Technical and organizational measures in accordance with art. 28 para. 3 lit. c and 32 GDPR

1. Confidentiality

1.1. Physical access to SEO for Jobs premises is only possible with prior authorization. Conventional security locks are used, for which the keys are only issued to authorized employees.

1.2. The group of authorized persons is defined.

1.3. Visitors have to ring the doorbell and are let in by employees of SEO for Jobs.

1.4. Visitors are accompanied throughout.

1.5. The employees are committed to confidentiality and data secrecy in writing.

1.6. Access to workstations and notebooks is protected by individual user accounts.

1.7. A distinction is made between "normal" users and administrators.

1.8. No use of collective users.

1.9. The login to servers is protected by separate administrator accounts that are only used by authorized administrators.

1.10. The allocation of any user accounts is approved by the management.

1.11. Access authorizations to computers are assigned on a person-specific basis.

1.12. Access authorizations are also assigned for network drives on a person-specific basis.

1.13. The group of authorized persons is limited to what is necessary for operations.

1.14. Where technically possible, 2-factor authentication is used.

1.15. Access authorizations are assigned role-based in the applications. The “need-to-know” and “need-to-do” principles are used.

1.16. The roles are managed in the applications.

1.17. Each authorized user can only access data that he needs to carry out the tasks and functions assigned to him.

1.18. Client separation in the SEO for Jobs applications.

1.19. Separate databases for different applications.

1.20. There is no local storage of personal data. All data is stored centrally on servers.

1.21. Data transmission with and between the SEO for Jobs systems is encrypted.

1.22. The hard drives of mobile computers are generally encrypted.

1.23. E-mails can be sent and received end-to-end encrypted (PGP). Keys are created for each email address.

1.24. In the context of data processing on behalf of the client, SEO for Jobs processes the personal data provided exclusively on the basis of and on the basis of contractually agreed instructions from the client.

1.25. SEO for Jobs supports the client in the exercise of their control obligations.

1.26. SEO for Jobs carries out random internal order controls at irregular intervals.

1.27. Contracts for order (data) processing are concluded with service providers and subcontractors, which contain regulations with which the measures contained in this confirmation are also imposed on the service providers.

2. Integrity

2.1. Access authorizations are assigned role-based in the applications. The “need-to-know” and “need-to-do” principles are used.

2.2. The employees are committed to confidentiality and data secrecy in writing.

2.3. SEO for Jobs protects its systems using virus software and a firewall.

2.4. Personal data will be deleted when the reason for processing no longer applies. Legal and contractual retention requirements are observed.

2.5. The person in charge and the time of processing are automatically logged.

2.6. The logs are protected against unauthorized access.

2.7. In the context of data processing on behalf of the client, SEO for Jobs processes the personal data provided exclusively on the basis of and on the basis of contractually agreed instructions from the client.

2.8. Each authorized user can only access data that he needs to exercise the functions assigned to him.

2.9. Client separation in the SEO for Jobs applications.

2.10. Separate databases for different applications.

2.11. Data transmission with and between the SEO for Jobs systems is encrypted.

2.12. E-mails can be sent and received end-to-end encrypted (PGP). Keys are created for each email address.

2.13. In the context of data processing on behalf of the client, SEO for Jobs processes the personal data provided exclusively on the basis of and on the basis of contractually agreed instructions from the client.

2.14. SEO for Jobs carries out random internal order controls at irregular intervals.

3. Availability

3.1. The login to servers is protected by separate administrator accounts that are only used by authorized administrators.

3.2. The allocation of any user accounts is approved by the management.

3.3. Access authorizations to the computers are assigned on a person-specific basis.

3.4. Access authorizations are also assigned for network drives on a person-specific basis.

3.5. The group of authorized persons is limited to what is necessary for operations.

3.6. Access authorizations are assigned role-based in the applications. The “need-to-know” and “need-to-do” principles are used.

3.7. The roles are managed in the applications.

3.8. Each authorized user can only access data that he needs to exercise the functions assigned to him.

3.9. The person in charge and the time of processing are automatically logged, the logs are protected against unauthorized access.

3.10. SEO for Jobs protects its systems using virus software and a firewall.

3.11. There is no local data storage on workstations.

3.12. The databases and servers are backed up daily and before new functionalities are deployed.

3.13. The backups are stored outside the SEO for Jobs premises.

3.14. SEO for Jobs carries out random internal order controls at irregular intervals.

3.15. Contracts for order (data) processing are concluded with service providers and subcontractors, which contain regulations with which the measures contained in this confirmation are also imposed on the service providers.

4. Resilience

4.1. SEO for Jobs protects its systems using virus software and a firewall.

4.2. There is no local data storage on workstations.

4.3. There are distributed systems and data centers at different locations.

4.4. The databases and servers are backed up daily and before new functionalities are deployed.