

Ochrana vašich údajov

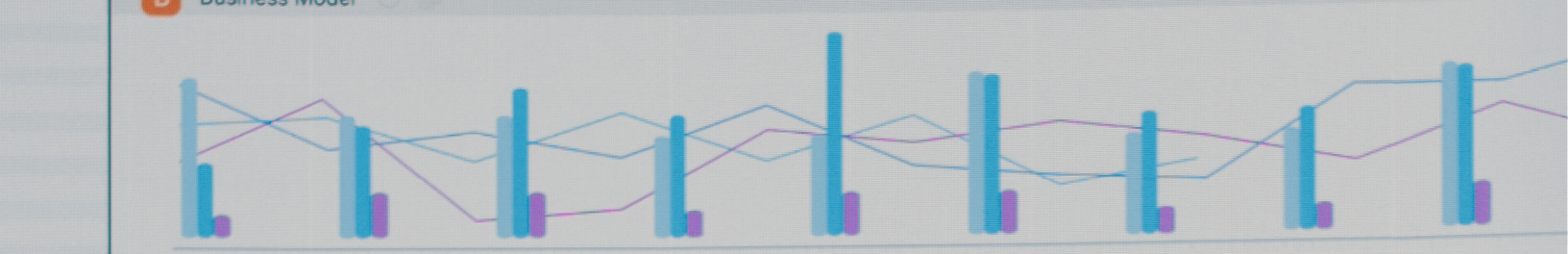
Prístup EY k ochrane
osobných údajov
a informačnej
bezpečnosti



The better the question. The better the answer.
The better the world works.



Shape the future
with confidence



V EY sme presvedčení, že dobrá povesť podniku je podmienená spoľahlivými mechanizmami ochrany údajov a informačnej bezpečnosti. Ochranu údajov a informačnú bezpečnosť považujeme za základnú súčasť obchodnej činnosti. Naším cieľom je chrániť informácie, osobné údaje a klientske údaje. Sme presvedčení, že spoľahlivé mechanizmy ochrany údajov a informačnej bezpečnosti sú pre popredné spoločnosti poskytujúce odborné služby nevyhnutnosťou. Účelom tohto dokumentu je priblížiť zásady, ktoré v danej oblasti uplatňujeme, konkrétne ako pristupujeme k zabezpečeniu informácií týkajúcich sa klientov, a aké informačné systémy na tieto účely využívame. Špecifiká súvisiacich opatrení sa môžu líšiť v závislosti od typu poskytovaných služieb a príslušných regulačných požiadaviek danej krajiny. Naše programy a postupy v oblasti ochrany údajov a bezpečnosti informácií sú koncipované tak, aby zdieľanie údajov prebiehalo zodpovedajúcim spôsobom a v súlade s platnými právnymi predpismi a zároveň, aby sa zachovala dôvernosť, integrita a dostupnosť týchto informácií.



Premyslená stratégia informačnej bezpečnosti a ochrany údajov

EY poskytuje fungujúce, stabilné a vysokokvalitné služby klientom po celom svete. Bez účinnej stratégie v oblasti ochrany údajov a informačnej bezpečnosti by to však nebolo možné. Chrániť informácie, osobné údaje či dáta klientov sa usilujeme za všetkých okolností – či už ide o ich vytváranie, spracúvanie, prenos, alebo uchovávanie. V rámci efektívnej správy týchto položiek priebežne kontrolujeme dodržiavanie platných národných aj medzinárodných regulačných štandardov. Za implementáciu a realizáciu programov a postupov EY v oblasti ochrany osobných údajov a informačnej bezpečnosti zodpovedajú dva samostatné úseky EY, ktoré však medzi sebou úzko spolupracujú: globálna sieť na ochranu osobných údajov a globálna organizácia pre bezpečnosť informácií. Ich úlohou je chrániť informácie EY a klientov EY pred neoprávneným zhromažďovaním, uchovávaním, používaním, zverejňovaním, úpravami či zničením. Na tieto účely presadzujú primerané zásady, štandardy, postupy, pokyny, technologické a administratívne kontroly, vrátane priebežných školení a iniciatív zameraných na zvyšovanie povedomia zamestnancov spoločnosti. Globálne tímy pre ochranu osobných údajov a informačnú bezpečnosť postupujú vo vzájomnom súlade, pokiaľ ide o globálne priority uplatňované v rámci celosvetovej siete EY. V súvislosti s ochranou informácií, osobných údajov a klientskych dát sa tak orientujeme podľa jednotnej a súdržnej vízie.

Uplatňovaný rámec ochrany osobných údajov

Rámec ochrany osobných údajov, ktorým sa spoločnosť EY riadi, vychádza z platného práva (vrátane všeobecného nariadenia o ochrane údajov (GDPR)), ďalších regulačných požiadaviek a príslušných odborných štandardov. Je založený na záväzku všetkých členských spoločností EY chrániť osobné údaje a dôverné informácie (vrátane klientskych informácií) podľa nasledujúcich zásad:

- **Zákonnosť, spravodlivosť a transparentnosť:** so všetkými osobnými údajmi narábame spôsobom, ktorý je etický, primeraný, jasne komunikovaný a zákonný.
- **Obmedzenie účelu:** osobné údaje používame len na definované a schválené účely.
- **Minimalizácia údajov:** zhromažďujeme a spracúvame len tie osobné údaje, ktoré sú nevyhnutné na daný účel.
- **Presnosť:** overujeme, či sú údaje presné a dostatočne kvalitné na navrhovaný účel.
- **Obmedzenie uchovávania:** osobné údaje uchováваме len na obdobie nevyhnutné na dosiahnutie účelu, na ktorý sa zhromaždili.
- **Integrita a dôvernosť:** overujeme, či sa osobné údaje uchovávajú bezpečne a dôverne a či sa prístup k nim kontroluje na základe prísneho princípu „potreby vedieť“.
- **Zodpovednosť:** preukazujeme dodržiavanie zásad ochrany osobných údajov v súlade s globálnou smernicou EY o ochrane osobných údajov a dôvernosti informácií a s globálnym etickým kódexom EY.
- **Citlivé informácie:** venujeme zvýšenú opatrnosť pri spracovaní citlivých osobných údajov alebo citlivých klientskych informácií.
- **Externí spracovatelia:** overujeme, či tretie strany, ktoré spracúvajú osobné údaje alebo dôverné informácie, vrátane údajov o klientoch, v mene organizácie EY prijali rámec ochrany údajov, ktorý zabezpečuje primeranú ochranu týchto údajov, a či zmluvy s týmito tretími stranami obsahujú podmienky ochrany údajov v súlade s platnými právnymi predpismi.



Prvky nášho rámca na ochranu osobných údajov

Medzinárodné prenosy osobných údajov

Medzinárodné prenosy osobných údajov sú prísne regulované kľúčovými zákonmi a predpismi o ochrane osobných údajov (napr. európskou legislatívou na ochranu osobných údajov). Rôzne právne predpisy po celom svete zakazujú prenos osobných údajov do zahraničia, pokiaľ subjekt prenášajúci tieto údaje nezaviedol príslušné bezpečnostné opatrenia. Tímy EY používajú schválené mechanizmy prenosu údajov, aby dodržiavali právne predpisy o ochrane osobných údajov. Pri prenosoch európskych osobných údajov do krajín mimo Európskeho hospodárskeho priestoru, ktoré nemajú komplexný legislatívny prístup k ochrane údajov, takže podľa EÚ neposkytujú dostatočnú úroveň ochrany práv jednotlivcov na súkromie, berieme do úvahy aj rozsudok Súdneho dvora Európskej únie (SD EÚ) vo veci Schrems II.

- Tímy EY vykonávajú posúdenia vplyvu prenosu údajov z hľadiska lokálnych právnych predpisov a postupov a podľa potreby zahŕňajú primerané dodatočné opatrenia na overenie primeranej ochrany osobných údajov.
- Tímy EY zaviedli záväzné vnútropodnikové pravidlá (BCR) pre činnosti prevádzkovateľa a sprostredkovateľa ako mechanizmus umožňujúci medzinárodný prenos osobných údajov medzi členskými spoločnosťami EY. BCR nám pomáhajú uskutočňovať plynulé prenosy osobných údajov v rámci členských spoločností EY, čo uľahčuje spoluprácu tímov z jednotlivých servisných divízií. Tieto BCR, ktoré sa vzťahujú na všetky členské spoločnosti EY na celom svete, sú zverejnené na adrese https://www.ey.com/en_gl/legal-and-privacy/data-protection-binding-corporate-rules-program.
- Členské spoločnosti EY ďalej využívajú v zmluvách s klientmi a tretími osobami v opodstatnených prípadoch aj schválené štandardné zmluvné doložky (ŠZD).
- Ernst & Young LLP, USA a jej pridružené subjekty v USA dodržiavajú Rámec na ochranu osobných údajov medzi EÚ a USA, rozšírenie Rámca na ochranu osobných údajov medzi EÚ a USA pre Spojené kráľovstvo a Rámec na ochranu osobných údajov medzi Švajčiarskom a USA, ktoré zverejnilo Ministerstvo obchodu USA. Ďalšie informácie nájdete tu: [Ernst & Young LLP EU-US Data Privacy Framework Privacy Statement](#).

Zodpovedná AI

Nové technológie, najmä umelá inteligencia (AI), zažívajú bezprecedentný rast s obrovským transformačným potenciálom. Tento rýchly rozvoj však môže priniesť nové alebo väčšie výzvy vrátane nových právnych a regulačných požiadaviek, nových alebo zvýšených rizík v oblasti ochrany osobných údajov, etických otázok a potreby rozsiahlych rámcov pre správu AI. Ochrana osobných údajov je neoddeliteľnou súčasťou nášho rámca zodpovednej AI a presahuje bežné dodržiavanie predpisov až po začlenenie zásad ochrany údajov do základov návrhu, vývoja a používania AI. EY sa zaväzuje k zodpovednému používaniu osobných údajov a dôverných informácií (vrátane informácií o klientoch) v technológiách AI v súlade s platnými zákonmi, predpismi a odbornými štandardmi, ktoré sa vzťahujú na používanie a správu systémov AI a súvisiacich dát. Ďalšie informácie nájdete v [zásadách zodpovednej AI spoločnosti EY](#).



Zladenie priorít v oblasti ochrany údajov a informačnej bezpečnosti zodpovedá jednotnej a súdržnej vízii, ktorú EY globálne presadzuje v spojitosti s ochranou informácií, osobných údajov a dát klientov.

Školiace a osvetové programy

Spolu s nástupom nových technológií a meniacimi sa metódami útokov je nevyhnutné prispôsobovať aj obsah informácií, pokynov a školení, ktoré poskytujeme našim zamestnancom. Zvyšovanie povedomia o hrozbách týkajúcich sa ochrany osobných údajov a informačnej bezpečnosti a podpora našich odborníkov v zodpovednom využívaní nových technológií, vrátane umelej inteligencie, v súlade s meniacimi sa zákonmi, predpismi a odbornými štandardmi predstavuje priebežný a dynamický proces. Dôležitosť, ktorú mu pripisujeme, sa odzrkadľuje nielen v povinných školeniach, ktoré pravidelne aktualizujeme pre každú servisnú divíziu EY, ale aj v mnohých ďalších činnostiach, ktorých cieľom je zvýšiť povedomie o danej problematike v rámci globálnej komunity EY.

Globálne zásady informačnej bezpečnosti

Naše zásady v oblasti informačnej bezpečnosti vrátane podporných štandardov a kontrol sa priebežne preverujú s cieľom potvrdiť, že sú stále aktuálne a presné a že zodpovedajú právnym a regulačným požiadavkám, ktoré sa na nás vzťahujú. V súlade s uznávanými rámcami, napr. ISO 27001, povinné a odporúčané zásady zahŕňajú takmer tucet široko uznávaných oblastí informačnej bezpečnosti, ku ktorým patria najmä:

- správa identít a prístupových práv
- správa aktív: klasifikácia a kontrola
- bezpečnosť komunikácie, sietí a prevádzky
- bezpečnosť ľudských zdrojov: personál
- zabezpečenie, vývoj a údržba systémov informačnej bezpečnosti
- fyzická a environmentálna bezpečnosť
- riadenie rizík

Dôraz na technické aspekty bezpečnosti

Náš prístup k informačnej bezpečnosti nie je založený len na deklarovanej bezpečnostných zásadách či štandardoch. Dôvernoscť, integritu a dostupnosť údajov zaisťujeme aj prostredníctvom ochrany našich technologických zdrojov a aktív. Medzi súvisiace opatrenia patria napríklad:

- šifrovanie diskov stolových počítačov a notebookov
- firewally stolových počítačov a notebookov
- vymeniteľné médiá: prístup k zápisu je buď vo východiskovom nastavení zablokovaný, alebo je povolený so šifrovaním
- používanie antivírusov a softvéru na ochranu proti malvéru
- viacfaktorové autentifikačné riešenia
- automatizovaná inštalácia opráv a hodnotenie zraniteľnosti bezpečnosti
- dôkladné kontroly fyzického stavu, prostredia, sietí a bezpečnostného perimetra
- technológie detekcie a prevencie narušenia
- monitorovacie a detekčné systémy

Okrem toho investujeme značné množstvo času a prostriedkov do najmodernejších bezpečnostných technológií. Stratégiu zabezpečenia informácií vytvárame v súlade so svojím plánom nasadzovania technológií a ponukou technologických služieb pre klientov. Vďaka tomu sme schopní primerane čeliť bezpečnostným problémom, ktoré by inak mohli ohroziť dôvernoscť, integritu či dostupnosť našich technologických zdrojov.





Globálny etický kódex

Naši odborníci dodržiavajú príslušné profesijné a odborné štandardy, ako aj zásady obsiahnuté v globálnom etickom kódexe EY. Tieto štandardy, ktoré sú verejne dostupné na globálnych webových stránkach EY (https://www.ey.com/en_gl/about-us/globalcode-of-conduct), predstavujú záväzné zásady, ktoré platia pre všetky členské spoločnosti EY na celom svete. Globálny etický kódex EY vychádza zo širšieho behaviorálneho a etického rámca. Usmerňuje každodenné rozhodnutia prijímané všetkými zamestnancami EY bez ohľadu na ich funkciu, pozíciu či členskú spoločnosť, v ktorej pôsobia. V zmysle tohto kódexu sa od všetkých odborníkov EY požaduje, aby rešpektovali a chránili osobné údaje aj dôverné informácie, ktoré od organizácie EY, jej pracovníkov, klientov alebo tretích osôb získajú, resp. ktoré sa týchto subjektov týkajú.





Informačná bezpečnosť

Zabezpečenie kontinuity podnikania a obnova činnosti po havárii

Náš trvalý záväzok chrániť firemné a klientske údaje je reflektovaný okrem iného v možnostiach obnovy činnosti po havárii a zabezpečenia kontinuity podnikania v súlade s ISO 22301. Sme odhodlaní chrániť zamestnancov, zariadenia, infraštruktúru, podnikové procesy, aplikácie a údaje EY pred mimoriadnymi udalosťami (haváriami), počas nich a po nich. Postupy, podľa ktorých konáme pri reakcii na haváriu či pri obnove systému v prípade kľúčových služieb, podliehajú starostlivej príprave a testovaniu. Medzi konkrétnymi metodikami obnovy činnosti po havárii a zabezpečenia kontinuity podnikania figurujú napr.:

- posúdenia vplyvu na podnikanie
- plány obnovy činnosti pre kľúčové úlohy zostavené podľa popredných odvetvových štandardov
- asistencia certifikovaných odborníkov pre danú oblasť
- pravidelné testovanie plánov obnovy činnosti po havárii a zabezpečenie kontinuity podnikania na účely overenia prevádzkovej pripravenosti

Analýza rizík dodávateľského reťazca

V súlade s našimi procesmi náležitej starostlivosti pri riadení dodávateľov analyzujeme činnosti tretích strán v oblasti informačnej bezpečnosti, obstarávania, zmlúv, ochrany údajov a nezávislosti, vrátane:

- hodnotenia potenciálnych dodávateľov z hľadiska súladu s našimi globálnymi zásadami a kontrolnými mechanizmami v súlade s normou ISO 27001/2
- due diligence vrátane podrobného zhodnotenia rizík a zistení
- opatrení na zníženie dôsledkov identifikovaných rizík
- podpory pri výbere dodávateľov a zmluvných rokovaniach

Pri hodnotení inherentných a reziduálnych rizík v oblasti informačnej bezpečnosti, dodržiavania predpisov a ďalších kategórií rizík, ako sú klasifikácia dát, umiestnenie hostingu, prístup a typ prenosu dát, používame štandardné bezpečnostné hodnotenia.

Bezpečnostná stratégia a zodpovednosť

Bez dodržiavania všeobecných požiadaviek na informačnú bezpečnosť a etické správanie jednotlivcov by presadzovanie komplexne formulovaného programu bezpečnosti nebolo možné. Náš program je koncipovaný tak, aby podnecoval zachovávať dôvernú, integritu a dostupnosť osobných aj klientskych údajov. Túto snahu podporujeme prostredníctvom technológií na ochranu údajov používaných v súlade s platnými právnymi a regulačnými požiadavkami, ako aj medzinárodne uznávanou normou ISO 27001 definujúcou požiadavky na systém riadenia informačnej bezpečnosti (ISMS).

Naša organizácia aktívne zabezpečuje a riadne spravuje dôverné a osobné údaje prostredníctvom programu informačnej bezpečnosti založeného na norme ISO27001/2, ktorý zahŕňa:

- primerané zásady, štandardy, pokyny a postupy riadenia programu
- dôsledné kontroly bezpečnosti technických aspektov
- zabezpečenie súladu s bezpečnostnými požiadavkami zahŕňajúcimi bezpečnostné kontroly, certifikácie a audity
- jasne vymedzenú bezpečnostnú stratégiu a definovaný plán zohľadňujúci tieto faktory:
 - o ochrana údajov: právne, regulačné a procedurálne požiadavky
 - o podnikanie: predpísané postupy a požiadavky
 - o technológie: zásady, normy a postupy
 - o vonkajšie hrozby: sledovanie vývoja bezpečnostných hrozieb
- program riadenia bezpečnostných incidentov zameraný na účinnú kontrolu a riešenie incidentov súvisiacich s bezpečnosťou, vrátane pravidiel týkajúcich sa reakcie na výskyt zraniteľnosti v systéme ochrany pred kybernetickými útokmi



Dodržiavanie predpisov a auditu

Ako organizácia disponujeme globálnymi programami na ochranu osobných údajov a informačnej bezpečnosti. Využívame účinný riadiaci rámec a dohliadame na súlad s predpismi prostredníctvom formálnych auditov. Pri plnení svojich povinností týkajúcich sa ochrany osobných údajov a informačnej bezpečnosti sa spoliehame na nasledujúci súbor kontrol a postupov.

Certifikácia bezpečnosti systémov

Všetky aplikácie a systémy sú pred implementáciou podrobené bezpečnostnej certifikácii, aby sme preukázali, že boli vyvinuté v súlade s našimi globálnymi zásadami v oblasti informačnej bezpečnosti, ako aj štandardmi bezpečného vývoja aplikácií.

Tento certifikačný proces zahŕňa hodnotenie rizík, prieskum dokumentácie a posúdenie zraniteľností. Vzťahuje sa na ľubovoľné aplikácie alebo systémy používané na vytváranie, ukladanie či správu informácií v našom mene a prispieva k zachovaniu dôvernosti, integrity a dostupnosti údajov spoločnosti EY a jej klientov.

Posúdenie vplyvu na ochranu súkromia a dôvernosti

Pri aplikáciách a projektoch, ktoré pracujú s osobnými údajmi či údajmi o klientoch, posudzujeme závažnosť dosahu na ochranu súkromia a dôvernosti informácií (PIA). V rámci každého takéhoto posúdenia sa hodnotí spôsobilosť danej aplikácie či iniciatívy voči globálnym štandardom a v prípade potreby sa predkladajú relevantné odporúčania.

Prehľad konkrétnych opatrení na zmiernenie rizík spolu s podrobnými pokynmi sa následne po PIA vyhotovujú pre všetkých používateľov a správcov uvedeného systému. Uskutočnená analýza zahŕňa aj prieskum všetkých cezhraničných prenosov údajov s cieľom overiť ich súlad s príslušnými právnymi a regulačnými požiadavkami.

Disponujeme rozsiahlym súborom podnikových zásad a pokynov, ktoré nám umožňujú nasadzovať systémy a nástroje v súlade s platnými normami či štandardmi a požiadavkami v oblasti ochrany údajov.

Posudzovanie účinnosti kontrol

Aby sme overili fungovanie a účinnosť zavádzaných kontrol, vykonávame v súvislosti s nimi viacnásobné testy a posudky, ktoré okrem iného zahŕňajú:

- analýzy zraniteľnosti sietí a aplikácií, ktoré sa zameriavajú na technické aspekty globálnych zásad v oblasti informačnej bezpečnosti, ako sú správa opráv, bezpečnosť aplikácií a bezpečnosť infraštruktúry
- hodnotenia prevádzkovej účinnosti, ktoré skúmajú technické kontroly a procesy súvisiace s komponentmi, ako sú operačné systémy, databázy a infraštruktúra
- priebežný monitoring účinnosti kontrol na účely overenia, či sú bezpečnostné kontroly správne implementované a nakonfigurované

Audity informačnej bezpečnosti

Aby sme klientom a regulačným orgánom poskytli ucelenejší pohľad na dodržiavanie predpisov v oblasti informačnej bezpečnosti, podliehajú globálne technické produkty, služby a dátové centrá EY auditom. Tímy EY vyžadujú uskutočnenie niekoľkých auditov, napr.:

- nezávislé externé audity zhody s normou ISO 27001 na účely certifikácie systému riadenia informačnej bezpečnosti používaného v našich troch globálnych dátových centrách v USA, Nemecku a Singapure a v miestnych dataroomoch
- nezávislé externé audity zhody s normou ISO 27017 na účely certifikácie kontrol informačnej bezpečnosti v cloudovom výpočtovom prostredí klientskej technologickej platformy EY Fabric
- nezávislé externé audity zhody s normou ISO 22301 zahŕňajúce prvky globálneho systému riadenia kontinuity podnikania EY
- každoročné správy SOC 2 (typ 2) o riadiacich a kontrolných mechanizmoch vypracované nezávislým externým audítorom, ktoré obsahujú zásady bezpečnosti, dôveryhodnosti a dostupnosti a zahŕňajú naše tri globálne dátové centrá v USA, Nemecku a Singapure, miestne dataroomy, ako aj klientsku technologickú platformu EY Fabric umiestnenú v externom cloude
- osvedčenia ISAE 3402 a SOC 1 (typ 2) pre naše tri globálne dátové centrá v USA, Nemecku a Singapure, miestne dataroomy, ako aj klientsku technologickú platformu EY Fabric umiestnenú v externom cloude, prostredníctvom ktorých sú naše bezpečnostné kontroly testované a overované nezávislou treťou stranou
- audity základných prvkov, ktoré okrem iného skúmajú technické kontroly a procesy zostavenia komponentov, ako sú operačné systémy, databázy a infraštruktúra, prostredníctvom ktorých sú naše bezpečnostné kontroly testované a overované nezávislou treťou stranou
- audity na mieste, ktoré zahŕňajú rozhovory s kľúčovými členmi vedenia, detailné prehliadky na mieste, revízie dokumentácie a skeny zraniteľnosti siete. Ide o najvýznamnejšiu a najpodrobnejšiu formu auditu, pri ktorej sa posudzuje súlad so všetkými aspektmi globálnych zásad spoločnosti o informačnej bezpečnosti

Záver auditu dodržiavania zásad v oblasti informačnej bezpečnosti zhromažďuje a preveruje vrcholové vedenie. Následne sa v prípade potreby nastavujú a riadia plány nápravných opatrení.

Akceptácia rizík v oblasti informačnej bezpečnosti

Ak niektorý proces nemožno riešiť prostredníctvom plánu nápravných opatrení, uplatní sa proces akceptácie rizika, ktorého cieľom je preskúmať riziká súvisiace s daným problémom a zvážiť možné alternatívy. Tento proces zahŕňa formálny schvaľovací postup, pravidelné preskúvanie každého akceptovaného rizika a bezpečnostné posúdenie s priradeným ratingom rizika. Schválené žiadosti o akceptáciu rizika sú spravidla sprevádzané kompenzačnými kontrolami, ktoré pomáhajú primerane zmierniť riziká, ktoré môžu vzniknúť v dôsledku identifikovaných zistení. Tento proces akceptácie rizika zabezpečuje, že akceptované riziká, ako aj prípadné následné plány nápravných opatrení sú riadne zdokumentované, riadené a preskúmané minimálne raz ročne.

Zhrnutie

Informácie klientov EY sú u nás v bezpečí vďaka integrovanej stratégii ochrany údajov a informačnej bezpečnosti:

- Pri globálnych aplikáciách a systémoch posudzujeme konkrétne vplyvy na ochranu súkromia a podrobujeme ich bezpečnostným certifikáciám s cieľom zabezpečiť ich bezproblémové nasadenie a prevádzku.
- Osobné údaje v rámci siete EY chránime pomocou zodpovedajúcich fyzických, technologických a organizačných bezpečnostných opatrení.
- Zmluvy uzatvárané s externými dodávateľmi obsahujú ustanovenia, ktoré korešpondujú s našimi zásadami, postupmi a kontrolnými mechanizmami, aby sme zabezpečili, že vaše údaje sa spravujú riadnym a bezpečným spôsobom, ako aj v súlade s právnymi a regulačnými požiadavkami.

Klienti aj jednotlivci sú oprávnení požadovať zodpovednosť akýchkoľvek subjektov, ktoré nakladajú s ich osobnými údajmi a dôvernými informáciami.

Uvedomujeme si dôležitosť prijímania primeraných opatrení na ochranu informačných aktív a zaväzujeme sa chrániť informácie týkajúce sa klientov a zamestnancov EY.

Ak máte prípadné otázky alebo sa chcete dozvedieť ďalšie informácie o tom, ako chránime vás a vaše podnikanie, obráťte sa na zástupcu spoločnosti EY.

EY | Building a better working world

EY prispieva k budovaniu lepšie fungujúceho sveta tým, že vytvára hodnotu pre klientov, zamestnancov, spoločnosť aj celú planétu a posilňuje dôveru na kapitálových trhoch.

Tímy odborníkov EY vybavené dátami a využívajúce najmodernejšie technológie vrátane umelej inteligencie pomáhajú klientom formovať budúcnosť s dôverou a hľadať riešenia pre výzvy súčasnosti aj budúcnosti.

Vďaka detailnej znalosti problematiky ekonomických odvetví, globálne prepojenej multidisciplinárnej sieti a ekosystému najrôznejších partnerských organizácií môžu naši odborníci poskytovať komplexné služby v oblasti auditu, poradenstva, daní, práva a stratégií a transakcií vo viac než 150 krajinách a teritóriách sveta.

All in to shape the future with confidence.

EY označuje celosvetovú organizáciu a môže zahŕňať jednu alebo viac členských spoločností Ernst & Young Global Limited, pričom každá je samostatná právnická osoba. Ernst & Young Global Limited, britská spoločnosť s ručením obmedzeným, neposkytuje služby klientom. Informácie o tom, ako EY zhromažďuje a používa osobné údaje, a opis práv, ktoré jednotlivci majú podľa predpisov o ochrane osobných údajov, sú k dispozícii na ey.com/privacy. Členské spoločnosti EY neposkytujú právne služby v krajinách, kde to zákon neumožňuje. Ďalšie informácie o našej organizácii nájdete na našich webových stránkach ey.com.

© 2025 EYGM Limited
Všetky práva vyhradené.

EYG no. 008242-25GbI
2507-10837-CS
ED None

Tento materiál má výlučne všeobecný informačný charakter a nemožno sa naň spoliehať ako na účtovné, daňové, právne ani iné odborné poradenstvo. V prípade potreby sa obráťte na svojho konkrétneho poradcu.

ey.com