

Politika bezpečnosti informací a ochrany osobních údajů



Společnosti TÜV SÜD v České republice zavádějí a udržují systém bezpečnosti informací zahrnující ochranu dat a osobních údajů podle principů ISMS a GDPR a v souladu s Etickým kodexem Skupiny TÜV SÜD. Cílem je chránit informace klientů, dodavatelů a partnerů, zajistit důvěryhodnost poskytovaných služeb a trvale zvyšovat úroveň řízení bezpečnosti informací.

Základní zásady

- Chráníme informace a osobní údaje v souladu s legislativou a požadavky partnerů.
- Udržujeme funkční systém řízení bezpečnosti informací (ISMS) a GDPR a pravidelně jej zlepšujeme.
- Zajišťujeme integraci požadavků ISMS a GDPR do procesů organizace.
- Definujeme jasné role, odpovědnosti a pravomoci pro oblast bezpečnosti informací.
- Stanovujeme a plníme cíle v oblasti bezpečnosti informací a ochrany dat.
- Poskytujeme dostatečné zdroje pro udržování a rozvoj systému bezpečnosti informací.

Závazek vedení společností TÜV SÜD Czech a TÜV SÜD Central Eastern Europe

- pravidelně přezkoumávat systém ochrany dat a osobních údajů, politiku a cíle,
- podporovat efektivní řízení rizik a stanovit kritéria pro jejich akceptaci,
- zajistit pravidelné interní audity, monitoring a ověřování účinnosti přijatých opatření,
- komunikovat význam bezpečnosti informací směrem k zaměstnancům i externím partnerům,
- podporovat zaměstnance při plnění úkolů souvisejících s bezpečností informací.

Cíl politiky ochrany informací a osobních údajů

- zajistit dostupnost, integritu a důvěrnost informací,
- chránit osobní údaje v souladu s GDPR,
- minimalizovat rizika a předcházet incidentům,
- zvyšovat důvěryhodnost poskytovaných služeb a plnit očekávání klientů.

V Praze, 1. dubna 2026

Jiří Socha
jednatel TÜV SÜD Czech

Jakub Pecháček
jednatel TÜV SÜD CEE

Information Security and Personal Data Protection Policy



TÜV SÜD companies in the Czech Republic implement and maintain an information security system including data and personal data protection according to the principles of ISMS and GDPR and in accordance with the TÜV SÜD Group Code of Conduct.

The aim is to protect the information of clients, suppliers and partners, to ensure the credibility of the services provided and to continuously increase the level of information security management.

Basic principles

- We protect information and personal data in accordance with legislation and partner requirements.
- We maintain a functional information security management system (ISMS) and GDPR and improve it regularly.
- We ensure the integration of ISMS and GDPR requirements into the organization's processes.
- We define clear roles, responsibilities and authorizations in the field of information security.
- We set and meet goals in the area of information security and data protection.
- We provide sufficient resources for maintaining and developing the information security system.

Commitment of the management of TÜV SÜD Czech and TÜV SÜD Central Eastern Europe

- regularly review the data and personal data protection system, policy and objectives;
- promote effective risk management and establish criteria for their acceptance;
- ensure regular internal audits, monitoring and verification of the effectiveness of the measures taken,
- communicate the importance of information security to employees and external partners,
- support employees in performing tasks related to information security.

Objective of the information and personal data protection policy

- ensure the availability, integrity and confidentiality of information;
- protect personal data in accordance with the GDPR,
- minimize risks and prevent incidents,
- increase the credibility of the services provided and meet client expectations.

Prague, April 1, 2026


Jiří Socha
CEO TÜV SÜD Czech


Jakub Pecháček
CEO TÜV SÜD CEE