

# Free checklist: Data Protection for Remote Working

This is a free template or checklist from activeMind.legal for data protection and data security purposes. The latest version can be found [here](https://www.activemind.legal/legal-advice/gdpr/). This document can be tailored to the needs of your company, saved and printed. Please note that activeMind.legal accepts no liability for errors.

If you have any questions or issues, please do not hesitate to contact us.

Your activeMind.legal team

Phone: +49 (0)89 / 91 92 94 – 900

E-Mail: info@activemind.legal

Web: https://www.activemind.legal

# Checklist for Data Protection Compliance when remote working (from home)

|  |  |  |
| --- | --- | --- |
| Area | Measures | Content |
| 1. Organisation of information security | Creating security measures or policies for IT use and remote working | * Types of communication (internet, fax, mobile phone) * Data classification: Which data may leave the company and how? * Adopting information security requirements, e.g. rules regarding data backup, virus protection, firewall, encryption methods (for all sensitive data) * Data transfer and access to data: VPN, email, USB, printouts * Disposal of media such as storage media (e.g. paper, electronic data carriers) * If necessary, policies for remote equipment maintenance * Communication of policy to employees and publication of policy |
|  | Defining an information security concept for remote working | * Setting out information security objectives * Protection requirements for processed information and related risks |
| 2. Human resources security | Employee training | * Instructing employees on how to work remotely * Staff training, awareness-raising(e.g. dealing with printed documents) |
| 3. Equipment Management | Documentation of company IT equipment (e.g. laptop, printer) | Documentation should contain information about:   * allocation of equipment to employees * return of equipment from employees |
|  | If necessary, having an agreement relating to rights of access to employee’s home/premises where remote working takes place for the purpose of inspection and access to documents |  |
| 4. Access control | Access authorization and access administration | Users should only be provided with access to the network and network services that they have been specifically authorized to use (need-to-know principle). |
|  | Logging | * Authentication * Logfiles * Unsuccessful and successful attempts * Administrative activities * Errors |
|  | Management of privileged access rights (Admin privileges) | * Procedures for privileged access rights * Control of privileged access rights * System administrator and system operator activities should be logged * Limiting admin privileges for employees |
| 5. Cryptography | Encryption | * Mobile devices * Storage media * Emails |
| 6. Physical and environmental security | Workplace security measures/safeguards | * Defining access rights * Defining security perimeters to protect sensitive or critical information |
|  | Clean-Desk Policy | * Reducing the risk of information theft, fraud, or a security breach caused by sensitive information being left unattended and visible |
|  | Desktop | * Enforcing password protected screensaver (GPO) |
| 7. Operation security | Updates | * Installed and up-to-date |
|  | Virus Protection | * Installed and up-to-date |
|  | Firewall | * Activated |
|  | Boot Protection | * Activation recommended |
|  | Data Security | * Policies and Monitoring |
| 8. Communication security | Separation of Data | * Separating private data from company-owned information |
| 9. Compliance | Engaging freelancers | * If necessary, signing a Data Processing Agreement (for processing on behalf of a controller) |