

COMMUNICATION PORTAL USER REMEMBER Approved 25.03.2012 Revised 03.04.2019 2 2 The guide is aimed at new users of the social portal and provides an overview of what to think about before registering as a user of the portal and what to pay attention to while using it. The guide helps increase your security and awareness on the social portal and helps prevent you from becoming a victim of personal data crimes. We would like to draw your attention to the fact that you yourself do not endanger your privacy and the integrity of your private life by excessively publishing your data. BEFORE you start using any social networking site, review this reminder.

1. Is this social portal for you? Before registering as a user, make sure that this portal is suitable. Check out the user terms of the social portal. Be sure to disclose your real age to the portal, as social networking sites often take the user's age into account and increase security and privacy themselves. Before creating a user account, think about the impression you want to leave on other users and how it could affect your future. In Estonia, persons from the age of 13 are allowed to create their own social media account. For all minors, this is permitted only with the consent of the legal representative.
2. Explore the privacy settings. Be sure to familiarize yourself with the privacy settings of the social portal and read the terms of use. They provide an overview of how much your data is stored and how accessible it is made to others. See also who owns the social portal, whether it is a foreign or Estonian portal. Prefer portals that publish their contact details and have clear data protection conditions (may also be listed under the name of privacy conditions).
3. Use an alias. If you create a user account, you could use a fictional name or just a first name instead of your real name to increase security and privacy on the social portal and on the Internet in general. It is not allowed to use the names of other existing persons, as this may harm their rights and bring you criminal liability.
4. Copyright protection. When publishing images, photos, videos, music, etc., always consider copyright requirements. Do not publish other people's work without the author's consent.
5. Advertising. Avoid disclosing your e-mail address or phone number on your user account, as you may start receiving unwanted advertising. You can usually limit yourself from receiving advertising. Be sure to think before you open an advertising banner - it may direct you to a page that may be related to malware.

**BE SURE TO FOLLOW THESE SIMPLE RULES DURING USE.**

6. The Internet doesn't forget. Remember that everything you publish on the Internet is recorded. All information that you have published about yourself or others will be available again later, even if you think you have deleted it. Think before you publish anything at all.
7. Password. Choose a password as unpredictable as possible. Come up with a memorable system to help you use secure but easy to remember passwords. When creating a password, combine uppercase and lowercase letters and numbers. You should also change your password every certain time. If the social portal allows it, be sure to use two-step

authentication. Read more recommendations [here](#) and [here](#). 8. Regular review. Review your posts, messages and comments regularly. Delete anything that seems unnecessary and exhausted. 9. Sharing Your Data. If someone starts communicating with you on the Internet, do not share your or your loved ones' information with them until you are convinced that it is a reliable person. Don't lightly accept friend requests from people you don't know. Under the privacy settings, make your personal data visible only to close acquaintances. We do not recommend publishing your phone number, home address, daily schedule and other similar information. Such data puts both you and your loved ones at risk. 10. Disclosure of Others and Consequences. Don't do to others what you don't want done to you. Do not disclose other people's information without their consent. Do not defame or 3 3 insult others. Think before you publish, because the internet is not anonymous and consider that you can be identified later. 11. Photos and videos. If you add pictures and videos to your profile, review them carefully, as the picture may include someone else who does not want this picture to be public. Do not publish pictures of yourself that you should be ashamed of in the future. For example, when a relationship breaks up, publishing nude pictures as revenge is unfortunately very common. Do not upload images with location data attached. They are added to the metadata of the image whenever you have taken the image with a smart device that has GPS activated. 12. Login with a smart device. Many social networking sites also allow users to access their user accounts via a smartphone. When visiting the social portal with a mobile phone, think about whether you want GPS positioning to determine your location and announce it on the social portal. Check your phone settings. 13. If not using, log out of the service. 14. Can your data be found through search engines? It is also worth checking the availability of your data through various search engines such as Google, Yahoo, Yandex, etc. By searching for your name, see if your profile on the social portal can be found. The discoverability of the profile can also usually be changed under the privacy settings. 15. Deleting a user account. If you have decided to delete the user account, make sure that the personal data is really deleted and the account is closed (not deactivated). If it is not possible to delete the account, contact the portal administrators or replace all personal data with arbitrary letters and numbers. 16. Use of your personal data without consent. a. if there has been identity theft<sup>1</sup> and someone impersonates you, contact the police. b. in case of defamation and insult, communicate with the portal administrator and, if necessary, take the person to court<sup>2</sup>. If you wish, you can also demand compensation for damages and the prohibition of publishing data in the future; c. if you want the portal to stop processing your personal data and delete your account, contact the portal administrator - preferably in writing. If the portal administrator does not respond, submit an intervention request to the Data Protection Inspectorate. An alternative option is to go to court. 1 Penal

Code § 157<sup>2</sup> - For transmitting personal data identifying or enabling the identification of another person without his consent, providing access to them or using them with the aim of creating a knowingly incorrect image of him by impersonating another person, if this has caused damage to the rights or interests of another person protected by law, or concealing a crime - shall be punished by a monetary penalty or imprisonment for up to three years. 2 The application form can be found at <https://www.kohus.ee/et/kohtumenetlus/dokumentide-vormistastestiest>. In certain cases, you can also use the state's legal aid <https://www.kohus.ee/et/oigusabi/riigi-oigusabi> if necessary when going to court.