

At CD PROJEKT, we pay special attention to the security of the information we share. For this reason, we recommend that the external entities we work with meet certain security requirements.

We have specified three levels of security requirements depending on the criticality of the data we entrust.

For each level of data vulnerability, our contractors should meet specific security requirements in the areas of procedures, physical security, incident response, continuity of operations, data security, infrastructure security, access and identity management.

Security requirements for the CDPR's high level of data vulnerability

1. Procedures

- 1.1. The contractor should possess and observe management rules governing use of mobile devices, along with security measures related to mobile devices which are used to process CDPR data.
- 1.2. All of the contractor's employees, as well, as – in justifiable cases – the contractor's business partners, should undergo security awareness training and be regularly informed of the organisational principles and procedures, depending on their specific function.
- 1.3. The ability to use portable data carriers should be disabled on devices used to process CDPR data.
- 1.4. Prior to initiating collaboration with an external entity which involves granting access to any CDPR data thereto, the contractor should make sure that the relevant entity has obtained clearance from CDPR to access CDPR data.

2. Physical security

- 2.1. The contractor should deploy physical security systems (e.g. locks, CCTV cameras, card readers, alarm systems) around areas where CDPR data is processed.
- 2.2. All physical resources used to process CDPR data (such as external hard drives and printouts) should be stored at a secure location.
- 2.3. The contractor should maintain a logbook of guests entering areas where CDPR data is processed.
- 2.4. Guests entering areas where CDPR data is processed should at all times be accompanied by a representative of the contractor.

3. Incident response

- 3.1. The contractor should possess a security incident response plan which specifies actions to be taken when a security incident involving CDPR data occurs.
- 3.2. The contractor should appoint a person responsible for key aspects of security, and provide that person's contact details to CDPR.
- 3.3. Any security incident which may potentially involve CDPR data should be immediately reported to security@cdprojektred.com.

4. Continuity of operations

- 4.1. The contractor should possess an operational continuity plan, and perform regular backup recovery tests.

5. Data security

- 5.1. The contractor should identify IT resources used to process CDPR data, and maintain a list thereof. All such resources should have assigned owners, responsible for their proper and secure operation.
- 5.2. The hardware and software used to process CDPR data should receive regular security updates. The contractor should perform ongoing monitoring of the availability of security updates for each component of its hardware and software infrastructure.
- 5.3. Access to CDPR data must be restricted to persons who have been tasked with processing such data by the contractor.
- 5.4. Each individual tasked with processing CDPR data should be covered by a valid non-disclosure agreement with the contractor.
- 5.5. The contractor should have a valid non-disclosure agreement with CDPR.
- 5.6. The contractor should deploy malware protection measures (detection, prevention, recovery); in particular, the contractor should regularly create backup copies on separate media.
- 5.7. The contractor should ensure permanent protection of CDPR data through encryption, both at rest and in transit.
- 5.8. The contractor should only transfer CDPR data in an encrypted form, or transfer it using encrypted channels (e.g. VPN).

6. Infrastructure security

- 6.1. The contractor should employ network connectivity based on minimum entitlements, in accordance with the zero-trust policy, and ensure network segmentation (e.g. VLAN) or physical separation of network resources.
- 6.2. Remote access to the contractor's intranet where CDPR data is processed should be limited in scope and restricted to VPN which implements two-factor authentication.
- 6.3. All devices should have distinct profiles and be centrally managed.

7. Access and identity management

- 7.1. IT systems where CDPR data is processed should be secured with individual user logins and passwords.
- 7.2. Each user should only be able to access the specific CDPR data which they require (resource segmentation and access management based on the need-to-know principle).
- 7.3. The contractor should grant and modify user access on the fly, depending on existing requirements (recruitment/dismissal/reassignment of employees, or change in the scope of employment).
- 7.4. An IT resource owner should be appointed and charged with regularly reviewing and validating user access levels.