

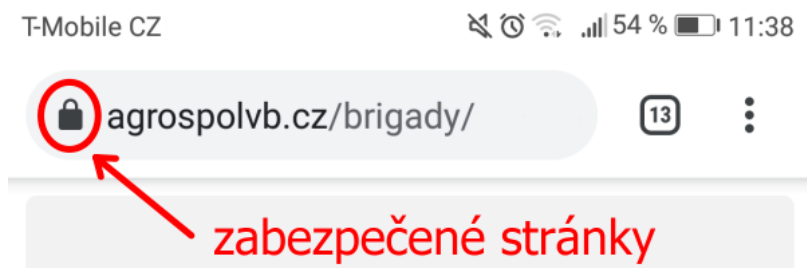
# Informace o zabezpečení vkládaných dat

Vážení brigádníci,

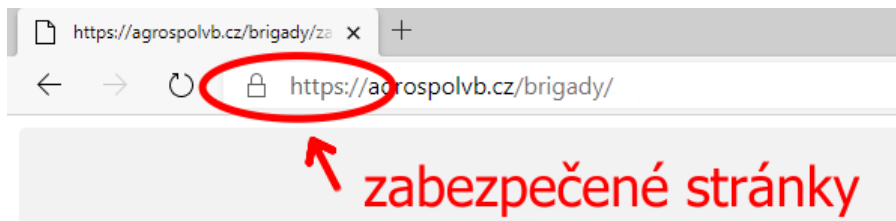
formulář po Vás požaduje vyplnění extrémně citlivých dat, proto považujeme za férové se zmínit o jejich zabezpečení a nakládání s údaji, které zde vkládáte:

- Celý web firmy **Agrospol Velká Bystřice s.r.o.** má zabezpečené spojení, proto všechna data, která do formuláře vložíte, budou nejprve zašifrována a následně v zašifrované podobě odeslána na server. Zabezpečené stránky poznáte tak, že nalevo od adresy je **ikona s uzamčeným zámekem**, na počítači navíc adresa začíná textem **https://**, viz obrázky.

## Jak poznat zabezpečené stránky na mobilu:



## Jak poznat zabezpečené stránky na počítači:



- Na našem serveru budou tato data zpracována, **zašifrována veřejným klíčem** a v zašifrované podobě **uložena do databáze**. Takto zašifrovaná data lze přečíst jen se znalostí **soukromého klíče**, který se z bezpečnostních důvodů nenachází na internetu. Proto i v případě neoprávněného získání dat má útočník k dispozici pouze zašifrovaná data (viz obrázek), která jsou mu bez znalosti soukromého klíče k ničemu.

ID	HASH	DATA	VLOZENO	STAZENO
70	618559dce44649a920d7c8f	eTtFvBMBgrNgWhdgB/jeWc5ZkDTPDWekRhQYq9pBhc7UK	2021-02-09 07:51:55	0
71	bdcd4ee57ab8eab4388801e	RTaToy2sjsluoMuLtdns2lMeVntRN0SW/bfSNxsa3il1k1G+..	2021-02-09 16:22:54	0

- Zašifrovaná data budou průběžně stahována do našeho informačního systému a po stažení budou z databáze smazána.
- Veškerá vložená data budou použita pouze v souvislosti s touto brigádou a povinnostmi, které nám v tomto směru ukládá zákon.
- Pro zájemce o podrobnější informace:
  - O **asymetrické kryptografii**, principu soukromého a veřejného klíče, si můžete přečíst např. zde: [https://cs.wikipedia.org/wiki/Asymetrická\\_kryptografie](https://cs.wikipedia.org/wiki/Asymetrická_kryptografie).
  - Princip fungování si vyzkoušíte např. zde: <https://travistidwell.com/jsencrypt/demo>.
  - V současné době je považován za bezpečný pár RSA klíčů o délce 2048 bitů.
  - My pro šifrování dat používáme pár RSA klíčů o délce 4096 bitů.