The Economics Institute GDPR instructions - Translation

Česká verze *Pokynů* týkajících se ochrany osobních údajů je k dispozici na stránce https://cz.cerge-ei.cz/o-cerge-ei/ochrana-osobnich-udaju-pokyny

Pro účely agendy ochrany osobních údajů je určena kontaktní osoba: Petr Veselý, oddělení výpočetní techniky
GDPR primary contact person: Petr Veselý, Head of Computer Office
Primární kontaktní email / Primary contact: helpdesk@cerge-ei.cz

---

Instruction no. 5 – Minimizing computer threats and risks, protection of personal data

Recommendations for employee for the protection of personal data and minimizing threats and risks when working with computers, in mobile communication, or on networks while working from home.

Be careful of e-mail scams

Fraudulent e-mails could appear to be very trustworthy. The aim of these attacks is usually the unjust procurement of funds or access to the information system in order to, for example, employ ransomware. The purpose of such an attack could also be to paralyze the entire institution (encryption and/or damage of local and shared files, stealing of data, stealing of passwords, gaining of elevated privileges, etc.)

We are currently witnessing an increased activity of hackers attempting to misuse the situation surrounding the ongoing pandemic and requests for information relating to the novel coronavirus. **One of the most common means is sending fraudulent e-mails with attachments or links that seemingly contain important information on the coronavirus.**

It is no longer true that you can recognize e-mail scams by the use of flawed Czech. In addition, do not be fooled by the notion that a person you know is sending the e-mail.

If you think an attachment is untrustworthy in any way or you are not expecting an e-mail with such an attachment, do not open it. Moreover, malicious code may not be immediately apparent after running it. If in doubt, always contact the IT office.

Do not open suspicious links in e-mails

Phishing emails usually hide where the links lead. The hidden path for the link is the first

indication of a fraudulent email.

How do I find out where a link from an email leads? Right-click (NOT LEFT) on the link and select “copy link address” from the menu. Then copy it into Notepad or a file and you will see where the link really leads. Also, **beware of URL shortenings that mask the real link.**

Do not confuse your work computer with a private one

Use work computer only for work agenda. Never allow access to the computer by third parties or family members.

It is better to check with the IT office in advance of any intended third party software use or installation.

In case you use a work notebook/device, never attempt run or install any unlicensed software.

Knowing that Internet access while working from home does not normally take place through a connection provided by your employer could lead to reduced caution when using the Internet on institutional equipment. Employees could also access sites that are typically characterized by the increased occurrence of various malicious programs - pages they would never access on the employer’s network. This behavior could introduce a malicious program to an otherwise “clean” device, which in turn could pose a serious threat to both the device itself and the information stored on it and to the organization’s information systems later.
Similarly, increased caution is required when a private computer is used for remote access to the employer’s information system.

Avoid using public Wi-Fi networks

Personal data and other sensitive information should not be transmitted by a Wi-Fi network in public places without special precautions.
We strongly recommend not using public Wi-Fi networks and prefer safer connections via mobile data or the use of some form of VPN if applicable.

If you use EDUROAM, be sure that your password is complex enough and is at least 10 characters long.

Be careful when selecting passwords

Never ever let the web browser or the computer store your passwords (the only exception is password stored in trustworthy email client, but be sure the password is different from your other network passwords)

Do not use the same passwords at home and at work. Never use the same passwords for different information systems.

This recommendation is especially valid for the credentials you use to log in to work remotely. In the

event of a successful attack on your home computer, it is usually easy to acquire stored login information from browsers and email clients. An attacker should not be able to log on to the work e-mail using the password for a private e-mail account or access anything else.

Do not enable macros in documents

New versions of office programs are able to work with older versions of documents, and there is no need to install or enable anything.

Most crypto-viruses use fraudulent e-mails with an attached document. This includes a prompt to enable active content and macros in the attached documents. The attachment itself might look like a message that the document is written in an older version of a text editor and the actual content of the file cannot be displayed without the macros enabled. Never comply with such a request, as this would result in malicious code being downloaded and installed.

Do not underestimate the physical security of computers

Even your private computer should require identity verification, e.g. by entering a password or biometric authentication.
You can greatly mitigate the effects of theft by turning on hard disk encryption. For most computers, this feature can be turned on or installed for free, and the impact on performance is small. Encryption greatly reduces the risk when a device is lost.

Follow other practical security measures

Measures should be proportional to the level of risk. Adequate security relating to preventing access of other family members to a device (its content) is also important. This is especially true for children who could unknowingly also be the cause of some of the risks mentioned in this document.

When should you contact the IT office?

- Files with unknown extensions are on the disk instead of your regular documents.
- There are new files on the disk containing information on accessing files after paying a ransom. They usually contain words like decrypt, recover, ransom, etc. in the file name and content.
- The desktop wallpaper has changed or a notification is displayed directly on the screen.
- In other cases, if you suspect your device is behaving abnormally.
- To take preventive measures – if you want to act responsively and prevent your device from any problems mentioned here, you may consult the suitability of your security settings and procedures taken.

When should you report a security incident?

Please be aware that there is an obligation to report any security incident to the Data Protection Officer. Reporting is the responsibility of any employee or their supervisor who discovers any of the following:

- A device or document containing a personal data file was lost or stolen;
- An unauthorized person has been given access to personal data in the device or document;
- Personal data, in whatever form, were placed without adequate access protection in a location where unauthorized access could be made;
- Personal data has been corrupted or lost;
- Personal data may have been changed or modified, but it is not possible to verify that this has occurred.

Any loss must be reported to the following e-mail address: gdpr@cerge-ei.cz

---

Instruction no. 4 – Addressing multiple recipients in emails

In the case of **sending an email to the private addresses of multiple recipients, it is strongly recommended to put their email addresses into the Bcc: address field** (Blind carbon copy) only. Using the To: or Cc: fields exposes their private email addresses to the other recipients and violates privacy principles (a private email address is considered to be personal data).

This instruction does not apply to situations where recipient addresses are their working emails (no matter whether an internal or third party) or communication participants obviously know each other.

Instruction no. 3 – Using private e-mail addresses in work communication

For the purpose of work communication within the Economics Institute (EI) or towards third parties, EI employees may use only their work e-mail addresses with the cerge-ei.cz (or ei.cas.cz) domain. The GDPR does not permit the use personal e-mail addresses for any type of work communication including communication with students.

As an exception, EI employees may use e-mail addresses from other official domains for the purpose of work communication related to their EI work agendas when they are employees of any of the following organizations associated with the domains: Charles University, the Czech Academy of Sciences (including their joint workplaces), university/faculty hospitals, CESNET, or official domains of other universities and public research institutions.

EI employees may only use e-mail forwarding from the cerge-ei domain to an e-mail account in any of the above listed domains.

The above instructions do not address the placement of e-mail accounts of third-party recipients.

As always, the e-mail content may only include personal data that do not influence the recipient or that were originally included in the communication by the recipient.

Instruction no. 2 – Publishing of students/alumni lists

The publishing of lists of students and/or alumni in printed form (in annual reports, etc.) or on a public web page is not allowed without their explicit consent.

Gained consent may be used in accordance with its specific purpose only. It must be specific and 'individual' so that you get separate consent for separate things.

Instruction no. 1 – Reporting a Lost Device

Any lost or stolen electronic/data device must be reported to the GDPR primary contact person at helpdesk@cerge-ei.cz?subject=[GDPR] Reporting of Lost Device, either by the affected employee/student or his/her superior. The incident will be analyzed and appropriate remedies assessed. CERGE-EI is obliged to document and assess such incidents and report on them to the Data Protection Office (ÚOOÚ) or other subjects involved in the incident.

This instruction concerns any device containing personal data which might conceivably be lost or stolen or containing passwords, the stealing of which might lead to personal data loss (typically PCs, laptops, portable devices including tablets and mobile phones, external data drives and cards, etc.). Personal data include, e.g. students' seminar papers, seminar attendance lists, students' grades, personal information contained in research data files, etc.

Email Disclaimer modification

Dosavadní znění upozornění zůstává v platnosti, za poslední větu tohoto upozornění se nově doplňuje věta:

„Obsahuje-li tento e-mail nebo některá z jeho příloh osobní údaje, dbejte při jeho dalším zpracování (zejména při archivaci) souladu s pravidly evropského nařízení GDPR.“

The original disclaimer remains the same, only the following sentence should be appended:

„If this e-mail or any of its attachments contains personal data, please be aware of data processing (particularly document management and archival policy) in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council on GDPR.“

Full text of CERGE-EI disclaimer is available here.