Appendix no.1 to the Ordinance no.30
of the Rector of the Cracow University of Technology
of May 21, 2018.



Personal Data Protection

Policy of Cracow University of Technology

**I. The subject of Policy**

Legal basis:

* Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals in relation to the processing of the personal data and on the free movement of such data, as well as repealing the Directive 95/46/WE/ General Data Protection Regulation – (GDPR) (Official Journal of EU of 4.5.2016 No. L.119, p88).
* The Act of 10 May 2018 on the protection of personal data,
1. The subject of Personal Data Protection Policy of the Cracow University of Technology
2. Policy of the Personal Data Protection defines the management rules and the procedure for the security of processing personal data.
3. The Authorities of the Cracow University of Technology (PK) are aware of the importance of problems related to the protection of personal data and declare the intention to take all necessary actions to protect the rights and justified interests of individuals related to the security or personal data processing.

2. General Security Bylaws obligatory to processing the personal data

1. Every employee of PK is obliged to protect personal data at their workplace and can bear responsibility for their actions or omissions.
2. PK employees that process personal data are obliged to secure materials that contain personal data in a way that prevents unauthorized disclosure of data, unauthorized access, not allowed: duplication, modifications, destruction, loss, incorrect use or theft.
3. Employees who have access to personal data cannot disclose them.
4. The transfer of personal data within the internal PK structure may only take place between authorised units.
5. Documents that contain personal data should be stored in lockers.
6. While processing personal data in a paper form, PK employees are obliged not to leave materials that contain personal data in a place that enables physical access to unauthorized people.
7. PK employees are obliged to close and secure access to all rooms where personal data are processed, during their temporary absence in the work room and after its completion (so-called clean desk).
8. PK employees who process personal data using equipment such as, for instance, computers are required to maintain carefulness while using it.

**II. Personal data processing area**

|  |  |  |
| --- | --- | --- |
| **No.** | **Address** | **Name of the building, number and marking** |
| 1. | Kraków, 24 Warszawska Street  | Wydział Inżynierii Lądowej (Civil Engineering Department), building nr 10-20 (W-1) |
| 2. | Kraków, 24 Warszawska Street  | Wydział Inżynierii Środowiska (Environment Engineering Department), building nr 10-19 (W-2) |
| 3. | Kraków, 24 Warszawska Street  | Wydział Inżynierii Elektrycznej I Komputerowej (Electric and IT Engineering Development), building nr 10-21 (W-3) |
| 4. | Kraków, 24 Warszawska Street  | PK Library, building nr 10-22 (W-4) |
| 5. | Kraków, 24 Warszawska Street  | Library Pavilion, the reading room, building nr 10-28 (W-6) |
| 6. | Kraków, 24 Warszawska Street  | “Detention” Building, building nr 10-45 (W-8) |
| 7. | Kraków, 24 Warszawska Street  | Didactic-administration building – “CUP” , building nr 10-24 (W-9) |
| 8. | Kraków, 24 Warszawska Street  | Architecture Department, building nr 10-25 (W-10) |
| 9. | Kraków, 24 Warszawska Street  | Wydział Inżynerii I Technologii Chemicznej (Chemical technology and Engineering Department), building nr 10-35 (W-12) |
| 10. | Kraków, 24 Warszawska Street  | Instytut Materiałów I Konstrukcji Budowlanych (The Institute of Building Materials and Construction), building nr 10-29 (W-13) |
| 11. | Kraków, 24 Warszawska Street  | Didactic- Administration Building – “Houston”, building nr 10-34 (W-15) |
| 12. | Kraków, 24 Warszawska Street  | Międzywydziałowe Centrum Edukacyjno-Badawcze Politechniki Krakowskiej (Educational-Research Inter-faculty Centre of the Cracow Unversity of Technology) – „Działownia”, building nr 10-61 (W-23) |
| 13. | Kraków, 24 Warszawska Street  | Małopolskie Laboratorium Budownictwa Energooszczędnego (Laboratory of Energy Efficient), building nr 10-65 (W-24) |
| 14. | Kraków, 24 Warszawska Street  | Building of the gallery “Gil”, building nr 10-36 (W-7) |
| 15. | Kraków, 1 Podchorążych Street  | Cadet school building, building nr 11-1 (PP-1) |
| 16. | Kraków, 1 Kanoniczna Street  | Institute Building A-1, building nr 14-1 (KN-1) |
| 17. | Kraków, 17 Kamienna Street  | Sports Hall, building nr 16-1 (HS-1) |
| 18. | Kraków- Czyżyny, 37 Jana Pawła II avenue  | The building of Mechanical Department A, building nr 17-1 (CZ-A) |
| **No.** | **Address** | **Name of the building, number and marking** |
| 19. | Kraków- Czyżyny3,5,7,9 Skarżyńskiego Street  | Student HousesNr 1 - building nr 21-1 (DS-1)Nr 2 - building nr 21-2 (DS-2)Nr 3 - building nr 21-3 (DS-3)Nr 4 - building nr 21-7 (DS-4) |
| 20. | Kraków-Czyżyny, 2 Skarżyńskiego Street  | Assistant’s House, building nr 21-6 (DS-5) |
| 21. | Kraków, 1 Skarżyńskiego Street  | School Canteen, building nr 21-4 (DS-6) |
| 22. | Kraków, 19 Bydgoska Street  | DS Bydgoska, building nr 20/1A (B-1) |
| 23. | Kraków, 114 Juliusza Lea Street  | Office building A, building nr 18-1 |
| 24. | Kraków, 114 Juliusza Lea Street | Office building B, building nr 18-2 |

**III. Personal dataset, applications used for processing**

Collections of personal data that are processed at the Cracow University of Technology:

* PK employees,
* PK pensioners, PK retired people,
* PK employee organizations, student organizations and associations in PK,
* Civil law contracts,
* Recruitment for PK studies,
* PK students,
* Participants of courses and trainings,
* PK graduates
* PK Library users,
* PK correspondence register,
* PK websites,
* Contractors,
* PK gallery,
* Residents of Student House Estate, Assistant’s House and PK guest rooms,
* Electronic Platform of Competence Analysis,
* Users of an interdisciplinary multilingual dictionary.

Personal datasets are processed in paper files, registers and in electronic forms – HMS system



Legend:

* Moduły HMS - HMS modules
* Moduły eHMS – eHMS modules
* Aplikacje zewnętrzne – outside applications
* Akademicki System Archiwizacji Prac – Academic Archivic Work System
* POL-on / GUS
* Legitymacje OPTICamp Perso (ELS/ELD) – ID cards OPTICamp Perso (ELS/ELD)
* Banki – banks
* LDAP
* Gospodarka materiałowa HMS/geem –HMS/geem material economics
* Środki trwałe HMS/este, jHMS/gest – Fixed assets HMS/este, jHMS/gest
* Obsługa transportu jHMS/trans – jHMS/trans Transport service
* NIeruchomości jHMS/goni – jHMS/goni real estate
* Sttudium języków obcych HMS/djos – foreign languages studies HMS/djos
* Obsługa toku studiów HMS/dsys, jHMS/dsys – Service of studies process HMS/dsys, jHMS/dsys
* Osiedle studenckie HMS/dees – Student House Estate HMS/dees
* Płatności masowe HMS/dkas – Mass Payments HMS/dkas
* Wynagrodzenia osobowe HMS/ plac – Individual salary HMS/plac
* Kadry HMS/kadr, jHMS/kadr – Human Resources HMS/kadr, jHMS/kadr
* Finanse i księgowość HMS/efka – finances and accountancy HMS/efka
* Bezosobowy fundusz wynagrodzeń HMS/bfpl – Impersonal payment fund HMS/bfpl
* Działalność socjalna uczelni jHMS/soc – university’s social activities jHMS/soc
* Kasa zapomogowo-pożyczkowa HMS/kazp – Assistace and Loan Fund HMS/kazp
* Limity i budżetowanie jHMS/limi – Limits and Budgeting jHMS/limi
* Rekrutacja eHMS/irka – Recruitment eHMS/irka
* Wirtualny dziekanat eHMS/dsys – Virtual Dean’s office eHMS/dsys
* Pensum eHMS/pens – workload eHMS/pens
* Wirtualne kadry eHMS/kadr – Virtual HR eHMS/kadr
* Wirtualne limity eHMS/limi – Virtual Limits eHMS/limi.

**IV. Register of personal data processing activities**

1. The register of data processing activities is a comprehensive record of all operations carried out on personal data at the Cracow University of Technology.

2. The register contains the following information:

* Administrator’s contact details,
* Purposes of data processing,
* Description of the categories of people that data concern,
* Description of the categories of personal data that are processed,
* Categories of recipients to whom personal data have been or will be disclosed,
* Recipients in the so-called third countries or in international organizations,
* When the above applies – information concerning transfer of personal data to a third country or international organisation, include the name of this third country or international organisation, and in the case of transfers referred to art. 49. sec. 1 second paragraph of GDPR, also documentation of appropriate security,
* Planned dates to delete some of the individual categories of data,
* General description of technical and organizational security, in accordance with the requirements of art. 32 sec. 1 of GDPR.

3. The register of data processing activities is kept in electronic format.

4. Every head of an organizational unit at the Cracow University of Technology is obliged to submit an up-to-date register of data processing activities to the Personal Data Protection Officer once a year. The electronic version of the template of the register of data processing activities is available at PK Employee Information Service, in the Personal Data Protection tab.

5. Personal Data Protection Officer keeps a central register of personal data processing activities on behalf of the personal data administrator (The Rector of PK).

**V. Personal data protection risk management**

**Data Protection Action Assessment**

If a given type of processing – especially with the use of new technologies – due to its nature, context and purposes, is likely to cause a high risk of violating the rights or freedoms of natural persons, the local personal data administrator (LODO) before starting the processing, will assess the effects of the planned processing operations for the protection of personal data(art. 35 sec. 1 g).

**The assessment includes at least:**

a) **a systematic description of the planned processing operations and processing purposes**, including, the legitimate interests pursued by the controller,

b) **assessment of whether the processing operations** are necessary and proportionate to the purposes,

c) **assessment of the risk of violating the rights or freedoms** of individuals,

d) **the measures planned to manage the risk**, that include as well the safeguards and security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation.

**The expected outcome of the assessment**

The effect of the assessment considering the nature, scope, context and purposes of processing, as well as the risk of violating the rights and freedoms of individuals with different probabilities and severe threats, is **the implementation by the local controller (LADO) correct technical and organizational measures** to ensure that the processing is carried out in accordance with GDPR. These measures, if necessary, are reviewed and updated.

**Definition of the processing context**

The purpose of the processing context is to define and document:

1. the character of the processing of personal data,
2. the scope of processing in relation to the purposes, for which the data is processed,
3. the context, in which the personal data was collected,
4. purpose of processing,
5. recipients and processors of personal data,
6. the period of personal data storage,
7. processing operations,
8. assets used for processing information.

Types of data processing operations that can cause high risks:

1. assessment or scoring, including profiling,
2. automatic decision-making with legal or similar affect,
3. systematic monitoring,
4. sensitive personal data,
5. data processed on a large scale,
6. datasets that have been matched or combined,
7. depriving individuals of their rights and freedoms or the ability to control their personal data,
8. innovative use or practice of technological or organizational solutions,
9. transfer the data outside the European Union.

**Assessment of necessity and proportionality of data processing**

In order, to assess the necessity and proportionality of data processing, it is important to verify and document whether:

1. personal data is collected for specific, explicit and legitimate purposes,
2. personal data is processed in accordance with the law,
3. personal data is adequate, relevant and limited to what is necessary in relation to the purposes for why they are processed,
4. the time of data storage has been limited,
5. in the case of data collection, appropriate means are provided with any information for the person whom data concern,
6. the number of data recipients was limited.

**Analysis and assessment of assets used for processing operations**

As part of the data processing, it is important to identify and make an inventory of assets or group of assets that are used for personal data processing operations.

These are the following types of assets:

1. **processes and activities** – a series of related activities or tasks that implement personal data processing operations or lead to achieving the purpose of data processing,
2. **personnel** – all groups of people involved in the data processing: decision makers, users, operation/maintenance personnel, software developers,
3. **equipment** – all physical devices in the organisation: portable, stationary, peripheral devices, data carriers
4. **headquarters** – all locations used for data processing and physical resources needed for them to function: headquarters, safety zones, municipal and technical services,
5. **software** – all programs involved in the data processing operations: operating systems, business applications; service, maintenance or administration software,
6. **network** – all telecommunication devices used to connect many physically distant computers or elements of the information system: media and supporting services, active or passive relays, communication interfaces,
7. **organisation** – all human structures assigned to the processing of personal data and procedures controlling these structures: authorities, organization structure, subcontractors, suppliers, manufacturers,
8. **information** – data processing in paper or electronic version.

**Analysis and risk assessment of assets used for processing operations**

Threats that may affect the violation of the rights and freedoms of individuals should be assigned to the identified assets and/or group of assets used for data processing operations. A threat should be consider as a potential cause of an undesirable incident that may result in a violation of the rights and freedoms of individuals.

|  |
| --- |
| **The name of the threat** |
| **Physical damage** |
| **Loss of essential services** |
| **Violation of rights and freedoms of individuals** |
| Accidental or illegal destruction of data |
| Loss of data |
| Unauthorized modification of data |
| Unauthorized disclosure of data |
| Unauthorized access to the processed data |
| Unauthorized access to stored data |
| Unauthorized data processing |
| **Violation of information security** |
| Interception of signals due to the incident of interference |
| Remote spying |
| Wiretap  |
| Theft of media or documents |
| Theft of devices |
| Recycling from reused or discarded media |
| Disclosure  |
| Data from unreliable sources |
| Manipulation of the device |
| Falsify the software |
| Location detection |
| **Technical failures** |
| Failures of devices |
| Devices malfunction |
| Information system overload |
| Software malfunction |
| **Unauthorized activities** |
| Unauthorized use of devices |
| Unauthorized software copying  |
| Use of false or copied software |
| Data corruption |
| **Violation of function security** |
| Illegal data processing |
| Usage error |
| Violation of rights |
| Falsification of rights |
| Activities denied |
| Violation of staff availability |
| **Personal threats** |
| Hacker (system hack) |
| Computer Criminal (cyber stalking, impersonation) |

**Analysis and assessment of effects of the materialisation of threats**

For each threat identified as a part of the assets or/and group of assets that are used for data processing operations, the impact (effects) on the materialization of threats should be analysed in the context of violation of right and freedoms of natural persons.

|  |  |
| --- | --- |
| **No.** | **Catalogue of the effects of violation of the rights and freedoms of individuals** |
| 1 | Discrimination |
| 2 | Identity theft or identity fraud  |
| 3 | Financial loss |
| 4 | Violation of a good name |
| 5 | Violation of confidentiality of personal data protected by a professional secrecy |
| 6 | Unauthorised reversal of pseudonymization  |
| 7 | Any other significant, economic or social damage |

|  |
| --- |
| **Assessment of the effects of the violation of rights and freedoms of individuals** |
| **Value** (S) | **Name** | **Description** |
| 3 | High | The consequences can lead to high physical, material or non-material damage. |
| 2 | Low to medium | The consequences can lead to physical, material or non-material damages for individuals; however they are not high.  |
| 0 | Not applicable | These effects in the context of materialisation of the analysed threat, do not occur.  |

**Analysis and assessment of vulnerability of assets used for processing operations**

Vulnerabilities should be assigned to each threat identified withing an asset and/or group of assets used for data processing operations. Vulnerability should be understood as a source of threat, weakness or vulnerability in assets or security that can be used to materialize the threat.

|  |  |
| --- | --- |
| Types of assets | Example of vulnerability |
| Organisation | No developed, updated, tested business continuity plans |
| No technical documentation of the systems |
| No documentation required by law  |
| No list of authorized people to access the processing of personal data |
| No access procedures to the premises  |
| No developed or updated operating procedures |
| No procedures of data and software changes |
| No procedure for monitoring the use of information processing devices  |
| No established mechanisms to monitor security violation |
| No security requirements in the development processes  |
| Poor procedures of control changes |

|  |  |
| --- | --- |
| Network | No security of telecommunication lines |
| No security of personal data transmission |
| Transmissions of passwords in clear forms |
| Software | No updates of software (network services and operating systems) |
| No control of software download |
| Lack of or insufficient software testing procedures |
| No identification of authentication mechanisms |
| No mechanisms for monitoring the user activity (event loggings) |
| No formulated security requirements for the created applications  |
| Insufficient password management (easy to guess passwords) |
| Storage of passwords in clear forms, insufficient frequency of password changes |
| No control of copied data |
| Improperly configured applications, services or operating systems |
| Complicated user interface |
| Use of services commonly recognized as not guaranteeing security |
| Known errors (holes), vulnerabilities in software or databases |
| No regular audits |
| Personnel | No regular supervision procedures |
| No safety requirements at workstations |
| Lack of responsible people for systems, processes and resources |
| Incorrect allocation of access rights |
| Work of employees as external entities without supervision |
| Keeping a copy in the place of production |
| Absence of the personnel |
| No “clean desk and screen” policy |
| No logout when leaving the workplace |
| No security training |
| Equipment | No testing of power devices |
| No alternative connection rules |
| No backup/archive |
| Improper preparation to reuse the media  |
| Improper disposal of media |
| Improper wiring protection |
| Single point of damage (no reserve)  |
| Headquarters | No electronic access control |
| Lack of physical security of buildings, doors and windows |
| No guaranteed power supply |

|  |
| --- |
| **Assessment of possibilities to use the vulnerabilities** |
| **Value** *(PPod)* | **Name** | **Description** |
| **3** | Very susceptible | The vulnerability occurs often over a year or on a regular basis. |
| **2** | Susceptible | The vulnerability occurred in the last year or occurs irregularly.  |
| **1** | Not very susceptible | The vulnerability has not occurred in the last 2-3 years (could have happened earlier). |
| **0** | Invulnerable  | The vulnerability has not been reported. |

**Assessment of the possibility of materializing the threat**

Each threat identified as a part of assets or/and group of assets used for processing operations, considering the identified vulnerabilities and existing security measures, should be assessed in the context of rights to the similarity of the materialisation of the threat.

|  |
| --- |
| **Assessment of the possibility for threats to occur** |
| **Value (S)** | **Name**  | **Description**  |
| **5** | Almost certain | There are reasonable reasons to judge that the threat will happen in the near future (almost 90%). |
| **4** | Highly probable | There are reasonable reasons to judge that the threat is likely to occur, there is more than a half chance to occur. It has happened over the last year.  |
| **3** | Very probable | The occurrence of the threat is real but does not exceed 50% of the probability. It happened sporadically in the past (in the last 2 years). |
| **2** | Medium probability | The threat may occur sporadically. It happened sporadically in the past (in the last 3 years). |
| **1** | Low probability | The threat is unlikely to occur, or the possibility of its occurrence is negligible (close to zero). The threat has not happened in the past. |

**Assessment of the seriousness of the risk of violation the rights and freedoms of natural persons**

The assessment of the seriousness of the risk of violation the rights and freedoms of natural persons can be calculated on the basis of the following formula:

𝑹 = 𝑺 ∗ 𝑷𝑷𝒐𝒅 ∗ 𝑷𝑷𝒃

Where:

* *R* – assessment of the seriousness of the risk of violation the rights and freedoms of individuals
* *S* – Assessment of side effects of the violation of rights and freedoms of individuals
* *PPod* – Assessment of vulnerability of assets used for processing operations
* *PPb –* assessment of possibility of materializing the threats

|  |  |
| --- | --- |
| Assessment of possibility | Assessment of side effects x assessment of vulnerability |
|  | 2 | 3 | 4 | 6 | 9 |
| 1 | 2 | 3 | 4 | 6 | 9 |
| 2 | 4 | 6 | 6 | 12 | 18 |
| 3 | 6 | 9 | 12 | 18 | 27 |
| 4 | 8 | 12 | 16 | 24 | 36 |
| 5 | 10 | 15 | 20 | 30 | 45 |

|  |  |  |
| --- | --- | --- |
| Level | Value scale | Description |
| Low risk | From 2 to 16 | Acceptable risks, no further actions required |
| High risk | From 18 to 45 | Unacceptable risks, required actions to manage the risk |

**Risk handling**

The purpose of managing the risk is to choose a risk management option and to plan organizational and technical safeguards to ensure the protection of personal data and to show compliance with GDPR, considering the rights and legitimate interests of individuals whom the data concerns.

Legend:

Punkt decyzyjny ryzyka 1/2 – risk decision point

Wyniki szacowania ryzyka – result of estimated risk

Szacowanie satysfakcjonujące – Satisfied estimation

Warianty postępowania z ryzykiem – options to manage the risk

Redukowanie ryzyka – risk reduction

Zachowanie ryzyka – risk behaviour

Unikanie ryzyka – risk avoidance

Przeniesienie ryzyka – risk tranfer

Ryzyka szczątkowe (rezydualne) – residual risks

Postępowanie satysfakcjonujące – Satisfying conduct

**Informing about risk and consultation**

In the process of informing about risk and consultation, the parties that should take part in every stage of the personal data protection risk management process are:

a) personal data controller

b) personal data protection officer

c) owners of resources used to carry out personal data processing operations

d) owners of processes responsible for verifications:

* Compliance with legal requirements and internal regulations
* The effectiveness of implementation and maintaining personal data protection in organisation.

**Consultation with the supervisory authority**

If carrying out the risk management, after applying risk minimization measures related to:

a) the necessity and proportionality of data processing,

b) high risk of violation the rights and freedoms of natural persons,

is still not possible to reduce the risk to an acceptable level and ensure compliance and requirements of GDPR, the personal data administrator must consult the President of the Office for Personal Data Protection before the start of the process.

**Monitoring and review of the risk**

Monitoring and review of the personal data protection mechanisms should be carried out at every stage of the personal data protection risk management process:

1. Verification whether the context of data processing has not changed or its modifications were planned e.g. implementation of a new technology or business solutions, which may result in the implementation of new data processing operations and/or modifications of assets used for data processing,
2. Verification if the processing operations that are excluded from carrying out the assessment of side effects, do not currently occur a high risk of violation of the rights and freedoms of individuals,
3. Verification whether the supervisory authority established a new or updated list of types of processing operations, subjected or not subjected to the requirements to conduct a data protection effects assessment,
4. Verification whether the conditions that contribute to the necessity and proportionality of data processing, have not changed or are planned to change,
5. Verification whether the identified risks of violating the rights and freedoms of individuals are still adequate,
6. Verification whether the applied security measures and/or limitation of data processing are effective and still have an impact on minimizing the risk.

**Diagram of the protection risk of personal data management**

Legend:

* Kontekst przetwarzania danych (art. 35, sec.7, letter a) – Context of processing data (art.35, sec. 7, letter A)
* Monitorowanie i orzegląd ryzyka (art. 35, sec. 11) (art.39, sec. 1c) – monitoring and risk management (art. 35, sec. 11) (art.39, sec. 1c)
* Informowanie o ryzyku i konsultacje (art.35, sec. 1,2,9) – information about the risk and consultation (art. 35, act 1,2,9)
* Ocena konieczności i proporcjalności przetwarzania danych ( art.35, sec.7, letter b) – assessment of necessity and proportionality of data processing (art.35, sec. 7, letter b)
* Ocena ryzyka naruszenia praw i wolności osób fizycznych (art.37, sec.7, letter c) – assessment of the risk of violation of rights and freedoms of natural persons (art.37, sec. 7, letter C)
* Postępowanie z ryzykiem (art.35, sec.7, letter d) – risk management (art. 35, sec. 7, letter d)
* Czy rodzaj operacji prztwarzania danych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? (art.35 sec. 1,3,4) – Can the type of data processing operation cause high risks of violating the rights and freedoms of individuals (art.35 sec. 1,3,4)
* Czy rodzaj operacji przetwarzania danych zwolniony jest z przeprowadzenia oceny skutków dla ochrony danych? (art.35, sec.5, 1O) – Is the type of data processing operation discharged from conducting the assessment of effects for data security?
* Czy ryzyko jest akceptowane? – Is the risk acceptable?
* Czy ryzyko szczątkowe jest akceptowane? – Is the risk residually acceptable?

**Assessment of the risk for violation of rights and freedoms of natural persons**

Legend:

* Analiza I ocena aktywów wykorzystywanych do operacji przetwarzania – Analysis and assessment of assets used for processing operations
* Analiza i ocena zagrożeń aktywów wykorzystanych do operacji przetwarzania - Analysis and assessment of threats of assets used for processing operations
* Analiza i ocena podatności aktywów wykorzystanych do operacji przetwarzania - Analysis and assessment of vulnerability of assets used for processing operations
* Analiza i ocena skutków urzeczywistnienia się zagrożeń - Analysis and assessment of effects of materializing of threats
* Ocena prawdopodobieństwa urzeczywistnienia się zagrożenia – Assessment of the possibility of materilalizing of the threat
* Ocena powagi ryzyka naruszenia praw i wolności osób fizycznych – Assessment of seriousness of risks of violation the rights and freedoms of individuals
* Czy ryzyko jest akceptowalne? – Is the risk acceptable?
* Monitorowanie i przegląd ryzyka – Monitoring and review of the risk
* Postępowanie z ryzykiem – Risk management.

**VI. Measures ensuring the confidentiality, integrity and accountability of the processed personal data**

**1. Organisational protection mechanisms:**

1. appointment of Local Personal Data Controllers,
2. appointment of a Personal Data Protection Officer,
3. appointment of Information Technology System Administrators,
4. PK personal data security Policy
5. Instruction for the management of a system for processing personal data
6. records of people authorised to process personal data,
7. register of personal data processing activities,
8. register of categories of personal data processing activities,
9. register of breach.

**2. Logical protection mechanisms:**

1. user certifying mechanisms with the use of passwords,
2. accountability mechanisms for user transactions,
3. backup tools,
4. firewall software,
5. remote connections via VPN,
6. limitation of user rights on workstations,
7. a centrally managed antivirus system,
8. system software update using the WSUS mechanism and the local repository Centos.

3. Physical protection mechanisms:

1. access to the HMS server room for authorised persons only,
2. a forced entry and assault alarm system in the HMS server room,
3. the HMS server room is located in a building protected 24 hours a day,
4. security of the room where paper files (figures, records) are processed in lockable cabinets.

The personal data Administrator shall apply technical and organisational measures to ensure the protection of personal data processed appropriate to the risks and categories of data to be protected, applying and referring in particular to the risk assessment made.

**VII. Administrators’ duties and responsibilities**

**Duties of the Local Personal Data Administrator (LPDA)**

The Local Personal Data Administrator shall be directly subordinate to the PK Personal Data Administrator and shall follow the recommendations of the Personal Data Protection Officer in the area of personal data protection. The Local Personal Data Administrator is obliged to apply technical and organisational measures to ensure the protection of the processed personal data appropriate to the risks and categories of data to be protected in subordinate organisational units. Furthermore, the Local Personal Data Administrator shall safeguard personal data against unauthorised access, against carrying away by an unauthorised person, processing in breach of the Personal Data Protection Act, alteration, damage or destruction. The Local Personal Data Administrator is also specifically responsible for:

1. authorising the processing of personal data - granting and revoking authorisations,
2. appointment of Information Technology System Administrators,
3. monitoring of compliance with the rules on the processing of personal data,
4. initiating and undertaking measures to improve data protection,
5. cooperation with the Personal Data Protection Officer in the field of personal data protection.

**2. Duties of Information Technology System Administrator (ITSA)**

Information Technology System Administrator is responsible for:

1. granting and revoking authorisations to system users on the basis of authorisations issued or revoking authorisations and entitlements,
2. supervising the correctness of personal data security mechanisms in the IT system,
3. analysis of performance of the IT system that processes personal data in order to detect potential threats to the personal data being processed,
4. proper security of backups,
5. controlling repairs and maintenance of hardware and software used to process personal data to be carried out in a safe manner,
6. maintaining the confidentiality of information relating to the protection of personal data, in particular data from personal data files. This obligation is also valid after the termination of employment.

**VIII. Personal Data Protection Officer’s duties and responsibilities (PDPO)**

Personal Data Protection Officer is responsible for supervising the compliance of PK employees with the principles of personal data processing protection at PK.

Personal Data Protection Officer reports directly to the Rector and is required to do the following:

1. to inform the Personal Data Administrator and employees who process personal data of the obligations incumbent on them,
2. to monitor compliance with GDPR and data protection policies, procedures and instructions, including division of responsibilities, personal data protection awareness activities,
3. to record personal data sets,
4. to verify the conformity of the documentation (including records) with the actual state,
5. to make recommendations on the data protection impact assessment upon request and to monitor its implementation in accordance with Article 35 GDPR,
6. to cooperate with the supervisory authority - the President of Personal Data Protection,
7. to act as a contact point for the supervisory authority on processing issues,
8. to act as a contact point for data subjects in all matters relating to the processing of their personal data and to the exercise of their rights under this Regulation,
9. to run a central register of personal data processing activities,
10. to run a register of categories of activities,
11. to submit periodically (once a year) reports with conclusions of the inspections carried out to the Personal Data Administrator (Rector),
12. to take immediate action to remedy any personal data security breach identified,
13. to maintain a list of persons authorised to process personal data, taking into account their functions and powers.

**In order to ensure the independence of the Personal Data Protection Officer (PDPO), the general data protection regulation introduces several solutions:**

1. supporting the PDPO in fulfilling his/her tasks,
2. ensuring the participation of the PDPO in all data protection issues,
3. prohibiting the issuing of instructions to the PDPO as to the performance of his/her tasks,
4. avoiding conflicts of interest for the PDPO,
5. prohibition of dismissal and punishment of the Personal Data Protection Officer.

**IX. Principles of procedure for responding to data protection breaches:**

****

 *Legend to the figure:*

* *Incydent bezpieczeństwa danych osobowych* - Personal data security incident
* *Ocena, czy incydent stanowi naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 GDPR* - Assessing whether the incident constitutes a data protection breach within the meaning of Art. 4 point 12 of GDPR
* *Incydent nie stanowi naruszenia ochrony danych osobowych - działania administratora wynikające z wewnętrznych regulacji*  - Incident does not constitute a personal data protection breach - controller's actions resulting from internal regulations
* *Incydent stanowi naruszenie ochrony danych osobowych - ocena, czy naruszenie to skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych -* The incident constitutes a personal data breach - assessing whether the breach results in a risk of violations of the rights or freedoms of individuals
* *Ryzyko naruszenia praw lub wolności osób fizycznych nie występuje lub jest małe -* Little or no risk of violation of the rights or freedoms of individuals
* *Działania administratora wynikające z wewnętrznych regulacji -* Controller's actions resulting from internal regulations
* *Ryzyko naruszenia praw lub wolności osób fizycznych jest większe niż małe -* The risk of violation of the rights or freedoms of individuals is more than little
* *Zgłoszenie naruszenia do organu nadzoru -* Notification of the breach to the supervisory authority.
* *Treść zgłoszenia (art.33 sec. 3 GDPR); opisanie charakteru naruszenia; imię i nazwisko oraz dane kontaktowe inspektora ochrony danych; opisanie możliwych konsekwencji naruszenia; opis zastosowanych środków -* Content of the notification (Article 33(3) GDPR); description of the shape of the breach; name and contact details of the Data Protection Officer; description of the possible consequences of the breach; description of the measures taken
* *Ryzyko naruszenia praw lub wolności osób fizycznych jest wysokie -* The risk of violation of the rights or freedoms of individuals is high
* *Zgłoszenie naruszenia do organu nadzoru -* Notification of the breach to the supervisory authority.
* *Treść zgłoszenia (art.33 sec. 3 GDPR); opisanie charakteru naruszenia; imię i nazwisko oraz dane kontaktowe inspektora ochrony danych; opisanie możliwych konsekwencji naruszenia; opis zastosowanych środków -* Content of the notification (Article 33(3) GDPR); description of the shape of the breach; name and contact details of the Data Protection Officer; description of the possible consequences of the breach; description of the measures taken
* *Zawiadomienie o naruszeniu osoby, której dane dotyczą -* Notification of a breach to a data subject

1. Cases categorised as a breach or reasonable suspicion of a breach of the personal data protection regime include, but are not limited to:

1. breach or attempted breach of the integrity of personal data processed, whether in traditional or electronic form, understood as any modification.
2. use of illegal applications or illegal software components,
3. a significant disruption in the workflow of procedures ensuring the protection of personal data processing (e.g. impossibility to enter a required document or to confirm such operation), the appearance of a relevant alert message from these procedures (e.g. loss of access to data),
4. transfer of personal data to an unauthorised person,
5. unauthorised access or attempted access to rooms where personal data are processed,
6. disclosure of individual passwords to access personal data,
7. making unauthorised copies of personal data,
8. modification or deletion of data stored on backup copies or archive copies,
9. loss of media containing personal data,
10. other situations indicating or confirming a personal data security breach.

2. The person authorised to process personal data in any case of a breach or reasonable suspicion of a breach of the personal data protection system is obliged to:

1. immediately notify his or her line manager and the Personal Data Protection Officer,
2. refrain from commencing or continuing the work or from taking any action which might obliterate traces or evidence,
3. secure elements of the IT system,
4. secure paper documents until the arrival of the Personal Data Protection Officer.

3. The Personal Data Protection Officer shall make a report of the incident and record the incident in the breach register. A copy of the report shall be promptly forwarded to the Rector.

4. The Personal Data Protection Officer shall take steps aiming at the elimination of breaches of the personal data protection system and to prevent their occurrence in the future.

5. Persons authorised to process personal data may only proceed with the work after receiving permission from the Personal Data Protection Officer.

**X. Consequences resulting from breaches of data protection legislation:**

Administrative penalty payment in the General Data Protection Regulation (GDPR)

GDPR highlights three features of administrative penalty payments:

1) **effectiveness**, a measure of the achievement of the objective of restoring the state of compliance on the one hand and preventing future infringements on the other,

2) **proportionality.** The penalty payment is to be proportionate to the nature and other circumstances of the breach. Proportionality is assessed by the criteria set out in Article 83(2) GDPR,

3) t**he deterrent nature of the penalty** - its preventive nature, preventing similar infringements from being committed in the future.

The most important feature of penalty payments of an administrative nature is that liability arises from the mere breach of a legal obligation.

**Entity imposing a penalty payment**

The imposition of administrative penalties falls within the competence of the supervisory authority (Article 58(2) GDPR); it imposes the penalty irrespective of the application of other remedies. Remedial measures include, but are not limited to, warnings, admonitions, commandments, temporary restriction of data processing, revocation of certification. A penalty payment is an additional measure imposed on the entity in addition to any other remedial measure.

**Entities subject to penalty payments**

Penalties under GDPR will be imposed on:

1) the data controller,

2) a data processor on behalf of the controller,

3) the certifying entity

4) the monitoring entity.

**Factors influencing the decision of penalty payment and the amount of the penalty**

Article 83(2) of GDPR indicates the criteria that should guide the supervisory authority. According to this provision, the authority should take into account the following factors:

1. the nature, gravity and duration of the breach with regard to the nature, scope or purpose of the processing in question, the number of data subjects affected and the extent of the damage suffered by them,
2. the intentional or unintentional nature of the breach
3. the steps taken by the controller or the processing entity (entrustment) to minimise the damage suffered by the data subjects,
4. the degree of responsibility of the administrator or processing entity taking into account the technical and organisational measures they have implemented under Article 25 (requirement to consider data protection by design and by default) and Article 32 (implementation of security measures appropriate to the risk),
5. the degree of cooperation with the supervisory authority to remedy the breach and mitigate its possible negative effects,
6. the categories of personal data affected by the breach,
7. the way the supervisory authority instructor or processor reported the breach,
8. if corrective measures referred to in Article 58(2) GDPR (warnings, reminders, injunctions, etc.) have previously been applied to the administrator or processor concerned in the same case, compliance with these measures,
9. the use of approved codes of conduct or approved certification mechanisms;
10. any other aggravating or mitigating factors applicable to the circumstances of the case, such as the financial gains made directly or indirectly in connection with the breach or the losses avoided.

**The amount of the administrative penalty payment**

The number of penalties has been determined by indicating maximum thresholds, given in percentages and specific amounts. GDPR sets out two maximum thresholds: a higher and a lower one (depending on the category of the act). In a first step, the authority determines the amount of turnover, then calculates how much is (depending on the type of act) 2% or 4% of the annual worldwide turnover. In the next step, the authority compares the amount thus determined with the amount of €10 million or €20 million and chooses the higher of the two. The amount determined is the basis for determining the final amount of the penalty, and it is at this stage that the authority takes into account the criteria mentioned above (from Article 83(2) GDPR). Pursuant to Article 9 of the Public Finance Act of 27 August 2009 - an administrative fine of up to PLN 100,000 for public entities.

**Breach subject to a penalty payment**

**Penalties of up to €10 million** according to the lower threshold are applicable to breaches of the following obligations:

1. breach of the conditions of the child's consent in relation to the use of information society services (Article 8),
2. processing which does not require identification (Article 11); this includes the situation where data are processed when the purpose of the processing no longer requires the identification of the person,
3. no data protection by design or no data protection by default (Article 25),
4. obligations arising from joint administrative control of data (Article 26), e.g. failure to agree on the division of responsibility for carrying out specific duties
5. breach of the obligations imposed by Article 28 in relation to the processing of data on behalf of the administrator by a processor; the breach may consist, for example, of entrusting the processing to an entity that does not provide a guarantee of data security or of further entrusting the processing to another entity without the prior consent of the administrator.
6. the obligation of a processor or other person to process data only on instructions from the administrator (Article 29),
7. obligation to register processing operations (Article 30),
8. the obligation of the administrator or processor and their representatives to cooperate with the supervisory authority at the latter's request, in the performance of the authority's tasks (Article 31),
9. breach of security rules for data processing (Article 32),
10. the obligation to report the data breach to the supervisory authority (Article 33) and to notify the data subject (Article 34),
11. breach of obligations relating to the assessment of the effects of processing (Article 35),
12. failure to appoint a Data Protection Officer despite the existence of such an obligation (Article 37(1)),
13. a breach of obligations related to the status of PDPO, e.g. by failing to provide him/her with the resources necessary to perform his/her tasks (Article 38),
14. breach of certification obligations, whether by the administrator, processor or certifier (Articles 42 and 43).

**Acts punishable by a higher penalty of up to €20 million are:**

1. breach of the basic principles of data processing (Article 5),
2. processing of data without a legal basis (Article 6),
3. breach of conditions related to consent for data processing (Art. 7),
4. processing of special categories of data without a legal basis (Article 9),
5. breach of the principles of transparency of information and communication (Article 12),
6. breach of the information obligation (Articles 13 and 14),
7. violation of the person's right of access to data and information about processing the data (Article 15),
8. violation of the right of rectifying the data (Article 16),
9. violation of the person's right to erasure of his/her data ("right to be forgotten" - Article 17),
10. violation of the right to restrict data processing (Article 18),
11. violation of the right to data transfer (Article 20),
12. non -acceptance of objections to data processing (Article 21),
13. violation of the person's right not to be subject to automated decisions (Article 22),

The lower threshold of penalties applies to acts related to personal data security in the broad sense. The higher threshold of penalties applies to violations of the rights of the data subject (individual).

Notwithstanding the above, pursuant to Article 83(6) of GDPR, non-compliance with an order issued by a supervisory authority pursuant to Article 58(2) is subject to a penalty payment of up to €20 million. This refers to an order issued by a supervisory authority irrespective of the imposition of a monetary penalty.

Consequences arising from infringements of the provisions of GDPR relating to individuals- civil action prosecution:

1. where pecuniary or non-pecuniary damage has been suffered as a result of a breach of the Regulation - Article 82 (sec. 146-147),
2. violations are subject to an administrative penalty payment of up to €10,000,000, or in the case of an enterprise, up to 2% of its total annual worldwide turnover in the preceding financial year - Article 83(4).
3. violations are subject to an administrative penalty payment of up to EUR 20,000,000 and, in the case of an enterprise, of up to 4% of its total annual worldwide turnover in the preceding financial year Article 83(6).

Breach of the applicable law on confidentiality and professional secrecy, the intentional modification, loss, destruction, theft or sale of information to competitors are subject to the following criminal sanctions:

1. in the case of disclosure or use of information - criminal liability under Article 266 of the Polish Penal Code,
2. in the case of unauthorised obtaining of information - criminal liability under Article 267 of the Polish Penal Code,
3. in the case of violation of the integrity or destruction of a record of protected information - criminal liability under Article 268 of the Polish Penal Code,
4. in the event of destruction of information of special importance (state secret, university secret), there is criminal liability under Article 269 of the Polish Penal Code. In addition, the violation of the provisions of the applicable law on confidentiality and professional secrecy, the intentional modification, loss, destruction, theft or sale of information to competing companies is qualified as a grave breach of employee duties and therefore threatened with termination of the employment contract without notice.

**XI. Deletion of personal data (anonymisation and pseudonymisation)**

**Data anonymisation** is the transformation of personal data, after which individual personal or material information can no longer be attributed to a specific or identifiable individual.

**Pseudonymisation** involves replacing one attribute (generally an atypical attribute) in a record with another attribute. Therefore, there is still a likelihood of indirectly identifying an individual.

In the context of the application of GDPR, it is highlighted that pseudonymisation can be one method of securing data. It reduces the risk to data subjects and helps to meet the administrator's data protection obligations.

The main difference is that t**he effect of anonymisation is to make it irreversibly impossible to identify a person**. In contrast, **with pseudonymisation, there is still a likelihood of indirectly identifying an individual.**

**The right to be forgotten**

Article 17(1) of GDPR gives the right to erasure data, known as the 'right to be forgotten', whereby the data subject has the right to request from the administrator the immediate erasure of his/her personal data and the administrator is obliged to erase the personal data without undue delay. These processes must be permanent, irreversible and carried out within a foreseeable period of time, which is as short as possible from the receipt of the request for erasure of personal data. The right to be forgotten does not apply to data whose processing is necessary:

1. to exercise the right to freedom of expression and information,
2. to comply with a legal obligation requiring the processing under Union law or the law of a Member State to which the administrator is subject, or to perform a task carried out in the public interest or in the exercise of official authority vested in the administrator,
3. for reasons of public interest in the field of public health,
4. for archiving purposes in the public interest, for scientific or historical research or for statistical purposes,
5. to establish, exercise or defend claims

Legal bases allowing personal data to be stored after the end of the purpose:

1. the Labour Code of 26 June 1974 (Journal of Laws 2018, item 108, as amended),

2. Law on Higher Education of 27 July 2005 (Journal of Laws 2017, item 2138, as amended),

3. the Regulation of the Minister of Science and Higher Education on the documentation of the course of studies of 16 September 2016. (Journal of Laws of 2016, item 1554, as amended),

4. Accounting Act of 22 June 2016. (Journal of Laws of 2018, item 395, as amended),

5. Tax Law of 29 August 1997 (Journal of Laws of 2018, item 800),

6. Law on the National Archive and Archive Resources of 14 July 1983 (Journal of Laws of 2018, item 217),

7. Penal Code of 6 June 1997 (Journal of Laws of 2017, item 2204),

8. Ordinance No. 82 of the Rector of PK of 14 December 2017 on the introduction of the Registry and Archives Regulations at PK.

**XII. Agreement on entrustment of personal data processing**

The controller shall entrust the processing of personal data only to processors that provide sufficient guarantees, in particular in terms of expertise, reliability and resources, of the implementation of technical and organisational measures that comply with the requirements of GDPR.

The scope of the basic provisions that will have to be included in the agreement on entrustment of personal data processing.

In accordance with the wording of Article 28(3) GDPR, the agreement must contain the processor's obligations according to which:

1. the processor shall only process personal data on the documented instructions of the administrator,
2. the processor shall ensure that persons authorised to process personal data commit themselves to secrecy or are subject to an appropriate statutory secrecy obligation,
3. the processor shall take all measures required pursuant to Article 32 of GDPR,
4. taking into account the nature of the processing, assist the administrator, as far as possible, by appropriate technical and organisational measures, to fulfil the obligation to respond to the data subject's requests for the exercise of his/her rights,
5. taking into account the nature of the processing and the information available to him/her, the processor shall assist the data administrator in complying with the obligations set out in Articles 32 to 36 of GDPR
6. upon termination of the processing services at the discretion of the Administrator, the processor shall erase or return to the Administrator any personal data and delete any existing copies thereof, unless Union or Member State law requires the continued storage of such personal data,
7. the processor shall make available to the controller all information necessary to demonstrate compliance with personal data protection obligations.

**XIII Online services**

The provisions of GDPR are intended to protect users of online services (websites, e-shops, apps and social networks) in all kinds of IT systems from the misuse of collected personal data.

Cracow University of Technology, as the owner of online services that process personal data, ensures the security of data processing for our users in accordance with GDPR.

Managers of organisational entities of Cracow University of Technology who are substantially responsible for online services where personal data are processed are obliged to monitor and make necessary amendments to online service bylaws and privacy policies to comply with the applicable legislation.

Information about the legal owner of the website and privacy policy clauses should be included in the footer of the website.

Service owners (substantively responsible managers of PK units) complete a register of categories of personal data processing activities once a year in accordance with Article 30(2) of GDPR (a template of the register of categories of personal data processing activities is available in the SIP PK)

**XIV. Employee Organisations, Student Organisations and Associations**

Organisations of Cracow University of Technology employees - trade unions active at PK (NSZZ Solidarność, ZNP), Employee Loan and Benefit Fund and student organisations, the Cracow University of Technology Alumni Association are obliged to apply the principles of personal data protection in accordance with GDPR, introduced by an ordinance of the Rector of Cracow University of Technology, and legislation according to the regulations of which they are based.

The collection of personal data of members of the above organisations is processed in paper and electronic format.

**XV. Information and consent clauses**

Information clause - general model

In accordance with Article 13(1) and (2) of the General Data Protection Regulation of 27 April 2016. (GDPR)\*[[1]](#footnote-1) it is informed that:

1. the controller of your personal data is Tadeusz Kościuszko Cracow University of Technology based in Cracow, ul. Warszawska 24, 31-155 Cracow,
2. contact with the Data Protection Officer at Tadeusz Kościuszko Cracow University of Technology is possible at e-mail address: iodo@pk.edu.pl and number 12 628 22 37.
3. your personal data will be processed for **the purpose of ......................**..,
4. your personal data will be processed on the basis of Article 6(1)(c) as stated in the General Data Protection Regulation (GDPR), in particular:
* Act of 27 July 2005. Law on Higher Education (Journal of Laws 2016, item 1842, as amended).
* Indicate other substantive legal grounds
1. your personal data will be stored **for a period of** .................. (indicate the criteria for determining this period and the legal basis),
2. you have the right of access to the content of your data and the right to rectification, erasure, restriction of processing, the right to data portability, the right to object, the right to withdraw consent at any time without affecting the lawfulness of the processing carried out on the basis of consent before its withdrawal,
3. you have the right to lodge a complaint with the PUODO (**Personal Data Protection Office)** if you consider that the processing of personal data concerning you violates the provisions of the General Data Protection Regulation of 27 April 2016,
4. your provision of personal data is a legal requirement/condition for entering into contract,
5. there is no automated decision-making involved in the processing of the personal data provided.

Consent clause - general model

Place and date

Personal information:

Surname………….

First name……….

Personal number PESEL………

Phone number…………

E-mail address………

**Consent to process personal data**

I, undersigned, consent to the collection and processing of my personal data in accordance with Article 7(2) of the EU Parliament and Council Regulation 2016/679 of 27 April 2016. (GDPR)\*[[2]](#footnote-2). The controller of my personal data is Tadeusz Kościuszko Cracow University of Technology based in Cracow, ul. Warszawska 24, 31-155 Cracow.

I provide my personal data for the purpose of ...................................................................

I declare that I am entitled to withdraw my consent at any time. I have also been informed that my personal data is voluntary, that I have the right to inspect and correct it and that the data will not be shared with other entities. I have been informed that no automated decision-making takes place in the processing of the personal data provided.

………………………

signature

**XV.Forms and records models**

Model data breach notification

Place, date

…………………………………….

Personal Data Controller (stamp)

Reference of the letter

**President of Personal Data Protection Office**

NOTIFICATION OF A PERSONAL DATA BREACH

TO THE PRESIDENT OF THE DATA PROTECTION OFFICE

Pursuant to Article 33 of the General Data Protection Regulation, I am reporting a data protection breach that occurred on .....................................

1 Personal Data Protection Officer/ Personal Data Controller:

………………………………………………………………………………………………….

2 Nature of the personal data breach:

………………………………………………………………………………………………….

3 Possible consequences of a data breach:

a) ...........

b) ..............

4 Data protection breach prevention measures applied by the administrator:

………………………………………………………………………………………………….

Witness interview record (personal data breach)

Place, date……………….

Report of the hearing of a witness

Prepared by

………………………………………………………………………………………………………..

(name, position or function)

Witness details:

name .............................................................................................

date and place of birth ..................................................................

place of residence .........................................................................

place of employment (name of PK organisational unit) ..................................................

position .........................................................................................

Criminal penalties for false testimony

The witness acknowledges with his/her signature that he/she has been warned of the criminal liability under Article 233 § 1-3 of the Penal Code for giving false testimony or concealing the truth, and has been instructed on the situations in which he/she may refuse to give testimony or answer questions.

..............................................................

(witness's own legible signature)

Witness statement:

...........................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................................

There being no further comments, the report was concluded.

............................................ ...................................................

 (signature of the witness) (signature of the person drawing up report)

3.Inspection report (cyclical inspections carried out by the PDPO)

Inspection report

Type of inspection activities carried out:

.................................................................................................................................................................

Place where the inspection activity was carried out (name of the PK organisational unit):

.................................................................................................................................................................

Person carrying out the inspection (name, position or function):

.................................................................................................................................................................

Persons participating in the inspection activities:

.................................................................................................................................................................

.................................................................................................................................................................

A description of the facts established as a result of the inspection activities, including the irregularities detected, the reasons for their occurrence, their extent and effects, and the persons responsible for them:

.................................................................................................................................................................

.................................................................................................................................................................

.................................................................................................................................................................

Notification of the right, manner and time limit to object to the findings of the report and the right to refuse to sign the report

.................................................................................................................................................................

............................................................

(signature of the person carrying out the inspection)

...................................................................................

..................................................................................

(signatures of persons taking part in the inspection activities)

In the event of a refusal to sign the report, a note about that:

.................................................................................................................................................................

4 Register of persons authorised to process personal data

REGISTER OF PERSONS AUTHORISED TO PROCESS PERSONAL DATA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **name and surname****of the authorised person** | **date of authorisation** | **date of revoking authorisation** | **the scope of the authorisation to process personal data** | **identifier (in the IT system)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

5 Register of personal data protection breaches

REGISTER OF PERSONAL DATA PROTECTION BREACHES

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ordinal** | **date of the breach** | **type of breach** | **description of the breach** | **consequences of the breach** | **action taken** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. \*Regulation 2016/679 of the European Parliament and of the EU Council 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). [↑](#footnote-ref-1)
2. \*Regulation 2016/679 of the European Parliament and of the EU Council 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). [↑](#footnote-ref-2)