

TRUST CENTER — IT SECURITY & PRIVACY

KRAFTEC, s.r.o.

Verejný prehľad postojov Kraftec k informačnej bezpečnosti a ochrane súkromia pre B2B partnerov a obstarávateľov

Verzia 2.0 • Účinné od: 1. 6. 2026. Slovenská verzia je jediná právne záväzná. Anglická verzia je informatívnym prekladom a v prípade rozporu má prednosť slovenská verzia.

Bezpečnosť a súkromie tvoria základ dôvery medzi Kraftec a našimi zákazníkmi. Tento dokument zhŕňa naše princípy, opatrenia a kontakty v oblasti informačnej bezpečnosti a ochrany osobných údajov pre B2B obstarávateľov a security/privacy tímy, ktorí vyhodnocujú spoluprácu s Kraftec. Detailné záväzné dokumenty (Privacy Policy, DPA template, Politika informačnej bezpečnosti) sú k dispozícii na vyžiadanie alebo na kraftec3d.com.

TRUST CENTER — IT SECURITY & PRIVACY

KRAFTEC, s.r.o.

Public overview of Kraftec's information-security and privacy posture for B2B partners and procurement teams

Version 2.0 • Effective from: 1 June 2026. The Slovak version is the only legally binding version. The English version is a non-binding courtesy translation; the Slovak version prevails in case of conflict.

Security and privacy are foundational to the trust between Kraftec and our customers. This document summarises our principles, measures and contacts in information security and personal-data protection for B2B procurement and security/privacy teams evaluating cooperation with Kraftec. The detailed binding documents (Privacy Policy, DPA template, Information Security Policy) are available on request or at kraftec3d.com.

1. NÁŠ ZÁVÄZOK

1.1 Kraftec sa zaväzuje k transparentnej, primeranej a kontinuálne zlepšovanej ochrane informačných aktív a osobných údajov svojich zákazníkov, zamestnancov a partnerov. Naše opatrenia vychádzajú z čl. 32 GDPR, princípov ISO/IEC 27001:2022 a NIS2 (smernica EÚ 2022/2555 v rozsahu primeranom našej veľkosti).

1. OUR COMMITMENT

1.1 Kraftec is committed to transparent, proportionate and continuously improving protection of information assets and personal data of our customers, employees and partners. Our measures derive from Art. 32 GDPR, ISO/IEC 27001:2022 principles and NIS2 (EU Directive 2022/2555 to the extent proportionate to our size).

2. KONTAKT PRE BEZPEČNOSŤ A PRIVACY

2.1 Hlásenie incidentov a zraniteľností (responsible disclosure): [security@kraftec.sk]. Otázky ochrany osobných údajov: gdpr@kraftec.sk. Všeobecné B2B otázky: info@kraftec.sk.

2.2 Cieľová reakčná doba: kritické bezpečnostné incidenty do 24 hodín, ostatné požiadavky do 5 pracovných dní.

2. SECURITY AND PRIVACY CONTACT

2.1 Incident and vulnerability reporting (responsible disclosure): [security@kraftec.sk]. Data-protection inquiries: gdpr@kraftec.sk. General B2B inquiries: info@kraftec.sk.

2.2 Target response time: critical security incidents within 24 hours, other requests within 5 working days.

3. CERTIFIKÁCIE A SÚLAD

3.1 Aktuálny stav (k 1. 6. 2026):

- ISO 9001:2015 — interný systém pripravený, certifikácia v procese.
- ISO 14001:2015 — interný systém pripravený, certifikácia v procese.
- ISO/IEC 27001:2022 — princípy uplatňované, formálna certifikácia zvažovaná podľa rozvoja podnikania.
- Plánované sektorové certifikácie: IATF 16949 (automotive), AS9100 (aerospace).
- Súlad s GDPR (nariadenie (EÚ) 2016/679), zákonom č. 18/2018 Z. z., §109 zák. č. 452/2021 Z. z. (cookies), nariadením (EÚ) 2023/988 (GPSR).

3. CERTIFICATIONS AND COMPLIANCE

3.1 Current status (as of 1 June 2026):

- ISO 9001:2015 — internal system prepared, certification in progress.
- ISO 14001:2015 — internal system prepared, certification in progress.
- ISO/IEC 27001:2022 — principles applied, formal certification considered based on business development.
- Planned sector certifications: IATF 16949 (automotive), AS9100 (aerospace).
- Compliance with GDPR (Regulation (EU) 2016/679), Act No. 18/2018 Coll., §109 of Act No. 452/2021 Coll. (cookies), Regulation (EU) 2023/988 (GPSR).

4. TECHNICKÉ A ORGANIZAČNÉ OPATRENIA (TOM)

4.1 Riadenie prístupu

- Princíp najmenších oprávnení (least privilege) a need-to-know.
- Dvojfaktorová autentifikácia (MFA) pre všetky kritické systémy.
- Pravidelná revízia prístupových oprávnení (každých 6 mesiacov) + okamžitá deaktivácia pri zmene/skončení vzťahu.

4. TECHNICAL AND ORGANISATIONAL MEASURES (TOMs)

4.1 Access control

- Least-privilege and need-to-know principle.
- Multi-factor authentication (MFA) for all critical systems.
- Periodic access-rights review (every 6 months) + immediate deactivation on role change/end of engagement.

4.2 Šifrovanie

- Šifrovanie v prenose: TLS 1.2+ pre všetky externé komunikácie.
- Šifrovanie diskov (full-disk encryption) na všetkých prenosných zariadeniach a serveroch s dôvernými údajmi.
- Bezpečné mazanie pri vyradení (NIST SP 800-88).

4.3 Sieť a koncové zariadenia

- Firewall, IDS/IPS, segmentácia siete (oddelenie produkčnej, kancelárskej a hostí Wi-Fi siete).
- Antivirus/EDR na všetkých koncových zariadeniach; ochrana pred ransomwarom; automatické bezpečnostné záplaty.
- Vzdialený prístup len cez VPN s MFA.

4.4 Zálohovanie a kontinuita prevádzky

- Denné zálohovanie kritických systémov; off-site záloha aspoň raz týždenne. Pravidlo 3-2-1.
- Testovanie obnovy zo zálohy minimálne raz za 6 mesiacov.
- Business Continuity Plan (BCP) a Disaster Recovery Plan (DRP) s definovaným RTO/RPO.

4.5 Klasifikácia informácií

- 4 úrovne: verejné / interné / dôverné / prísne dôverné — s primeranými pravidlami zaobchádzania pre každú úroveň.
- Vstupné dáta zákazníkov (CAD/3D súbory, výkresy, meracie protokoly) zaobchádzame ako s dôvernými alebo prísne dôvernými podľa povahy projektu.

4.2 Encryption

- Encryption in transit: TLS 1.2+ for all external communications.
- Full-disk encryption on all portable devices and servers with confidential data.
- Secure deletion on device disposal (NIST SP 800-88).

4.3 Network and endpoints

- Firewall, IDS/IPS, network segmentation (separation of production, office and guest Wi-Fi networks).
- Antivirus/EDR on all endpoints; ransomware protection; automatic security patching.
- Remote access only via VPN with MFA.

4.4 Backup and business continuity

- Daily backup of critical systems; off-site backup at least weekly. 3-2-1 rule.
- Backup-restore testing at least every 6 months.
- Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) with defined RTO/RPO.

4.5 Information classification

- 4 levels: public / internal / confidential / strictly confidential — with appropriate handling rules per level.
- Customer input data (CAD/3D files, drawings, measurement reports) is treated as confidential or strictly confidential depending on project nature.

5. OCHRANA OSOBNÝCH ÚDAJOV

5.1 Kraftec ako prevádzkovateľ spracúva osobné údaje v súlade s GDPR a zákonom č. 18/2018 Z. z. Detaily v Zásadách ochrany osobných údajov (kraftec3d.com).

5.2 Pri spracúvaní v mene B2B zákazníka (typicky CAD/3D súbory s osobnými údajmi alebo zákaznícky portál) uzatvárame samostatnú Sprostredkovateľskú zmluvu (DPA) podľa čl. 28 GDPR. Vzor je dostupný na vyžiadanie na gdpr@kraftec.sk.

5.3 Doba uchovávania zákazníckych dátových súborov (CAD, 3D skeny, meracie protokoly): zákazník si pri Objednávke zvolí (a) automatické vymazanie do 30 dní od fakturácie alebo (b) uchovanie do žiadosti o vymazanie.

5.4 Prenos osobných údajov mimo EHP: výlučne na základe EU-US Data Privacy Framework (rozhodnutie 2023/1795) alebo štandardných zmluvných doložiek (rozhodnutie 2021/914).

5. PERSONAL DATA PROTECTION

5.1 As a controller, Kraftec processes personal data in compliance with GDPR and Act No. 18/2018 Coll. Details in the Privacy Policy (kraftec3d.com).

5.2 When processing on behalf of a B2B customer (typically CAD/3D files with personal data or a customer portal), we conclude a separate Data Processing Agreement (DPA) under Art. 28 GDPR. Template available on request at gdpr@kraftec.sk.

5.3 Retention of customer data files (CAD, 3D scans, measurement reports): the customer chooses per Order between (a) automatic deletion within 30 days of invoicing or (b) retention until deletion request.

5.4 Personal data transfers outside the EEA: only based on the EU-US Data Privacy Framework (Decision 2023/1795) or Standard Contractual Clauses (Decision 2021/914).

6. SUB-PROCESSORY A DODÁVATEĽSKÝ REŤAZEC

6.1 Typickí sub-processor v aktuálnej prevádzke (zoznam udržiavame v Prílohe č. 3 vzoru DPA a aktualizujeme pri zmene):

- Externá účtovná kancelária (SK) — účtovníctvo, fakturácia.
- Hosting a IT infraštruktúra (EÚ) — prevádzka webu, e-shopu, CRM, cloud.
- Doručovatelia (Slovenská pošta, GLS, DPD, DHL, FedEx) — doručenie tovaru.
- Platobné brány a banky — spracovanie platieb.
- Mailchimp / Brevo — e-mailový marketing (EÚ/USA, DPF/SCCs).
- Google (Workspace, Analytics, Ads) — produktivita, analytika, reklama (USA, DPF).
- Meta Platforms Ireland, LinkedIn Ireland — pixels a remarketing (so súhlasom v cookie banneri).

6.2 Všetkých sub-processorov si Kraftec vyberá na základe due diligence a uzatvára s nimi Sprostredkovateľské zmluvy alebo rovnocenné data-protection clauses.

6. SUB-PROCESSORS AND SUPPLY CHAIN

6.1 Typical sub-processors in current operations (list maintained in Annex 3 of the DPA template and updated on change):

- External accounting office (SK) — bookkeeping, invoicing.
- Hosting and IT infrastructure (EU) — website, e-shop, CRM, cloud operation.
- Carriers (Slovak Post, GLS, DPD, DHL, FedEx) — goods delivery.
- Payment gateways and banks — payment processing.
- Mailchimp / Brevo — email marketing (EU/USA, DPF/SCCs).
- Google (Workspace, Analytics, Ads) — productivity, analytics, ads (USA, DPF).
- Meta Platforms Ireland, LinkedIn Ireland — pixels and remarketing (with consent via cookie banner).

6.2 All sub-processors are selected based on due diligence; Kraftec concludes Data Processing Agreements or equivalent data-protection clauses with them.

7. INCIDENT RESPONSE

7.1 Pri zistení bezpečnostného incidentu Kraftec:

7. INCIDENT RESPONSE

7.1 On discovery of a security incident, Kraftec:

- Bezodkladne začne containment a eradication.
- Pri porušení ochrany osobných údajov notifikuje ÚOOÚ do 72 hodín (čl. 33 GDPR).
- Pri spracúvaní v mene zákazníka notifikuje zákazníka do 48 hodín v zmysle DPA.
- Vykoná korešnú analýzu (RCA) a nápravné opatrenia (CAPA); dokumentuje v registri incidentov.
- Immediately initiates containment and eradication.
- On personal-data breach, notifies the Office for Personal Data Protection within 72 hours (Art. 33 GDPR).
- When processing on behalf of a customer, notifies the customer within 48 hours per the DPA.
- Performs root-cause analysis (RCA) and corrective action (CAPA); documents in incident register.

8. RESPONSIBLE DISCLOSURE

8.1 Kraftec víta zodpovedné nahlásenie bezpečnostných zraniteľností v jeho systémoch alebo produktoch. Nahlásenie posielajte na [security@kraftec.sk] s opisom zraniteľnosti, krokmi na reprodukciu a vplyvom. Kraftec sa zaväzuje:

- Potvrdiť prijatie do 5 pracovných dní.
- Vyhodnotiť a komunikovať plán nápravy do 30 dní.
- Nepodnikne právne kroky voči nahlasovateľovi, ktorý postupuje v dobrej viere a v súlade s týmito princípmi.

8. RESPONSIBLE DISCLOSURE

8.1 Kraftec welcomes responsible disclosure of security vulnerabilities in its systems or products. Reports should be sent to [security@kraftec.sk] with vulnerability description, reproduction steps and impact. Kraftec commits to:

- Acknowledging receipt within 5 working days.
- Evaluating and communicating a remediation plan within 30 days.
- Not taking legal action against a good-faith reporter complying with these principles.

9. KDE SA HOSTUJÚ ÚDAJE

9.1 Primárna lokácia hostovania produkčných systémov: EÚ. Niektoré sub-processor (Google Workspace, Mailchimp) môžu spracúvať údaje v dátových centrách v USA — vždy s primeranými zárukami (DPF/SCCs).

9.2 Pre konkrétne projekty s vyššími nárokmi na suverenitu údajov (napr. obrana, vládne sektory) Kraftec môže zaviazat' na EÚ-only hosting v individuálnej zmluve.

9. WHERE DATA IS HOSTED

9.1 Primary hosting location for production systems: EU. Some sub-processors (Google Workspace, Mailchimp) may process data in US datacentres — always with adequate safeguards (DPF/SCCs).

9.2 For specific projects with higher data-sovereignty requirements (e.g. defence, government sectors), Kraftec may commit to EU-only hosting in the individual contract.

10. SECURITY QUESTIONNAIRES

10.1 Kraftec vyplňuje štandardné security dotazníky pre B2B obstarávateľov (napr. SIG Lite, CAIQ, individuálne zákaznícke dotazníky) v primeranej lehote. Žiadosti zasielajte na [security@kraftec.sk].

10.2 Pre často sa opakujúce otázky pripravuje Kraftec Security FAQ ako rozšírenie tejto Trust Page (pripravujeme).

10. SECURITY QUESTIONNAIRES

10.1 Kraftec completes standard security questionnaires for B2B procurement (e.g. SIG Lite, CAIQ, individual customer questionnaires) within a reasonable timeframe. Requests to [security@kraftec.sk].

10.2 For frequently recurring questions, Kraftec is preparing a Security FAQ as an extension to this Trust Page (in preparation).

11. ZMENY A VERZIA

11.1 Trust Page sa aktualizuje pri zmene infraštruktúry, sub-processorov, certifikácií alebo právnych predpisov; minimálne raz ročne.

11.2 Verzia: 2.0. Účinné od: 1. 6. 2026. Plánovaná najbližšia

11. CHANGES AND VERSION

11.1 The Trust Page is updated on changes in infrastructure, sub-processors, certifications or law; at least annually.

11.2 Version: 2.0. Effective from: 1 June 2026. Next planned

revízia: 1. 1. 2027.

review: 1 January 2027.

ZÁVEREČNÉ USTANOVENIA — ÚČINNOSŤ, REVÍZIA, SCHVÁLENIE / FINAL PROVISIONS — VALIDITY, REVISION, APPROVAL

Účinnosť / Platnosť: tento dokument je účinný od 1. 6. 2026. Najbližšia plánovaná revízia: 1. 1. 2027. Spoločnosť Kraftec, s.r.o. si vyhradzuje právo dokument kedykoľvek aktualizovať alebo upraviť skôr, ak si to vyžiada zmena právnych predpisov, rozhodnutie orgánu verejnej moci, zmena obchodných procesov alebo iný oprávnený dôvod. Zodpovednosť zákazníka / používateľa za aktuálne znenie: zákazník, používateľ alebo iná dotknutá osoba je povinná pred každým úkonom (najmä pred odoslaním objednávky, podpisom zmluvy, podaním reklamácie alebo iným uplatnením práva) skontrolovať aktuálne platné znenie tohto dokumentu uverejnené na webových sídlach kraftec3d.com a kraftec.sk (sekcia „Dokumenty / Documents“). Záväzná je verzia uverejnená a označená ako účinná ku dňu rozhodujúceho úkonu.
Schválil / Vydal: Marek Kočkovský, konateľ spoločnosti Kraftec, s.r.o., v Trenčianskych Tepliciach dňa 1. 6. 2026.

Validity / Effect: this document is effective from 1 June 2026. Next scheduled revision: 1 January 2027. Kraftec, s.r.o. reserves the right to update or amend this document at any time earlier if required by a change of law, an order of a public authority, a change of business processes or another legitimate reason. Customer / user responsibility for the current version: the customer, user or other data subject is obliged, before each action (in particular before placing an order, signing an agreement, filing a complaint or otherwise exercising a right), to check the currently valid version of this document published on the websites kraftec3d.com and kraftec.sk (section "Dokumenty / Documents"). The binding version is the one published and marked as effective on the date of the relevant action.
Approved / Issued by: Marek Kočkovský, Managing Director (konateľ) of Kraftec, s.r.o., in Trenčianske Teplice on 1 June 2026.

— KONIEC DOKUMENTU / END OF DOCUMENT —