Dear colleague,

You have received this e-mail because you have been authorised for *Verzuimsignaal*, the online absence tracking system of the UT.
Starting **Wednesday, December 12th**, access to *Verzuimsignaal* will be subject to extra security. This means you need a second authentication when logging in. This second authentication happens via your smartphone.

**Why 2-factor authentication?**

The requirements for the processing of special categories of personal data have become more severe in the General Data Protection Regulation (GDPR). Due to their nature, special categories of personal data are very sensitive and are subject to extra protection in the GDPR. Logging on with only a username and password no longer suffices.
The UT uses multiple applications that involve the processing of special categories of personal data. On the basis of the GDPR, the UT has to provide extra security to these applications through 2-factor authentication: Two Factor Authenticatie (2FA).

*Verzuimsignaal* is the first application for which the UT will implement 2FA. In *Verzuimsignaal*, data concerning the health of staff members is processed. This means the online absence tracking system is among the most sensitive applications. Other applications will follow at a later date.

**Second authentication via smartphone**

Various 2FA applications are available for smartphones. The UT chose *NetIQ Advanced Authentication* and *Google Authenticator (TOTP)*. In order to gain access to the extra-secured information systems, one of these apps must be installed on your smartphone.

Do you not have a UT smartphone and do you not want to use a private smartphone for the 2FA? You can purchase a low-budget smartphone via the [LISA self-service portal](http://www.pronuntio.utwente.nl/2-1gxo_sauRReGI_R7LQ8rH6-5D5YZZjIW9UGpAY1AlYAARyDKdq6k6CQTc5wy88SIYbgSw92urpOfXovG9pBEo1NWXFQJT9VyevDoM9g9Db21antEu3MhOQ) at the expense of the faculty/service.

**Installing and activating 2FA application**

If you log on, on or after **Wednesday, December 12th 16.00 hrs.**, you will be automatically redirected to the MyID registration portal. This portal controls the installation and activation process of the authenticator on your smartphone. At the end of the process, you will receive a recovery key. You need this recovery key to deactivate the authenticator on your old device and to activate it on your new device in case of loss or replacement. It is important to save the recovery key in a safe location. [LISA CyberSafety](http://www.pronuntio.utwente.nl/2-1gxo_sauRReGI_R7LQ8rH6-5D5YZZjIW9UGpAY1AlYAARyDKdq6k6EoM_voFJvLZYbgSw92urpOfXovG9pBEo7qRw0oBgixSsHwEftJRzNgDZ351bJrrjQ) recommends the LastPass password manager.

**Access to verzuimsignaal**

Now that 2FA has been activated, all you have to do is log in to verzuimsignaal and validate the connection with your smartphone.

**Questions**

Do you have any questions about the installation/activation and use of the 2FA application? Please, contact the [FAQ](http://www.pronuntio.utwente.nl/2-1gxo_sauRReGI_R7LQ8rH6-5D5YZZjIW9UGpAY1AlYAARyDKdq6k6OJv75QKM0PgYbgSw92urpOfXovG9pBEo2FVvhiPOci70KQJUaJlX2Q04OMIto9oQA) or contact the Service Desk ICT.

Kind regards,

Service Desk ICT

Library, ICT Services & Archive (LISA)