Appendix to Ordinance no. 30

of the PK Rector from 21 May 2018



Instruction

 for managing IT system

 used for processing of personal data

at the

 Cracow University of Technology

# Introduction

This instruction specifies the principles of exploitation and management of IT systems used for processing of personal data at the Cracow University of Technology. The rules described in the hereby document are based on the following legal acts:

* The Act of 10 May 2018 on the Protection of Personal Data,
* Regulation of the European Parliament and Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of EU L.119 from 4.5.2016, p. 88 (GDPR);

# Abbreviations and definitions used

**PK** – The Tadeusz Kościuszko Cracow University of Technology

**PDC** – Personal Data Controller

**LPDC** – Local Personal Data Controller

**PDPO** – Personal Data Protection Officer

 **ISA** – IT System Administrator

**System user** – a person who in accordance with the regulations applicable at PK obtained authorisation, entitlement and passwords to access processing of personal data in the IT system.

**Password** – shall be understood as a string of characters, digits or other, known only by the system user.

**User Identifier** – shall be understood as a string of characters, digits or other, unambiguously identifying the system user.

**Accessibility** – a property of the IT system which consists in providing access to data and services upon demand of an authorized user.

**Integrity** – a property of the IT system which consists in securing it against unauthorized change or data removal.

**Confidentiality** – a property of the IT system which consists in securing it from unauthorized access to data.

**IT system** – it is a complex of cooperating with one another technical measures, processing procedures, software tools used for data processing.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Date of release:25.05.2018 |
| 1. **Granting of the authorization for processing of personal data**
 | Procedure no.: 1version: 01 |

* 1. Only authorized persons may be permitted to process personal data.
	2. The authorization is granted by the Local Personal Data Controller authorized to act in this respect on behalf of the Personal Data Controller.
	3. The authorization is granted upon request of an immediate superior of the authorized person.
	4. Templates of “*Application for granting authorization and assigning rights to process personal data at the Cracow University of Technology and declaration”* constitute appendices No. 3 and No. 4 to Ordinance no. 30 of the PK Rector from 21 May 2018.
	5. This application is drawn up with designation for:
		1. an authorized person,
		2. the Department of Personal and Social Affairs as an annex to Employee Duties Card
		3. the Personal Data Protection Officer.
	6. Local Personal Data Collector informs an applying person about the granting of authorization or refusal of granting the authorization for processing of personal data.
	7. It is possible to appeal to the Personal Data Collector – PK Rector against the refusal to grant the authorization by the Local Personal Data Collector.
	8. After obtaining the authorization, the superior of the authorized person:
		1. familiarizes the authorized subordinate employee with the rules of secure processing of personal data and informs about the duties associated with providing protection of personal data;
		2. accepts a written statement from the above-specified person with signature on the authorization for processing of personal data;
		3. provides an appropriate copy of the authorization to:
			1. the authorized person
			2. Department of Personal and Social Affairs
			3. Personal Data Protection Officer

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **2. Granting of the authorization for processing of personal data in IT systems**  | Procedure No.: 2version: 01 |

1. The basis for granting access to the system and granting rights to the person authorized to process personal data in the IT system is the authorization granted in compliance with the procedure of granting the rights to process personal data.
2. The Personal Data Officer provides the authorization for processing of personal data at PK and the completed application for the account creation in the IT system to the IT system Administrator (Application form for the account creation in the HMS system is available in SIP).
3. The ISA, based on the provided authorization and application for the account creation in the system,:
	1. creates the user account and grants it required permissions in the system,
	2. provides the user with his identification (login) and initial password in a secure manner,
	3. informs the superior of the user about the fact of granting such rights,
	4. provides authorization to the Personal Data Protection Officer after entering user identification in the authorization (table intended for ISA).
4. Encrypted electronic mail message or user’s personal collection (after confirming identity) is considered to be a secure way to transfer the identification and the password.
5. After obtaining from the ISA information about the created account, the user:
	1. logs into the system using identification and initial password,
	2. changes the initial password to his own password which is compliant with the rights accepted in the particular system,
	3. validates the accuracy of the account and the granted rights.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **3. The withdrawal of authorization and rights to process personal data**  | Procedure No.: 3version: 01 |

1. The withdrawal of authorization and rights to process personal datais issued by the Local Personal Data Collector on *the Card of the withdrawal of authorization and rights to process personal data at PK.*
2. The withdrawal of authorization is issued at the request of the direct superior of the authorized person in the case of:
	1. the expiration of the employment contract at PK,
	2. the prolonged absence of the employee (sick live above 35 days, unpaid leave, parental leave),
	3. the change of the job position,
	4. the change of the place of work at PK,
	5. the change of the scope of professional duties,
	6. violation of the protection of personal data procedures in the IT system,
	7. other (completion of works at the collegial, departmental committees).
3. The withdrawal card template constitutes appendix No. 5 to Ordinance no. 30 of the PK Rector from 21 May 2018.
4. The Card is drawn up in three copies intended for:
	1. the authorized person (organizational entity),
	2. Department of Personal Affairs,
	3. Personal Data Protection Officer.
5. Local Personal Data Controller informs the applying person about the withdrawal of authorization for processing of personal data.
6. After withdrawal of the rights of authorized person, the superior of that person:
	1. provides him with the card of withdrawal with the decision of LPDC for subsequent signature;
	2. provides appropriate copy of the signed card of withdrawal to:
		1. Department of Personal and Social Affairs
		2. Personal Data Protection Officer.
7. Personal Data Protection Officer provides ISA with “the Card of withdrawal of authorization and rights to process personal data at PK” in order to close the account in the IT system.
8. ISA, based on the provided Card of withdrawal,:
	1. withdraws the rights granted in the system,
	2. provides the “Cards of withdrawal…” to the Personal Data Protection Officer after confirmation of the withdrawal of rights on the Card of withdrawal.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date:25.05.2018 |
| **4. Methods and measures of authentication in IT systems**  | Procedure No.: 4version: 01 |

1. Authentication in IT systems is intended to protect information from unauthorized access, disclosure, accidental or unauthorized destruction or modification of data. Application of the rules of the system users’ authentication has a direct impact on maintaining data confidentiality (it implies the characteristic of the IT system ensuring that the data is not made available to unauthorized entities), accountability of data (it implies the characteristic, ensuring that activities of an entity can be unambiguously attributed only to this entity) and the data integrity (it implies the characteristic ensuring, that the personal data was not changed or destroyed in an unauthorized way).
2. In IT systems of PK the two-step authentication is used at the level of:
	1. access to LAN,
	2. access to the application.
3. Unique identifiers and passwords are applied for authentication of a user in the system on both levels.
4. The user is not allowed to use accounts of other users, administrators or guests.
5. The password to access the system consists of a minimum of 8 characters, small and capital letters, digits and special characters.
6. The system automatically imposes a change of the password not less than once in a month and it does not allow for it to be repeated in the last five months.
7. Commonly used words cannot be passwords. In particular, words such as: dates, names, surnames, initials, car registration numbers, phone numbers or other words directly associated with a given user cannot be used as passwords
8. The password may not be revealed to another person even after the password expires.
9. The password has to be changed by the user immediately in case of suspicion or confirmation of its disclosure.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date:25.05.2018 |
| **5. Commencement, suspension and completion of work by system users**  | Procedure No.: 5version: 01 |

1. When commencing work, a person must:
	1. start the computer which is a part of the IT system and log in by providing his own identifier and the password for access,
	2. run the chosen application in a way prescribed in its operating instruction,
	3. log in to the application in the same way as presented above.
2. Each time a computer workstation is left by a person he must ensure that no information or data is displayed on the screen.
3. Each user is obliged to comply with the security standards of the IT system in accordance with the IT Security Policy at PK (Ordinance no. 20 of the PK Rector from 17 April 2018)
4. When completing work in the system, a person must:
	1. save the results of work in the application,
	2. close the application in accordance with the instruction,
	3. check whether electronic data carriers containing the personal data were not left in the drive,
	4. close the computer operating system and wait until it turns off,
	5. turn off the monitor,
	6. secure possible information data carriers.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **6. Procedures for creating backup copies of the HMS system data** | Procedure No.: 6version: 01 |

1. The IT System Administrator (ISA) is responsible for creating backup copies of personal data and programs used for their processing.
2. The backup copies of the HMS system data are saved on the data backup Avamar01 server located in the WIL server room. Copies are created according to following scheme:
	1. daily copies - seven copies,
	2. weekly copies – five copies,
	3. monthly copies – five copies.
3. Backup copies are created with the use of the operating system mechanisms, database and the Avamar system.
4. The backup copies that were created are subject to verification on account of the correctness of the recording. The ISA is responsible for verifying recordings’ correctness.
5. The data recorded in the Avamar01 system are synchronized with the Avamar02 backup system located in the server room of the teaching and administrative building “CUP” (W-9) within a framework of daily data replication.
6. ISA is responsible for the implementation of replacement activities in case when such activities are necessary due to a breakdown of the IT system. After resuming the IT system, ISA conducts tests of the system’s operation correctness before returning it to the user.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **7. Storage of information data carriers containing data and backup copies** | Procedure No.: 7version: 01 |

1. Personal data are processed in accordance with the purpose and for a specified period of time justified by the purpose for which they are processed. After the above purpose and time expires, data are anonymized or pseudonymized.
2. Personal data processed on dedicated servers and workstations are stored in an electronic form on drives of these systems.
3. Devices through the use of which the processing of personal data is made, should be located in the area of personal data processing, protected against access by persons unauthorized to process personal data, as well as persons not having the rights to operate them.
4. The storage of personal data on portable storage devices is allowed only in justified cases.
5. In case of withdrawal from use of a computer equipment, personal data saved on it are destroyed using specialized software for secure data removal. The appropriate ISA is responsible for data removal. If data cannot be destroyed using the software, the drive is physically destroyed.
6. External (portable) data carriers are physically destroyed with the use of a shredder dedicated for that purpose after the need to store them ceased.
7. The destruction of the data carrier is confirmed by a protocol drawn up by the person destroying the data media. The protocol is stored by ISA and is made available to the Personal Data Officer in case of an inspection.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **8. Manner of securing the IT system against the activity of a malicious software** | Procedure No.: 8version: 01 |

1. In order to secure the IT system used for processing of personal data against the activity of the harmful software, it is forbidden to:
	1. run any software which was not confirmed as fit for use by PK without the consent of ISA,
	2. use portable storage devices without permission,
	3. open electronic mail, title of which does not imply a connection with the performed official duties (in doubtful cases a person should consult his direct superior),
	4. send internal correspondence via electronic mail without encryption and digital signing of a message,
	5. access websites not related to performed official duties and, in particular, websites not owned by reliable organizations or entities.
2. In case of detecting signs which may indicate presence of a harmful software, the employee is obliged to promptly notify ISA of this fact.
3. The above signs include:
	1. Substantial slow-down of an IT operating system,
	2. abnormal performance of the application,
	3. abnormal notifications,
	4. data loss or modification of data.
4. The IT system used for processing of personal data is secured against the activity of harmful software by:
	1. a centrally managed antivirus system,
	2. a firewall with the restrictive policy of filtering the network traffic,
	3. restricting the rights of users on workstations,
	4. updating the system software,
	5. restricting the possibility to connect third-party devices to the network,
	6. filtering URL recipients,
	7. mechanisms scanning the network for vulnerability detection.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **9. Procedure for using portable devices containing personal data** | Procedure No.: 8version: 01 |

1. Each portable device (smartphone, laptop, tablet) used for processing of personal data should be secured against access of unauthorized persons by blocking access to it with an appropriate password, PIN code or biometric access control.
2. The data stored on the portable device should be secured with the appropriate cryptographic software (such as appropriate functionality present in Android and Windows systems).
3. Regardless of access to the device, access to the programs which enable access to data should be additionally secured by a password.
4. The user of a portable device should ensure that the portable device used for processing of personal data is not left unattended (in particular, leaving it on display in a public place, on the car seat etc.)
5. Each portable device should be regularly updated.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **10. Procedure for reviewing the system, maintenance of the system and of the information data carriers used for processing of personal data** | Procedure No.: 9version: 01 |

1. The review and maintenance of the IT equipment used for processing of personal data may be carried out only by authorized PK employees and authorized external entities.
2. Maintenance work carried out at PK by external entities are subject to the direct supervision of ISA.
3. Sending IT equipment for repair outside of PK is allowed under the condition of removing media containing personal data,
4. Sending of the IT equipment is confirmed by the protocol which allows to unambiguously identify the person sending and receiving the equipment.
5. All the maintenance work carried out by external entities requires drawing up the service protocol which contains the following information:
	1. indication of the person carrying out the maintenance work and the entity of which that person is an employee,
	2. indication of the person supervising the course of maintenance work (refers to the situation when work is carried out at the PK’s headquarters),
	3. subject of maintenance work (in particular, identification of equipment in case the maintenance work concerns the equipment),
	4. range of maintenance work and its results,
	5. time in which maintenance work is carried out.
6. The originals of the protocols referred to above are stored by ISA, and the PDPO has access to them.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **11. New data sets creation** | Procedure No.: 10version: 01 |

1. The creation of a new personal data set requires permission from the Personal Data Controller of PK.
2. A person applying for the creation of a new personal data set provides the Personal Data Protection Officer with the following information:
	1. the legal basis authorizing the creation of the set,
	2. the purpose of data processing,
	3. the description of the category of persons which data concern and the range of processed data,
	4. the method of collecting and sharing data,
	5. information on the recipients or categories of recipients to whom the data may be transferred,
	6. information on the way of fulfilling the technical and organizational conditions in order to secure personal data,
	7. information regarding a possible transfer of data to a third country,
	8. list of PK’s organizational units expected to process data from this set.
3. PDC submits the application to the Personal Data Protection Officer for an opinion.
4. After receiving the favourable opinion of the application, the Personal Data Controller gives his consent to create the new set.
5. The processing of personal data in the set may take place after preparation of the record in the register of data processing operations by the PDPO.
6. The Personal Data Protection Officer enters the new personal data set processed at PK into the register.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **12. Sharing personal data of HMS with third parties** | Procedure No.: 11version: 01 |

1. Sharing personal data with third parties may take place only with the consent of the Personal Data Officer. The consent may of be one-off or permanent character.
2. The consent of PDC - PK Rector should be expressed in writing.
3. The person sharing data enters information concerning the entity with which data has been shared, the scope of the shared data and dates when the data were shared into the HMS system.
4. The transfer of data to the state authority or to the local government authorities in connection with the conducted proceedings is not subject to the record referred to in point 3. The above transfer does not constitute sharing within the meaning of the GDPR.
5. Sharing of personal data is recorded in the HMS system in the field:
	* “Any data of student” in case of data concerning students or candidates for studies and graduates of the Cracow University of Technology,
	* “Any data of employee” in case of data concerning employees of the Cracow University of Technology,
	* “Any data” in case of data concerning dormitory tenants.

|  |  |  |
| --- | --- | --- |
| pklogo NB-c | **The instruction for managing the IT system used for processing of personal data at the Cracow University of Technology** | Release date: 25.05.2018 |
| **13. Infringement of legal rules of personal data protection**  | Procedure No.: 12version: 01 |

The rules of conduct in case infringement of the protection of personal data is confirmed:

1. Cases classified as the infringement or the justified suspicion of the infringement of the personal data protection system are, among others:
	* the infringement or attempts to breach the integrity of personal data processed, both in traditional and electronic form, understood as any modification,
	* the use of illegal applications or illegal software components,
	* the significant disruption of workflows of procedures ensuring the protection of personal data processing (e.g. no possibility to enter the required document or confirmation of such operation), the appearance of an appropriate emergency message from these procedures (e.g. loss of access to data),
	* transmission of personal data to an unauthorized person,
	* unauthorized access or attempt to access rooms where personal data are processed,
	* disclosure of individual passwords to access personal data,
	* making of unauthorized copies of personal data,
	* change or removal of data saved on backup security copies or archival backup copies,
	* loss of the carrier containing personal data,
	* inappropriate destruction of personal data carrier allowing to be read,
	* inappropriate environmental conditions, such as temperature, humidity of the room in which the personal data are processed,
	* other situations indicating or confirming the infringement of security of personal data.
2. The person authorized to process personal data in every case of the infringement or justified suspicion of the infringement of the personal data protection system is obliged to:
	* refrain from commencing or continuing work, as well as from taking any action which could cause an obliteration of traces or evidence, secure the components of the IT system, secure paper documents until the Personal Data Protection Officer arrives,
	* promptly inform his direct superior and the Personal Data Protection Officer at PK about this.
3. The Personal Data Protection Officer draws up a report on the course of the event. The copy of the report is promptly provided to the Rector. The Personal Data Protection Officer takes measures to liquidate the infringements of the personal data protection system and to prevent them from occurring in the future.

# The persons authorized to process personal data may continue to work only after obtaining a permission from the Personal Data Protection Officer.

(form concerning the documentation of the infringement, the record of infringements are published on SIP.)