Declaration of security

The gReception application puts great emphasis on securing their processes, user data and people with access to the data. Security can be divided into three parts:

Software

The whole application is programmed with the use of advanced Django framework which protects it against basic kinds of attacks – XSS (cross site scripting), CSRF (cross site request forgery). SQL injection, Clickjacking, Host header validation, Session security, etc.

The entire communication with the sever is encrypted by means of 256 bit SHA key with RSA encryption.

All functions are programmed so that they prevent unnoticed manipulation with date or transferring finance to a third party account.

Data

Data is saved to cloud servers and the whole content of the database is encrypted and divided into several physically separated machines. Thus it is not possible to maintain access to them even in case of gaining control of the data centre. Thanks to this, data is protected against loss, being always accessible from more locations.

Regular back-ups are made every 24 hours.

People

Only software provider programmers and the server administrator can access all gReception data and they are bound by strict secrecy agreements.

Furthermore, all user data is accessible to the service provider super administrators (Global Services & Assistance, s.r.o.) who are bound by secrecy agreements.

Even stricter security during electronic voting

System vs. voter

When voting, a voter identified by means of registration is asked to make a profile at gReception. After entering an e-mail address, the voter is sent a confirmation message to their e-mail with a link to create a password to get a gReception profile. Thus double protection is provided – the owner of the account is verified thanks to their access to the email and a password is created for the profile. Only a user registered in this way who is invited to a specific vote is entitled to participate in voting, having been checked by gReception.

The system allows an authorized user vote only once. Thus it is made impossible to vote repeatedly within one vote. Yet it does not exclude the possibility that someone else will vote on the behalf of the user (* if a user contrary to the rules provides their logging information – see the General terms of trade). The user is not obliged to complete the voting form and send it so it is not necessary to vote, but if they want to send their answers, all voting questions are obligatory, which makes it impossible to skip any of them.

As soon as the user sends the voting form, they cannot edit, resp. change their choices; they can only display them. The registered users will find all their votes in their profiles at "My completed forms" so they can retrospectively check how they voted.

System vs. administrator

As soon as online voting is launched, the system locks the form against changes that could manipulate voting. Only when voting is finished, the administrator of electronic voting can modify the criterion for adopting, quorum and type of voting. They also cannot edit the setting of voting check-boxes nor the possible answers. They are not allowed to add, edit or remove the voters nor change the weight of the vote.

In the secret vote mode, no data is available during voting nor the specific choice of the individual voters to any participant of the voting process, not even to the administrator of the electronic voting (client´s representatives) or the super administrators (representatives of the service providers).

The outcome is only the total result of voting when it is finished and there is no record on the tangible votes of the individual users. Only the users themselves can view their specific voting forms to check how they voted.

Results of voting

Depending on the initial setting of the electronic voting system, the results of voting can be:

- Made available for all voters
- Made available only for the administrator of voting, including viewing voting of the individual

users (open vote)

•	Displayed only to the administrator of voting but without the access to the records of the individual voters (secret vote).