

## Obecně o zabezpečení gReception

Aplikace gReception klade na zabezpečení svých procesů, uživatelských dat a osob, které mají k datům přístup, velký důraz. Zabezpečení se dá rozdělit do tří částí:

### Software

Celá aplikace je naprogramována za použití pokročilého frameworku Django, které chrání před základními druhy napadení - XSS (cross site scripting), CSRF (cross site request forgery). SQL injection, Clickjacking, Host header validation, Session security, atd. Veškerá komunikace se serverem je šifrována za použití 256 bitového SHA klíče se šifrováním RSA. Veškeré funkce jsou programovány tak, aby nemohlo dojít k nepozorované manipulaci s daty nebo odvedením finančních prostředků na účet třetích stran.

### Data

Data jsou ukládána na serverech provozovaných v cloudu, kdy je veškerý obsah databáze zašifrován a rozdělen na několik fyzicky oddělených strojů. Není tedy možné k nim získat přístup ani při ovládnutí serverovny. Data jsou díky tomu také chráněna před ztrátou, neboť jsou v aktuální moment vždy dostupná z více lokalit, navíc jsou dělány pravidelné zálohy 1x za 24 hodin. Všechna hesla nastavená dodavatelem softwaru splňují doporučení pro tvorbu bezpečných hesel.

### Lidé

Ke všem datům gReception mají přístup pouze dva programátoři dodavatele softwaru a správce serveru, kteří jsou vázáni přísnými smlouvami o mlčenlivosti. Při ukončení spolupráce jsou těmto zaměstnancům odebrány veškeré přístupy. Dále jsou všechna uživatelská data přístupná pro dva superadministrátory poskytovatele služby (Global Services & Assistance, s.r.o.), kteří jsou rovněž vázáni smlouvami o mlčenlivosti.). Ostatní uživatelé systému gReception jsou rozděleni do uživatelských skupin s různým stupněm oprávnění a přístupem jen k datům, které spadají pod jejich správu. K jiným datům nemají umožněn přístup.

## **Ještě přísnější zabezpečení během elektronického hlasování**

### **System vs. hlasující**

Při uzavřeném hlasování je hlasující vyzván, aby si vytvořil profil na gReception. Po zadání e-mailové adresy je mu na tento e-mail zaslána potvrzující zpráva, ve které je odkaz na zřízení hesla k profilu gReception. Vzniká tu tedy dvojitá ochrana - je ověřen majitel emailu tím, že má přístup k dané e-mailové schránce a je zřízeno heslo k profilu. Pouze takto přihlášený uživatel, který je pozvaný ke konkrétní volbě, je oprávněn zúčastnit se uzavřené volby.

System jednomu oprávněnému uživateli neumožní hlasovat vícekrát, než jednou. Tímto je vyloučeno, že by někdo mohl hlasovat vícekrát. Nevylučuje to ale možnost, že za uživatele bude hlasovat někdo jiný (\* pokud někomu uživatel v rozporu s pravidly poskytne své přihlašovací údaje - viz. VOP).

Uživatel nemá za povinnost dokončit hlasovací formulář a odeslat jej, tedy nemusí se volby zúčastnit, ale pokud chce své odpovědi odeslat, jsou všechny hlasovací otázky povinné, tedy není možné některou nevyplnit.

Jakmile uživatel odešle hlasovací formulář, nemůže své volby editovat resp. měnit, smí si je pouze zobrazit. Registrovaní uživatelé najdou všechna svá hlasování ve svém profilu pod "moje vyplněné formuláře" a mohou tedy zpětně zkontrolovat, jak hlasovali.

### **System vs. administrátor**

Jakmile je spuštěno on-line hlasování, system uzamkne formulář proti změnám, které by mohly zmanipulovat hlasování. Administrátor elektronické volby pak až do ukončení hlasování nemůže upravovat kritérium pro přijetí, kvorum a typ hlasování. Nemůže také editovat nastavení hlasovacích polí ani varianty odpovědí. Není mu povoleno přidávat, editovat nebo odstraňovat hlasující, stejně jako měnit váhy hlasu.

V režimu tajného hlasování nejsou zpřístupněna data o průběhu hlasování či konkrétní volbě jednotlivých hlasujících nikomu z účastníků hlasování, ani samotnému administrátorovi elektronické volby (zástupci klienta), ani superadministrátorům (zástupcům poskytovatele služby). Výstupem je pouze celkový výsledek hlasování po jeho ukončení a neexistuje žádný záznam o konkrétním hlasování jednotlivých uživatelů. Pouze samotný uživatel si může zobrazit svůj konkrétní hlasovací formulář pro ověření, jak hlasoval.

## Výsledky hlasování

V závislosti na počítačném nastavení elektronického hlasování mohou být výsledky hlasování:

- zpřístupněny všem hlasujícím
- zpřístupněny pouze administrátorovi hlasování, včetně zobrazení hlasování jednotlivých uživatelů (veřejné hlasování)
- zobrazeny pouze administrátorovi hlasování, ale bez přístupu k záznamům jednotlivých hlasujících (tajné hlasování).