|  |  |  |  |
| --- | --- | --- | --- |
| **Issue in question** | **Yes** | **No** | **Additional explanations** |
| 1. | Has the entity appointed a Data Protection Officer? |  |  |  |
| 2. | Does the entity have policies, procedures and instructions developed and implemented that comply with the rules of personal data processing specified in the GDPR? |  |  |  |
| 3. | Do employees with access to personal data have written authorizations to process personal data? |  |  |  |
| 4. | Is a register of persons authorized to process personal data kept? |  |  |  |
| 5. | Are employees processing personal data trained in the rules of personal data protection? |  |  |  |
| 6. | Is the processing of personal data carried out in conditions that protect the data against unauthorized access? (clean desk policy, monitors not facing entrances, computer access passwords, lockable cabinets in which personal data are stored, electronic access control to rooms) |  |  |  |
| 7. | Have persons with access to personal data been obliged to keep the data confidential? Have they signed confidentiality statements? |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8. | Are the following: anonymization, pseudonymization, encryption and data minimization used to ensure the security of processing? |  |  |  |
| 9. | Does the entity have technical and organizational measures implemented to be able to continuously ensure confidentiality, integrity, availability and resilience of processing systems and services, as well as to quickly restore the availability of personal data and access to them in the event of a physical or technical incident? (backup disks, backups)  |  |  |  |
| 10. | Does the entity apply the accountability principle, i.e. is it able to demonstrate compliance with personal data protection regulations? |  |  |  |
| 11. | Does the entity keep a register of the categories of processing activities performed on behalf of data controllers? |  |  |  |
| 12. | Does the entity have procedures for reporting personal data breaches to the data controller implemented? |  |  |  |
| 13. | Do IT systems ensure that users are forced to periodically change their passwords and change them if necessary? |  |  |  |
| 14. | Is it forbidden to reuse the same passwords? |  |  |  |
| 15. | Are the accounts and passwords of a given user, with whom your company terminates the cooperation, immediately revoked? |  |  |  |
| 16. | Has antivirus software been provided at all stations? |  |  |  |
| 17. | Is the software licensed and is it updated on a regular basis? |  |  |  |
| 18. | Does each employee receive a personal identifier for IT systems? |  |  |  |
| 19. | Is drive encryption of notebooks used? |  |  |  |
| 20. | Are backups made? |  |  |  |
| 21. |  Does the entity transfer personal data to third countries? If so, does it comply with the requirements for the transfer of personal data to third countries and international organizations, as referred to in Chapter V of the GDPR? |  |  |  |

**Completed for the organization by:**

Name:…………………………………………

Function:……………………………………

Phone number:………………………….

Email:…………………………………………

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Location, date