplikačními rolemi.

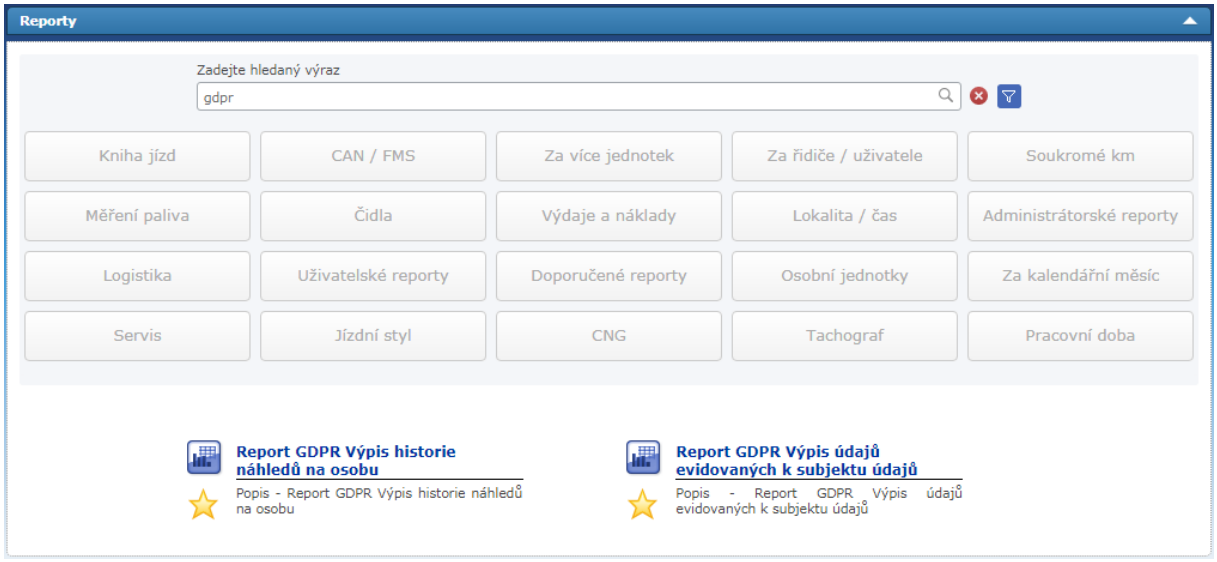
Admin → Uživatelé → detail Uživatele → záložka Identifikace



3. Právo na přístup a právo na přenositelnost údajů

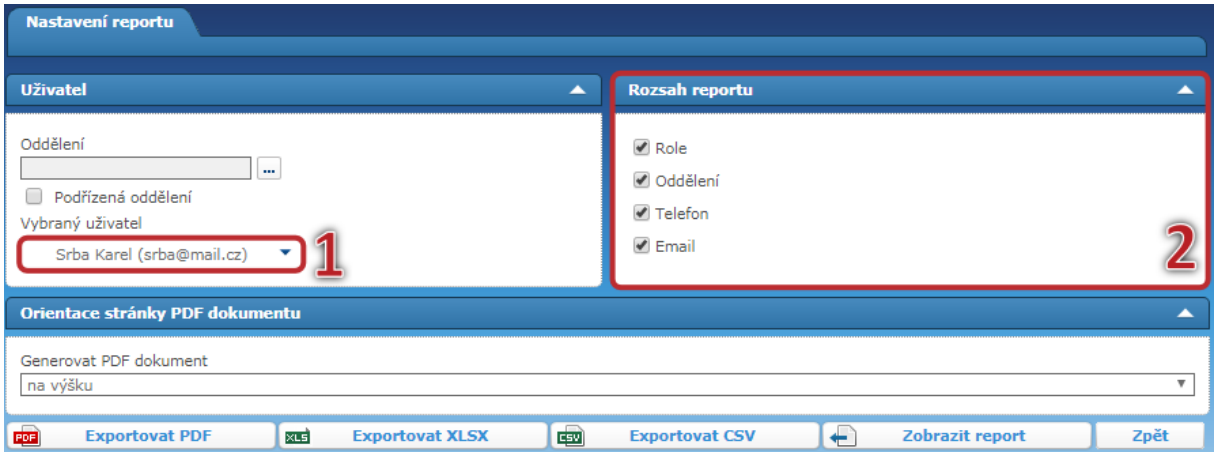
Právo na přístup k osobním údajům, stejně jako právo na přenositelnost údajů je řešeno pomocí GDPR reportů. Reporty je možné jak zobrazit (vytisknout), tak vyexportovat ve formátech CSV, XLSX, HTML nebo PDF. O generování reportu pro Subjekty údajů je vždy proveden záznam do Historie aplikace.

Reporty → Reporty



Report GDPR Výpis údajů evidovaných k Subjektu údajů

Report umožňuje uživateli s právem GDPR ve firmě vygenerovat údaje evidované k Subjektu údajů - tedy jednoho libovolného uživatele z firmy. Ve **výběrníku uživatelů (1)** jsou dostupní všichni uživatelé aplikace. Pro rozlišení uživatelů je součástí výběrníku také telefonní číslo uživatele a email (pokud jsou tyto informace na kartě uživatele dostupné). V sekci **Rozsah reportu (2)** si můžete zvolit, jaké informace chcete v reportu zobrazit.



Výstup reportu zobrazuje všechny dostupné informace evidované v aplikaci k Subjektu údajů, viz následující obrázek.

Report GDPR Výpis údajů evidovaných k subjektu údajů

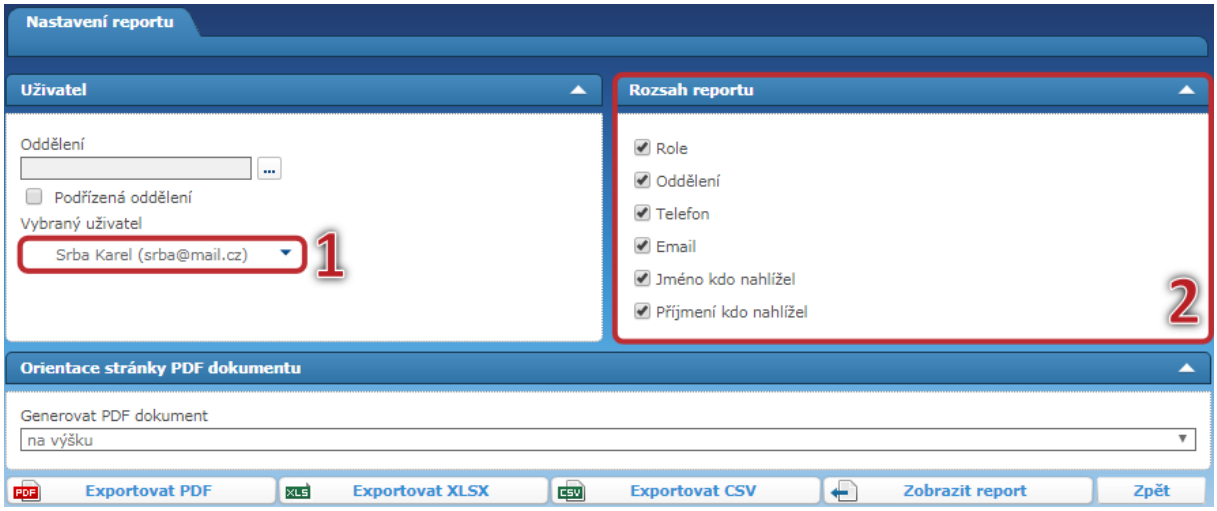
Společnost: **Firma s.r.o.** Vytiskl: **Petr Macháček**, dne: 22.5.2018

Základní údaje	
Jméno	Karel
Příjmení	Srba
Role	Uživatel
Oddělení	Firma s.r.o.
Kontaktní údaje	
Telefonní číslo	
Email	srba@mail.cz

Report GDPR Výpis historie náhledů na osobu

Report umožňuje uživateli s právem GDPR ve firmě vygenerovat historii náhledů na Subjekt údajů - tedy jednoho libovolného uživatele z firmy. Ve **výběrníku uživatelů (1)** jsou dostupní všichni uživatelé aplikace. Pro rozlišení uživatelů je součástí výběrníku také telefonní číslo uživatele a email (pokud jsou tyto informace na kartě uživatele dostupné). V sekci **Rozsah reportu (2)** si můžete zvolit, jaké informace chcete v reportu zobrazit.

Výpisy historie náhledů v reportu se sdružují pod jeden záznam v rámci jednoho dne podle data, pracovní pozice, příjmení a jména a akce. Pokud nad jedním záznamem bude provedeno více náhledů za den, zobrazí se v Reportu pouze jednou.



Výstup reportu zobrazuje detailní výpis historie náhledů na osobní informace Subjektu údajů, včetně uživatelů s právy přístupu k vozidlům, kde je veden Subjekt údajů jako řidič nebo spolujezdec, viz následující obrázek.

Report GDPR Výpis historie náhledů na osobu

Společnost: **Firma s.r.o.** Vytiskl: **Petr Macháček**, dne: 22.5.2018

Detail osoby	
Jméno	Karel
Příjmení	Srba
Role	Uživatel
Telefonní číslo	
Email	srba@mail.cz
Oddělení	Firma s.r.o.

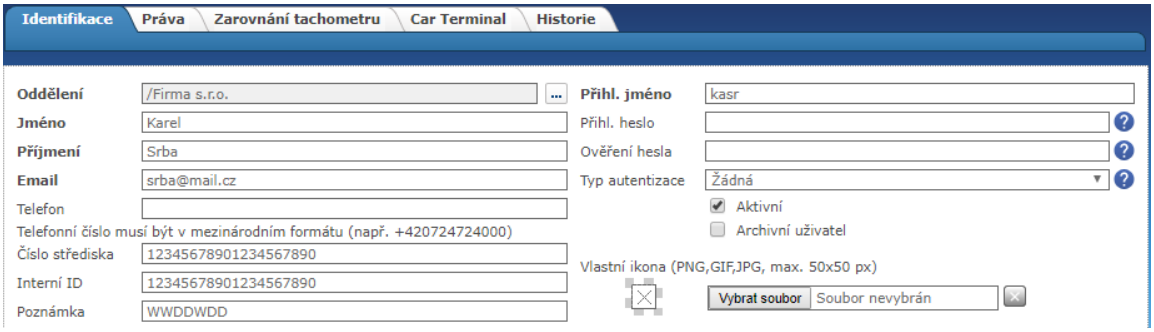
Výpis historie náhledů

Datum	Pracovní pozice	Jméno	Příjmení	Typ dokumentu	Akce
16.05.2018	Admin	Petr	Macháček	Uživatel	Otevření dokumentu
16.05.2018	Admin	Petr	Macháček	Report GDPR	Otevření dokumentu
18.05.2018	Admin	Petr	Macháček	Jednotka	Otevření dokumentu
22.05.2018	Admin	Petr	Macháček	Report GDPR	Otevření dokumentu

4. Právo na opravu

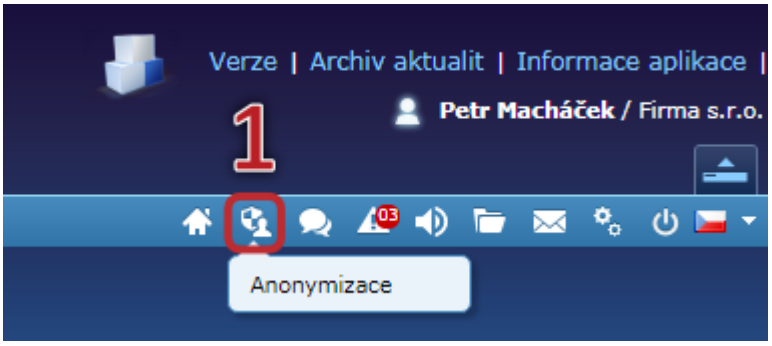
Právo na opravu lze řešit pomocí stávající funkčnosti aplikace, kdy uživatel s rolí Admin provede editaci osobních údajů Subjektu údajů. O editaci údajů je vždy veden záznam do Historie karty uživatele. Toto nemůže provést uživatel s rolí GDPR, protože ten nemá dostupný modul Admin.

Amin → Uživatelé → detail Uživatele → záložka Identifikace

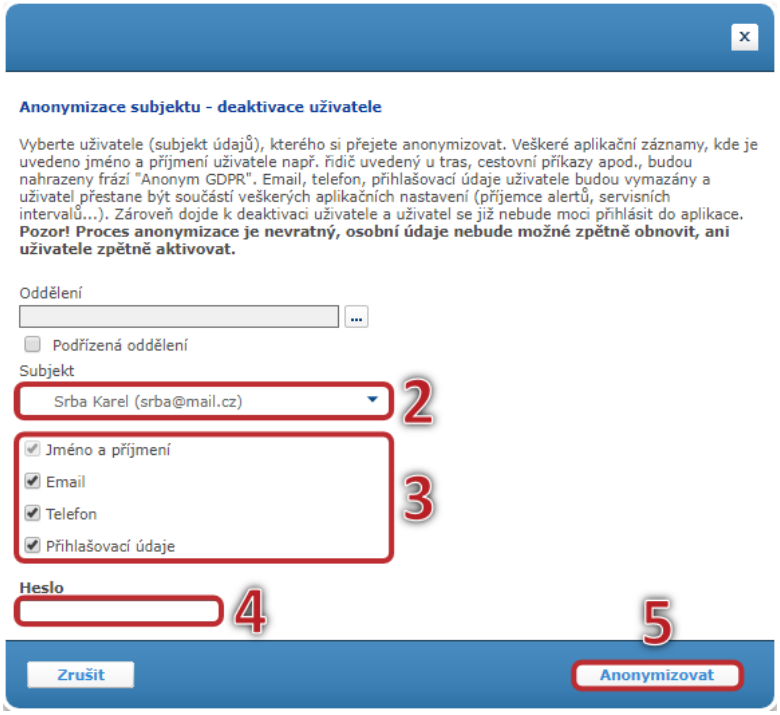


5. Právo na výmaz, Právo být zapomenut – Anonymizace OÚ

Pro naplnění práva na být zapomenut jsme připravili nový nástroj **Anonymizace (1)**. Nástroj je určený pro anonymizaci osobních údajů Subjektů údajů a je dostupný v horní liště pod ikonou . Kliknutí na ikonu vyvolá Průvodce, který vám pomůže s anonymizací osobních údajů vždy jednoho Subjektu údajů. Provedení Anonymizace potvrdí uživatel/pověřenec GDPR svým přihlašovacím heslem a tlačítkem Anonymizovat. Následně aplikace změní jméno a příjmení u Subjektu údajů na hodnoty [Anonym GDPR] v kartě uživatele i všude jinde, kde se jméno a příjmení Subjektu údajů vyskytovalo (např. v Trasách, Cestovních příkazech, v Autopůjčovně, i v Historii). Hodnoty email, telefon, přihlašovací údaje budou vymazány. Subjektu údajů je dále nastaven příznak Neaktivní, uživatel se již nemůže přihlásit do aplikace. Použití nástroje Anonymizace je zaznamenáno do Historie v aplikaci.
POZOR tento krok je nevratný!!!



V průvodci vyberte **Subjekt (2)** a **údaje (3)**, které mají být anonymizovány. Pro potvrzení zadejte své **uživatelské heslo (4)** pro přístup do aplikace a klikněte na tlačítko **Anonymizovat (5)**.



TIP!

Pokud anonymizujete uživatele jen částečně (např. pouze Jméno a Přijmení), tak je možné daného uživatele anonymizovat znovu. Pokud je uživatel anonymizován již v plném rozsahu, tak se v nástroji nebude znovu nabízet.

6. Právo vznést námitku

Právo vznést námitku, týkající se zpracování osobních údajů, je v řešení na straně správce (firmy zákazníka. Toto není obsahem řešení GDPR v aplikaci.